МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
КАФЕДРА ПРИКЛАДНОЇ МАТЕМАТИКИ І ІНФОРМАТИКИ

16.06.2024

Архітектура систем захисту інформації

Електронне видання

Методичні вказівки
з дисципліни «Архітектура систем захисту інформації»
до виконання лабораторних занять
для студентів всіх спеціальностей
галузі знань 12 Інформаційні технології

Луцьк
ДВНЗ «ДонНТУ»
2024

УДК 004.72:004.056](072)

М 54

Методичні вказівки з дисципліни «Архітектура систем захисту інформації» до виконання лабораторних занять для студентів всіх спеціальностей галузі знань 12 Інформаційні технології [Електронне видання] / уклад. Я.Ю. Дорогий, Т.В. Алтухова. – Луцьк : ДВНЗ «ДонНТУ», 2024. – 90 с.

Методичні вказівки призначені для студентів всіх спеціальностей галузі знань 12 Інформаційні технології. В методичних вказівках наведена тематика 10-и лабораторних робіт, короткі теоретичні відомості, список рекомендованої літератури.

Укладачі: Я.Ю. Дорогий, д.т.н., доц., професор кафедри ПМІ

Т.В. Алтухова, к.т.н., доц., доцент кафедри ПМІ

Рецензент: В.В. Цуркан, к.т.н., доц., доцент Спеціальної кафедри №5 ІСЗЗІ КПІ ім. Ігоря Сікорського

Відповідальний за випуск: Н.О. Маслова, к.т.н., доц., завідувачка кафедри ПМІ

Затверджено навчально-методичним відділом ДонНТУ,
протокол № 11 від 13.06.2024 р.

Розглянуто на засіданні кафедри прикладної математики та інформатики
протокол № 7 від 12.06.2024 р.

ЗМІСТ

ВСТУП

Практична суть освіти полягає в тому, що завдання викладача, є не стільки передача певних знань студенту, скільки вміння навчити студента, маючи деякий мінімальний обсяг інформації, методам збільшення цього обсягу як на практичних заняттях під керівництвом викладача, так і вдома, в бібліотеці тощо.

Лише постійне самостійне навчання дає можливість наблизитись до глибин знань певної галузі, оволодіти достатньою сумою знань і вмінь, які б дали змогу почувати себе професіоналом.

ЛАБОРАТОРНЕ ЗАНЯТТЯ №1. ОСНОВНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ. СИСТЕМА НОРМАТИВНО-ПРАВОВОГО ТА ОРГАНІЗАЦІЙНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ. МІЖНАРОДНІ СТАНДАРТИ ТА РЕКОМЕНДАЦІЇ В ГАЛУЗІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Мета — вивчення основних понять інформаційної безпеки держави та базових напрямів нормативно-правового та організаційного управління інформаційною безпекою та ознайомлення з основоположними міжнародними стандартами, що регламентують порядок створення та експлуатації комплексних систем захисту інформації.

Основні завдання:

1. вивчення поняття інформаційної безпеки, а також визначення об’єктів та суб’єктів інформаційної діяльності, що підлягають захисту;

2. введення визначення інформаційної системи та її властивостей, як об’єктів захисту інформації;

3. вивчення базових понять і основних напрямів захисту інформаційної системи та її ресурсів;

4. визначення основних категорій, які регулюють нормативно-правовий порядок забезпечення інформаційної безпеки держави;

5. визначення основних недоліків законодавчої системи України в галузі захисту інформації;

6. визначення переліку базових міжнародних стандартів у сфері інформаційної безпеки.

1.1 Завдання на лабораторну роботу

Кожному студенту потрібно розглянути наступні питання:

1. Основні поняття інформаційної безпеки;

2. Інформаційна система, як об’єкт захисту;

3. Нормативно-правове забезпечення інформаційної безпеки (охарактеризувати основні пункти щодо інформаційної безпеки);

4. Стандарт ISO/IEC 27001:2005 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги» (охарактеризувати основні пункти щодо інформаційної безпеки);

5. Стандарт ISO/IEC 27002:2005 «Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою» (охарактеризувати основні пункти щодо інформаційної безпеки);

6. Здійснити порівняльний аналіз міжнародних стандартів та нормативно-правового забезпечення інформаційної безпеки України

Звіт з лабораторної роботи за обсягом повинен бути до 10 сторінок основного тексту + титульний лист, зміст та список використаної літератури.

1.2 Запитання для самоперевірки

1. Наведіть визначення інформаційної безпеки.

2. Назвіть об’єкти інформаційної безпеки.

3. Визначте інтереси держави в інформаційній сфері.

4. Що розуміють під загрозою інформаційним ресурсам?

5. Назвіть основні напрями забезпечення безпеки інформації.

6. Назвіть основні характеристики інформаційної системи.

7. Які існують базові принципи захисту інформаційних систем?

8. Які рівні захисту інформаційних систем вам відомі?

9. У чому полягають основні недоліки системи законодавства України в галузі захисту інформації?

10. Які міжнародні стандарти інформаційної безпеки вам відомі?

11. Визначте мету стандарту ISO/IEC 27001:2005.

12. Наведіть визначення поняття системи менеджменту інформаційної безпеки.

13. З яких основних розділів складається стандарт ISO/IEC 27002:2005?

ЛАБОРАТОРНЕ ЗАНЯТТЯ №2. ДОСЛІДЖЕННЯ СТРУКТУРИ ОБ'ЄКТУ ЗАХИСТУ

Мета роботи – надбання теоретичних знань та практичних навичок з аналізу структури об'єкта захисту.

2.1 Короткі теоретичні відомості

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

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.

Комплексна система захисту інформації 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

Першим кроком 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 КСЗІ. Саме тому, якість результату процесу КСЗІ 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 уніфікованих методик 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.

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.

КСЗІ у сучасних організаціях має складну багатокомпонентну, багаторівневу, територіально і логічно розподілену структуру. Компоненти системи безпеки інтегровані в інформаційну інфраструктуру підприємства. Крім програмних і технічних засобів забезпечення ІБ, які можуть бути вбудовані в телекомунікаційне і комп’ютерне обладнання, операційні системи і додатки, а також спеціалізованих засобів захисту інформації, архітектура КСЗІ обов’язково включає в себе також систему організаційних заходів і процесів із забезпечення БІТ.

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

1. Зовнішній захищений шлюз і засоби забезпечення міжмережевих взаємодій.

2. Підсистема захисту серверів ЛМ.

3. Засоби захисту робочих станцій.

4. Підсистема моніторингу і аудиту безпеки.

5. Засоби виявлення атак і автоматичного реагування.

6. Підсистема резервного копіювання та відновлення даних.

7. Засоби аналізу захищеності і управління політикою безпеки.

8. Засоби контролю цілісності даних.

9. Засоби криптографічного захисту інформації.

10. Інфраструктура відкритих ключів.

11. Підсистема комплексного антивірусного захисту.

12. Система оновлення ПЗ.

13. Засоби адміністрування безпеки.

14. Засоби технічного захисту інформації.

15. Підсистема організаційного захисту інформації.

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

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

2.2 Завдання на лабораторну роботу

1. Виконати попереднє дослідження об’єкта (див. табл. 2.1) 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.

Таблиця 2.1 – Варіанти предметних областей (об’єкт дослідження)

№	Предметна галузь	№	Предметна галузь
1	Вугледобувне підприємство	16	Інвестиційна компанія
2	Інформаційне агентство	17	Авіакомпанія
3	Хімічний завод	18	Проєктна організація
4	Електротехнічне підприємство	19	Підприємство з виробництва ювелірних прикрас
5	Транспортне підприємство (залізничний транспорт)	20	Підприємство з виробництва зброї
6	Підприємство з вироблення програмного забезпечення	21	Геологічне підприємство
7	Підприємство з виробництва будівельних матеріалів	22	Аптека
8	Фармацевтичний завод	23	Збагачувальна фабрика
9	Банківська установа	24	Приладобудівне підприємство
10	Вищий навчальний заклад (університет, інститут)	25	Шахтобудівне підприємство
11	Видавництво	26	Мобільні оператори
12	Підприємство нафтогазової промисловості	27	Туристична компанія
13	Конструкторське бюро	28	Електроенергетичне підприємство
14	Інтернет-провайдер	29	Суднобудівне підприємство
15	Інвестиційне підприємство	30	Машинобудівне підприємство

2.3 Запитання для самоперевірки

1. Що є основною метою проектування КСЗІ?
2. Які компоненти включає технічний проект КСЗІ?
3. Чому технічне проектування КСЗІ є необхідною умовою для реалізації комплексного підходу щодо забезпечення безпеки?
4. Які етапи включає процес створення і підтримки КСЗІ?
5. Що є першим кроком у процесі проектування КСЗІ?

6. Чому аналіз об'єкта захисту є обов'язковою складовою процесу проектування КСЗІ?

7. Які основні аспекти включає аналіз об'єкта захисту?

8. Які основні компоненти повинна містити архітектура КСЗІ в сучасних організаціях?

9. Які підсистеми і засоби включаються до складу КСЗІ для забезпечення її функціонування?

10. Чому важливо виконати комплексний аналіз об'єкта при проектуванні КСЗІ?

ЛАБОРАТОРНЕ ЗАНЯТТЯ №3. ІДЕНТИФІКАЦІЯ НЕБЕЗПЕЧНИХ ЧИННИКІВ НА ОБ'ЄКТІ ЗАХИСТУ

Мета роботи – надбання та опанування практичних навичок з визначення та ідентифікації загроз для заданого об'єкта захисту.

3.1 Завдання на лабораторну роботу

1. До заданих інформаційних ресурсів та інформаційних потоків (визначених у попередній лабораторній 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.

Результат виконання лабораторної роботи представити у вигляді звіту.

3.2 Запитання для самоперевірки

1. Які кроки необхідно виконати для визначення переліку загроз інформаційним ресурсам та потокам?
2. Які основні типи загроз можуть виникати для інформаційних ресурсів та потоків?
3. Де можна знайти статистику частоти появи загроз для аналізу?
4. Як визначити ймовірність виникнення загроз на основі статистики?
5. Які фактори впливають на адекватність знайденої статистики для конкретного об'єкта захисту?

6. Які висновки можна зробити на основі аналізу загроз та їх ймовірності?

7. Які методи можна використовувати для зниження ймовірності виникнення загроз?

8. Як документувати результати аналізу загроз та оцінки їх ймовірності?

9. Чому важливо враховувати всі можливі загрози для інформаційних ресурсів та потоків?

10. Як часто слід переглядати та оновлювати аналіз загроз для об'єкта захисту?

ЛАБОРАТОРНЕ ЗАНЯТТЯ № 4. МОДЕЛЬ ПОРУШНИКА

Мета роботи – ознайомитись з основними моделями порушників та їх класифікацією.

4.1 Короткі 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 життєво важливого 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.

Класифікація порушників наведена в таблиця 4.2.

Таблиця 4.2 – Класифікація порушників

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 що використовуються)	➢ застосовує чисто агентурні методи отримання відомостей; ➢ застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи); ➢ 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.

4.2 Завдання на лабораторну роботу

1. Побудувати модель порушника для свого об’єкта дослідження (відповідно до обраного варіанту з попередньої лабораторної роботи).

2. Підготувати звіт з лабораторної роботи.

4.3 Запитання для самоперевірки

1. Хто такий порушник в контексті інформаційної безпеки?

2. Які мотиви можуть мати порушники для здійснення своїх дій?

3. Які основні типи порушників розглядаються у системах безпеки?

4. Які категорії зовнішніх порушників виділяються у тексті?

5. Хто може входити до групи внутрішніх порушників?

6. Які категорії персоналу належать до внутрішніх порушників?

7. Хто може бути сторонніми особами, що становлять загрозу?

8. Що таке модель порушника?

9. Які припущення враховуються при розробці моделі порушника?

10. Чому важливо вибрати правильний тип порушника для проектування системи безпеки?

11. Як можна класифікувати порушників за їх мотивами?

12. Чому порушення, викликані безвідповідальністю, можуть бути небезпечними?

13. Як дії порушників, спрямовані на самоствердження, можуть вплинути на безпеку?

ЛАБОРАТОРНЕ ЗАНЯТТЯ № 5. МОДЕЛЬ ЗАГРОЗ. КЛАСИФІКАЦІЯ МОДЕЛІ ЗАГРОЗ

Мета роботи – ознайомитись з основними питаннями оцінювання дій загроз в інформаційних системах.

5.1 Короткі теоретичні відомості

5.1.1 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.

5.1.2 Загальні питання захисту інформації

Загрозою є будь-яка обставина або подія, котра потенційно може заподіяти шкоду інформаційній системі чи процесу шляхом знищення, розголошення, зміни даних або відмови в обслуговуванні. Із безлічі способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатами їх впливу на інформацію та систему її обробки. Загрози

поділяються на чотири класи (конфіденційності, цілісності, доступності втрати спостережності):

- загрози порушення конфіденційності інформації (ознайомлення із інформацією неавторизованими користувачами або процесами);
- загрози порушення цілісності інформації (несанкціонована модифікація інформації неавторизованим користувачем);
- загроза порушення доступності інформаційних ресурсів (порушення доступу до інформаційних ресурсів для користувачів, що володіють відповідними повноваженнями);
- загрози порушення спостережності (обмеження можливостей інформаційної системи контролювати користувачів, процеси і пасивні об'єкти з метою забезпечення установленої політики безпеки).

Для забезпечення конфіденційності, цілісності, доступності і втрати спостережності необхідно захищати інформацію не тільки від несанкціонованого доступу, але і виключити можливість негативного впливу на інформацію, втручання у процес її обробки, порушення працездатності інформаційної системи тощо. Таким чином, захищати необхідно всі компоненти інформаційної системи: апаратуру та обладнання, програми, дані, персонал.

Загрози за природою їхнього виникнення поділяються на природні та техногенні.

Природні загрози – це загрози, викликані впливами на інформаційну систему та її елементи об'єктивних фізичних процесів чи стихійних природних явищ, що не залежать від людини.

Техногенні загрози – це загрози інформаційній системі, викликані діяльністю людини, технічними засобами і системами.

Серед техногенних загроз, виходячи з мотивації дій, можна виділити передбачені та непередбачені.

Варто помітити, що частіше всього для досягнення поставленої мети зловмисник використовує не один, а деяку сукупність з перерахованих вище шляхів.

Далі наведено варіант структурованої бази потенційних загроз для інформації в інформаційній системі, яка базується на наведених вище обґрунтуваннях (див. рис. 5.1).

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу інформаційної системи засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами інформаційної системи. Виділяють чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає до себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей проведення діалогу з ін-формаційною системою - можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням інформаційної системи, тобто впливом на базове програмне забезпечення системи та на склад і конфігурацію її устаткування;
- четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів інформаційної системи, аж до включення до складу інформаційної системи власних засобів з новими функціями обробки інформації.

Припускається, що у своєму рівні порушник - це фахівець вищої кваліфікації, який має повну інформацію про інформаційну систему і комплекс засобів захисту.

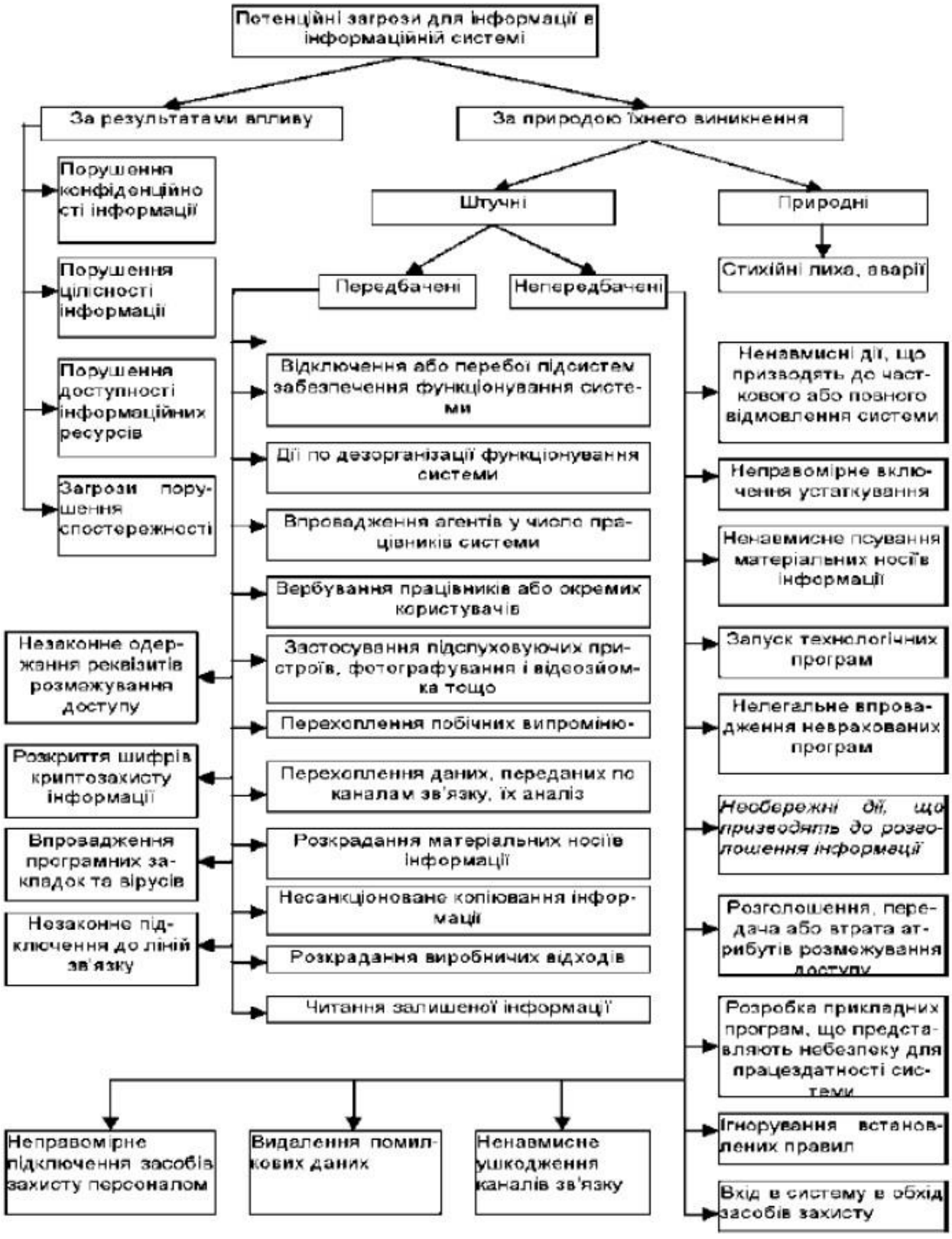

Рисунок 5.1 – Потенційні загрози в ІС

У кожному конкретному випадку, виходячи з конкретної технології обробки інформації, може бути визначена модель порушника, що має бути

адекватна реальному порушнику для даної інформаційної системи. При розробці моделі порушника визначається:

- припущення про категорії осіб, до яких може належати порушник;
- припущення про кваліфікацію порушника і його технічну оснащеність (про використані для здійснення порушення методи і засоби);
- припущення про мотиви дій порушника (переслідувані порушником цілі);
- обмеження та припущення про характер можливих дій порушників.

Стосовно інформаційної системи порушники можуть бути внутрішніми (з числа персоналу системи) або зовнішніми (сторонніми особами).

Можливо виділити три основні мотиви порушень: безвідповідальність, корисливий інтерес, самоствердження.

Усіх порушників можна класифікувати в такий спосіб:

- за рівнем знань про інформаційну систему;
- за рівнем можливостей (використаним методом і засобом);
- за часом дії;
- за місцем дії.

Визначення конкретних значень характеристик можливих порушників у значній мірі суб’єктивне. Так, помилки персоналу можуть становити 55%, нечесні співробітники - 10%, скривджені особи - 9%, зовнішній напад - 1..3%, віруси - 4%, проблеми фізичного захисту (стихійні лиха, порушення електроживлення (зниження або підвищення напруги, коливання потужності) і опалення тощо) - 20%. Інформаційні системи не самі пишуть віруси, викривлюють дані, викрадають важливу інформацію і обладнання.

У разі використовування більш ранніх оцінювань загроз потрібно знати, що загрози постійно модифікуються, особливо якщо ділове оточення чи інформація змінюються. На-приклад, сучасні віруси значно складніші ніж були декілька років тому. Цікаво, що реалізація засобів захисту, таких як перевірка на наявність вірусу, майже завжди веде до розробляння нових вірусів, що мають імунітет до поточних засобів захисту. Після визначання

джерела загрози (хто і що викликало загрозу) і її спрямованості (тобто на які елементи системи може вплинути загроза) необхідно визначити імовірність виникнення загрози. У цьому випадку потрібно брати до уваги:

- частоту загроз (як часто вони можуть виникати, спираючись на досвід, статистичні дослідження та інше), якщо статистичні дослідження існують;
- мотивацію, усвідомлені можливості і здатності, ресурси, доступні потенційним нападникам, і привабливі моменти та вразливості активів системи інформаційних технологій для потенційного нападника і навмисних джерел загрози;
- географічні чинники, такі як близькість до хімічних чи нафтових заводів, можливість появи критичних метеорологічних умов і чинники, що можуть впливати на людські помилки і несправність устаткування, випадкові джерела загрози.

Зупинимось на основних етапах оцінки дій загроз в інформаційних системах обробки інформації, які мають чітку логічну послідовність у часі при розв’язанні складних науково-технічних проблем, до яких належить і проблема захисту інформації з обмеженим доступом в інформаційних системах:

Тому, базуючись на інформації в якості товару, для сучасних інформаційних технологій характерно:

- методологія їх створення базується на використанні результатів фундаментальних теоретичних досліджень та інформації з обмеженим доступом;
- адаптація до широкого кола автоматизованих систем;
- значна фінансова вартість використання таких високоінтелектуальних технологій.

Етап створення інформаційних систем є самим тривалим за часом, комплексним за своїм змістом, наповненням і його детальним описом виконання далі не буде наведений.

Відмітимо лише деякі характерні особливості виконання цього етапу:

- на основі отриманих теоретичних результатів і моделювання обґрунтовується структура конкретної системи із заданими інформаційними і технічними характеристиками;
- специфіка функціонування кожної системи визначається класом завдань, які вирішуються такою системою в основному на базі розробки програмного математичного забезпечення;
- завдання захисту інформації при створенні системи є одним з головних і в основному визначають специфіку, цінність, адаптацію до загроз самої системи.

На етапі налагодження, випробувань і введення в експлуатацію інформаційних систем є можливість формування бази знань функціонування розробленої системи з метою визначення життєвого циклу системи на основі:

- розрахунків характеристик надійності;
- розробки методології регламентних і ремонтних робіт;
- створення відповідних баз даних вимірювань поточних характеристик і параметрів механізмів, пристроїв системи;
- методик прогнозу стану системи та інших.

5.1.3Завдання аналізу дій загроз у інформаційних системах

База знань функціонування інформаційної системи обробки включає складову компоненту бази знань захисту інформації.

Необхідно відмітити, що до завдань захисту інформації належать класичні завдання виявлення корисних сигналів при дії завад, завдання визначення їх характеристик, завдання розпізнання .

Як правило, для вирішення таких завдань використовуються статистичні методи теорії випадкових процесів і математичної статистики.

Найбільш обґрунтований підхід до аналізу функціонування інформаційної системи зводиться до аналізу такої структурної схеми.

Основні завдання оцінки дій загроз в інформаційних системах обробки інформації з обмеженим доступом можна умовно поділити на дві групи, які тісно взаємозв'язані між собою, а саме:

- завдання аналізу функціонування інформаційної системи у відповідності загроз;
- завдання аналізу функціонування інформаційної системи за наявності загроз.

Коло завдань групи б значно ширше у порівнянні з задачами групи , але саме результати вирішення завдань групи а є необхідною умовою отримання оцінки дії загроз. Розглянемо принципово нові завдання групи б.

На основі результатів аналізу функціонування конкретної інформаційної системи: класу основних завдань і сфер використання результатів їхнього вирішення; специфіки і характеру досліджуваної інформації; рівня конфіденційності інформації; оцінки умовної цінності інформації у технічному і економічному аспектах обґрунтувати множину потенційних загроз і визначити імовірні шляхи і методи їхньої реалізації.

У більшості випадків моделі загроз описуються випадковими функціями. Наприклад, неоднорідний пуасонівський випадковий процес з незалежними приростами може описувати певну послідовність появи загроз, які відбуваються випадково за часом й за інтенсивністю.

Завдання випадкових моделей загроз базується на визначенні послідовності скінчених вимірів. У більшості випадків на практиці обмежуються аналізом досліджуваних випадкових процесів у рамках кореляційної теорії. При цьому використовується одновимірна і двовимірна функція розподілу випадкового процесу, який досліджується. Як правило, вибір того чи іншого закону розподілу ймовірностей формується як та чи інша статистична гіпотеза, підтвердження якої обґрунтовується результатами

статистичної обробки даних вимірів досліджуваної загрози. По суті, завдання ідентифікації досліджуваної загрози зводиться до обчислення статистичної оцінки її характеристик, параметрів на основі обробки даних вимірів і підтвердження статистичної гіпотези належності моделі загрози до відповідного класу випадкових процесів, наприклад, гаусівського, стаціонарного, періодичного, лінійного та інших. При заданих характеристиках, параметрах моделей і пристроїв інформаційної системи, моделей загроз аналіз дій загроз проводиться у рамках проведення:

- теоретичних досліджень;
- моделювання;
- статистичної обробки даних вимірювань експериментальних досліджень на основі постановки відповідних завдань, обґрунтування застосування методів їхнього вирішення і отримання результатів вирішення завдань.

Аналіз отриманих результатів дає можливість зробити оцінку технічних, економічних витрат від дії загроз.

Наведені основні завдання аналізу дій потенційних загроз в інформаційних системах обробки інформації. У більшості випадків для вирішення таких завдань використовуються методи теорії випадкових процесів і математичної статистики.

Результати вирішення завдань дають можливість зробити оцінку технічних, економічних втрат від загроз, є основою для розробки методології і практичного втілення розв’язання науково-технічної проблеми захисту інформації у досліджуваній інформаційній системі.

5.2 Завдання на лабораторну роботу

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

2. Виконати аналіз наявних в приміщенні типів технічних засобів, для цього використати таблицю наступного вигляду (див. табл. 5.1).

Таблиця 5.1 – Технічні засоби

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

3. Визначити можливі джерела зняття інформації.

Визначити за рахунок наявних технічних засобів у приміщенні можливі канали витоку інформації, для цього використати таблицю наступного вигляду (див. рис. 5.2).

Таблиця 5.2 – Можливі джерела зняття інформації

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

4. 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 тактих 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 (див. табл. 5.3).

Таблиця 5.3 – Допоміжні технічні засоби

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)	

5. Складіть модель загроз з визначенням рівня ризиків та збитків як виконано в прикладу (див. лекцію №4).

6. Наведіть рекомендації для підвищення рівня безпеки обраного для аналізу приміщення.

5.3 Запитання для самоперевірки

1. Яка із способів класифікації загроз є найпридатнішою?
2. Охарактеризуйте загрози за природою їх винекнення.
3. Який етап в житті інформаційної системи є найбільш тривалим за часом ?

ЛАБОРАТОРНЕ ЗАНЯТТЯ № 6. РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мета роботи – отримати практичні навички з розробки політики інформаційної безпеки.

6.1 Короткі теоретичні відомості

6.1.1 Спрямованість стандарту ISO17799

Стандарт ISO17799 визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, відповідальність співробітників, використання оцінки ризиків і т.д. в контексті інформаційної безпеки. В процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої – скорочення матеріальних втрат, пов'язаних з порушенням інформаційної безпеки. Стандарт покликаний заощадити підприємству засоби, а в деяких випадках навіть врятувати від банкрутства, і не є якоюсь зовнішньою обов'язковою вимогою, що приводить до появи додаткової статті витрат.

ISO17799 - це модель системи менеджменту, і в цьому сенсі не є технічним стандартом. Цей підхід до інформаційної безпеки на основі цілей менеджменту, а не фіксованих технічних специфікацій є принциповим для ISO17799 як стандарту системи управління.

У стандарті ISO17799 приводяться рекомендації по управлінню інформаційною безпекою. Він складає загальну основу для різних організацій при розробці, реалізації і оцінці ефективності процедур управління безпекою, а також дає можливість встановити довірчі відносини між організаціями.

Даний документ можна використовувати як загальноприйнятий стандарт при встановленні ділових відносин між організаціями і при висновку

контрактів з субпідрядниками або придбанні інформаційних систем або продуктів.

6.1.2 Зміст інформаційної безпеки

Мета інформаційної безпеки — забезпечити безперебійну роботу організації і звести до мінімуму збиток від подій, що таять загрозу безпеці, за допомогою їх запобігання і зведення наслідків до мінімуму.

Управління інформаційною безпекою дає можливість колективно використовувати інформацію, забезпечуючи при цьому її захист і захист обчислювальних ресурсів.

Інформаційна безпека складається з трьох основних компонентів:

а) конфіденційність: захист конфіденційної інформації від несанкціонованого розкриття або перехоплення;

б) цілісність: забезпечення точності і повноти інформації і комп'ютерних програм;

в) доступність: забезпечення доступності інформації і життєво важливих сервісів для користувачів, коли це потрібно.

Інформація існує в різних формах. Її можна зберігати на комп'ютерах, передавати по обчислювальних мережах, роздруковувати або записувати на папері, а також озвучувати в розмовах. З погляду безпеки всі види інформації,

включаючи паперову документацію, бази даних, плівки, мікрофільми, моделі, магнітні стрічки, дискети, розмови і інші способи, використовувані для передачі знань і ідей, вимагають належного захисту.

6.1.3 Необхідність захисту

Інформація і що підтримують її інформаційні системи і мережі є цінними виробничими ресурсами організації. Їх доступність, цілісність і конфіденційність можуть мати особливе значення для забезпечення

конкурентоспроможності, руху грошової готівки, рентабельності, відповідності правовим нормам і іміджу організації. Сучасні організації можуть зіткнутися із зростаючою загрозою порушення режиму безпеки, що йде від цілого ряду джерел. Інформаційним системам і мережам можуть загрожувати такі небезпеки, як комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, а також інші джерела відмов і аварій. З'являються все нові загрози, здатні завдати збитку організації, такі, як, широко відомі комп'ютерні віруси або хакери. Передбачається, що такі загрози інформаційній безпеці з часом стануть поширенішими, небезпечнішими і витонченішими. В той же час із-за зростаючої залежності організацій від інформаційних систем і сервісів, вони можуть стати уразливішими по відношенню до загроз порушення захисту. Розповсюдження обчислювальних мереж надає нові можливості для несанкціонованого доступу до комп'ютерних систем, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості централізованого контролю інформаційних систем фахівцями.

Захисні заходи виявляються значно дешевшими і ефективнішими, якщо вони вбудовані в інформаційні системи і сервіси на стадіях завдання вимог і проектування. Чим швидше організація прикмет міри по захисту своїх інформаційних систем, тим більше дешевими і ефективними вони будуть для неї згодом.

6.1.4 Структура стандарту ISO/IEC 17799

Пропоновані практичні правила розбиті на наступних 10 розділів:

Розділ 1. Політика безпеки

Розділ 2. Організація захисту

Розділ 3. Класифікація ресурсів і їх контроль

Розділ 4. Безпека персоналу

Розділ 5. Фізична безпека і безпека навколишнього середовища

Розділ 6. Адміністрування комп'ютерних систем і обчислювальних мереж

Розділ 7. Управління доступом до систем

Розділ 8. Розробка і супровід інформаційних систем

Розділ 9. Планування безперебійної роботи організації

Розділ 10. Виконання вимог

У цих розділах представлений вичерпний набір засобів управління безпекою, заснованих на реальних заходах по захисту інформації, таких, що реалізовуються зараз в британських і міжнародних організаціях.

6.1.5 Застосовність засобів управління безпекою

Не всі засоби контролю застосовні до кожного інформаційного середовища; їх треба використовувати вибірково з урахуванням місцевих умов. Це ставати ясно з опису. Проте більшість засобів контролю, описаних в даному документі, широко застосовуються крупними організаціями з великим досвідом роботи, і їх використання рекомендується для всіх ситуацій, зрозуміло, з урахуванням обмежень, що накладаються технологією і навколишнім середовищем. Ці загальноприйняті засоби контролю називають базовими засобами управління безпекою, оскільки всі вони в сукупності визначають базовий промисловий стандарт на підтримку режиму безпеки.

Десять ключових засобів контролю, пропоновані цим стандартом, є особливо важливими. Ці ключові засоби є хорошою відправною точкою для управління інформаційною безпекою.

При використанні деяких із засобів контролю, наприклад, шифрування даних, можуть знадобитись поради фахівців з безпеки і оцінки ризиків, щоб визначити, чи потрібні вони і яким чином їх реалізувати. Для забезпечення вищого рівня захисту особливо цінних ресурсів або надання протидії виключно високим рівням загроз порушення режиму безпеки, в ряду випадках можуть потрібно сильніші засоби контролю, які виходять за рамки цих правил.

6.1.6 Ключові засоби контролю

Десять ключових засобів контролю є або обов'язкові вимоги, наприклад, вимоги чинного законодавства, або вважаються основними структурними елементами інформаційної безпеки, наприклад, навчання правилам безпеки. Ці засоби контролю застосовні до всіх організаціях і середовищам і відмічені символом ключа. Вони служать як основа для організацій, що приступають до реалізації засобів управління інформаційною безпекою.

Ключовими є наступні засоби контролю:

- документ про політику інформаційної безпеки (див. Документ про політику інформаційної безпеки);
- розподіл обов'язків по забезпеченню інформаційної безпеки (див. Розподіл обов'язків по забезпеченню інформаційної безпеки);
- навчання і підготовка персоналу до підтримки режиму інформаційної безпеки (див. Навчання правилам інформаційної безпеки);
- повідомлення про випадки порушення захисту (див. Повідомлення про інциденти в системі безпеки);
- засоби захисту від вірусів (див. Засоби захисту від вірусів);
- процес планування безперебійної роботи організації (див. Процес планування безперебійної роботи організації);
- контроль за копіюванням програмного забезпечення, захищеного законом про авторське право (див. Контроль за копіюванням ПЗ, захищеного законом про авторське право);
- захист документації організації (див. Захист документації організації);
- захист даних (див. Захист даних);
- відповідність політиці безпеки (див. Відповідність політиці безпеки).

6.1.7 Задання вимог до інформаційної безпеки організації

Існують три основні групи вимог до системи безпеки в будь-якій організації:

1) — це унікальний набір ризиків порушення безпеки, що складається із загроз, яким піддаються інформаційні ресурси, та їх вразливостей і можлива дія цих ризиків на роботу організації. Більшість з цих ризиків описані в справжніх правилах і їм можна успішно протистояти, якщо скористатися наведеними тут рекомендаціями. Проте існують ризики, що вимагають спеціального звернення, і їх необхідно розглядати з урахуванням їх оцінки в кожній конкретній організації або для кожного конкретного компоненту системи.

2) — це набір правових і договірних вимог, яким повинні задовольняти організація, її торгові партнери, підрядчики і постачальники послуг; при цьому зростає необхідність стандартизації у міру розповсюдження електронного обміну інформацією по мережах між організаціями. Дані практичні правила можуть служити надійною основою для завдання загальних вимог цього типу.

3) — це унікальний набір принципів, цілей і вимог до обробки інформації, який розроблений організацією для виробничих цілей. Важливо (наприклад, для забезпечення конкурентоспроможності), щоб в політиці безпеки були відображені ці вимоги, і життєво важливо, щоб реалізація або відсутність засобів управління безпекою в інформаційній інфраструктурі не заважали виробничої діяльності організації.

Залучення належних засобів контролю і необхідна гнучкість з самого початку процесу планування інформаційних систем є необхідними умовами для успішного завершення роботи.

6.1.8 Оцінка ризиків порушення безпеки

Витрати на систему захисту інформації необхідно зіставити і привести у відповідність з цінністю інформації, що захищається, і інших інформаційних

ресурсів, піддаються ризику, а також із збитком, який може бути нанесений організації із-за збоїв в системі захисту.

Зазвичай методики аналізу ризиків (див. Аналіз ризиків) застосовуються до повних інформаційних систем і сервісів, але цими ж методиками можна скористатися і для окремих компонентів системи або сервісів, якщо це доцільно і практично. Для оцінки ризиків необхідно систематично розглядати наступні аспекти:

а) збиток, який може нанести діяльності організації серйозне порушення інформаційної безпеки, з урахуванням можливих наслідків порушення конфіденційності, цілісності і доступності інформації;

б) реальна вірогідність такого порушення захисту в світлі превалюючих загроз і засобів контролю.

Результати цієї оцінки необхідні для розробки основної лінії і визначення належних дій і пріоритетів для управління ризиками порушення інформаційної безпеки, а також для реалізації засобів контролю, що рекомендуються в справжніх практичних правилах. Оцінка цих двох аспектів ризики залежить від наступних чинників:

- характеру виробничої інформації і систем;
- виробничій меті, для якої інформація використовується;
- середовища, в якому система використовується і управляється;
- захисту, що забезпечується існуючими засобами контролю.

Оцінка ризиків може виявити виключно високий ризик порушення інформаційної безпеки організації, що вимагає реалізації додаткових, сильніших засобів контролю, ніж ті, які рекомендуються в справжніх правилах. Використання таких засобів контролю необхідно обґрунтувати виходячи з виводів, отриманих в результаті оцінки ризиків.

6.1.9 Умови успішної реалізації системи інформаційної безпеки

Перераховані нижче чинники є визначальний для успішної реалізації системи інформаційної безпеки в організації:

а) цілі безпеки і її забезпечення повинні ґрунтуватися на виробничих цілях і вимогах; функції управління безпекою повинно узяти на себе керівництво організації;

б) явна підтримка і прихильність до підтримки режиму безпеки вищого керівництва;

в) хороше розуміння ризиків порушення безпеки (як загроз, так і вразливостей), яким піддаються ресурси організації, і рівня їх захищеності в організації, який повинен ґрунтуватися на цінності і важливості цих ресурсів;

г) ознайомлення з системою безпеки всіх керівників і рядових співробітників організації;

д) надання вичерпного посібника з політики і стандартів інформаційної безпеки всім співробітникам і підрядчикам.

6.1.10 Розробка власних рекомендацій

Не існує єдиної оптимальної структури захисту інформації. Кожна категорія користувачів (див. Спеціальний привілей) або фахівців з інформаційних технологій, що працюють в конкретному середовищі, може мати свій власний, такий, що відрізняється від інших, набір вимог, проблем і пріоритетів, залежно від функцій конкретної організації і виробничого або обчислювального середовища.

Багато організацій вирішують цю проблему, розробляючи набір окремих керівних принципів для відповідних груп співробітників, щоб забезпечити ефективніше розповсюдження знань в області захисту інформації. Організаціям, що вирішили прийняти іншу структуру (або навіть розробити свої рекомендації), бажано ввести перехресні посилання на текст діючих

правил, щоб їх майбутні ділові партнери або аудитори могли встановити прямі зв'язки між цим стандартом і прийнятими в даній організації принципами системи захисту інформації.

6.1.10.1 Політика інформаційної безпеки

Метою політики інформаційної безпеки сформулювати мету і забезпечити підтримку інформаційної безпеки керівництвом організації.

Вище керівництво повинне поставити чітку мету і всесторонньо подавати свою підтримку інформаційної безпеки за допомогою розповсюдження політики безпеки серед співробітників організації.

6.1.10.2 Документ про політику інформаційної безпеки

Письмовий документ про політику безпеки повинен бути доступний всім співробітникам, що відповідають за забезпечення режиму інформаційної безпеки.

Вище керівництво повинне надати задокументовану політику інформаційної безпеки всім підрозділам організації. Цей документ повинен містити принаймні наступне:

1) визначення інформаційної безпеки, її основні цілі і область її застосування, а також її значення як механізму, що дає можливість колективно використовувати інформацію (див. Введення);

2) виклад позиції керівництва по питаннях реалізації цілей і принципів інформаційної безпеки;

3) роз'яснення конкретних варіантів політики безпеки, принципів, стандартів і вимог до її дотримання, включаючи:

- виконання правових і договірних вимог;
- вимоги до навчання персоналу правилам безпеки;
- політика попередження і виявлення вірусів;

- політика забезпечення безперебійної роботи організації.

4) визначення загальних і конкретних обов'язків по забезпеченню режиму інформаційної безпеки;

5) роз'яснення процесу повідомлення про події, що таять загрозу безпеці.

Необхідно розробити процес перевірки, визначити обов'язку і задати дати перевірок для дотримання вимог документа про політику безпеки.

6.1.10.3 Приклад політики безпеки

Нижче представлений витяг з еталонної політики безпеки Підприємства, яка включає наступні розділи:

1. Загальні положення;
2. Політика управління паролями;
3. Ідентифікація користувачів;
4. Повноваження користувачів;
5. Захист інформаційних ресурсів ІС від комп'ютерних вірусів;
6. Правила установки і контролю мережних з'єднань;
7. Правила політики безпеки по роботі з системою електронної пошти;
8. Правила забезпечення безпеки інформаційних ресурсів.

У прикладі представлено перші два розділи Політики безпеки.

Загальні положення

Забезпечення інформаційної безпеки є необхідною умовою для здійснення діяльності Підприємства. Порушення інформаційної безпеки може привести до серйозних наслідків, включаючи втрату довіри з боку клієнтів і зниження конкурентоспроможності.

Основою заходів по забезпеченню режиму інформаційної безпеки адміністративного рівня, тобто заходів, що робляться керівництвом організації, є політика безпеки. Під політикою безпеки розуміється сукупність документованих управлінських рішень, направлених на захист інформації і

асоційованих з нею ресурсів. Політика безпеки Підприємства визначає основні напрями і вимоги по забезпеченню інформаційної безпеки Підприємства.

Забезпечення безпеки інформації включає будь-яку діяльність, направлену на захист інформації і/або підтримуючої інфраструктури. Справжня політика інформаційної безпеки охоплює всі автоматизовані і телекомунікаційні системи, власником і користувачем яких є Підприємство. Положення цього документа відносяться до всього штатного персоналу, тимчасових службовців і інших співробітників Підприємства, а також клієнтів Підприємства і третіх осіб, що мають доступ до автоматизованих і телекомунікаційних систем Підприємства.

Політика управління паролями

Користувачі повинні вибирати нестандартні паролі. Це означає, що паролі не повинні бути пов'язані із заняттями або особистим життям користувачів. Наприклад, не можна використовувати як пароль номер власного автомобіля, ім'я дружини або частину адреси. Це також означає, що пароль не повинен бути просто словом із словника. Так, не повинні використовуватися як паролі імена власні, географічні назви, технічні терміни і сленг. Якщо є відповідні системні програмні засоби для здійснення контролю надійності що призначаються користувачам паролів, то необхідно використовувати ці засоби для того, щоб заборонити користувачам вибір легко вгадуваних паролів.

Користувачі можуть вибрати паролі, що легко запам'ятовуються, які в теж час є важко вгадуваними для третіх осіб, якщо буде виконано хоч би одна з наступних умов:

- Декілька слів написано злито (такі паролі відомі під назвою «passphrases»);
- При наборі слова на клавіатурі використані клавіші, зміщені щодо потрібних, на один ряд вгору, вниз, управо або вліво;

- Слово набране із зсувом на певну кількість букв вгору або вниз за абеткою;
- Комбінація цифр і звичайного слова;
- Навмисно неправильне написання слова (але не звичайна в даному слові орфографічна помилка).

Рекомендується, щоб в паролі були не тільки букви, але і інші символи, тобто цифри (0-9) і знаки пунктуації. Використання символів, що управляють, і інших знаків, що не відображаються, не рекомендується, оскільки через це можуть виникнути проблеми при передачі даних по мережі, несподівано активізуватися певні системні утиліти або виникнути інші побічні ефекти.

Всі паролі повинні полягати не менше чим з шести символів. Довжина паролів винна завжди автоматично перевірятися в той момент, коли користувачі створюють або вибирають паролі.

Користувачі не повинні створювати паролі, які ідентичні або в значній мірі повторюють раніше використовувані ними паролі. Якщо є відповідні системні програмні засоби, необхідно заборонити користувачам, повторно використовувати свої попередні паролі.

Паролі не повинні зберігатися в доступній для читання формі в командних файлах, сценаріях автоматичної реєстрації, програмних макросах, функціональних клавішах терміналу, на комп'ютерах з неконтрольованим доступом, а також в інших місцях, де не уповноважені особи можуть дістати до них доступ. Наприклад, ні в яких застосуваннях користувачі не повинні вибирати таку опцію конфігурації, як автоматичне збереження пароля.

Не можна записувати паролі і залишати ці записи в місцях, де до них можуть дістати доступ не уповноважені особи. Пароль повинен бути негайно змінений, якщо є підстави вважати, що цей пароль став відомий кому-небудь ще, окрім самого користувача.

6.2 Завдання на лабораторну роботу

1. Розробити політику безпеки організації у відповідності з рекомендаціями стандарту ISO/IEC 17799.

2. Обґрунтувати запропоновану політику безпеки.

3. Оформити звіт за результатами виконання роботи.

6.3 Запитання для самоперевірки

1. Охарактеризувати спрямованість стандарту ISO/IEC 17799.

2. В чому полягає зміст інформаційної безпеки?

3. Описати структуру стандарту ISO/IEC 17799.

4. Які засоби контролю використовуються при управлінні безпекою?

5. Які групи вимог до системи безпеки організації визначаються стандартом ISO/IEC 17799?

6. Які аспекти розглядаються при оцінці ризиків безпеки?

7. Які умови необхідно виконати для успішної реалізації системи інформаційної безпеки?

8. Яку інформацію повинен містити документ про політику інформаційної безпеки?

9. Описати структуру документу про політику інформаційної безпеки організації?

ЛАБОРАТОРНЕ ЗАНЯТТЯ № 7. ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, РОЗРАХУНКУ РИЗИКІВ І ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ МЕТОДОЛОГІЇ MSAT (MICROSOFT SECURITY ASSESSMENT TOOL)

Мета роботи – отримати практичні навички при формуванні основних положень політики інформаційної безпеки, розрахунку ризиків і захисту інформації за допомогою методології MSAT за предметною галуззю (попередні лабораторні роботи).

7.1 Короткі теоретичні відомості

Корпорація Майкрософт пропонує цілісний підхід для управління ризиками підприємств будь-якого розміру. Методика застосування цього підходу викладена у процес оцінки ризиків визначає найбільш важливі ризики, дає кількісну оцінку, засновану на певних ролях та обов'язках. Цей підхід враховує безліч деталей і дозволяє отримати повне уявлення про основні ризики. Процес включає чотири етапи, що циклічно повторюються:

- перший етап (оцінка та пріоритезація ризиків);
- другий етап (оцінка рішень для контрзаходів);
- третій етап (реалізація контрзаходів);
- четвертий етап (оцінка ефективності програми).

Корпорацією розроблено спрощену методику управління ризиками для підприємств малого та середнього бізнесу. Ця методика підтримується безкоштовною програмою оцінки безпеки підприємства MSAT (Microsoft Security Assessment Tool). Інструкцію для роботи з цією програмою наведено в методику, закладена у програмі, використовує цілісний підхід до вимірювання рівня безпеки та охоплює такі галузі, як персонал, процеси та технології. Майже MSAT охоплює перші два етапи методики. Результатом застосування програми є: ситуаційно-оцінний аналіз, список рекомендацій

щодо пріоритетних дій щодо забезпечення безпеки підприємства. Крім того, програма дозволяє оцінити підприємство на відповідність діючим стандартам з інформаційної безпеки.

Регулярне застосування MSAT дає можливість мати постійну поінформованість про рівень безпеки корпоративної мережі, у тому числі і після реалізації контрзаходів. Оцінка проводиться з урахуванням інфраструктури ешелонованого захисту на основі чинних міжнародних та національних стандартів. Програма дозволяє отримувати звіти різного ступеня подробиці, що порівнюють базові показники із впровадженими контрзаходами. Звіти включають розпоряджені за пріоритетністю рекомендації щодо дій для покращення безпеки обчислювальних мереж. У цьому використовується досвід Microsoft.

Методика MSAT містить опитувальник із понад 200 питань, на які мають відповісти фахівці підприємства. За відповідями на ці питання програма формує рекомендації щодо покращення безпеки шляхом вжиття необхідних дій щодо зниження ризиків. Програма містить посилання на додаткові інформаційні ресурси, які фахівці можуть використовувати для поглиблення знань про специфічні засоби та методи, які застосовуються у безпеці в IT-середовищі підприємства.

Двісті питань опитувальника програми охоплюють чотири специфічні галузі аналізу інформаційної безпеки корпоративної мережі підприємства. Ця область умовно названа: інфраструктура, додатки, експлуатація та персонал.

Інфраструктура – інфраструктура корпоративної мережі: захист мережного периметра, автентифікація, управління та моніторинг, захист робочих станцій тощо.

Програми – програми, що забезпечують функціональність користувачів, що потребують роботи операційної системи.

Експлуатація – корпоративне середовище, політика безпеки, резервне копіювання та відновлення, керування виправленнями вразливостей програмного забезпечення та оновленнями.

Персонал – вимоги та оцінки, політики та процедури, підготовка та обізнаність працівників підприємства в галузі захисту інформації.

Запитання і пов'язані з ними відповіді відображають загальноприйняті практики у комп'ютерній безпеці, а також вимоги чинних стандартів (ISO 27000 та NIST-800). Також враховані рекомендації та приписи від групи фахівців Microsoft та інших джерел безпеки. У табл. 1 показані області, включені в ризик-оцінку методики MSAT.

Проведення оцінки безпеки за методикою дозволяє ідентифікувати можливі ризики на підприємстві і надати контрзаходи, розміщені, щоб їх зменшити.

Таблиця 6.1 – Області оцінки загроз безпеки методики MSAT

Інфраструктура	Важливість для безпеки
Захист периметра	Захист периметра стосується безпеки на межах мережі, де внутрішня мережа з'єднується з зовнішнім світом. Вона складає першу лінію ешелонованої оборони проти порушників.
Аутентифікація	Суворі процедури автентифікації для користувачів, адміністраторів та віддалених користувачів запобігають неавторизованому доступу до мережі шляхом використання локальних та віддалених атак.
Управління моніторинг	Управління, моніторинг та правильне ведення журналу аудиту мають ключове значення для підтримки та аналізу IT-середовищ. Ці кошти ще більш важливі після того, як атака відбулася і потрібен аналіз інциденту.
Робочі станції	Захист окремих робочих станцій є ключовим фактором у захисті будь-якого середовища, особливо коли дозволено віддалений доступ. Робочі станції повинні мати заходи безпеки для захисту від поширених атак.

Програми	Важливість для безпеки
Розгортання та використання	Коли ключові для бізнесу програми розгортаються в корпоративному обчислювальному середовищі, необхідно захистити безпеку та доступність цих програм та серверів. Безперервне обслуговування важливе для надійного виправлення помилок безпеки і щоб уникнути внесення до комп'ютерне середовище нових вразливостей.
Проектування додатків	Проектування, яке не належно вирішує питання з такими механізмами безпеки, як автентифікація, авторизація та перевірка даних, може дозволити хакерам скористатися вразливістю безпеки і таким чином отримати доступ до важливої інформації.
Зберігання та передача інформації	Цілісність та конфіденційність даних є однією з першочергових турбот для будь-кого бізнесу. Втрата або крадіжка даних може негативно вплинути на прибутки організації, так само як і на її репутацію. Важливо розуміти, наскільки ключові для бізнесу дані захищені в прикладаннях
Експлуатація	Важливість для безпеки
Середа	Безпека підприємства залежить від робочих процедур, процесів та рекомендацій, застосованих до корпоративного середовища. Вони можуть підвищувати безпеку організації, включаючи більше, ніж просто технології. Точне документування середовища та наявність посібників мають критичне значення для здатності керувати, підтримувати та обслуговувати безпеку середовища.
Політика безпеки	Корпоративна політика безпеки включає окремі політики та керівні рекомендації, які існують для

	управління безпечним та правильним використанням технології та процесів усередині підприємства. Приватні політики безпеки можуть стосуватися безпеки користувачів, системи та даних.
Резервне копіювання та відновлення становлення	Резервне копіювання та відновлення мають ключове значення для підтримки безперервності бізнес-процесів у разі катастрофічних подій або збою в обладнанні. програмному забезпеченні. Відсутні належні процедури резервного копіювання та відновлення можуть призвести до значних втрат даних та фінансових втрат. Під загрозою може також опинитися репутація підприємства.
Управління виправленнями та оновленнями	Правильно організоване управління виправленнями та оновленнями важливо для забезпечення безпеки IT-середовища підприємства. Це необхідно для захисту від відомих та потенційних вразливостей.
Персонал	Важливість для безпеки
Вимоги та оцінки	Вимоги безпеки повинні бути зрозумілі всім керівникам підприємства, що приймають рішення. Мета: технічні та бізнес-рішення повинні покращувати безпеку, а не конфліктувати між собою. Регулярні оцінки стану безпеки сторонніми консультантами можуть допомогти підприємству у переоцінці прийнятих контрзаходів та визначення областей для поліпшень.
Політики та процедури	Чіткі та практичні процедури при реалізації відносин з постачальниками та партнерами можуть допомогти підприємству у запобіганні виникненню ситуацій, пов'язаних із ризиком. Такі ж процедури, що охоплюють наймання та звільнення працівників,

	можуть допомогти захистити компанію від нерозбірливих у засобах та розлючених співробітників.
Перепідготовка та підвищення кваліфікації	Співробітники повинні бути навчені і регулярно підвищувати свою обізнаність з чинними безпековими політиками, особливо в частині їхніх безпосередніх обов'язків на робочому місці. Це зменшує ймовірність ненавмисного створення співробітниками ситуацій, що загрожують інформаційним активам.

7.2 Завдання на лабораторну роботу

1. Проаналізувати структуру програмного засобу Microsoft Security Assessment Tool та визначити основні його можливості.

2. Виконати експериментальний аналіз ризиків порушення захищеності інформаційних систем за обраною предметною галуззю та результатами проведених теоретичних досліджень в попередніх лабораторних роботах.

3. Проаналізувати отримані результати експериментального аналізу.

4. Оформити звіт за результатами виконання роботи.

7.3 Запитання для самоперевірки

1. Які основні етапи включає процес управління ризиками за методикою корпорації Microsoft?

2. Чим відрізняється методика управління ризиками для малого та середнього бізнесу від загальної методики Microsoft?

3. Які етапи процесу управління ризиками охоплює програма MSAT?

4. Які переваги надає використання MSAT для підприємств?

5. Які специфічні галузі аналізу інформаційної безпеки охоплює опитувальник MSAT?

6. Як оцінка інфраструктури корпоративної мережі включена до методики MSAT?

7. Що охоплює галузь "Експлуатація" у методиці MSAT?

8. Як враховуються вимоги чинних стандартів інформаційної безпеки в методиці MSAT?

9. Які дані містять звіти, сформовані за результатами використання MSAT?

10. Як методика MSAT сприяє зниженню ризиків у корпоративній мережі підприємства?

ЛАБОРАТОРНЕ ЗАНЯТТЯ №8. РОЗРОБКА ТЕХНІЧНОГО ЗАВДАННЯ НА СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Мета роботи – отримати навички розробки технічного завдання на КСЗІ за нормативними вимогами.

8.1 Короткі теоретичні відомості

Фахівці Виконавця розробляють і погоджують із Замовником документ "Технічне завдання на створення КСЗІ", яке визначає всі основні вимоги до КСЗІ і можливих варіантів реалізації її складових елементів. Після узгодження "Технічного завдання на створення КСЗІ" із Замовником, документ узгоджується з Контролюючим органом.

У ТЗ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, які забезпечують безпеку інформації в процесі її обробки в обчислювальній системі ІТС, а також вимоги до організаційних, фізичних та інших заходів захисту, які реалізуються поза обчислювальною системою ІТС в доповнення до комплексу програмно-технічних засобів захисту інформації.

"Технічне завдання на створення КСЗІ" може розроблятися для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС у вигляді окремого розділу ТЗ на створення ІТС, окремого (часткового) ТЗ або доповнення до ТЗ на створення ІТС.

ТЗ на створення КСЗІ в ІТС є засадним організаційно-технічним документом, який визначає вимоги із захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

Для оформлення ТЗ на КСЗІ можуть бути використані такі варіанти:

- у вигляді окремого розділу ТЗ на створення ІТС;
- у вигляді окремого (часткового) ТЗ.

Перший варіант рекомендується застосовувати для вперше створюваних ІТС. Другий варіант рекомендується застосовувати у випадку модернізації КСЗІ, модернізації діючих ІТС, а також для ІТС, які вже мають затверджене ТЗ на створення, в якому не міститься окремого розділу із захисту інформації.

Вимоги в частині захисту від НСД мають бути викладені відповідно до НД ТЗІ 2.5-004-99 Згідно з цим документом в процесі оцінки захищеності ІТС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій. Відповідно, в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

Для будь-якого варіанту розроблення та оформлення ТЗ на КСЗІ його зміст, порядок погодження та затвердження повинен відповідати НД ТЗІ 3.7-001-99 та ГОСТ 34.602.

8.1.1 Загальні вимоги до розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

Загальні положення

Технічне завдання на створення КСЗІ в АС (ТЗ на КСЗІ) є засадничим організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі.

Технічне завдання на КСЗІ розробляється у разі необхідності розробки або модернізації КСЗІ існуючої (що функціонує) АС. В разі розробки КСЗІ в процесі проектування АС допускається оформлення вимог з захисту інформації в АС у вигляді окремого (часткового) ТЗ, доповнення до загального ТЗ на АС або розділу загального ТЗ на АС.

Технічне завдання на КСЗІ повинно розроблятись з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину

систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу АС.

В технічному завданні на КСЗІ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її оброблення в обчислювальній системі АС. Додатково треба викласти вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальною системою АС у доповнення до комплексу програмно- технічних засобів захисту інформації.

Перелік вимог з захисту інформації, які включаються в ТЗ на КСЗІ, може бути для кожної конкретної АС як розширений, так і скорочений відносно рекомендованого в даному документі переліку в рамках діючих законодавчих і нормативних документів.

Вимоги повинні передбачати розроблення та використання сучасних ефективних засобів і методів захисту, які дають можливість забезпечити виконання цих вимог з найменшими матеріальними затратами.

Технічне завдання на КСЗІ є одним із обов'язкових засадничих документів під час проведення експертизи АС на відповідність вимогам захищеності інформації.

Порядок розроблення технічного завдання

Вихідними даними для розроблення ТЗ на КСЗІ є функціональний профіль захищеності КС від НСД і вимоги до захищеності інформації від витоку технічними каналами.

Функціональний профіль захищеності інформації в конкретній АС може бути визначений в результаті проведення аналізу загроз та оцінки ризиків або обраний на підставі класу АС відповідно до НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу".

Вимоги до захищеності інформації від витоку технічними каналами визначаються на підставі НД ТЗІ ТР ЕОТ-95 “Тимчасові рекомендації з

технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок" і ТР ПЕМВН-95 "Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок ".

В технічному завданні повинно бути наведено обгрунтування вибору функціонального профілю захищеності і вимог до показників захищеності інформації від витоку технічними каналами.

Перелік основних робіт етапу формування ТЗ такий:

- класифікація та опис ресурсів АС (ОС, засобів зв'язку і комунікацій, інформації, її категорій, виду подання, місця зберігання, технології обробки тощо, обслуговуючого персоналу і користувачів, території і приміщень і т. ін.);
- розробка інформаційної моделі для існуючої АС, тобто опис (формальний або неформальний) інформаційних потоків АС, інтерфейсів між користувачем і АС і т. ін.;
- визначення переліку загроз і можливих каналів витоку інформації;
- експертна оцінка очікуваних втрат у разі здійснення загроз;
- визначення послуг безпеки, які треба реалізувати;
- обгрунтування необхідності проведення спецперевірок і спецдосліджень ЗОТ та інших технічних засобів, а також спеціального обладнання приміщень;
- визначення вимог до організаційних, фізичних та інших заходів захисту, що реалізуються у доповнення до комплексу програмно- технічних засобів захисту;
- визначення вимог до метрологічного забезпечення робіт;
- визначення переліку макетів, що розробляються, і технологічних стендів;
- оцінка вартості і ефективності обраних засобів;
- прийняття остаточного рішення про склад КСЗІ.

Вимоги з захисту інформації визначаються замовником, погоджуються з розробником АС і виконавцем робіт по створенню КСЗІ в АС. Виконавець повинен мати відповідну ліцензію Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (Департамент). У випадках, передбачених Положенням про технічний захист інформації в Україні, ТЗ на КСЗІ погоджується з Департаментом.

8.1.2 Зміст технічного завдання

Технічне завдання на КСЗІ оформлюється відповідно до того ж самого ДСТУ, що і основне ТЗ на АС, і в загальному випадку повинно містити такі основні підрозділи:

- загальні відомості;
- мета і призначення комплексної системи захисту інформації;
- загальна характеристика автоматизованої системи та умов її функціонування;
- вимоги до комплексної системи захисту інформації;
- вимоги до складу проектної та експлуатаційної документації;
- етапи виконання робіт;
- порядок внесення змін і доповнень до ТЗ;
- порядок проведення випробувань комплексної системи захисту інформації.

Вимоги до змісту розділів технічного завдання

В підрозділі зазначають:

- повне найменування КСЗІ та її умовне позначення;
- шифр теми і реквізити договору;
- найменування підприємств-розробників і замовника (користувача) КСЗІ та їх реквізити;

- перелік документів, на підставі яких створюється КСЗІ, ким і коли затверджені ці документи;
- планові терміни початку і закінчення роботи із створення КСЗІ;
- відомості про джерела і порядок фінансування робіт;
- порядок оформлення і подання замовнику результатів робіт із створення КСЗІ, з виготовлення і налагодження окремих засобів (технічних, програмних, інформаційних) і програмно-технічних (програмно-методичних) комплексів системи.

Мета і призначення комплексної системи захисту інформації

Вказується мета розробки КСЗІ в АС, функціональне призначення і особливості застосування. Необхідно зазначати, на підставі яких нормативно-правових актів, інших нормативних документів регламентується порядок захисту інформації в АС.

Загальна характеристика автоматизованої системи і умов її функціонування

В підрозділі рекомендується зазначити такі моменти, які впливають на безпеку інформації під час її оброблення в АС та на загальні вимоги до реалізації СЗІ:

- загальну структурну схему і склад ОС АС (перелік і склад устаткування, технічних і програмних засобів, їх зв'язки, особливості конфігурації і архітектури, особливості підключення до локальних або глобальних мереж тощо);
- технічні характеристики каналів зв'язку (пропускна спроможність, типи кабельних ліній, види зв'язку з віддаленими сегментами АС і користувачами і т. ін.);

- характеристики інформації, що обробляється (категорії інформації, вищий гриф секретності і т. ін.);
- характеристики персоналу (кількість користувачів і категорій користувачів, форми допуску тощо);
- характеристики фізичного середовища (наявність категорованих приміщень, територіальне розміщення компонентів АС, їх фізичні
- параметри, вплив на них чинників навколишнього середовища, захищеність від засобів технічної розвідки і т.п.);
- загальну технічну характеристику АС (обсяги основних інформаційних масивів і потоків, швидкість обміну інформацією і продуктивність системи під час розв'язання функціональних завдань, тривалість процедури підготовки АС до роботи після подачі живлення на її компоненти, тривалість процедури відновлення працездатності після збоїв, наявність засобів підвищення надійності і живучості і т. ін.);
- особливості функціонування АС (надання машинного часу або устаткування в оренду стороннім організаціям, цілодобовий режим роботи без відключення живлення тощо);
- особливості реалізованих або припустимих заходів організаційних, фізичних та інших заходів захисту (режимні заходи в приміщеннях і на території, охорона, сигналізація, протипожежна охорона і т. ін.);
- інші чинники, що впливають на безпеку оброблюваної інформації;
- потенційні загрози інформації (способи здійснення НСД, можливі технічні канали витоку інформації і умови їх формування, стихійні лиха і т. ін.), а також можливі наслідки їх реалізації;
- клас АС згідно з НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу".

Крім того, треба описати функціонуючі в складі АС (для існуючої АС) засоби захисту, а також засоби захисту, реалізовані в компонентах, які планується використовувати для побудови АС. При цьому треба враховувати,

що функції захисту, які реалізуються засобами імпортного виробництва, не мають зв'язаного з ними рівня гарантій. Використання таких засобів у складі КСЗІ можливе тільки за наявності експертного висновку, зареєстрованого Департаментомспеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

В підрозділі не вказуються ті характеристики і умови функціонування АС, опис яких є в ТЗ на АС або в інших документах. Даються тільки посилання на розділи цих документів.

8.1.3Вимоги до комплексної системи захисту інформації

Вимоги до комплексної системи захисту інформації в АС в частині захисту від несанкціонованого доступу.

Вимоги до комплексної системи захисту інформації в АС в частині захисту від НСД мають бути викладені відповідно до НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності комп'ютерних систем від несанкціонованого доступу " (далі - Критерії). Згідно з цим документом в процесі оцінки захищеності КС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій. Відповідно, в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

Має бути вказаний функціональний профіль захищеності, який передбачається реалізувати. Профіль може бути або вибраний із профілів, описаних в НД ТЗІ 2.5-005-99, або визначений як упорядкована сукупність рівнів послуг згідно з вимогами зазначеного документа. Повинен бути вказаний рівень гарантій, що передбачається досягти.

Опису послуг має передувати опис політики безпеки інформації, яку повинен реалізувати комплекс засобів захисту ОС АС. Опис політики безпеки має включати в себе опис:

- об'єктів (елементів ресурсів) ОС;

- принципів керування доступом користувачів до інформації (довірче і/або адміністративне керування доступом);
- правил розмежування інформаційних потоків;
- правил маркірування носіїв інформації;
- основних атрибутів доступу користувачів, процесів і пасивних об'єктів;
- правил розмежування доступу користувачів і процесів до пасивних об'єктів;
- правил адміністрування КЗЗ і реєстрації дій користувачів;
- інші загальні моменти політики безпеки, які вважає за потрібне описати розробник ТЗ.

Вимоги до послуг безпеки мають бути викладені і згруповані в тому порядку і стилі, в якому вони подані в Критеріях. В розділі мають бути викладені вимоги до реалізації послуг забезпечення:

- конфіденційності;
- цілісності;
- доступності;
- спостереженості.

Для кожної включеної до розділу послуги відповідно до Критеріїв має бути визначений рівень послуги, який передбачається реалізувати. Має бути описана політика даної послуги: визначення об'єктів, до яких застосовується дана послуга, і правил (в тому числі, що застосовуються за умовчуванням), відповідно до яких повинні функціонувати механізми, що реалізують послугу. Відповідно до особливостей розроблюваної АС мають бути конкретизовані всі вимоги, що викладені в Критеріях для відповідного рівня кожної послуги.

У разі, якщо передбачається реалізувати послуги безпеки, які не зазначені в Критеріях, їх також необхідно описати, дотримуючись, по можливості, стилю, прийнятого для опису інших послуг.

Вимоги до гарантій також мають бути викладені і згруповані в тому порядку і стилі, як вони подані в Критеріях. Це передбачає включення вимог:

- до архітектури КЗЗ (додатково до загальних вимог до архітектури на даному етапі бажано визначити основні модулі (підсистеми), з яких повинен складатися КЗЗ);
- до середовища розробки (організації процесу розробки і системи керування конфігурацією);
- до гарантій проектування (етапності розробки і проектної документації);
- до середовища функціонування;
- до експлуатаційної документації;
- до випробувань комплексу засобів захисту.

Всі вимоги повинні відповідати належному рівню гарантій.

Оскільки деякі з вимог гарантій стосуються розроблюваної системи в цілому, а не тільки КЗЗ, то в даному розділі допускається дати посилання на інші підрозділи ТЗ. Зокрема, вимоги до етапності розробки і складу документації мають бути визначені в розділах "Вимоги до складу проектної та експлуатаційної документації" та "Етапи виконання робіт". Крім того, допускаються посилання на інші документи, що розробляються на більш пізніх етапах.

Вимоги до комплексної системи захисту інформації в АС в частині захисту від витоку інформації технічними каналами.

Мають бути сформульовані загальні вимоги до об'єктів (компонентів АС), що захищаються, визначені засоби захисту і засоби їх використання (наприклад, реалізація вимог до захищеності повинна досягатись без застосування екранування приміщень, активні засоби мають застосовуватись тільки для захисту інформації головного сервера АС і т. ін.).

Наводиться перелік нормативних і методичних документів, відповідно до яких повинні проводитись роботи щодо захисту інформації від витоку технічними каналами.

Мають бути вказані вимоги до розмірів зони безпеки інформації.

Мають бути вказані необхідні величини показників захищеності, що враховують реальну завадову обстановку на об'єкті електронної обчислювальної техніки. Основними показниками є:

відношення величин електричної і магнітної складових напруженості поля побічних електромагнітних випромінювань до рівня завад на об'єкті ЕОТ;

відношення величини напруженості інформативного сигналу в провідних комунікаціях на межі зони безпеки інформації до рівня завад на об'єкті ЕОТ;

величина нерівномірності струму, який споживається по мережі електроживлення;

коефіцієнт екранування засобів обчислювальної техніки, в тому числі від впливу зовнішніх ЕМВ.

Гранично допустимі значення основних показників є нормованими величинами і визначаються за відповідними методиками.

Відношення розрахованих (виміряних) значень основних показників до гранично допустимих (нормованих) значень визначають необхідні умови захисту інформації.

Мають бути вказані вимоги щодо застосування способів, методів і засобів досягнення необхідних показників захищеності. Рекомендується застосування таких способів, методів і засобів:

а) системо- і схемотехнічних методів:

- обмеження використання інтерфейсів з передачею сигналів у вигляді послідовного коду і в режимі багатократних повторень;
- використання мультиплексних режимів обробки інформації, а також ЗОТ і системного забезпечення, що базуються на багаторозрядних

платформах, інтерфейсів з передачею сигналів у вигляді багаторозрядного паралельного коду;

- використання раціональних способів монтажу, за яких забезпечується мінімальна довжина електричних зв'язків і комунікацій;
- використання ЗОТ і технічних засобів, до складу яких входять стійкі до самозбудження схеми, розв'язувальні і фільтрувальні елементи, комплектуючі з низькими рівнями ЕМВ;
- використання мережевих фільтрів для блокування витоку ІзОД мережами електроживлення, а також лінійних (високочастотних) фільтрів для блокування витоку ІзОД лініями зв'язку;
- використання ЗОТ і технічних засобів у захисному виконанні;

б) засобів просторового і лінійного "зашумлення";

в) засобів локального або загального екранування;

г) засобів оптимального розміщення ЗОТ і технічних засобів з метою мінімізації зони, в межах якої граничне відношення сигнал/шум не перевищує встановлених норм.

Мають бути вказані вимоги до проведення спецдосліджень ЗОТ і технічних засобів, мета яких — пряме вимірювання показників ЕМВ.

Мають бути вказані вимоги до проведення спецперевірки ЗОТ, мета якої — виявлення та вилучення (блокування) спеціальних електронних (закладних) пристроїв.

Вимоги до складу проектної та експлуатаційної документації.

В цьому розділі слід навести перелік проектної та експлуатаційної документації, що розробляється в процесі створення КСЗІ в АС.

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.

Етапи виконання робіт.

Процес створення КСЗІ доцільно поділяти на три основні етапи: попередній, проектування і розробки КСЗІ, проведення випробувань і передачі в експлуатацію КСЗІ. Кожний з етапів допускається поділяти на окремі підетапи.

Приблизний перелік основних робіт, що проводяться на попередньому етапі, наведено в підрозділі 5.

До переліку робіт етапу проектування і розробки КСЗІ включаються роботи з вибору і модернізації штатних засобів захисту ПЗ і апаратури, що використовуються, архітектури ЗОТ, стандартних інтерфейсів і протоколів обміну, а також з розробки додаткового ПЗ і апаратної частини засобів захисту.

Етап випробувань і передачі в експлуатацію КСЗІ містить роботи, пов'язані з забезпеченням організації та проведення випробувань, включаючи, в разі необхідності, розробку спеціальної апаратури, ПЗ і відповідної документації.

Всі основні роботи кожного етапу відображаються в календарному плані, де зазначаються терміни проведення робіт за окремими етапами, види звітності і форми подання результатів замовнику.

Порядок внесення змін і доповнень до технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

Зміни затвердженого ТЗ на створення КСЗІ в АС, необхідність внесення яких виявлена в процесі виконання робіт, оформляються окремим

доповненням, яке погоджується і затверджується в тому ж порядку і на тому ж рівні, що і основний документ.

Доповнення до ТЗ на створення КСЗІ в АС складається з вступної частини і змінюваних підрозділів. У вступній частині зазначається причина випуску доповнення. В змінюваних підрозділах наводяться номери та зміст змінюваних, нових або пунктів, що скасовуються.

8.1.4 Порядок проведення випробувань комплексної системи захисту інформації

Для кожного виду випробувань (попередніх, державних, сертифікаційних та ін.) комплексної системи (підсистеми, компонента) захисту виконавець розробляє "Програму і методику випробувань комплексної системи (підсистеми, компонента) захисту інформації в АС", яка затверджується в установленому порядку. Терміни подання проекту Програми, його розгляду і затвердження погоджуються з замовником.

Для проведення випробувань замовником призначається комісія, склад якої погоджується з розробником КСЗІ.

Випробування проводяться з використанням умовної інформації (що не є ІзОД).

Наводиться необхідне для проведення випробувань забезпечення (необхідна нормативна, методична та інша документація, програмні та технічні засоби, метрологічне, спеціальне та інше обладнання, створення інших умов для проведення випробувань), сторона, що його надає, порядок усунення зауважень і т.ін.

Наводиться перелік документів, якими завершуються випробування (етапи випробувань): акт приймання, сертифікат (атестат, експертний висновок) відповідності встановленим критеріям, наказ про введення в експлуатацію тощо.

8.2 Завдання на лабораторну роботу

1. Відповідно до варіанту предметної галузі та результатів проведених теоретичних досліджень в попередніх лабораторних роботах розробити технічне завдання (ТЗ) на КСЗІ гіпотетичної ІКС, яка автоматизую діяльність підприємства предметної галузі.

2. Підготувати розширений звіт з поясненнями основних етапів розробки ТЗ.

8.3 Запитання для самоперевірки

1. Які основні етапи розробки технічного завдання на створення комплексної системи захисту інформації?

2. Які цілі та завдання має визначати технічне завдання для комплексної системи захисту інформації?

3. Які ключові вимоги до інформаційної безпеки повинні бути враховані у технічному завданні?

4. Як оцінюється поточний стан інформаційної безпеки організації при розробці технічного завдання?

5. Які методи і засоби аналізу ризиків використовуються при розробці технічного завдання?

6. Яким чином визначаються критичні інформаційні ресурси та вразливості при створенні технічного завдання?

7. Які основні компоненти (апаратні, програмні, організаційні) включає комплексна система захисту інформації?

8. Як формулюються вимоги до моніторингу та реагування на інциденти інформаційної безпеки в технічному завданні?

9. Які стандарти та нормативні документи використовуються при розробці технічного завдання на створення системи захисту інформації?

10. Як визначаються критерії ефективності та методи перевірки роботи комплексної системи захисту інформації у технічному завданні?

ЛАБОРАТОРНЕ ЗАНЯТТЯ №9. РОЗРОБКА ПРОЕКТУ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Мета роботи – отримати навички розробки проекту КСЗІ.

9.1 Короткі теоретичні відомості

Роботи зі створення КСЗІ виконуються організацією-власником ІТС. За умови відсутності у неї відповідних ліцензій або дозволу на здійснення окремих видів робіт із захисту інформації до виконання цих робіт залучаються суб'єкти господарювання, які мають такі ліцензії. Дозвіл на проведення робіт з технічного захисту інформації (далі – ТЗІ) для власних потреб дається Державною службою спеціального зв'язку та захисту інформації (далі – ДССЗЗІ) України у порядку, який визначено Положенням про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб.

КСЗІ розробляється і впроваджується в ІТС, що створюються, а також у діючих ІТС, якщо виникла необхідність забезпечення в них захисту інформації.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розробку і впровадження інформаційної технології, що забезпечує обробку інформації в ІТС згідно з вимогами, встановленими державними стандартами, нормативно- правовими актами та нормативними документами у сфері захисту інформації.

Комплексна система захисту інформації є невід'ємною складовою частиною автоматизованої системи (далі – АС) і на неї поширюються всі вимоги державних стандартів щодо створення АС.

Для створення КСЗІ використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за

результатами державної експертизи у сфері технічного та криптографічного захисту інформації.

9.1.1 Послідовність робіт зі створення КсЗІ

Нормативними документами в сфері ТЗІ визначений порядок проведення робіт зі створення КСЗІ. Основними етапами створення КСЗІ є:

− формування служби захисту інформації (призначення відповідальної особи) для організації робіт зі створення КСЗІ, її експлуатації та контролю за станом захищеності інформації;

− обстеження умов функціонування ІТС та розробка технічного завдання на створення КСЗІ;

− розробка та реалізація проекту КСЗІ;

− введення КСЗІ в дію та оцінка захищеності інформаційних ресурсів ІТС.

Стадії та етапи робіт, які виконуються під час створення КСЗІ в конкретній ІТС, їх зміст і результати, терміни виконання визначаються технічним завданням на створення КСЗІ та договорами між замовником і виконавцями робіт.

Вимоги щодо захисту інформації, які реалізуються КСЗІ, визначаються необхідним рівнем забезпечення властивостей, що характеризують захищеність інформації: цілісність, конфіденційність, доступність.

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

− витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

− несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з

метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів та ін.;

− спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються рівнем критичності оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС відповідно до нормативних документів з захисту інформації.

Створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, яка становить державну таємницю або коли необхідність цього визначена власником інформації.

Створення комплексу засобів захисту(далі – КЗЗ) інформації від несанкціонованого доступу (далі – НСД) здійснюється у всіх ІТС, де обробляється інформація, яка є власністю держави або що відноситься до державної таємниці, або до окремих видів інформації, захист яких гарантується державою, а також в ІТС, де така необхідність визначена власником інформації.

Порядок розробки, впровадження, використання у складі КСЗІ засобів і систем криптографічного захисту інформації регламентується нормативно-правовими актами та нормативними документами з криптографічного захисту інформації.

9.1.2 Етапи створення КСЗІ

1 етап. Обстеження ІТС та підготовка вихідних даних для формування вимог до КСЗІ.

На цьому етапі в загальному випадку виконується:

- аналіз нормативно-правових актів, на підставі яких можуть встановлюватися обмеження доступу до певних видів інформації або заборона такого обмеження, визначається необхідність забезпечення захисту інформації згідно з іншими критеріями;
- визначаються переліки інформації, що підлягає автоматизованій обробці, і здійснюється її класифікація щодо рівня обмеження доступу до неї, вимог щодо забезпечення цілісності та вимог щодо забезпечення доступності відповідно до нормативно-правових актів.

При обстеженні ІТС розглядається як організаційно – технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі – середовища функціонування ІТС).

Метою обстеження є опис кожного середовища функціонування ІТС та виявлення в них елементів, які безпосередньо або опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт. 2 етап. Формування політики безпеки На цьому етапі здійснюється:

- аналіз ризиків (вивчення моделі загроз та моделі порушника, можливих наслідків від реалізації потенційних загроз);
- визначення вимог до заходів, методів і засобів захисту інформації;
- вибір основних рішень з протидії всім суттєвим загрозам, формування вимог, правил, обмежень, рекомендацій, які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, а також регламентують діяльність користувачів всіх категорій;
- документальне оформлення політики безпеки інформації.

Політика безпеки повинна враховувати особливості окремих компонентів КСЗІ та може розроблятися для ІТС в цілому, для окремих складових компонента, для окремої функціональної задачі, для окремої

технології обробки інформації. Політика безпеки оформляється у вигляді окремого документа Плану захисту.

2 етап. Розробка технічного завдання (далі – ТЗ) на створення КСЗІ.

Технічне завдання на створення КСЗІ в ІТС є вихідним організаційно-технічним документом, в якому визначаються вимоги щодо захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

Технічне завдання на створення КСЗІ розробляється з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеки інформації на всіх етапах життєвого циклу ІТС.

ТЗ на КСЗІ може розроблятися для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС.

ТЗ на КСЗІ може бути оформлений:

- у вигляді окремого розділу загальної технічної задачі на створення ІТС;
- у вигляді окремого (часткового) ТЗ;
- у вигляді доповнення до загального ТЗ на створення ІТС.

Для інтегрованих ІТС (що складаються з декількох окремих інформаційних чи телекомунікаційних систем, які можуть функціонувати як самостійно, так і взаємодіяти між собою) рекомендується для кожної із складових частин ІТС створювати окремі КСЗІ і оформляти вимоги окремими ТЗ. Можлива розробка одного ТЗ на кілька однотипних складових частин ІТС, вказавши існуючі між ними відмінності або особливості.

3 етап. Розробка і реалізація проекту КСЗІ в ІТС.

Проект КСЗІ розробляється на підставі та у відповідності з Технічним завданням на створення ІТС і виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робоча документація.

При розробці проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають можливість забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і засобів захисту інформації.

Виконується розробка спільних рішень, необхідних для реалізації вимог ТЗ на КСЗІ, щодо організаційної структури КСЗІ, структури технічних і програмних засобів, алгоритмів функціонування та умов використання засобів захисту, реалізації визначених функціональним профілем захищеності послуг безпеки інформації.

4 етап. Введення КСЗІ в дію.

На цьому етапі повинна бути завершена розробка КСЗІ і затверджені документи, які входять до Плану захисту.

Проводиться навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів) основним положенням та процедурами документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації.

Проводиться атестація впровадженого комплексу технічного захисту інформації від витоку технічними каналами, за результатами якого видається документ: «Акт атестації комплексу технічного захисту інформації».

Здійснюється згідно з документацією робочого проекту інсталяція, ініціалізація та перевірка працездатності комплексу засобів захисту інформації від НСД.

Під час інсталяції повинні бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, механізми контролю за діями користувачів, а також контролю цілісності програмного забезпечення та бази даних захисту.

До бази даних захисту вносяться відомості про користувачів ІТС, встановлюються їх повноваження щодо доступу до захищених об’єктах ІТС, їх створення, модифікації, архівування, знищення, експорту / імпорту із системи.

5 етап. Попередні випробування.

Метою попередніх випробувань є перевірка працездатності КСЗІ, її відповідності технічним завданням і визначення можливості прийняття КСЗІ в дослідну експлуатацію.

Попередні випробування проводяться у відповідності з програмою і методиками випробувань. Їх організовує замовник ІТС, а проводить – розробник КСЗІ спільно із замовником.

6 етап. Дослідна експлуатація.

Під час дослідної експлуатації КСЗІ:

- відпрацьовуються технології захисту оброблюваної інформації, оббіг машинних носіїв інформації, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;
- співробітники системи захисту інформації (далі – СЗІ) та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань забезпечення режиму доступу;
- здійснюється доопрацювання програмного забезпечення, додаткове налаштування та конфігурування КЗЗ від НСД;
- здійснюється коригування робочої та експлуатаційної документації.

Дослідна експлуатація ІТС повинна здійснюватися без використання інформації, що становить державну таємницю.

У разі використання в складі КСЗІ комплексу засобів захисту інформації від НСД, який не має експертного висновку про відповідність вимогам НД ТЗІ, необхідно здійснити комплекс робіт з підготовки до проведення оцінки відповідності цього комплексу засобів захисту інформації вимогам НД ТЗІ під час проведення державної експертизи КСЗІ.

7 етап. Державна експертиза КСЗІ.

Комплексна система захисту інформації, що є власністю держави, або інформації з обмеженим доступом, або іншої інформації, захист якої гарантується державою, повинна мати атестат відповідності вимогам захисту інформації, який видається ДССЗЗІ України за результатами державної експертизи.

Державна експертиза КСЗІ проводиться з метою визначення її відповідності технічному завданню, вимогам нормативно-правових актів і нормативних документів щодо захисту інформації та з метою визначення можливості введення КСЗІ в експлуатацію в складі ІТС.

Державна експертиза КСЗІ є етапом приймальних випробувань ІТС та проводиться у відповідності до Положення про державну експертизу в сфері технічного захисту інформації.

Якщо в ІТС обробляється інформація, яка є власністю держави, або інформація, захист якої гарантується державою, то дозвіл на експлуатацію ІТС дається наказом керівника організації тільки за наявності атестату відповідності КСЗІ.

8 етап. Супровід КСЗІ.

На цьому етапі виконуються роботи з організаційного забезпечення функціонування КСЗІ, її планової модернізації та з управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ.

9.2 Завдання на лабораторну роботу

1. Відповідно до варіанту предметної галузі та результатів проведених теоретичних досліджень в попередніх лабораторних роботах та ТЗ на КСЗІ розробити проект КСЗІ гіпотетичної ІКС, яка автоматизує діяльність підприємства предметної галузі.

2. Підготувати розширений звіт з поясненнями основних етапів розробки проекту КСЗІ.

9.3 Запитання для самоперевірки

1. Які основні етапи включає процес розробки проекту комплексної системи захисту інформації?

2. Які методи і засоби оцінки ризиків використовуються при проектуванні комплексної системи захисту інформації?

3. Як визначаються і класифікуються інформаційні ресурси та їх вразливості під час розробки проекту захисту інформації?

4. Які компоненти повинні бути включені в архітектуру комплексної системи захисту інформації (апаратні, програмні, організаційні)?

5. Які основні функції та завдання повинні виконувати засоби захисту інформації у проекті?

6. Яким чином забезпечується безпека комунікаційних мереж у рамках комплексної системи захисту інформації?

7. Які стандарти та нормативні документи враховуються при розробці проекту комплексної системи захисту інформації?

8. Як визначаються і формулюються вимоги до засобів автентифікації та управління доступом у проекті?

9. Які методи та засоби моніторингу і реагування на інциденти інформаційної безпеки передбачені у проекті?

10. Як оцінюється ефективність реалізованих заходів і компонентів комплексної системи захисту інформації після їх впровадження?

ЛАБОРАТОРНЕ ЗАНЯТТЯ №10. ВВЕДЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ДІЮ ТА ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В ІТС

Мета роботи – ознайомити з процесом введення КСЗІ в дію.

10.1 Короткі теоретичні відомості

10.1.1 Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

Етап 1. Підготовка КСЗІ до введення в дію

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

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

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

Етап 2. Навчання користувачів

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

Етап 3. Пусконалагоджувальні роботи

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

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

Під час інсталяції мають бути задіяні механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення.

Етап 4. Попередні випробування

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

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

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

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

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

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

Етап 5. Дослідна експлуатація

Під час дослідної експлуатації КСЗІ:

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

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

Етап 6. Державна експертиза КСЗІ

Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІТС.

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

Державна експертиза КСЗІ в ІТС проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації, яке затверджене

наказом Адміністрації Держспецзвязку від 16.05.2007 №93 і зареєстроване в Міністерстві юстиції України 16 липня 2007 р. За №820/14087 (нова редакція Положення затверджена наказом Адміністрації Держспецзвязку від 13.10.2017 №565 та перебуває на опрацюванні в Міністерстві юстиції України на предмет можливості державної реєстрації).

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

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

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

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

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

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

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

10.2 Завдання на лабораторну роботу

1. Відповідно до варіанту предметної галузі та результатів проведених теоретичних досліджень в попередніх лабораторних роботах описати процес введення КСЗІ в дію та оцінити рівень захищеності інформації в ІТС.

2. Підготувати розширений звіт з виконання лабораторної роботи.

10.3 Запитання для самоперевірки

1. Які ключові кроки включає процес введення комплексної системи захисту інформації в дію?

2. Як проводиться тестування функціональності та ефективності компонентів комплексної системи захисту інформації перед її введенням в дію?

3. Які методи та інструменти використовуються для оцінки захищеності інформації в інформаційно-телекомунікаційних системах (ІТС)?

4. Які вимоги до документування процесу введення комплексної системи захисту інформації в дію?

5. Як забезпечується безперервність бізнес-процесів під час впровадження заходів захисту інформації?

6. Які критерії використовуються для оцінки відповідності впровадженої системи захисту інформації встановленим стандартам та нормативним вимогам?

7. Які заходи включає план управління інцидентами інформаційної безпеки при введенні комплексної системи захисту інформації в дію?

8. Як проводиться навчання персоналу та підвищення їхньої обізнаності щодо нових заходів захисту інформації?

9. Яким чином здійснюється постійний моніторинг та аудит захищеності інформації після введення комплексної системи в дію?

10. Які процедури та інструменти використовуються для оновлення та вдосконалення компонентів комплексної системи захисту інформації на основі результатів оцінки захищеності інформації в ІТС?

11 ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ ТА ВИМОГИ ДО РОБОТИ

11.1 Загальні рекомендації до виконання роботи

Згідно з учбовим планом, студенти денної форми навчання мають 32 годин лабораторних робіт та 86 годин самостійної роботи. Перед виконанням лабораторного заняття студент має детально вивчити матеріал з курсу «Архітектура систем захисту інформації», підібрати відповідну навчальну, методичну та спеціальну літературу за рекомендованим списком (а також самостійно підібраною).

11.2 Вимоги до виконання практичних робіт

При виконанні лабораторної роботи необхідно дотримуватись таких вимог:

– розв’язок завдань має супроводжуватись поясненням, при необхідності, формулами тощо.

– лабораторна робота повинна бути охайно оформленою, розбірливо написана без скорочення слів (крім загальновідомих скорочень);

– сторінки роботи повинні бути пронумеровані;

– всі етапи виконання алгоритму роботи/програм/скриптів повинні бути прокоментовані.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Основна література

1. Комплексні системи захисту інформації : навч. посіб. / Ю.Є. Яремчук, П. В. Павловський, В.С. Катаєв, В.В. Сінюгін. – Вінниця : ВНТУ, 2018. – 118 с.

2. Гребенніков В.В. Комплексні системи захисту інформації: проектування, впровадження, супровід / В. В. Гребенніков. - Ужгород : УжНУ, 2019. – 613 с.

3. Конспект лекцій з дисципліни «Архітектура та проектування програмного забезпечення» для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Інженерія програмного забезпечення» із спеціальності 121 – «Інженерія програмного забезпечення» / уклад. В.В. Завгородній, К.М. Ялова. – Кам'янське : ДДТУ, 2019.– 144 с.

4. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / 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.

5. Хорошко В.О. Проєктування комплексних систем захисту інформації : підручник / В.О. Хорошко, І.М. Павлов, Ю.Я. Бобало та ін. – Львів : Видавництво Львівської політехніки, 2020. - 320 с.

6. Богуш В.М. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посіб. / В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін. – Київ : Ліра-К, 2020. - 554 с.

Допоміжна література

1. Лужецький В.А. Основи інформаційної безпеки. Навчальний посібник / В.А. Лужецький, О.П. Войтович, В.Д. Кожухівський. – Вінниця ВНТУ, 2013. – 246 с.

2. Горохов С.М. Інформаційна безпека цифрових програмно-керованих АТС: навч. посіб. / С.М. Горохов, В.Г. Кононович, С.В. Стайкуца та ін. - Одеса, 2013. - 244 с.

3. Заплотинський Б. А. Основи інформаційної безпеки. Конспект лекцій [Електронний ресурс] / Б.А. Заплотинський. - КІІВіП НУ "ОЮА", кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с. - Режим доступу: http://dspace.onua.edu.ua/handle/11300/11111. – Назва з екрана.

4. Марущак А.І. Правові основи захисту інформації з обмеженим доступом: курс лекцій / А.І. Марущак. – Київ : КНТ, 2007. - 208 с.

5. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс] : держ. сайт. - Режим доступу http://surl.li/kebhct. – Назва з екрана.

Нормативна документація

1. Про захист інформації в інформаційно- телекомунікаційних системах: Закон України від 31.05.2005 р. № 2594-IV. - Станом на 28.06.2024 р. – Режим доступу : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text. – Назва з екрана.

2. Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 [Електронний ресурс]. – Чинний від 01.01.1997. – Режим доступу : https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69172. - Назва з екрана.

3. Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97 [Електронний ресурс]. – Чинний від 01.01.1998. – Режим доступу : https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69175. – Назва з екрана.

4. Автоматизовані системи. Терміни та визначення. ДСТУ 2226-93 [Електронний ресурс]. – Чинний від 01.07.1994. – Режим доступу : https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=61937. – Назва з екрана.

5. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] : НД ТЗІ 1.1-002-99 від 28.04.1999 № 22. – Режим доступу : https://tzi.com.ua/downloads/1.1-002-99.pdf. – Назва з екрана.

6. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс] : НД ТЗІ 1.1-003-99 від 28.04.1999 № 22. – Режим доступу : https://tzi.ua/assets/files/1.1_003_99.pdf. – Назва з екрана.

7. Типове положення про службу захисту інформації в автоматизованій системі [Електронний ресурс] : НД ТЗІ 1.4-001-2000 від 04.12.2000 № 53. – Режим доступу : https://tzi.com.ua/downloads/1.4-001-2000.pdf. – Назва з екрана.

8. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс] : НД ТЗІ 2.5-004-99 від 28.04.1999 № 22. – Режим доступу : https://tzi.com.ua/downloads/2.5-004-99.pdf. – Назва з екрана.

9. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс] : НД ТЗІ 2.5-005-99 від 28.04.1999 № 22. – Режим доступу : https://tzi.com.ua/downloads/2.5-005%20-99.pdf. – Назва з екрана.

10. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення [Електронний ресурс] : НД ТЗІ 1.1-005-07. – Режим доступу : https://tzi.com.ua/downloads/3.1-001-07.pdf. – Назва з екрана.

11. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи

[Електронний ресурс] : НД ТЗІ 3.1-001-07. - Режим доступу : https://tzi.com.ua/downloads/3.1-001-07.pdf. – Назва з екрана.

12. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [Електронний ресурс] : НД ТЗІ 3.7-001-99 від 28.04.1999 № 22. – Режим доступу : https://tzi.com.ua/downloads/3.7-001-99.pdf. – Назва з екрана.

13. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно- телекомунікаційній системі [Електронний ресурс] : НД ТЗІ 3.7-003-05 від 8.11. 2005 р. № 125. – Режим доступу : https://tzi.com.ua/downloads/3.7-003-2005.pdf. – Назва з екрана.

14. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 [Електронний ресурс] : НД ТЗІ 2.5-008-02 від 13.12.2002 № 84. – Режим доступу : https://tzi.com.ua/downloads/2.5-008-2002.pdf. – Назва з екрана.

15. Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу [Електронний ресурс] : НД ТЗІ 2.5-010-03 від 02.04.2003 № 33. - Режим доступу : https://tzi.com.ua/downloads/2.5-008-2002.pdf. – Назва з екрана.

16. Положення про державну експертизу в сфері технічного захисту інформації [Електронний ресурс] : наказ Адміністрації Держспецзвязку від 16.05.2007 №93 №820/14087. - Режим доступу : https://zakon.rada.gov.ua/laws/show/z0820-07#Text. – Назва з екрана.