МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

"На правах рукопису"
УДК 654.9

«До захисту допущено»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
“___” _____ 2021 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: Підвищення рівня ефективності систем захисту інформації в автоматизованих системах

Студент групи СЗДМ-61 Царенко Богдан Віталійович _____
(підпис)

Науковий керівник: Ахрамович Володимир Миколайович _____
(підпис)

Нормоконтроль: Гребенніков Асаді Болдхоядович _____
(підпис)

Київ – 2021 р.

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ

_____ _____
(підпис)

“___”_____
2021 р.

ЗАВДАННЯ

на магістерську атестаційну роботу

студенту Царенку Богдану Віталійовичу

1.Тема роботи: Підвищення рівня ефективності систем захисту інформації в автоматизованих системах

Затверджена наказом по університету “___”_____2021 р. № _____

2.Термін здачі студентом оформленої роботи “___”_____2021 р.

3.Об’єкт дослідження: системи захисту інформації, комплексні системи захисту інформації, автоматизовані системи, технічний проект.

4. Предмет дослідження: способи та методи підвищення, створення та модернізації в автоматизованих системах захисту інформації.

5.Мета дослідження: визначення шляхів розробки автоматизованих систем та технічного завдання на їх створення.

6.Перелік питань, які мають бути розроблені:

1. Основні поняття автоматизованих систем, нормативно-правова база.
2. Обгрунтування створення комплексного захисту інформації в автоматизованих системах.
3. Рекомендації що до розробка оцінки ефективності в Автоматизованих Системах.
4. Огляд вибору шляхів захисних заходів в автоматизованих системах.
5. Розроблення рекомендацій щодо використання пристроїв, методів та заходів захисту інформації в автоматизованих системах.

7.Перелік публікацій:

8. Перелік ілюстративного матеріалу: Презентанційний матеріал на слайдах.

Дата видачі завдання “___”_____ 2021 р.

Науковий керівник: _____ Ахрамович В.М.

Завдання прийнято _____ Царенко Б.В

до виконання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	**Примітка**
1	Підбір науково-технічної літератури		
2	Обґрунтування актуальності теми роботи		
3	Написання першого розділу роботи		
4	Написання другого розділу роботи		
5	Написання третього розділу роботи		
6	Написання висновків по роботі		
8	Підготовка демонстраційних матеріалів		
9	Підготовка доповіді		
10	Захист в ДЕК		

Студент _____ Царенко Богдан Віталійович

(підпис) (ініціали, прізвище)

Керівник роботи _____ Ахрамович В. М.

(підпис) (ініціали, прізвище)

РЕФЕРАТ

Дипломна робота містить: 80 сторінок, 20 джерело інформації, 14 таблиць.

Об'єкт дослідження - комплексна інформаційно-пошукова система в автоматизованих системах.

Метод спостереження – це систематичний аналіз методів і прийомів збору інформації з туру.

За результатами візиту спеціаліста ВКР було проаналізовано: законодавчу базу та поточний прогрес у проектуванні інтегрованих інформаційно-пошукових систем, призначених для оцінки ефективності реалізації математичних задач в автоматизованих системах автоматизації. Розробка рекомендацій щодо методів організації та інженерного пошуку інформації в автоматизованих системах.

Результати спеціаліста ВКР рекомендовані для успішного використання для подальшого вивчення, яке проводиться студентами на початковому етапі розробки системи та створення інформаційної системи на підприємстві.

Ключові слова: АВТОМАТИЗОВАНА СИСТЕМА, ІНФОРМАЦІЙНА БЕЗПЕКА, КОМПЛЕКСНА СИСТЕМА, ІНФОРМАЦІЙНІ БЕЗПЕКИ, СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ.

ANNOTATION

Thesis contains: 80 pages, 20 sources of information, 14 tables.

The object of study - a comprehensive information retrieval system in automated systems.

The method of observation is a systematic analysis of methods and techniques of collecting information from the tour.

According to the results of the visit of the WRC specialist, the following were analyzed: the legal framework and current progress in the design of integrated information retrieval systems designed to assess the effectiveness of the implementation of mathematical problems in automated automation systems. Development of recommendations on methods of organization and engineering search of information in automated systems.

The results of the WRC specialist are recommended for successful use for further study, which is conducted by students at the initial stage of system development and information system creation at the enterprise.

Key words: AUTOMATED SYSTEM, INFORMATION SECURITY, COMPREHENSIVE SYSTEM, INFORMATION SECURITY, INFORMATION PROTECTION SYSTEMS.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

КСЗІ – Комплексна система захисту інформації

АІС (АС) – Автоматизована інформаційна система

ВТСС – Допоміжні технічні засоби та системи

ДССЗІ – Державна служба спеціального зв'язку та захисту інформації

СІБ – Системи інформаційної безпеки

ЗЗ – Захисні заходи

ЗП – Захищене приміщення

ІТС – Інформаційно-телекомунікаційна система

НСД – несанкціонований доступ

СЗІ - Системи захисту інформації

ТЗ – Технічне завдання

ТРП – Технічно-робочий проект

ЕОМ - Електронно0обчислювальна машина

КЗ - Контрольована зона

ОТСС – Основні технічні засоби та системи

Вступ

інформаційної безпеки — це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Під інформаційним середовищем [information environment] розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на три основні предметні частини:

- створення і розповсюдження вихідної та похідної інформації;
- формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;
- споживання інформації;

Водночас, захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Кажучи про системи безпеки, слід зазначити, що вони повинні не тільки і не так обмежувати допуск користувачів до інформаційних ресурсів, скільки визначати та делегувати їх повноваження у спільному вирішенні завдань, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації та усувати їх наслідки, адаптуючи структуру в умовах відмов, часткової втрати чи тривалого блокування ресурсів.

Комплексна система захисту інформації – сукупність організаційних та інженерно-технічних заходів, спрямованих

на забезпечення захисту інформації від розголошення, витоку та несанкціонованого доступу. Організаційні заходи є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються у міру потреби.

КСЗІ призначена забезпечувати, з одного боку, функціонування надійних механізмів захисту, з іншого - управління механізмами захисту. У зв'язку з цим має передбачатися організація чіткої та налагодженої системи управління захистом інформації.

У цій роботі розглянуто основні засади створення КСЗІ для АІС (Автоматизована інформаційна система) .

1. Аналіз нормативно-правової бази в автоматизованих системах

Проектування захищених інформаційних систем процес досить складний, який передбачає наявність відповідних знань та досвіду у її творців.

Споживач може не вникати у розробку такого проекту та подробиці його розвитку, однак він зобов'язаний контролювати кожен його етап щодо відповідності технічному завданню та вимогам нормативних документів. У свою чергу персональний досвід проектувальників вимагає використання існуючих нормативних документів у цій галузі для отримання найбільш якісного результату.

Таким чином, процес проектування захищених інформаційних систем повинен ґрунтуватися на знанні та строгому виконанні вимог існуючих нормативних документів як з боку її розробників, так і з боку замовників.

1.1. Класифікація автоматизованих систем

Нормативним документом передбачається розподіл АС на 3 класи:

Клас 1 - однокористувацький комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності. Приклад - автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів.

Клас 2 - локалізований багатомашинний розрахований на багато користувачів комплекс, що обробляє інформацію різних категорій конфіденційності. Приклад – локальна обчислювальна мережа.

Клас 3 – розподілений багатомашинний розрахований на багато користувачів комплекс, який обробляє інформацію різних категорій конфіденційності. Приклад – глобальна обчислювальна мережа.

1.2 Системи інформаційної безпеки

Системи інформаційної безпеки(СІБ) – стан захищеності життєво важливих інтересів людини та громадянина, суспільства та держави, при якому запобігає завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисні спричинення негативних наслідків застосування інформаційних технологій.

СІБ є рішення, спрямоване забезпечення захисту критичної інформації організації від розголошення, витоку і несанкціонованого доступу. Як і КСЗІ, СІБ поєднує у собі комплекс організаційних заходів та технічних засобів захисту інформації.

СІБ в основному призначені для захисту інформації в АС класу 2 та класу 3. Проте між КСЗІ та СІБ є принципові відмінності.

Перша відмінність полягає в тому, що при побудові СІБ немає потреби виконувати вимоги нормативних документів у сфері технічного захисту інформації, оскільки основними споживачами СІБ є комерційні організації, які не обробляють інформацію, що належить державі. Другою важливою відмінністю є відсутність контролюючого органу, і, як

наслідок, спроектована СІБ не потребує проведення державної експертизи. Ще одна відмінність від КСЗІ – вільний вибір технічних засобів, можливе застосування будь-яких апаратних та програмних засобів захисту інформації.

СІБ можна рекомендувати комерційним організаціям, які дбають про збереження своєї комерційної (критичної) інформації або збираються вживати заходів щодо забезпечення безпеки своїх інформаційних активів.

Важливим моментом, що стосується експлуатації як КСЗІ АС класу 2 та класу 3, так і СІБ, є той факт, що недостатньо просто побудувати та експлуатувати ці системи захисту, необхідно постійно їх удосконалювати так само, як удосконалюються способи несанкціонованого доступу, методи зламування та хакерські атаки.

Надалі, при проектуванні системи захисту братимемо за основу АС класу 1 і 2, оскільки саме ці системи обробки інформації становлять найбільший інтерес у зловмисника з погляду її розкрадання.

Таблица 1.1 – Сравнительный анализ систем защиты информации

Особливості КСЗІ	РСО КСЗІ	АС класу 2 (3)	СІБ
Споживачі послуг	Органи державної влади, комерційні організації	Органи державної влади, комерційні організації	Комерційні організації
Оброблювана інформація	Конфіденційна інформація, що належить державі, або інформація, що містить державну таємницю	Конфіденційна інформація, що належить державі (фізичній особі), або відкрита інформація, що належить державі	Критична інформація організації (персональна, фінансова, договірна інформація, інформація про замовників)
Суб'єкти	Замовник Виконавець Контролюючий орган	Замовник Виконавець Контролюючий орган	Замовник Виконавець

Наявність ліцензії на проведення робіт із побудови	Ліцензія на проведення робіт з технічного захисту інформації	Ліцензія на проведення робіт з технічного захисту інформації	Не вимагається
Проведення державної експертизи	Обов'язково	Обов'язково	Не вимагається
Технічні засоби захисту інформації	Тільки сертифіковані кошти захисту інформації	Тільки сертифіковані кошти захисту інформації	Будь-які засоби захисту інформації
Виконання вимог нормативної бази	Обов'язково	Обов'язково	Не вимагається

1.3 Порядок створення комплексної системи захисту інформації

Створення КСЗІ в ІТС здійснюється відповідно до нормативного документа системи технічного захисту інформації на підставі технічного завдання (далі – ТЗ), розробленого відповідно до вимог нормативного документа системи технічного захисту інформації. Крім того, під час проектування КСЗІ можна керуватися стандартом.

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

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань та наведень, акустоелектричних та інших каналів;

- несанкціонованих дій та несанкціонованого доступу до інформації, які можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування помилкової інформації, застосування заставних пристроїв або програм, використання комп'ютерних вірусів тощо .

- спеціального впливу на інформацію, що може здійснюватися шляхом формування полів та сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Незважаючи на простоту структури розробки КСЗІ, більшість організацій дотримуються саме цього алгоритму. Проте цей алгоритм – це лише основа проектування. Кожен представлений етап відображає безліч рівнів у ході проектування, залежно від структури АС вимоги до її системи захисту.

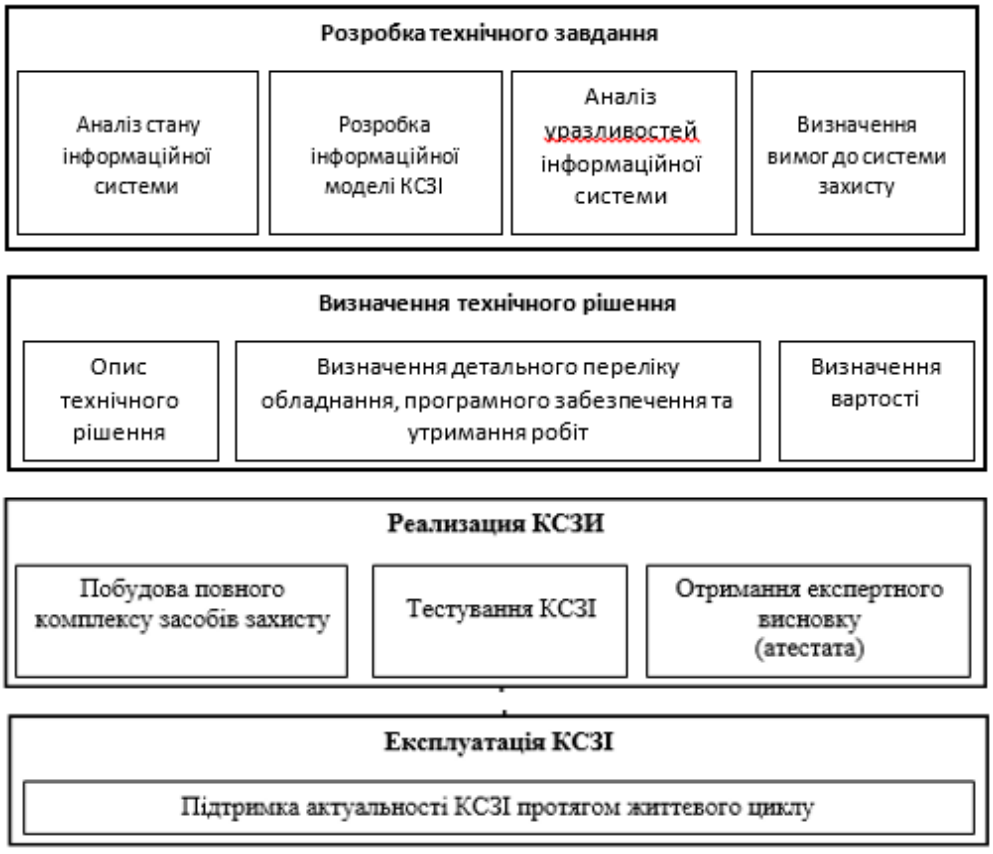

Рисунок 1.1 – Етапи проектування КСЗІ

1.3.1 Визначення технічного рішення

Загалом процес проектування можна поділити на такі етапи:

- підготовка ТЗ на створення системи захисту інформації;

- створення моделі СЗІ;

- розробка технічно-робочого проекту (ТРП) створення СЗІ та архітектури СЗІ. ТРП зі створення СЗІ включає такі документи:

1) пояснювальну записку, що містить опис основних технічних рішень щодо створення СЗІ та організаційних заходів щодо підготовки СЗІ до експлуатації;

2) обґрунтування обраних компонентів СЗІ та визначення місць їх розміщення. Опис розроблених профілів захисту;

3) специфікацію на комплекс технічних засобів СЗІ;

4) специфікацію на комплекс програмних засобів СЗІ;

5) визначення налаштувань та режиму функціонування компонентів СЗІ:

- розробка організаційно-розпорядчих документів системи управління ІБ (політик із забезпечення інформаційної безпеки, процедур, регламентів та ін.);

- розробка робочого проекту (включаючи документацію на засоби захисту та порядок адміністрування, план введення СЗІ в експлуатацію та ін.), планування навчання користувачів та обслуговуючого персоналу інформаційної системи;

- реалізація дозвільної системи допуску та організаційно-технічних заходів щодо захисту інформації в КСЗІ.

Технічне завдання створення КСЗИ може розроблятися для ІТС створюваних вперше, і навіть під час модернізації вже існуючих ІТС як окремого розділу ТЗ створення ІТС, окремого (часткового) ТЗ чи доповнення до ТЗ створення ІТС.

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

Проект КСЗІ розробляється на підставі та відповідно до ТЗ. Під час розробки проекту КСЗІ обґрунтовуються та приймаються проектні рішення, які дають можливість реалізувати вимоги ТЗ, забезпечити сумісність та взаємодію різних компонентів КСЗІ, а також різних заходів та способів захисту інформації. В результаті створюється комплект робочої та експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ.

1.3.2 Аналіз структури автоматизованої інформаційної системи

У ході цього етапу проводиться аналіз ризиків. Для перевірки здатності інформаційної системи протистояти спробам несанкціонованого доступу та на інформацію іноді доцільно виконувати тести на проникнення.

Існує кілька видів обстеження:

- передпроектне діагностичне обстеження, яке виконується при модернізації чи побудові СЗІ;

- аудит СЗІ на відповідність вимогам внутрішньокорпоративних стандартів або міжнародних/національних стандартів. Прикладом може бути сертифікаційний аудит системи управління ІБ за ISO;

- спеціальні види обстеження, наприклад, під час розслідування комп'ютерних інцидентів.

Кожен із виділених елементів має свої особливості, які необхідно враховувати щодо можливих загроз. За результатами аналізу можливих загроз безпеці АС формуються вимоги до захисту. Повний захист АС формується із приватних вимог захисту елементів шляхом поєднання функціонально однорідних вимог щодо забезпечення захисту.

За результатами даного етапу визначаються та формуються вимоги до захисту. Повний захист АС формується із приватних вимог захисту елементів.

1.3.3 Визначення технічного рішення

Проект повинен включати розділи, присвячені забезпеченню автоматизації діяльності співробітників організації, інформаційного обміну по високошвидкісних лініях зв'язку, захисту інформації. При необхідності розробляються завдання та проекти на інші роботи, наприклад, будівельно-монтажні. На основі цього документа буде створюватися КСЗІ, тому він повинен включати опис всіх впроваджуваних технічних засобів, їх налаштування, а також всі необхідні організаційні рішення.

До складу розроблюваної організаційно-технічної та експлуатаційної документації входять технічний паспорт на КСЗІ, інструкції та керівництва для користувачів, адміністраторів системи, з експлуатації технічних засобів, накази, акти та розпорядження, пов'язані з проектуванням, впровадженням, випробуваннями та введенням в експлуатацію системи.

Проект КСЗІ розробляється на підставі та відповідно до ТЗ. Під час розробки проекту КСЗІ обґрунтовуються та приймаються проектні рішення, які дають можливість реалізувати вимоги ТЗ, забезпечити сумісність та взаємодію різних компонентів КСЗІ, а також різних заходів та способів захисту інформації. В результаті створюється комплект робочої та експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ.

Під реалізацією дозвільної системи допуску та організаційно-технічних заходів щодо захисту інформації розуміються проведення наступних дій:

- визначення складу суб'єктів доступу до інформації, що захищається (співробітників організації);

- ознайомлення працівників з правилами обробки інформації, що захищається, та забезпечення інформаційної безпеки, накладення на всіх користувачів персональної відповідальності за розголошення довіреної ним інформації, що захищається, шляхом підпису ними відповідних документів;

- розробка та затвердження переліку інформаційних ресурсів, що захищаються, матриці доступу співробітників до ресурсів, що захищаються;

- визначення складу носіїв інформації, що захищається, та їх маркування;

- формування журналів обліку паролів, журналів обліку персональних ідентифікаторів, журналів обліку носіїв інформації, що захищається.

1.3.4 Реалізація КСЗІ

Тестування КСЗІ проводиться з метою перевірки її функціонування відповідно до встановлених вимог, а також виявлення недоліків та їх усунення. Вона здійснюється відповідно до програми, в якій вказуються умови та порядок функціонування АС у захищеному виконанні, тривалість дослідної експлуатації, порядок усунення виявлених недоліків.

Роботи з впровадження системи включають виконання наступних завдань:

- закупівля, встановлення та налаштування засобів захисту інформації в КСЗІ;

- проведення приймально-здавальних випробувань;

- атестація КСЗІ на відповідність вимогам керівних документів з безпеки інформації (добровільна);

- навчання користувачів;

- введення СЗІ в експлуатацію.

Закупівля, встановлення та налаштування (тестування) технічних засобів проводиться згідно з вимогами, наведеними у проекті на створення КСЗІ.

Тестування КСЗІ проводиться з метою перевірки її функціонування відповідно до встановлених вимог, а також виявлення недоліків та їх усунення. Вона здійснюється відповідно до програми, в якій вказуються умови та порядок функціонування АС у захищеному виконанні, тривалість дослідної експлуатації, порядок усунення виявлених недоліків.

Під час приймально-здавальних випробувань:

- відпрацьовують технології обробки інформації, обіг машинних носіїв інформації, управління засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю дій користувачів;

- співробітники служби захисту інформації та користувачі ІТС набувають практичних звичок щодо 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 потребою) доопрацювання програмного забезпечення, додаткове налагодження та конфігурування комплексу засобів захисту інформації від несанкціонованого доступу;

- здійснюється (за потребою) коригування робочої та експлуатаційної документації.

Як узгодження встановленої системи з робочим персоналом проводяться заходи щодо їх навчання. Такі заходи

дозволять, як правило, усунути некоректне використання встановлених компонентів системи (обладнання, програмне забезпечення тощо), виникнення помилок та інших загроз, що виникають з боку персоналу.

Останній етап передбачає ведення постійного контролю за станом КСЗІ, її роботи відповідно до розробленого регламенту та вимоги на її експлуатацію. Крім того, для підтримки якості роботи системи необхідно проводити перевірку ефективності засобів та методів захисту.

2.Обгрунтування створення комплексного захисту інформації в автоматизованих системах.

Для кожного типу загроз, що виникають при функціонуванні системи інформаційної безпеки, може бути один або кілька заходів протидії. Прийнята міра протидії з економічної точки зору буде прийнятною, якщо ефективність захисту з її допомогою, виражена через зниження ймовірних економічних збитків, перевищує витрати на її реалізацію. У цій ситуації можна визначити максимально допустимі рівні ризику у забезпеченні збереження інформації та вибрати на цій основі одну або кілька економічно обґрунтованих заходів протидії, що дозволяють знизити загальний ризик до такого ступеня, щоб його величина була нижчою за максимально допустимий рівень. З цього випливає, що потенційний порушник, який прагне раціонально використовувати надані йому можливості, не витрачатиме на виконання загрози більше, ніж він очікує виграти.

Стверджується, що більшість розробників засобів обчислювальної техніки розглядає будь-який механізм апаратного захисту як деякі додаткові витрати з бажанням за рахунок їх знизити загальні витрати. При вирішенні лише на рівні керівника проекту питання про створення апаратних засобів захисту необхідно враховувати співвідношення витрат за реалізацію процедури і рівня забезпечення безпеки інформації. Якщо визначати накладні витрати, пов'язані із захистом, як відношення кількості використання деякого ресурсу механізмом управління доступом до загальної кількості використання цього ресурсу, то застосування економічних важелів управління доступом дасть накладні витрати, що наближаються до нуля.

2.1 Оцінка необхідності захисту інформації від НСД

Оцінюючи необхідність захисту підприємства від несанкціонованого доступу до інформації можна вважати, що повні витрати (втрати) визначатись виразом, який потрібно мінімізувати

$$R_{затр} = r_{пот} P_{пи} P_{нпи} + r_{мер} R_{опи} R_{оопи} \rightarrow \min$$

Де повні втрати

$$r_{пот} = R_{нез.сд} + R_{сорв.сд},$$

Rнез.сд(неук.сг) - прибуток від неукладених угод

Rсорв.сд(пр.зу) - прибуток від зірваних угод

вартість витрат на інформаційний захист

r мер = R апп + R екв + R реж

Рапп. - Витрати на апаратуру;

Rекв. - Експлуатаційні витрати;

Rреж. - Витрати на організацію режиму на підприємстві;

РПІ - ймовірність втрат інформації;

РНП - умовна ймовірність невиявлення втрат інформації;

Ропі = (1-Рнпі) - ймовірність відсутності втрат інформації, (оскільки вони становлять повну групу подій);

Роопі - умовна ймовірність помилки у виявленні втрат інформації.

При цьому треба враховувати, що Рнпі > 1 за відсутності апаратних засобів контролю, а Roon > 0 за повного охоплення контролем.

Враховуючи необхідність мінімізації вираження повних втрат, доцільність використання захисту буде за умови дотримання умови

RпотРпіРнп > rмерРопіРопі

Фактично це можна визначити за формулою

RnomРпіРнп = krмер(1-Рпі)Ропі

При цьому k=(2-5) і він вибирається більше при більшому вкладенні цього підприємства (страхувальний підхід).

Можливість не виявлення втрат інформації

$$P_{нпш} = 1 - \sum_{i=1}^{N} P_i$$

Враховуючи певний досвід кількох підприємств, можна рахувати, що:

Р1 =0,1 - при установці апаратури захисту від підслуховування у приміщенні;

Р2 = 0,1-0,2 - при установці апаратури захисту від підслуховування по телефону;

Р3 =0,1-0,2- під час проведення заходів із захисту комп'ютерних мереж;

Р4 =0,1 - при введенні для підприємства особливого режиму;

Р5 =0,1 -при захисті від запису диктофон.

Незважаючи на інший (з точки зору знака та природи) характер залежності ймовірність помилки у виявленні втрат інформації можна наближено визначити як

$$P_{опш} = 1 - \sum_{i=1}^{N} P_i$$

Таким чином, застосування такого підходу в оцінці необхідності захисту інформації, безумовно, є правомірним на попередньому етапі рішення, оскільки не вимагає великої кількості статистичних даних.

2.2 Вимоги захисту інформації від НСД в АС

Вимоги захисту інформації від НСД можуть накладатися різні.

По-перше, на це впливає клас АС, який має на увазі обробку інформації різних категорій. Розглянута раніше класифікація АС, докладно визначає цю характеристику.

По-друге, важливість об'єкта та вартість (важливість) інформації. Якщо об'єкт є інформаційно важливим (не кажучи

вже про державний об'єкт, оскільки на цей випадок необхідно керуватися виключно нормативними документами), то в такому випадку слід оцінювати інформаційні ресурси, інформаційну систему в цілому на визначення її важливості (провести аудит інформаційної безпеки) . Після цього, як окремим етапом, формуються вимоги захисту даного об'єкта.

Технологія обробки інформації є захищеною, якщо вона містить програмно-технічні засоби захисту та організаційні заходи, що забезпечують виконання загальних вимог щодо захисту інформації.

Загальні вимоги передбачають:

категорії за цільовим призначенням, ступенем обмеження доступу окремої категорії користувачів та іншими класифікаційними ознаками;

- здійснення за допомогою СЗІ обліку вихідних даних, отриманих під час вирішення функціонального завдання, у формі надрукованих документів, що містять конфіденційну інформацію.

- наявність певного (створеного) відповідального підрозділу, якому надаються повноваження щодо організації та впровадження технології захисту інформації, контролю за станом захищеності інформації (далі – служба захисту в АС, СЗІ);

- можливість визначення засобами КСЗІ кількох ієрархічних рівнів повноважень користувачів та кількох класифікаційних рівнів інформації;

- створення КСЗІ, яка є сукупністю організаційних та інженерно-технічних заходів, програмно-апаратних засобів,

спрямованих на забезпечення захисту інформації під час функціонування АС;

- розробку плану захисту інформації в АС, зміст якого визначено у додатку до НД ТЗІ 1.4-001;

- заборона несанкціонованої та неконтрольованої модифікації конфіденційної інформації в АС;

- наявність атестату відповідності КСЗІ в АС нормативним документам із захисту інформації;

- обов'язковість реєстрації в АС всіх користувачів та їх дій щодо конфіденційної інформації;

- можливість надання користувачам лише за умови службової необхідності санкціонованого та контрольованого доступу до конфіденційної інформації, що обробляється в АС;

- наявність переліку конфіденційної інформації, що підлягає автоматизованій обробці; у разі потреби можлива її класифікація у межах

- заборона несанкціонованого копіювання, розмноження, розповсюдження конфіденційної інформації в електронному вигляді;

- забезпечення КСЗІ можливості своєчасного доступу зареєстрованих користувачів АС до конфіденційної інформації.

- забезпечення за допомогою СЗІ контролю за санкціонованим копіюванням, розмноженням, розповсюдженням конфіденційної інформації в електронному вигляді;

- можливість здійснення однозначної ідентифікації та аутентифікації кожного зареєстрованого користувача;

Наведені вимоги є базовими і застосовуються для захисту інформації від НСД у всіх типах АС.

Умовно розділивши АС на найважливіші підсистеми забезпечення захисту інформації (рис 1.2), можна перерахувати також вимоги, що пред'являються для захисту комп'ютерної інформації від НСД в АС для кожної окремої підсистеми.

Рисунок 1.2 – Підсистеми управління та забезпечення захисту інформації в АС

2.2.1 Вимоги щодо захисту конфіденційної інформації

Підсистема керування доступом повинна відповідати таким вимогам:

- здійснювати контроль доступу суб'єктів до ресурсів, що захищаються відповідно до матриці доступу;

Підсистема реєстрації та обліку повинна:

- реєструвати вхід (вихід) суб'єктів доступу до системи (із системи), або реєструвати завантаження та ініціалізацію операційної системи та її програмного зупинення. При цьому параметри реєстрації вказуються:

1) дата та час входу (виходу) суб'єкта доступу в систему (із системи) або завантаження (зупинки) системи;

2) результат спроби входу - успішна або неуспішна (при НДД);

3) ідентифікатор (код або прізвище) суб'єкта, пред'явлений під час спроби доступу;

4) код або пароль, пред'явлений у разі неуспішної спроби;

- ідентифікувати та перевіряти справжність суб'єктів доступу при вході до системи. При цьому це повинно здійснюватися за ідентифікатором (кодом) та паролем умовно-постійної дії довжиною не менше шести буквено-цифрових символів;

- ідентифікувати термінали, ЕОМ, вузли комп'ютерної мережі, канали зв'язку, зовнішні пристрої ЕОМ за їх логічними адресами (номерами);

- за іменами ідентифікувати програми, томи, каталоги, файли, записи та поля записів;

- реєстрація виходу із системи або зупинки не проводиться в моменти апаратурного відключення АС;

- реєструвати видачу друкованих (графічних) документів на «тверду» копію. При цьому параметри реєстрації вказуються:

1) дата та час видачі (звернення до підсистеми виведення);

2) короткий зміст документа (найменування, вид, код, шифр) та рівень його конфіденційності;

3) специфікація пристрою видачі (логічне ім'я (номер) зовнішнього устрою);

4) ідентифікатор суб'єкта доступу, який запросив документ;

- реєструвати спроби доступу програмних засобів (програм, процесів, завдань, завдань) до файлів, що захищаються. У параметрах реєстрації вказується:

1) дата і час спроби доступу до файлу, що захищається, із зазначенням її результату (успішна, неуспішна — несанкціонована);

2) ідентифікатор суб'єкта доступу;

3) специфікація файлу, що захищається.

- реєструвати запуск (завершення) програм і процесів (завдань, завдань), призначених для обробки файлів, що захищаються. При цьому у параметрах реєстрації вказується:

1) дата та час запуску;

2) ім'я (ідентифікатор) програми (процесу, завдання);

3) ідентифікатор суб'єкта доступу, який запросив програму (процес, завдання);

4) результат запуску (успішний, неуспішний - несанкціонований);

- реєструвати спроби доступу програмних засобів до додаткових об'єктів доступу (терміналів ЕОМ, вузлів мережі ЕОМ, ліній (каналів) зв'язку, зовнішніх пристроїв ЕОМ, програм, томів, каталогів, файлів, записів, полів записів). При цьому у параметрах реєстрації вказується:

1) дата і час спроби доступу до файлу, що захищається, із зазначенням її результату: успішна, неуспішна, несанкціонована;

2) ідентифікатор суб'єкта доступу;

3) специфікація об'єкта, що захищається [логічне ім'я (номер)];

Підсистема забезпечення цілісності має:

- цілісність програмного середовища забезпечується використанням трансляторів з мови високого рівня та відсутністю засобів модифікації об'єктного коду програм у процесі обробки та (або) зберігання інформації, що захищається;

- забезпечувати цілісність програмних засобів системи захисту інформації від НСД (СЗІ НСД), оброблюваної інформації, а також незмінність програмного середовища. При цьому:

- проводити періодичне тестування функцій СЗІ НСД при зміні програмного середовища та персоналу АС за допомогою тест-програм, що імітують спроби НСД;

- цілісність СЗІ НСД перевіряється під час завантаження системи за контрольними сумами компонент СЗІ;

- здійснювати фізичну охорону СВТ (пристроїв та носіїв інформації). При цьому мають передбачатися контроль доступу до приміщення АС сторонніх осіб, а також наявність надійних перешкод для несанкціонованого проникнення до

приміщення АС та сховища носіїв інформації. Особливо у неробочий час;

- мати у наявності засоби відновлення СЗІ НСД. При цьому передбачається ведення двох копій програмних засобів СЗІ НСД, а також їх періодичне оновлення та контроль працездатності;

2.2.2 Вимоги до захисту секретної інформації

У випадку вимоги до захисту секретної інформації схожі з вимогами до захисту конфіденційної інформації, проте існують принципові відмінності. Оскільки секретна інформація має вищий ранг, то вимоги до неї значно вище. Тому, через схожість у вимогах цих двох категорій інформації, зазначимо, лише ті пункти, які стосуються безпосередньо захисту секретної інформації.

Підсистема керування доступом має:

- керувати потоками інформації за допомогою міток конфіденційності. При цьому рівень конфіденційності накопичувача повинен бути не нижче рівня конфіденційності інформації, що записується на нього;

Підсистема реєстрації та обліку повинна:

- реєструвати спроби доступу програмних засобів (програм, процесів, завдань, завдань) до файлів, що захищаються. У параметрах реєстрації вказується:

1) ім'я програми (процесу, завдання, завдання), що здійснюють доступ до файлів;

2) вид запитуваної операції (читання, запис, видалення, виконання, розширення тощо);

- реєструвати спроби доступу програмних засобів до наступних додаткових об'єктів доступу, що захищаються: терміналів, ЕОМ, вузлів мережі ЕОМ, ліній (каналів) зв'язку, зовнішніх пристроїв ЕОМ, програм, томів, каталогів, файлів, записів, полів записів. У параметрах реєстрації вказується:

1) ім'я програми (процесу, завдання, завдання), що здійснюють доступ до файлів;

2) вид запитуваної операції (читання, запис, монтування, захоплення тощо);

- реєструвати видачу друкованих (графічних) документів на «тверду» копію. Ця дія має вказувати фактичний обсяг виданого документа (кількість сторінок, аркушів, копій) та результат видачі (успішний – весь обсяг, неуспішний);

- реєструвати зміни повноважень суб'єктів доступу та статусу об'єктів доступу. У параметрах реєстрації вказується:

1) дата та час зміни повноважень;

2) ідентифікатор суб'єкта доступу (адміністратора), який здійснив зміни;

- здійснювати автоматичний облік створюваних файлів за допомогою їх додаткового маркування, що використовується в підсистемі управління доступом. Маркування має відображати рівень конфіденційності об'єкта;

- проводити облік носіїв, що захищаються, з реєстрацією їх видачі (прийому) у спеціальному журналі (картотеці);

- проводити кілька видів обліку (дублюючих) носіїв інформації, що захищаються;

- сигналізувати про спроби порушення захисту;

Підсистема забезпечення цілісності має:

- здійснювати фізичну охорону СВТ (пристроїв та носіїв інформації). При цьому має передбачатись постійна наявність охорони на території будівлі та приміщень, де знаходиться АС. Охорона повинна проводитись за допомогою технічних засобів охорони та спеціального персоналу, а також з використанням суворого пропускного режиму та спеціального обладнання у приміщенні АС;

- передбачати наявність адміністратора або цілої служби захисту інформації, відповідальних за ведення, нормальне функціонування та контроль роботи СЗІ НСД. Адміністратор повинен мати свій термінал та необхідні засоби оперативного контролю та впливу на безпеку АС;

- використовувати лише сертифіковані засоби захисту. Їхню сертифікацію проводять спеціальні сертифікаційні центри або спеціалізовані підприємства, які мають ліцензію на проведення сертифікації засобів захисту СЗІ НСД;

- проводити періодичне тестування функцій СЗІ НСД при зміні програмного середовища та персоналу АС за допомогою спеціальних програмних засобів не рідше одного разу на рік;

Порівняємо дві розглянуті вище групи вимог та їх особливості для захисту інформації різних категорій (конфіденційної та секретної). Зрозуміло, що ключовими механізмами захисту, що утворюють основну групу механізмів захисту від НДД («Підсистема керування доступом»), є:

- контроль доступу суб'єктів до ресурсів, що захищаються, відповідно до матриці доступу.

- ідентифікація та перевірка справжності суб'єктів доступу при вході в систему за ідентифікатором (кодом) та паролем умовно-постійної дії;

Додатковою вимогою та принциповою відмінністю при захисті секретної інформації є те, що механізмом захисту має здійснюватись управління потоками інформації за допомогою міток конфіденційності. При цьому рівень конфіденційності накопичувача повинен бути не нижче рівня конфіденційності інформації, що записується на нього.

Усі три перераховані механізми є основними. Пов'язані вони так: всі права доступу до ресурсів (розмежувальна політика доступу до ресурсів) задаються для конкретного суб'єкта доступу (користувача). Тому суб'єкт доступу (користувач) має бути ідентифікований при вході до системи, відповідно, має бути проконтрольовано його автентичність. Зазвичай це робиться за допомогою секретного слова — пароля.

2.3 Основні принципи захисних заходів від НСД до АС

Провівши оцінку необхідності захисту від НСД, стає питання подальшому напрямі проектування системи захисту. Адже саме за отриманими результатами можна судити про складність системи, що проектується. Маючи такі результати, необхідно оцінити ймовірність загроз на інформаційну систему, а також сформувати модель порушника, після чого слід приступити до формування захисних заходів. Спираючись на вимоги захисту інформації від НСД, які були розглянуті

раніше, можна навести основні принципи захисних заходів від НСД в АС.

Уточнимо, що одним з основних компонентів АС є автоматизоване робоче місце (АРМ) – програмно-технічний комплекс АС (або засоби обчислювальної техніки (СВТ)), призначений для автоматизації діяльності певного виду. У найпростішому випадку АРМ представляється як ПЕОМ та працюючий на ній користувач.

Однак такі захисні заходи необхідно розпочинати безпосередньо з організаційних заходів. Останні, в рамках системи захисту інформації від НСД (СЗІ НСД) в АС, які обробляють або зберігають інформацію, що є власністю держави та віднесену до категорії секретної, повинні відповідати державним вимогам щодо забезпечення режиму секретності робіт, що проводяться.

Захист інформації від НСД є складовою загальної проблеми забезпечення безпеки інформації. Заходи щодо захисту інформації від НСД повинні здійснюватися взаємопов'язано з заходами щодо спеціального захисту основних та допоміжних засобів обчислювальної техніки, засобів та систем зв'язку від технічних засобів розвідки промислового шпигунства .

Тут же наводяться основні принципи захисту інформації від НСД, які включають:

- забезпечення захисту СВТ комплексом програмно-технічних засобів;

- забезпечення захисту АС комплексом програмно-технічних засобів та організаційних заходів, що їх підтримують.

У свою чергу, пропонується закриття каналів несанкціонованого отримання інформації починати з контролю доступу користувачів до ресурсів АС. Ця проблема вирішується шляхом низки наступних принципів:

- ПРИНЦИП ОБГРУННОСТІ ДОСТУПУ. Цей принцип полягає в обов'язковому виконанні двох основних умов: користувач повинен мати достатню "форму допуску" для отримання інформації необхідного рівня конфіденційності, і ця інформація необхідна йому для виконання його виробничих функцій. Зауважимо тут, що у сфері автоматизованої обробки інформації як користувачів можуть виступати активні програми та процеси, а також носії інформації різного ступеня складності. Тоді система доступу передбачає визначення для всіх користувачів відповідного програмно-апаратного середовища або інформаційних та програмних ресурсів, які будуть доступні для конкретних операцій.

- ПРИНЦИП ДОСИЛЬНОЇ ГЛУБИНИ КОНТРОЛЮ ДОСТУПУ. Засоби захисту мають включати механізми контролю доступу до всіх видів інформаційних та програмних ресурсів АС, які відповідно до принципу обґрунтованості доступу слід розділяти між користувачами.

- ПРИНЦИП РОЗМЕЖЕННЯ ПОТОКІВ ІНФОРМАЦІЇ. Для попередження порушення безпеки інформації, яке, наприклад, може мати місце при записі секретної інформації на несекретні носії та несекретні файли, її передачі програмам і процесам, не призначеним для обробки

секретної інформації, а також при передачі секретної інформації незахищеними каналами та лініями зв'язку , необхідно здійснювати відповідне розмежування потоків інформації

- ***ПРИНЦИП ЧИСТОТИ ПОВТОРНО ВИКОРИСТОВУВАНИХ РЕСУРСІВ***. Цей принцип полягає в очищенні ресурсів, що містять конфіденційну інформацію, при їх видаленні або звільненні користувачем до перерозподілу цих ресурсів іншим користувачам.

- ***ПРИНЦИП ПЕРСОНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ***. Кожен користувач повинен нести персональну відповідальність за свою діяльність у системі, включаючи будь-які операції з конфіденційною інформацією та можливі порушення її захисту, а також за випадкові чи навмисні дії, які можуть призвести до несанкціонованого ознайомлення з конфіденційною інформацією, її спотворення чи знищення, або виключення можливості доступу до такої інформації законних користувачів.

- ***ПРИНЦИП ЦІЛІСНОСТІ ЗАСОБІВ ЗАХИСТУ***. Цей принцип має на увазі, що засоби захисту інформації в АС повинні точно виконувати свої функції відповідно до перерахованих принципів і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації та впливу на процеси в системі.

Практичне створення монітора звернень, як видно з наведеного малюнка, передбачає розробку конкретних правил розмежування доступу як так званої моделі захисту.

Спроектувавши модель захисту інформації, необхідно перевірити її у дії. Проте реалізація такої моделі буде варто замовнику великих витрат, якщо при її реалізації одна або кілька захисних функцій системи не виявиться ефективною. Тому доцільно провести математичний аналіз ефективності захисних заходів.

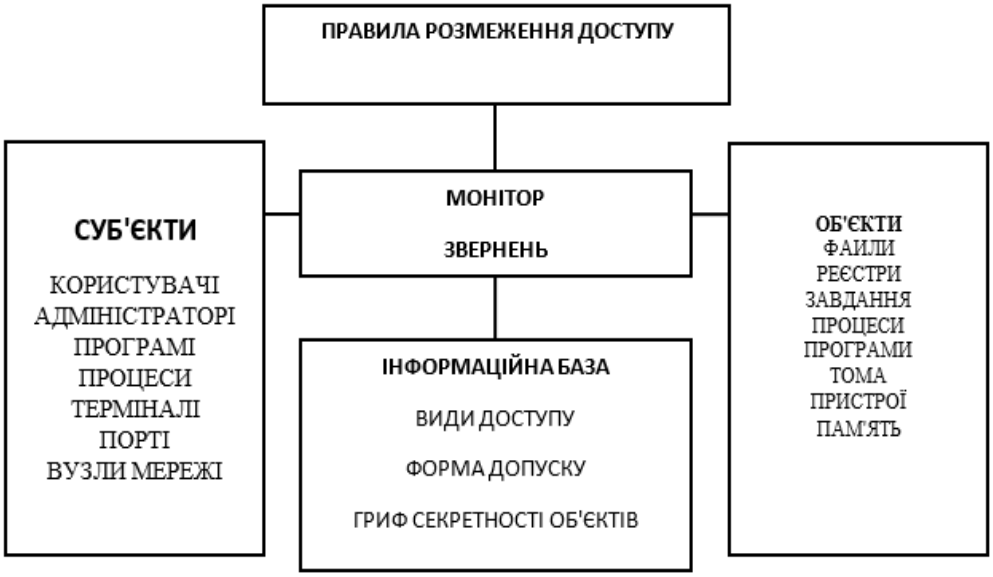

Рис. 2.2 – Структура монітора звернень

2.4 Математичний аналіз ефективності захисних заходів

Будь-яка система безпеки є організаційно оформлені кадрові та матеріально-технічні ресурси і діє завжди в часі та просторі загроз. Простір загроз утворюють об'єкти захисту - люди, що працюють у комерційній структурі, майно та кошти підприємства, відомості, що становлять комерційну чи службову таємницю. Головна функція системи безпеки – протидія загрозам за допомогою людей та техніки. Кожна

загроза спричиняє шкоду, а протидія покликана знизити його величину, в ідеалі - повністю. Вдається це далеко не завжди. Здатність системи безпеки виконувати свою головну функцію завжди має оцінюватися кількісно. Наприклад, можна виміряти відносну шкоду, запобігану нею (рис.2.3).

Рисунок 2.3 – Типова залежність ефективності Q0 та рентабельності r0 захисту від загальних ресурсів

Величина Q0 – міра загальної ефективності захисту. Чим більше Q0, тим менші збитки створять загрози. Таким чином, мірою ризику є величина (1-Q0). Прагнення забезпечити високоефективний захист, коли Q0 близько до 1 (або 100%), цілком природно, але це вимагатиме значних витрат на ресурси. Тобто чим вище сукупні асигнування (B0) на ресурси, тим більшу ефективність захисту можна розраховувати. Виникла у своїй залежність видно на рис.2.3. Проте надмірні витрати на власну безпеку не завжди виправдані економічно.

Можна стикнутися із ситуацією, коли вартість захисту (B0) перевищить рівень (R0) максимальної шкоди від реалізації загроз. У цьому випадку виникає небезпека загрози саморозорення від захисту. Її рівень можна оцінити, наприклад, величиною r різниці відносного «захищеного» шкоди Q0 і відносних витрат B0/P0 на ресурси. Назвемо цю величину рентабельністю захисту. Якщо вона позитивна (тобто B0<=P0Q0), то захист є рентабельним. На відміну від ефективності, що більше витрати (B0), то менше рентабельність. Ця протилежність створює неоднозначну ситуацію у виборі стратегії захисту.

Очевидними є і джерела економії витрат: використання більш економічних засобів і рішень універсального характеру; раціональний розподіл ресурсів та більш досконалі форми управління ними; Весь цей перелік притаманний великим комерційним структурам, проте для середнього та малого бізнесу він, на жаль, суттєво звужується. Ідеологія їхньої системи безпеки має будуватися на рентабельному захисті лише від окремих видів загроз. Інакше захист може себе не виправдати. Тому треба мати на увазі, що економії ресурсів у цих умовах сприятимуть кооперативним формам захисту в рамках єдиної місцевої або регіональної системи безпеки.

Рисунок 2.4 – Залежність ефективності та рентабельності захисту від максимальної шкоди R0

На ньому представлені характерні залежності величини ризику (R=R0(1-Q0) та загальних витрат (B0) на ресурси від ефективності автономного (I) та кооперативного (II) захисту. Точка перетину (A0) залежностей R(Q) та B(Q) для автономного захисту відповідає приблизно області мінімальних загальних втрат

R0(1-Q0)+B0. Економія ресурсів виявиться в тому, що вихідна залежність (I) виявиться «вищою» за нову залежність (II), яка відображає кооперацію у використанні ресурсів. Відповідно нова точка перетину кривих (A1) виявиться правіше колишньої (A0). Фактично це означає, що при збереженні рентабельності захисту збільшується її ефективність. Причому виграш тим суттєвіший, чим більша

економія. Насправді переважно кооперуються за двома формам - матеріально-технічним і кадровим ресурсам, які є складовими частинами загального. Що ж до першої форми, вона характерна для ситуацій, коли простір загроз не розширюється. Іншими словами, об'єднуються лише матеріально-технічні засоби одного й того самого підприємства, але призначені для різних цілей.

Рисунок 2.5 – Характерні залежності ризику R та витрат на ресурси B0 як функції від ефективності захисту Q0

Як приклад можна назвати комплексну систему майнового та інформаційного захисту. До загальних засобів можна віднести контрольно-пропускну систему, засоби обмеження доступу, телевізійні та інші системи виявлення та верифікації загроз, засоби пожежогасіння та ін. Ця форма ефективна лише для бізнесу. Другу форму, тобто кооперацію з кадрових ресурсів, використовують переважно під час вирішення проблеми безпеки на регіональному рівні, коли простір загроз навмисно розширюється (розглядаються кілька

комерційних підприємств в одному регіоні). І тут об'єднання відбувається лише рівні сил так званого швидкого реагування. Саме такі сили протидіють несанкціонованим та силовим проникненням, тероризму, пожежі тощо. Проблему, як правило, вирішують і із залученням сил швидкого реагування пожежного нагляду, органів МВС та ін.

Рисунок 2.6 – Залежність ефективності захисту Q0 від відносного часу Тр/Ту реакції системи з одночасним (I), випереджальним (II) та запізнюючим (III) протидією

На рис.2.6 представлена характерна залежність ефективності захисту від відносного часу реакції системи (Тр/Ту) всім трьох варіантів протидії.

Будь-яка загроза та протидія їй відбуваються, природно, у часі та характеризуються певними його масштабами. Виходячи з цього, збиток від реалізації загроз визначатиметься тим, наскільки повно дані події перетинаються в часі. Найнебажаніший варіант - запізнююча протидія, коли реакція системи захисту починається до моменту завершення загрози або після неї. Він уражає систем інформаційного захисту. Дещо найкращий варіант - одночасна протидія, тобто воно починається з появою загрози. І, нарешті, найкращий - протидія, що має випереджальний характер: реакція системи

захисту починається на початок реалізації небезпеки. Підставою реакції можуть бути оперативні дані, сигнали тривоги раннього оповіщення тощо.

Основні висновки та рекомендації очевидні. Одночасна протидія буде достатньою для високоефективного захисту від загрози, якщо реакція на неї буде швидкою. Це завдання цілком реальне для об'єктів великого бізнесу. А кооперативні форми протидії в умовах повільної реакції на загрози не принесуть ефекту, якщо відсутні засоби затримки та блокування загроз. Говорячи про тактичні питання системи безпеки бізнесу в частині технічних каналів зв'язку, насамперед мають на увазі швидкість її реакції, надійність рішень, блокування розвитку загроз та їхню ліквідацію. Особливо важливо забезпечити жорсткі вимоги до надійності всіх систем захисту, що залежить від часу їх функціонування та періодичності поновлення ресурсів. Якщо цей час перевищує 5 років, то вимога надійності реалізується декількома способами, серед яких – резервування рішень, багаторубежність захисту, автоматизація первинних рішень, централізоване управління ресурсами у кризових ситуаціях тощо. Перш ніж визначитися з питаннями тактики, слід пам'ятати, що вона має відповідати стратегії та спиратися на точний кількісний аналіз. Для об'єктів середнього та малого бізнесу такий аналіз є цілком реальним навіть без засобів автоматизації. Однак необхідно залучити фахівців та експертів, які б проаналізували обстановку та властивості об'єкта, що захищається, розробили модель загроз, вивчили ринок існуючих засобів та методів. Ці дані й допомогли б оцінити саму систему та за необхідності модернізувати її.

3. Розробка оцінки ефективності в Автоматизованих Системах

У випадку ефективність ЗМ оцінюється як у етапі розробки, і у процесі експлуатації системи захисту. В оцінці ефективності ЗМ, залежно від використовуваних показників та способів їх отримання, можна виділити три підходи :

- класичний;

- офіційний;

- експериментальний.

Оцінка ефективності є важливим елементом розробки проектних і планових рішень, що дозволяє визначити рівень прогресивності діючої структури, проектів або планових заходів, що розробляються, і проводиться з метою вибору найбільш раціонального варіанту структури або способу її вдосконалення. Ефективність захисних заходів (ЗМ) повинна оцінюватися на стадії проектування для отримання найкращих показників працездатності системи в цілому.

Під класичним підходом оцінки ефективності розуміється використання критеріїв ефективності, отриманих з допомогою показників ефективності. Значення показників ефективності утворюються шляхом моделювання або обчислюються за характеристиками реальної АС. Такий підхід використовується для розробки та модернізації КСЗІ. Проте можливості класичних методів комплексного оцінювання ефективності стосовно ЗМ обмежені з низки причин. Високий

рівень невизначеності вихідних даних, складність формалізації процесів функціонування, відсутність загальновизнаних методик розрахунку показників ефективності та вибору критеріїв оптимальності створюють значні труднощі для застосування класичних методів оцінки ефективності.

Велике практичне значення має підхід до визначення ефективності ЗМ, який умовно можна назвати офіційним. Політика безпеки інформаційних технологій проводиться державою та має спиратися на нормативні акти. У цих документах необхідно визначити вимоги щодо захищеності інформації різних категорій конфіденційності та важливості.

Під експериментальним підходом розуміється організація процесу визначення ефективності існуючих КСЗІ шляхом спроб подолання захисних механізмів системи фахівцями, які у ролі зловмисників. Такі дослідження проводяться в такий спосіб. Як умовний зловмисник вибирається один або кілька фахівців у галузі інформаційної боротьби найвищої кваліфікації. Складається план проведення експерименту. У ньому визначаються черговість та матеріально-технічне забезпечення проведення експериментів щодо визначення слабких ланок у системі захисту. При цьому можуть моделюватися дії зловмисників, що відповідають різним моделям поведінки порушників: від некваліфікованого зловмисника, який не має офіційного статусу досліджуваної АС, до висококваліфікованого співробітника служби безпеки.

Один із них зводиться порівняно з показниками, що характеризують ефективність організаційної структури еталонного варіанта системи захисту. Еталонний варіант може бути розроблений та спроектований з використанням усіх

наявних методів та засобів проектування систем захисту, на основі передового досвіду та застосування прогресивних організаційних рішень. Характеристики такого варіанту приймаються як нормативні, при цьому порівняльна ефективність аналізованої або проектованої системи визначається на основі зіставлення нормативних та фактичних (проектних) параметрів системи з використанням переважно кількісних методів порівняння. Може застосовуватися також порівняння з показниками ефективності та характеристиками системи управління, обраної як зразок, що визначає допустимий або достатній рівень ефективності організаційної структури.

Однак виникають деякі труднощі застосування зазначених підходів, які обумовлені необхідністю забезпечення сумісності порівнюваних варіантів. Тому часто замість них використовується експертна оцінка організаційно-технічного рівня аналізованої та проектованої системи, а також окремих її підсистем та прийнятих проектних та планових рішень, або комплексна оцінка системи захисту, заснована на використанні кількісно-якісного підходу, що дозволяє оцінювати ефективність ЗМ за значною сукупністю факторів . Експертна оцінка може бути складовим елементом комплексної оцінки ефективності системи захисту, що включає всі перелічені підходи як до окремих підсистем, так і до системи загалом.

Ефективність систем оцінюється з допомогою показників ефективності. Іноді використовується термін – показник якості. Показниками якості, зазвичай, характеризують ступінь досконалості будь-якого товару, устрою, машини. Щодо складних людино-машинних систем краще використання

терміна показник ефективності функціонування, який характеризує ступінь відповідності системи, що оцінюється, своєму призначенню.

Визначення показника ефективності можливе двома загальнонауковими методами: експериментом (випробуванням) та математичним моделюванням (нині часто називають обчислювальним експериментом).

Стосовно захисту інформації показники за значимістю ("знизу вгору") поділяються так: технічні - інформаційні (датчикові) - системні - надсистемні (ціннісні). Фізично, стосовно захисту інформації від витоку, цей ряд виглядає так: сигнал / шум - можливість виявлення об'єкта - джерела інформації - можливість його розтину - збиток від витоку інформації. У цьому всі приватні показники між собою функціонально пов'язуються.

Для того щоб оцінити ефективність системи захисту інформації або порівняти системи ефективності, необхідно задати деяке правило переваги. Таке правило чи співвідношення, заснований на використанні показників ефективності, називають критерієм ефективності. Для отримання критерію ефективності при використанні деякої множини k-показників використовують низку підходів. Зазвичай, при синтезі системи виникає проблема вирішення задачі з багатокритеріальним показником.

4. ВИБІР ШЛЯХ ЗАХИСНИХ ЗАХОДІВ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

4.1 Вибір контрольованих параметрів за максимальними значеннями (з урахуванням захисту каналу)

Вибір параметрів контролю за інформативним ознаками досить складний і потребує великих фактичних даних.

Для інженерних розрахунків прийнятними є методи лінійного та динамічного програмування.

Розглянемо застосування лінійного програмування для визначення номенклатури контрольованих параметрів з метою отримання максимальної інформації про технічний стан (захисту) каналу при заданому коефіцієнті готовності та виконанні низки обмежень (наприклад, вартість контролю, маса, габарити тощо).

Вирішення цього завдання можливе за певних припущень. Поставимо завдання у термінології лінійного програмування.

Знайти підмножина контрольованих параметрів ω множини Ω, що максимізує при дотриманні обмежень лінійну функцію B або

$$B_{\omega} = \max_{\omega \in \Omega} \{B / g_s \le G_s; s = 1,2...\}$$

де Gs - обмеження щодо вибору складу контрольованих параметрів;

gs - Досягнуте значення по s-му обмеженню.

У роботі автором розглядалося застосування як максимізованої функції критерію об'єктивності контролю у вигляді

$$B_\omega = \sum_{i \in \omega} b_i$$

Де

$$b_i = \frac{I_i}{\sum_{i \in \omega} I_i}$$

$$I_i = -\frac{\lambda_i}{\Lambda} \log_2 \frac{\Lambda}{\lambda_i} - \left(1 - \frac{\lambda_i}{\Lambda}\right) \log_2 \frac{1}{\left(1 - \frac{\lambda_i}{\Lambda}\right)}$$

Тут λ_i - інтенсивність проникнень в перший параметр;

Λ - інтенсивність проникнень у канал $\Lambda = \sum_{i \in \omega} \lambda_I$

Не змінюючи, фактично, суті міркувань, можна прийняти, $b_i = \lambda_i / \Lambda$ що істотно спрощує обчислення.

Приймаються такі припущення, придатні широкого класу каналів:

- надійність параметрів не змінюється під час введення КУ;

- параметри взаємонезалежні; для всіх параметрів виконується

$$\lambda_i << \Lambda$$

У середньому час пошуку несправного елемента τ від і (без КУ) більше, ніж час усунення несправності або

проникнення цього елемента; - час відновлення і-го елемента; для всіх елементів виконується умова

$$\tau_{\text{от ку i}} << \tau_{\text{ус i}}$$

4.2 Вибір контрольованих параметрів за заданим коефіцієнтом готовності

Як обов'язкове обмеження можна вимагати отримання будь-якої характеристики надійності заданого значення, наприклад, коефіцієнта готовності у вигляді

$$\sum_{i\in\omega} Z_i\gamma_i + \sum_{j\in\omega} Z_j\gamma_j \le \frac{1-\mathrm{K}_{\text{гз}}}{\mathrm{K}_{\text{гз}}}$$

$$\overline{\omega}\cup\omega=\Omega,\quad \overline{\omega}\cap\omega=\varnothing$$

Де $Z_i \neq Z_j$

$$Z_i, Z_j = \begin{cases} 0 \\ 1 \end{cases}$$

$$\gamma_i = \lambda_i\left(\tau_{\text{от ку i}} + \tau_{\text{ус i}}\right)$$
$$\gamma_j = \lambda_j\left(\tau_{\text{от ку j}} + \tau_{\text{ус j}}\right)$$
$$\lambda_i \approx \lambda_j;\ \tau_{\text{ус i}} \approx \tau_{\text{ус j}}$$

Як в якості λ_i можна використовувати можливість відмови, в припущенні $q_i \equiv \lambda_i$.

Формалізуємо умову завдання.

Визначити набір $Z = (z_1,\ z_2,\ \ldots,\ z_n)$ максимізуючий функцію

$$\sum_{i\in\omega} Z_i b_i + \sum_{j\in\omega} Z_j b_j,\ \omega \cap \bar{\omega} = \varnothing,\ \omega \cup \bar{\omega} = \Omega$$

За умов

$$\sum_{i\in\omega} Z_i \gamma_i + \sum_{j\in\omega} Z_j \gamma_j \le \frac{1 - \mathrm{K}_{\text{гз}}}{\mathrm{K}_{\text{гз}}}$$

$$\sum_{i\in\omega} Z_i g_{S_i} + \sum_{j\in\omega} Z_j g_{S_j} \le G_s$$

$$Z_i, Z_j = \begin{cases} 0 \\ 1 \end{cases};\ Z_i \ne Z_j$$

4.3 Вибір контрольованих параметрів за максимальним значенням ймовірності безвідмовної роботи після проведення діагностики

Методика вибору контрольованих параметрів, наведена в 4.2, може ефективно застосовуватися тільки за незалежності параметрів (кожен параметр залежить тільки від одного елемента або кожен елемент має тільки один параметр).

Розглянемо завдання вибору випадку, коли параметри взаємозалежні. Причому оптимальним вважається такий набір, при контролі якого досягається максимальна апостеріорна ймовірність безвідмовної роботи та дотримується умова обмеження (вартість контролю, час тощо).

Задачу выбора оптимального набора контролируемых параметров при ограничении можно решить методами

сокращенного перебора. Сокращение перебора достигается использованием специальных правил, позволяющих исключать заведомо неоптимальные наборы. Один из таких алгоритмов приведен в работе , но он на наш взгляд слишком сложен для применения в инженерной практике.

А. Метод вибору раціонального набору за кількістю максимально допустимих у наборі елементів.

Визначається середнє значення витрат на контроль одного параметра

$$g_c = \frac{\sum_{к=1}^{n} q_к}{M}$$

Передбачається, що витрати gк = gc = const та раціональний набір контрольованих параметрів знаходиться серед наборів з максимально допустимим числом параметрів. За максимально допустиме число приймається

$$n = \left]\frac{G_s}{g_s}\right[+ 1$$

Потім розглядаються всі набори по n параметрів, які

$$g_s \underset{w \to n}{\leq} G_s$$

і їх вибирається оптимальний π_n^0 за алгоритмом, викладеним раніше.

Застосування цього наближеного методу є ефективним при близьких значеннях витрат на контроль параметрів.

Б. Метод наближення до раціонального набору за наборами з найбільшим збільшенням ймовірності, що припадає на одиницю витрат (Метод якнайшвидшого спуску).

Передбачається, що з усіх поєднань по два найкращим є поєднання таких параметрів $\pi_{к1}^{0}$ і $\pi_{к2}^{0}$, що значення $V^{(к1\ 0)}$ - найбільше з усіх $V^{(к)}$ і $V^{(к1\ 0\ к2\ 0)}$ - найбільше з усіх $V^{(к1\ к2)}$. З усіх поєднань по три параметри найкращим є поєднання $\pi_{к1}^{0}\ \pi_{к2}^{0}\ \pi_{к3}^{0}$ у якого значення $V^{(к1\ 0\ к2\ 0\ к3\ 0)}$ найбільше. Таким чином, за оптимальний набір приймається набір $\pi_{к1}^{0}\ \ \pi_{к2}^{0}\ldots\pi_{кn}^{0}$. При цьому приєднання до цього набору будь-якого з приладів, що залишилися, не задовольняє умові обмеження на витрати

$$\sum_{i=1}^{n} g_{К_j^0} \le G_s \ \text{и} \ \sum_{i=1}^{n} g_{К_j^0} + g_{К_1} > G_s \quad \left(1 \notin к_j^0\right)$$

У цьому вся методі виходить найменше число переборів. Його застосування найбільше ефективно при різкій відмінності параметрів один від одного.

В. Комбінований метод, у якому застосовані попередні наближені методи та основні ідеї методу гілок та кордонів. За методом А визначається базовий набір $w_Б^0$, що складається з n параметрів при $g(w_Б^0) < G_s$. В наборах

$w_Б^0$ и $\quad w_Б^0\left(w_Б^0 \cap \overline{w}_Б^0 = \varnothing \ \text{и}\ w_Б^0 \cup \overline{w}_Б^0 \subseteq \overline{M}\right)$ відшукуються такі параметри, щоб

$$V^{\left(к \in w_Б^0\right)} > \overline{V}^{\left(1 \in w_Б^0\right)}$$

Комбінований метод, очевидно, найефективніший з розглянутих і дозволяє найбільш швидко підійти до вирішення задачі при

$$g\left(w_{Б}^{1}\right) \le G_{г}$$

$к \in w_{Б}^{1}$;

$1 \in \overline{w}_{Б}^{1}$.

При цьому оптимальним набором w_0 з $\{w_Б^0, w_Б^1, w_Б^2, ..., w_Б^m\}$ вважається той, у якого

$$P(w_0) = \max\left\{P(w_Б^0), P(w_Б^1), P(w_Б^2), \ldots, P(w_Б^m)\right\}.$$

Слід зазначити, що крок кроків розв'язання при використанні алгоритму Р.Р. Убору, реалізованого за допомогою методу гілок та кордонів. (при обліку допустимості та перспективності) дещо більше, ніж при методі В, і логіка алгоритму та елементарні обчислення складніші за наведені вище.

Приведем характеристики числа переборов вариантов без учета допустимости и перспективности планов (табл.4.3.1).

Следует отметить, что с ростом М и n различие в числе переборов для этих методов быстро возрастает. При учете допустимости и перспективности наборов число переборов в трех последних методах резко падает (метод А грубее остальных и может применяться только при сильных ограничениях).

Таблиця 4.3.1

Метод (алгоритм)	Максимальна кількість переборів	n= 5 M =7
Повний перебір	$\le \sum_{i=1}^{M} C_M^i$	127

А	$< C_{\text{M}}^{\text{n}}$	21
Б	$\leq \left(\text{nM} - \sum_{\text{i=1}}^{\text{n-1}} \text{i} \right)$	25
Алгоритм Р.Р.Убара	$< \left(\text{C}_{\text{M}}^{]\text{M/2}[} + \text{C}_{\text{M}}^{]\text{M/2}[+1} \right)$	70

За простотою алгоритму і за елементарністю обчислень, а також за швидкістю розв'язання найкращим є метод Б. Використовуючи поняття ваги (важливості) параметра можна замінити в матриці (4.3.3) величину аік на hік.

При цьому

$$\sum_{i=1}^{M} h_{\text{iк}} = 1$$

а hік показує (щодо) як сильно впливає і-ий елемент (точніше параметри елемента) на к-ий параметр. Така заміна особливо ефективна при переважній кількості параметричних відмов. Зауважимо, що не змінюючи сутності методу, можна замінити величину qi на λiτbi або на τbi/τcpi, (де λi – інтенсивність відмов і-го елемента; τcpi - середній час відновлення і-го елемента). При цьому у виразі (4.3.1) P(0) матиме сенс коефіцієнта готовності. Проілюструємо методи на прикладах.

Приклад: Об'єкт контролю задано матрицею виду (4.3.3)

$$\|a_{ik}\| = \begin{Vmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{Vmatrix}$$

елементи якої визначаються за умови (4.3.4).

Вихідні дані наведено у табл.4.3.2. обмеження Gy=7.

Таблиця 4.3.2

№	$q_i \times 10^3$	π_1	π_2	π_3	π_4	π_5
		витрати на контроль				
		2	2	2	3	3
1	3		3			
2	5			5	5	5
3	4	4				4
4	4			5		
5	4				4	
$S_к \times 10^3$	20	4	3	9	9	9
$1 - S_к$	0,980	0,996	0,997	0,991	0,991	0,991
$R_к = g_к(1 - S_к)$		-	-	1,882	-	-

Приклад 1. З табл.4.3.2 видно, що кращим контролю є параметр π3, тобто

$$\pi_{1^*} = \pi_3; \quad P^{(3)} = \frac{0,980}{0,991} = 0,998$$

Поєднання по два параметри визначення π2º представлені в табл. 4.3.3. З неї випливає, що доцільним для контролю є поєднання параметрів π3π4 = π2º

$$P^{(34)} = \frac{0{,}980}{1 - 0{,}013} = 0{,}993$$

Таблиця 4.3.3

№	$q_i \times 10^3$	12	13	14	15	23	24	25	34	35	45
		затраты на контроль $g_{(2)}$									
		4	4	5	5	4	5	5	5	5	6
1	3					3	3	3			
2	5		5	5	5	5	5	5	5	5	5
3	4	4	4	4	4			4		4	4
4	4					4			4		
5	4								4		4
$S_{к1} \times l0^3$		7	9	9	9	12	8	12	13	9	13
$(1 - S_{кl}) \times 10^3$		993	991	991	991	988	992	988	987	991	987
$(1 - S_{к1}) \times g(2)$		3,952									

4.4 Оцінка оптимального часу між проведенням функціональних перевірок інформаційного каналу

Якщо можливість виявлення відмов каналу чи проникнень у нього з допомогою безперервного контролю РНК, і з допомогою контролю Рфк = 1 - Рнк , то значення стаціонарного коефіцієнта готовності можна сказати співвідношенням

$$K_г = \frac{T_0}{T_0 + \tau_в + P_{фк} + T_{фк}/2} \quad \frac{T_{фк}}{T_{фк} + \tau_{фк}};$$

де Т0 – середній час роботи каналу між відмовами;

τв - середній час існування відмови (τв = τвід + τус);

ТФК – середній час між проведенням функціонального контролю;

τфк – середній час проведення функціонального контролю.

Оптимізація блоків контрольованої апаратури. Очевидно, що чим більше блоків розділений канал, тим краще її ремонтопридатність і, отже, коефіцієнт готовності. У той самий час зростає складність апаратури контролю та збільшується вплив її похибки (і проникнення канал).

Звідси випливає вимога доцільного розбиття каналу блоки з контрольованими параметрами.

У роботі отримано формулу для визначення оптимальної кількості блоків з контрольованою працездатністю, за умови

$$\tau << t << T_0 << T_{кі}$$

де τ – середня тривалість неробочих періодів;

t – поточний час роботи РЕА;

Ткі – середній час безвідмовної роботи одного блоку апаратури діагностики.

Легко бачити, що умова вище виконується для широкого класу РЕА та апаратури контролю. Оптимальна кількість блоків для досягнення максимального коефіцієнта готовності знаходиться за формулою

$$M = \frac{-B + \sqrt{B^2 - 4AC}}{2A}$$

Де

$$A = (\tau_{ус} + P_и \tau)(\tau + \tau_{ус});$$

$$B = 2\tau_{от}(P_и \tau + \tau_{ус})$$

$$C = \tau_{от}\left[\tau_{от} - \frac{\tau T_{ки}(1 - P_и)}{P_{ло} T_о}\right].$$

Тут Рі - ймовірність того, що канал використовується у будь-який довільний момент часу t (не залежить від t);

τот - середній час пошуку несправності або проникнення в апаратурі, не розділеної на блоки;

Рло - ймовірність того, що відмова блочного вузла апаратури діагностики виявляється у видачі неправильної інформації про справний блок (Рло = 1 – Рправ, де Рправ – ймовірність того, що блоковий вузол видає правильну інформацію про несправний блок за умови, що відмова або проникнення відбулися).

5. РОЗРОБКА РЕКОМЕНДАЦІЙ З ВИКОРИСТАННЯ ПРИСТРІЙ, МЕТОДІВ І ЗАХОДІВ ЗА ЗАХИСТОМ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

КСЗІ є сукупністю:

- організаційних заходів;

- інженерно-технічних заходів.

Вони спрямовані на забезпечення захисту інформації від розголошення, витоку та несанкціонованого доступу.

Організаційні заходи є обов'язковою складовою побудови будь-якого КСЗІ. Інженерно-технічні заходи здійснюються за необхідності.

5.1 Рекомендації щодо категорування інформації в інформаційній системі підприємства

Вся інформація на підприємстві має бути категорійована. Категорії критичності та пов'язані з ними заходи захисту для виробничої інформації повинні враховувати виробничу необхідність колективного використання інформації або обмеження доступу до неї, а також збитків для підприємства, пов'язаних з несанкціонованим доступом або пошкодженням інформації.

Відповідальність за визначення категорії критичності конкретному виду інформації, наприклад, документу, файлу даних або дискеті, а також за періодичну перевірку цієї категорії слід покласти на власника інформації.

Слід обережно підходити до інтерпретації категорій критичності на документах інших підприємств, оскільки однаковий чи схожий рівень критичності може бути визначений інакше.

При присвоєнні категорій критичності слід врахувати такі моменти:

- Критична інформація та вихідні дані систем, що містять критичну інформацію, повинні мати відповідні категорії критичності.

- Надмірне засекречування інформації може призвести до невиправданих додаткових витрат у компанії.

- Вихідним даним інформаційних систем, що містить критичну інформацію, має бути присвоєний відповідний рівень критичності. Цей рівень критичності повинен відображати категорію критичності найуразливішої інформації у вихідних даних.

Наприклад, для підприємства вводяться такі рівні категорій критичності інформації:

- загальнодоступно,

- конфіденційно,

- суворо конфіденційно,

- таємно.

Співробітникам підприємства суворо забороняється розголошувати будь-кому інформацію вище за рівень конфіденційно.

1) Загальнодоступною інформацією є інформація, що вже опублікована у засобах масової інформації.

Рішення про надання статусу загальнодоступно ухвалює генеральний чи технічний директор.

1) Конфіденційною інформацією для підприємства є будь-яка внутрішня інформація підприємства.

2) Суворо конфіденційною інформацією на підприємстві є:

- комерційна інформація: тексти договорів та угод з партнерами та клієнтами, розголошення яких було б небажаним для підприємства;

- технічна інформація (тексти звітів, ТЗ, значущі документи, продукти, ключі ліцензування тощо).

Рішення про надання статусу суворо конфіденційно-комерційної інформації приймає генеральний директор.

Рішення про надання статусу суворо конфіденційно-технічної інформації приймає технічний директор.

1) Секретною інформацією для підприємства є:

- фінансова інформація про діяльність підприємства;

- особливо важлива технічна інформація.

Рішення про надання статусу секретно-фінансової інформації приймає генеральний директор.

Рішення про надання статусу секретно-технічної інформації приймає технічний директор.

5.1.2 Рекомендації щодо категоріювання користувачів інформаційної системи підприємства

Користувачі інформаційної системи підприємства мають бути категоровані з метою визначення рівня доступу до ресурсів.

Наприклад, в інформаційній системі вводяться такі категорії користувачів:

- адміністратори,

- топ-менеджери,

- співробітники,

- стажери.

1) Група адміністраторів – входять спеціалісти служби інформаційних технологій та інформаційної безпеки. Адміністратори мають доступ до ресурсів інформаційної системи із можливістю адміністрування.

2) Група топ-менеджерів – входять президент компанії, генеральний директор, технічний директор.

3) Група співробітників – входять усі співробітники Компанії.

4) Група стажистів – входять працівники під час випробувального терміну. Користувачі цієї групи мають мінімальний рівень доступу до ресурсів інформаційної системи.

5.2 Інженерно-технічні заходи

Інженерно-технічні заходи - сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, яку необхідно забезпечити.

Інженерно-технічні заходи для захисту інформаційної інфраструктури організації можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування та захисту від несанкціонованого доступу.

Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовленнєвої) інформації.

Рекомендовані сучасні пристрої пошуку та захисту наведено у Додатку Б.

Розглянемо деякі технічні засоби, що використовуються в АС, що захищаються.

У разі потреби, у рамках проведення інженерно-технічних заходів, може здійснюватися установка у приміщеннях систем охоронно-пожежної сигналізації, систем контролю та управління доступом.

5.2.1 Рекомендації щодо усунення несанкціонованого використання диктофону

Проблема усунення небажаних записів на диктофон на відстані ближче 1,5-2м вирішується багатьма методами.

Однак, у деяких випадках ця відстань може знадобитися збільшити до 3-10м, що не дозволяють зробити потай відомі методи.

Запропонуємо використати для цього інтерференційний метод. Оскільки звуковий діапазон (до 20кГц) не може бути застосований для встановлення перешкоди через сприйняття його людським слухом, використовуємо два випромінювачі в ультразвуковому діапазоні (30-50кГц). Їх частоти F1 та F2 вибираємо таким чином, щоб $\Delta F = /F1-F2/<(1-3)$ кГц.

Розташовується апаратура як показано на рис.5.1.

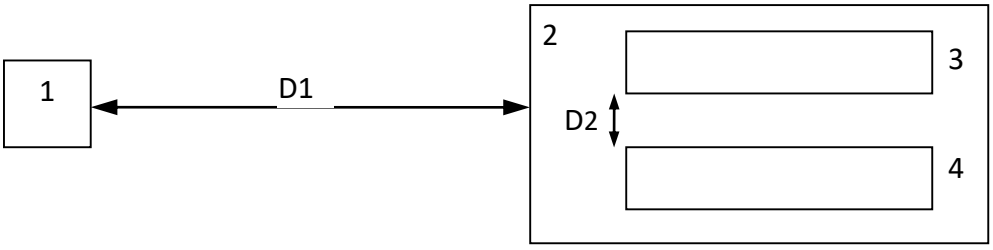

Рисунок 5.1 – Схема розташування апаратури блокування витоку інформації з використанням диктофону

Тут: 1-диктофон (передбачуваний);

2-апаратура усунення запису (приховано);

3-генератор гармонійного сигналу частоти F1 з ультразвуковим випромінювачем;

4 те ж на частоті F2;

D1 – відстань передбачуваного диктофона від апаратури усунення запису (постановника гармонійної інтерференційної перешкоди), можливо більше 1,5-2м;

D2 – відстань між випромінювачами (вибирається не більше від кількох сантиметрів до десятків).

Принцип роботи наступний: випромінювання гармонічних ультразвукових коливань кожного окремо не прослуховуються людським слухом (проте тренований собака їх може вловити). Людське вухо досить лінійно в амплітудному відношенні, і тому інтерференційних явищ не буде.

Мікрофон диктофона є суто нелінійним елементом і тому на вході диктофона виникне інтерференційний процес, який призведе до придушення запису мови сигналом різницевої частоти. Рівень ультразвукових коливань використовується в

межах 80-100дБ і краще, якщо він буде підібраний досвідченим шляхом в аналогічному приміщенні та з диктофоном схожим на передбачуваний.

Цей метод може використовуватися також і в автомобілях та літаках.

5.2.2 Рекомендації щодо захисту інформації постановкою перешкод

Розглянемо кілька пристроїв та методів, які можуть бути використані для покращення постановки перешкод із метою захисту від несанкціонованого доступу до інформації.

Перший пристрій може бути застосований при вирішенні різних завдань постановки перешкод та підвищення періоду випадковості у постановниках перешкод.

Функціональна схема містить генератор 1 рівномірно розподілених випадкових чисел, вихід якого з'єднаний з входом цифроаналогового перетворювача 2, блок 3 усереднення, вихід якого з'єднаний з входом суматора 4, вихід якого з'єднаний з входом блоку 5 порівняння, другий вхід якого з'єднаний з виходом цифроаналогового перетворювача 2, а вихід - через переривник 6 і формувач 7 імпульсів з'єднаний з входами генератора 1 рівномірно розподілених випадкових чисел і генератора 8 експоненційної напруги, вихід якого з'єднаний з входами блоку 3 усереднення та суматора 4.

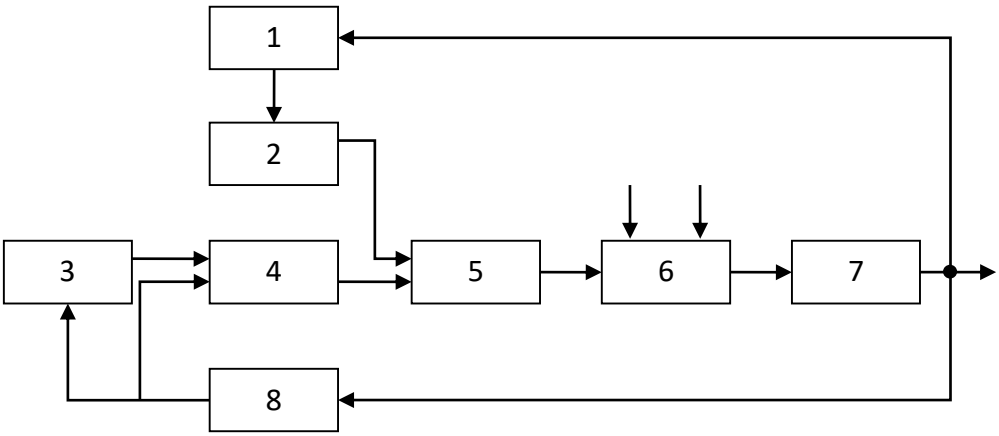

Рисунок 5.2 – Структурна схема пристрою встановлення перешкод

Генератор пуассонівського потоку імпульсів працює наступним чином.

Генератор 1 випадкових чисел виробляє випадкове число, рівномірно розподілене деякому фіксованому інтервалі. На виході цифроаналогового перетворювача 2 утворюється аналоговий сигнал, амплітуда якого пропорційна сформованого випадкового числа.

Синхронно з генератором 1 випадкових чисел включається і генератор 8, амплітуда вихідного сигналу якого зростає за експонентним законом. Сигнал з виходу генератора 8 надходить на один із входів суматора 4 і вхід блоку 3 усереднення, на виході якого утворюється сигнал пропорційний різниці теоретичного та поточного середніх значень безперервної випадкової напруги з рівномірним розподілом амплітуд з виходу генератора 8. Цей сигнал надходить на інший вхід суматора Напруга на виході суматора 4 за допомогою блоку 5 порівнюється з аналоговим напругою цифроаналогового перетворювача 2, і в момент рівності цих

напруг блок 5 видає сигнал, який, проходячи через переривник 6, надходить на вхід формувача 7 імпульсів.

Сигнал з виходу формувача 7 знову запускає генератор 8 експонентного напруги і зчитує з генератора 1 знову сформоване рівномірно розподілене число.

Сигнал з виходу блоку 3 усереднення виконує функцію сигналу зворотного зв'язку, який підтримує автоматично інтенсивність пуассоновского потоку на заданому рівні. Якщо поточна середня випадкова напруга з виходу генератора 8 збігається з теоретичним, сигнал на виході блоку 3 відсутня. При дрейфі параметрів пристрою на виході блоку 3 з'являється сигнал полярності різниця, відповідний відхилення інтенсивності потоку на виході пристрою від заданої. Цей сигнал, сумуючись з напругою, що експоненціально змінюється, компенсує дрейф.

Використання нових блоків. - суматора та блоку усереднення дозволяє підвищити точність результатів досліджень систем масового обслуговування, в яких застосовується датчик потоку електричних імпульсів, розподілених згідно із законом Пуассона; знизити вимоги до стабільності та температурної стійкості джерел живлення та вузлів датчика, що спростить конструктивні та схемні рішення; усунути додаткову похибку, викликану усіченням експоненційного закону розподілу, оскільки у запропонованому пристрої усувається необхідність виділення запасу за напругою у разі дрейфу параметрів.

Наступний пристрій може бути використаний для створення спеціалізованих моделюючих пристроїв, що застосовуються, зокрема, для моделювання потоків збоїв при передачі

дискретної інформації каналом зв'язку в тому числі і при несанкціонованому доступі до інформації.

Поставлена мета досягається тим, що в генератор випадкового імпульсного потоку, що містить послідовно з'єднані генератор імпульсів, лічильник імпульсів, цифроаналоговий перетворювач, інтегратор і суматор, другий вхід якого підключений до виходу додаткового цифроаналогового перетворювача, вихід суматора з'єднаний з другим входом компаратора, причому вихід формувача імпульсів з'єднаний з другим входом лічильника імпульсів, вихід блоку завдання входу нелінійного цифроаналогового перетворювача.

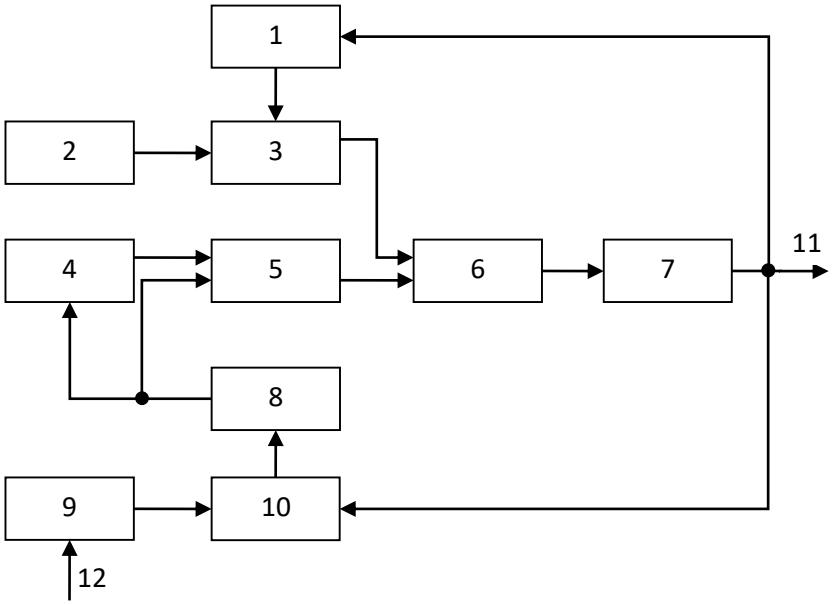

Рисунок 5.3 – Структурна схема пристрою 2

Генератор випадкового імпульсного потоку містить генератор 1 псевдовипадкової послідовності імпульсів, блок 2 завдання закону розподілу, нелінійний цифроаналоговий перетворювач 3, інтегратор 4, суматор 5, компаратор 6, формувач 7 імпульсів, цифроаналоговий перетворювач 8, керований генератор 0 виходу випадкового імпульсного потоку, шину входу 12 управління інтенсивністю випадкового потоку.

Генератор працює в такий спосіб.

На виході генератора 1 псевдовипадкової послідовності імпульсів формується n-розрядне двійкове рівномірно розподілене випадкове число, що надходить на входи нелінійного цифроаналогового перетворювача 3, на виході якого встановлюється рівень пропорційної напруги функції, зворотної функції розподілу, що задається блоком 2 завдання закону розподілу. Напруга з виходу нелінійного цифроаналогового перетворювача 3 надходить на один з входів компаратора 6, на інший вхід якого надходить напруга з виходу суматора 5, на входи якого подається лінійно змінюється напруга з виходу цифроаналогового перетворювача 8 і напруга з виходу інтегратора 4, представляє відповідними теоретичному і поточному середньому, лінійно змінюється напруги з виходу цифроаналогового перетворювача 8, підключеного до входу інтегратора 4. На розрядні входи цифроаналогового перетворювача 8 надходять числа з виходу лічильника 10, вміст якого , період надходження яких регулюється за необхідним законом шляхом подачі відповідного керуючого впливу на шину входу 12 управління інтенсивністю випадкового потоку. При порівнянні напруг компаратор 6 змінює свій стан, що викликає появу імпульсу на виході формувача 7 імпульсів, який, надходячи на шину зсуву генератора 1, викликає формування на виході нового випадкового числа, і, надходячи на вхід установки нуля лічильника 10, встановлює його в нульове стан. Потім процес формування імпульсу випадкового потоку повторюється.

Інтегратор 4 та суматор 5 служать для стабілізації інтенсивності випадкового потоку в процесі роботи генератора

випадкового імпульсного потоку в процесі роботи генератора випадкового імпульсного потоку. Так, наприклад, внаслідок температурного дрейфу параметрів змінилася інтенсивність потоку на виході пристрою. Інтегратор 4 формує напругу зсуву, рівне різниці напруг, відповідних теоретичному і поточному середньому лінійно змінюється напруги.

Напруга зсуву, надходячи на один із входів суматора 5, складається з лінійно змінним напругою з виходу цифроаналогового перетворювача 8, що надходить на інший вхід з суматора 5. Результуюча напруга з виходу суматора 5 надходить на один із входів компаратора 6, де відбувається компенсація температур. З допомогою нелінійного цифроаналогового перетворювача 3, що представляє собою поліноміальний цифроаналоговий перетворювач з регульованими коефіцієнтами полінома, можлива апроксимація з необхідною точністю широкого класу функція розподілу, що дозволяє формувати на виході генератора різні випадкові потоки.

Пропонований генератор дозволяє також генерувати випадкові нестаціонарні потоки з довільним законом зміни інтенсивності. Це значно розширює область використання генератора випадкового імпульсного потоку та усуває необхідність розробки низки спеціалізованих генераторів.

5.3 Рекомендації щодо захисту інформації, що обробляється в автоматизованих системах

В установі (підприємстві) має бути документально визначено перелік ЗП та осіб, відповідальних за їх експлуатацію

відповідно до встановлених вимог щодо захисту інформації, а також складено технічний паспорт на ЗП.

Захищаються приміщення повинні розміщуватися в межах КЗ. При цьому рекомендується розміщувати їх на віддаленні від кордонів КЗ, що забезпечує ефективний захист, що захищають конструкції (стіни, підлоги, стелі) не повинні бути суміжними з приміщеннями інших установ (підприємств).

Не рекомендується розташовувати ЗП на перших поверхах будівель.

Для запобігання перегляду текстової та графічної конфіденційної інформації через вікна приміщення рекомендується обладнати їх шторами (жалюзі).

Захищені приміщення рекомендується оснащувати сертифікованими за вимогами безпеки інформації ОТСС та ВТСС або засобами, що пройшли спеціальні дослідження та мають наказ на експлуатацію.

Експлуатація ОТСС, ВТСС повинна здійснюватися у суворій відповідності до приписів та експлутаційної документації на них.

Спеціальна перевірка ЗП та встановленого в ньому обладнання з метою виявлення можливо впроваджених у них електронних пристроїв перехоплення інформації "закладок" проводиться за необхідності за рішенням керівника підприємства.

Під час проведення конфіденційних заходів забороняється використання в ЗП радіотелефонів, кінцевих пристроїв стільникового, пейджингового та транкінгового зв'язку, переносних магнітофонів та інших засобів аудіо та відеозапису. При установці в ЗП телефонних та факсимільних

апаратів з автовідповідачем або спікерфоном, а також апаратів з автоматичним визначником номера слід відключати їх з мережі на час проведення цих заходів.

Для виключення можливості витоку інформації за рахунок електроакустичного перетворення рекомендується використовувати в ЗП як кінцеві пристрої телефонного зв'язку, що мають прямий вихід до міської АТС, телефонні апарати (ТА), що пройшли спеціальні дослідження, або обладнати їх сертифікованими засобами захисту інформації від витоку за рахунок електроакустичного перетворення .

Для виключення можливості потайного проключення ТА та прослуховування розмов, що ведуться в ЗП, не рекомендується встановлювати в них цифрові ТА цифрових АТС, які мають вихід до міської АТС або до якої підключені абоненти, які не є співробітниками установи (підприємства).

У разі потреби рекомендується використовувати сертифіковані за вимогами безпеки інформації цифрові АТС або встановлювати аналогові апарати в ці приміщення.

Введення системи міського радіотрансляційного мовлення на територію установи (підприємства) рекомендується здійснювати через радіотрансляційний вузол (буферний підсилювач), що розміщується у межах контрольованої зони.

При введенні системи міського радіомовлення без буферного підсилювача в ЗП слід використовувати абонентські гучномовці у захищеному від витоку інформації виконанні, а також трипрограмні абонентські гучномовці в режимі прийому 2-ї та 3-ї програми (з підсилювачем).

У разі використання однопрограмного або трипрограмного абонентського гучномовця у режимі прийому першої програми (без посилення) необхідно їх відключати на період проведення конфіденційних заходів.

У разі розміщення електрогодинної станції всередині КЗ використання в ЗП електровторинного годинника (ЕВЧ) можливе без засобів захисту інформації

При встановленні електрогодинної станції поза КЗ в лінії ЕВЧ, що мають вихід за межі КЗ, рекомендується встановлювати сертифіковані засоби захисту інформації.

Системи пожежної та охоронної сигналізації ЗП повинні будуватися лише за провідною схемою збору інформації (зв'язку з пультом) і, як правило, розміщуватися в межах однієї із ЗП контрольованої зони.

Як кінцеві пристрої пожежної та охоронної сигналізації в ЗП рекомендується використовувати вироби, сертифіковані за вимогами безпеки інформації, або зразки засобів, що пройшли спеціальні дослідження та мають припис на експлуатацію.

Звукоізоляція огороджувальних конструкцій ЗП, їх систем вентиляції та кондиціювання повинна забезпечувати відсутність можливості прослуховування розмов, що ведуться в ньому, з-за меж ЗП.

Перевірка достатності звукоізоляції здійснюється атестаційною комісією шляхом підтвердження відсутності можливості розбірливого прослуховування поза ЗП розмов, які у ньому.

При цьому рівень тестового мовного сигналу повинен бути не нижчим за приміщення, що використовується під час штатного режиму експлуатації.

Для забезпечення необхідного рівня звукоізоляції приміщень рекомендується обладнання дверних прорізів тамбурами з подвійними дверима, встановлення додаткових рам у віконних отворах, ущільнювальних прокладок у дверних та віконних притворах та застосування шумопоглиначів на виходах вентиляційних каналів.

Якщо запропонованими вище методами не вдається забезпечити необхідний акустичний захист, слід вживати організаційно-режимних заходів, обмежуючи на період проведення конфіденційних заходів доступ сторонніх осіб до місць можливого прослуховування розмов, що ведуть у ЗП.

Для зниження ймовірності перехоплення інформації по віброакустичному каналу слід організаційно-режимними заходами виключити можливість встановлення сторонніх (нештатних) предметів на зовнішній стороні конструкцій ЗП, що огороджують, і інженерних комунікацій (систем опалення, вентиляції, кондиціонування), що виходять з них.

Для зниження рівня віброакустичного сигналу рекомендується розташовані в ЗП елементи інженерно-технічних систем опалення, вентиляції обладнати звукоізолюючими екранами.

У випадку, якщо зазначені вище заходи захисту інформації від витоку по акустичному та віброакустичному каналах є недостатніми або недоцільними, рекомендується застосовувати метод активного акустичного або віброакустичного маскуючого зашумлення.

Для цієї мети слід застосовувати сертифіковані засоби активного захисту.

При експлуатації ЗП необхідно передбачати організаційно-режимні заходи, спрямовані на виключення несанкціонованого доступу до приміщення:

- двері ЗП у період між заходами, а також у неробочий час необхідно замикати на ключ;

- видача ключів від ЗП повинна проводитись особам, які працюють у ньому або відповідальним за це приміщення;

- встановлення та заміна обладнання, меблів, ремонт ЗП повинні проводитись лише за погодженням та під контролем підрозділу (фахівця) із захисту інформації установи (підприємства).

Джерела

1. Akhramovich V., Hrebennikov A., Tsarenko B., Stefurak O. Method of calculating the protection of personal data from the reputation of users / - Sciences of Europe, Praha, Czech Republic.2021/ VOL 1, No 80 (2021) Pp. 23-31. www.european-science.org

2. Концепція інформаційної безпеки України
https://www.osce.org/files/f/documents/0/2/175056.pdf

3. Alter Sign комплекс КСЗІ http://altersign.com.ua/korysna-informacija/pobudova-kszi/shcho-take-kompleksna-systema-zahystu-informaciji-kszi

4. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах
https://www.kmu.gov.ua/npas/32791826

5. Управління державної охорони України. Про затвердження порядку проведення державної експертизи в сфері технічного захисту інформації в Управлінні державної охорони України
https://zakon.rada.gov.ua/laws/show/z0728-18#Text

6. Studfile Оцінка ефективності функіонування автоматизованих інформаційних систем https://studfile.net/preview/3872078/page:26/

7. Комплексні системи захисту інформації спеціальних об'єктів та методика їх оцінки.
УДК 621.384 С.В. Толюпа, Ю.Я. Самохвалов, Н.В. Цьопа комплексні

8. Інформатика, математичне моделювання та інформаційні технології
Оцінка ефективності систем захисту інформації
О. І. Гарасимчук, Ю. М. Костів Національний університет “Львівська політехніка”, м. Львів УДК 681.3

9. Інформаційні технології управління: Учеб. посібник / За ред. Титоренко Г. А. - М.: ЮНІТІ-ДАНА, 2002.

10. ДСТУ 2938-94. Системи обробки інформації. Основні поняття. Терміни та визначення. - К.: Держстандарт України. - 1995. - 32 с.

11. ДСТУ 2940-94. Системи обробки інформації. Керування процесами обробки даних. Терміни та визначення. - К.: Держстандарт України. - 1995. - 28 с

12. ДСТУ 2941-94. Системи обробки інформації. Розроблення систем. Терміни та визначення. - К.: Держстандарт України. - 1995. - 20 с

13. ДСТУ 2566-94. Засоби радіоелектронні. Надійність резервованих систем. Загальні положення. - К.: Держстандарт України. - 1995. - 27 с

14. Випов Г. П., Саламатіна Л. І. Конструювання та функціонування програмного забезпечення АСУ. - К.: Наукова думка, 1990. - 156 с.

15. НД ТЗІ 1.4-001-2000 Типове положення про службу захист інформації в автоматизованій системі.

16. ДСТУ 3396.2-97 Захист інформації. Технічна захист інформації. Терміни та визначення

17. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі

18. Закон України № 2658-XII від 02.10.1992 р. / Верховна Рада України // Відомості Верховної Ради України. - 1992. - №48

19. Про Державну службу спеціальної зв'язку та захисту інформації України: Закон України № 3475-IV від 23.02.2006 р. / Верховна Рада України // Відомості Верховної Ради України. - 2006, № 30, ст. 258

20. Про державну таємницю [Текст] : Закон України № 3855-XII від 21.01.1994р. / Верховна Рада України // Відомості Верховної Ради України. - 1994, № 16, ст. 93.