**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ»**

на здобуття освітнього ступеня магістр
за спеціальності 123 Комп'ютерна інженерія
(код,найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Денис Лесик
(підпис) *(ім'я, ПРІЗВИЩЕ здобувача)*

Виконав: здобувач вищої освіти гр.КСДМ-62
Денис Лесик
(ім'я, ПРІЗВИЩЕ)

Керівник: Ярослав Торошанко
доктор філософії (PhD) *(ім'я, ПРІЗВИЩЕ)*

Рецензент: _____
науковий ступінь, вчене звання *(ім'я, ПРІЗВИЩЕ)*

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерної інженерії
Ступінь вищої освіти «Магістр»

Спеціальність 123 Комп'ютерна інженерія
Освітньо-професійна прорама Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерної інженерії
Наталія ЛАЩЕВСЬКА
(ім'я, ПРІЗВИЩЕ)
"____" _____2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лесику Денису Олександровичу
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Дослідження методів забезпечення стійкості комп'ютерної мережі в умовах надзвичайних ситуацій
керівник роботи к.т.н, доцент кафедри КІ Торошанко Я.І.
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" 10 2023 р. №145
2. Строк подання кваліфікаційної роботи
3. Вихідні дані кваліфікаційної роботи:
3.1. Методи забезпечення стійкості комп'ютерної мережі.
3.2. Інтернет ресурси стосовно комп'ютерних мереж в умовах НС.
3.3. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Аналіз поняття і класифікації інформаційних ресурсів.
4.2. Основні положення системи захисту інформації.
4.3. Систематизація реагування на надзвичайні ситуації.

5.Перелік ілюстраційного матеріалу: *презентація*

6. Дата видачі завдання “19” жовтня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	**Примітка**
1.	Підбір технічної літератури	.2023р. .2023р.	Виконано
2.	Аналіз поняття і класифікації інформаційних ресурсів	.2023р. .2023р.	Виконано
3.	Основні положення системи захисту інформації	.2023р. .2023р.	Виконано
4.	Систематизація реагування на надзвичайні ситуації	.2023р. .2023р.	Виконано
5.	Оформлення роботи, висновки	.2023р. .2023р.	Виконано
6.	Розробка демонстраційного матеріалу, доповідь	.2023р. .2023р.	Виконано

Здобувач вищої освіти Денис Лесик
(підпис) *(ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи Ярослав Торошанко
(підпис) *(ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття ступеня магістр: 87 стор., 6 табл., 15 рис., 20 джерел.

Мета роботи – забезпечення стійкості комп'ютерної мережі в умовах надзвичайних ситуацій.

Об'єкт дослідження – методи та технології, які можуть бути використані для забезпечення стійкості комп'ютерної мережі.

Предмет дослідження – комп'ютерні мережі в умовах надзвичайних ситуацій.

Короткий зміст роботи: З прискоренням інформаційного процесу комп'ютерна інформаційна система та мережа стали важливою соціальною інфраструктурою. На основі вивчення базової теорії, технології та застосування реагування на надзвичайні ситуації у сфері безпеки комп'ютерних мереж, ця дипломна робота зосереджується на відповідних стратегіях, спрямованих на створення ефективного механізму реагування на надзвичайні ситуації у сфері безпеки комп'ютерних мереж, аналізує склад стратегії, об'єкт функції та процес дії системної структури, а також розробляє структуру системи стратегії реагування на надзвичайні ситуації у сфері безпеки комп'ютерних мереж.

КЛЮЧОВІ СЛОВА: КОМП'ЮТЕРНІ МЕРЕЖІ, ІНФОРМАЦІЙНІ РЕСУРСИ, СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, НАДЗВИЧАЙНІ СИТУАЦІЇ, СИСТЕМАТИЗАЦІЯ РЕАГУВАННЯ

ЗМІСТ

ВСТУП

Стрімкий розвиток інформаційних технологій, розширення глобального інформаційного середовища, широке застосування засобів обміну інформацією, всеохоплююча комп’ютеризація всіх сфер життєдіяльності зумовлюють актуальність дослідження питань безпеки інформаційної інфраструктури. Забезпечення ефективного захисту інформації є надзвичайно актуальним для установ, де щоденно оброблюється великий обсяг інформації різного рівня конфіденційності. Ця інформація в більшості випадків і виступає об’єктом дій конкурентів, що і обумовлює загострення питань захисту інформації від її незаконного використання і несанкціонованого доступу до неї. Сьогодні у керівництва більшості установ немає сумнівів в необхідності серйозно піклуватися про інформаційну безпеку установи. Застосування сучасних інформаційних технологій розширює можливості для різних зловживань, пов’язаних з використанням комп’ютерної техніки.

З прискоренням інформаційного процесу комп'ютерна інформаційна система та мережа стали важливою соціальною інфраструктурою. На основі вивчення базової теорії, технології та застосування реагування на надзвичайні ситуації у сфері безпеки комп'ютерних мереж, ця дипломна робота зосереджується на відповідних стратегіях, спрямованих на створення ефективного механізму реагування на надзвичайні ситуації у сфері безпеки комп'ютерних мереж, аналізує склад стратегії, об'єкт функції та процес дії системної структури, а також розробляє структуру системи стратегії реагування на надзвичайні ситуації у сфері безпеки комп'ютерних мереж.

Актуальність даної дипломної роботи полягає в тому, що комп'ютерні мережі стають все більш важливими для функціонування різних організацій та суспільства в цілому. Однак, надзвичайні ситуації, такі як природні катастрофи, кібератаки або технічні збої, можуть серйозно підривати роботу комп'ютерних мереж і завдавати значних збитків. Тому, важливо дослідити методи забезпечення стійкості комп'ютерної мережі в умовах надзвичайних ситуацій.

1 АНАЛІЗ ПОНЯТТЯ І КЛАСИФІКАЦІЇ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1 Класифікація комп'ютерних мереж

Комп'ютерна мережа — сукупність пристроїв, з'єднаних каналами передавання даних, для спільного користування апаратними, програмними та інформаційними ресурсами під керуванням спеціального програмного забезпечення.

Комп'ютерні мережі призначені для:

- швидкого обміну даними між окремими комп'ютерами даних;
- віддаленого керування комп'ютерами;
- спільного доступу до периферійних пристроїв.

У комп'ютерній мережі комп'ютери можуть виконувати різні функції. Комп'ютер, який керує розподілом ресурсів мережі, називають сервером (від англ. server — той, хто подає); комп'ютери, які користуються ресурсами мережі, називають клієнтами, або робочими станціями.

На рисунку 1.1 представлено класифікацію комп'ютерних мереж.

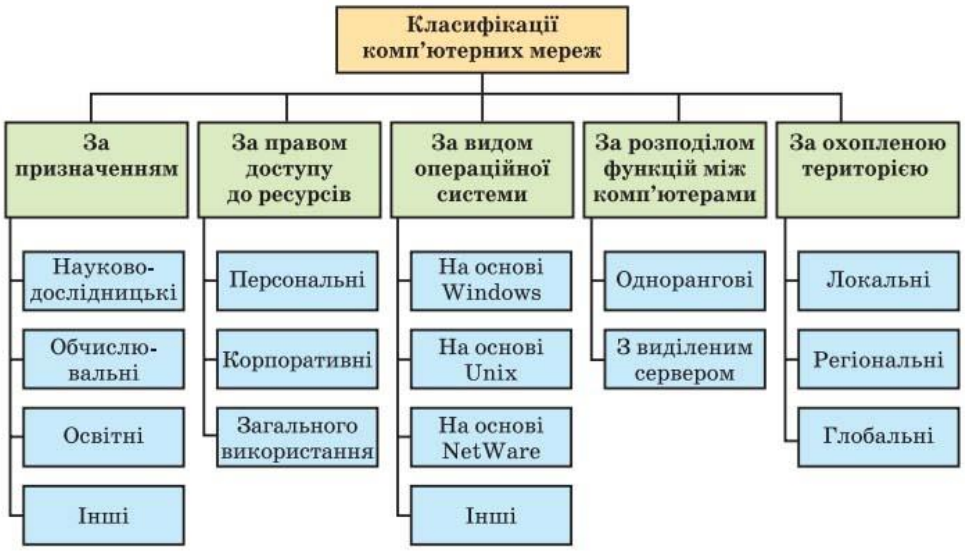

Рисунок 1.1 - Класифікація комп'ютерних мереж

За територією мережі поділяються таким чином.

- персональні (PAN, від англ. Personal Area Network — мережа особистого простору, персональна мережа) — мережі для взаємодії пристроїв, що належать

одній людині та об’єднують її власні електронні пристрої: персональні комп’ютери, ноутбуки, планшети, смартфони, комунікатори;

- локальні (LAN, від англ. Local Area Network — мережа локального простору) — з’єднують пристрої, розташовані на порівняно невеликій відстані один від одного, зазвичай у межах однієї або кількох сусідніх будівель, наприклад мережа навчального закладу;

- міські, регіональні (MAN, від англ. Metropolitan Area Network — мережа міського простору) — обласні й національні мережі. Приміром, www.ukr.net — це українська національна мережа.

- глобальні (WAN, від англ. Wide Area Network — мережа широкого простору) — об’єднують комп’ютерні мережі. Найвідомішою глобальною мережею є Інтернет.

Топологією називають фізичне розташування вузлів мережі один відносно одного та способи їхнього з’єднання лініями зв’язку. Комп’ютерні мережі поділяються також за топологією. Існують три базові топології («загальна шина», «кільце», «зірка») та додаткові, що є модифікацією або поєднанням базових, наприклад топологію «дерево» можна розглядати як комбінацію декількох «зірок».

За способом передавання даних мережі поділяють на кабельні (дротові) і бездротові.

Кабельною (дротовою), називають мережу якщо середовищем передавання даних є кабель. У такому середовищі дані передаються електричними або оптичними сигналами.

Сьогодні використовують такі типи кабелів:

Кручена пара — це декілька пар скручених мідних дротів у кольоровій пластиковій ізоляції . Пучки кручених пар дротів захищає зовнішнє обплетення. Такий кабель ви- користовують у телефонному зв’язку та в більшості мереж Ethernet (від англ. ether — ефір і net — мережа) — це пакетна технологія передачі даних, яка застосовується при побудові комп’ютерних мереж. Залежно від типу

кабелю максимальна відстань передавання даних без підсилення сигналу становить від 15 до 100 м, а швидкість передавання даних може досягати 100 Гбіт/с.

Коаксіальний кабель — це кабель із ізольованою мідною оточеною металевою оболонкою-екраном. Такий кабель використовують для під'єднання комп'ю терів до мережі та поширення сигналів телебачення. Максималь- на відстань передавання даних без підсилення сигналу становить 500 м, максимальна швидкість передавання даних може досягати 10 Мбіт/с.

Оптоволоконний кабель — це скляна або пластикова нитка, що використовується для перенесення світла за допомогою повного внутрішнього відображення. Структура оптоволоконного кабелю схожа на структуру коаксіального кабелю. Але замість центрального мідного дроту в такому кабелі використовується тонке (діаметром близько 1–10 мкм) оптоволокно, а замість внутрішньої ізоляції — скляна або пластикова оболонка, що не дозволяє світлу виходити за межі оптоволокна.

Застосування цього кабелю дозволяє реалізувати найшвидший на сьогодні спосіб передавання даних. Відстань передавання даних без підсилення сигналу становить 50 км, а швидкість передавання даних сягає від 10 Гбіт/с до 4–8 Тбіт/с.

Бездротовою називають мережу, в якій дані передаються радіосигналами.

Стандартами бездротових мереж є:

Wi-Fi (від англ. Wireless Fidelity — бездротова точність) — стандарт для обладнання бездротових мереж і торгова марка консорціуму Wi-Fi Alliance, до якого входять найбільші виробники комп'ютерного устаткування та обладнання Wi-Fi.

WiMAX, Mobile WiMAX, Mobile-Fi — технології бездротових мереж, які призначено для використання разом із технологією Wi-Fi (або замість неї) із метою розширення бездротових мереж. Зокрема, мережа WiMAX забезпечує кращий доступ до Інтернету, ніж Wi-Fi, і має більшу площу покриття.

LTE (від англ. Long-Term Evolution — довготривалий розвиток, часто позначається як 4G LTE) — стандарт бездротової високошвидкісної передачі даних для мобільних телефонів і інших терміналів, що працюють із даними.

Bluetooth — стандарт для бездротових персональних мереж. Технологія забезпечує обмін даними між кишеньковими та стаціонарними комп'ютерами, мобільними телефонами, ноутбуками, принтерами, цифровими фотокамерами тощо.

1.2 Класифікація інформаційних ресурсів

Інформаційні ресурси (ІР) досить широке поняття, і мають досить багато класифікацій. ІР класифікують за різними ознаками, кількість та зміст яких залежать від виду, сфери використання та значення ІР, режиму доступу тощо. У табл.1.1 наведені ознаки класифікації ІР, поділ ІР на категорії згідно з ознаками та зміст цих категорій (якщо він не очевидний та потребує пояснення) згідно із сучасними джерелами з різних напрямів дослідження ІР.

Аналіз ознак та видів ІР показує, що у певні ознаки з різними формулюваннями дослідники вкладають близький зміст, окрім того, деякі категорії повторюються у різних ознаках, або є специфічними, оскільки можуть бути застосовані у вузькій сфері діяльності. На рис. 1.1 наведено визначення та класифікацію ІР, запропоновану на підставі аналізу та узагальнення багатьох джерел з урахуванням важливості та універсальності ознак класифікації.

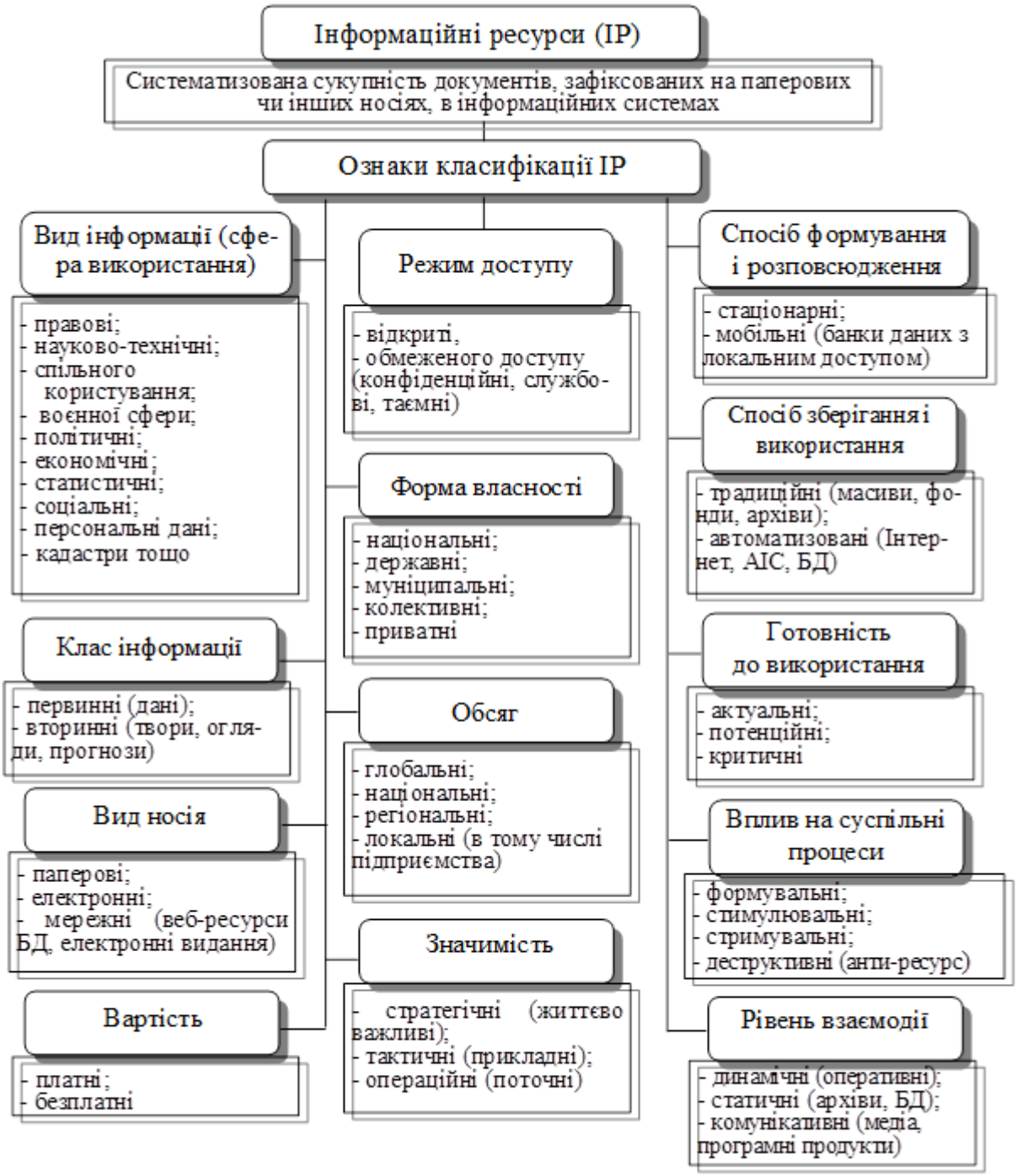

Рисунок 1.2 – Визначення та класифікація інформаційних ресурсів

Таблиця 1.1 – Класифікація інформаційних ресурсів

№	Ознака та джерело	Вид (категорія)	Зміст категорії
1	Вид інформації (сфера використання; функціональна ознака)	науково-технічні	систематизоване зібрання науково-технічної літератури і документації, зафіксованих на паперових чи інших носіях
		спільного користування	сукупність ІР державних органів науково-технічної інформації, а також науково-технічних комерційних організацій, з якими укладено договори про їх спільне використання
		правові, політичні, воєнної сфери [20], фінансово-економічні, статистичні, соціальні, персональні дані, кадастри (земельний, майновий, містобудівний, лісний), інші	
2	Клас інформації	первинні	утворюються незалежно від людини
		вторинні	результат інтелектуальної діяльності людини; результат аналітико-синтетичної обробки
3	Режим доступу (рівень; спосіб)	відкриті	загальнодоступні
		з обмеженим доступом	конфіденційні, службові, таємні
4	Обсяг (глобальність, територія)	глобальні, загальнонаціональні, регіональні, локальні (рівень самоврядування і окремих підрозділів)	
5	Вид (форма) носія	паперові, електронні мережні (веб-ресурси: сайти, бази даних, електронні видання, програмні продукти тощо)	
6	Форма власності	національні (об’єкт права власності будь якого суб’єкта України; мають загальнонаціональну цінність), державні, муніципальні, колективні, приватні	
7	Спосіб зберігання і використання	традиційні	масив, фонд документів, архів
		автоматизовані	Інтернет, банк даних, інформаційна система, база знань
8	Міра готовності до використання	актуальні	необхідна для суспільства інформація, яка забезпечує його життєдіяльність
		потенційні	потребують попередніх ресурсних витрат для перетворення на актуальні
		критичні	втрата яких супроводжується значними політичними, економічними, соціальними та іншими наслідками
9	Значущість	стратегічні	життєво важливі інформаційні ресурси (з позиції національної безпеки)
		тактичні	прикладні науково-технічні, економічні, екологічні та інші, необхідні для забезпечення нагальних проблем
		операційні	поточна ділова, комерційна та інша довідкова інформація
10	Характер впливу на суспільні процеси	формувальні	спрямовані на створення суспільних процесів
		стимулювальні	орієнтовані на розвиток суспільних процесів
		стримувальні	визначають межі суспільних процесів
		деструктивні	спрямовані на знищення визначених процесів
11	Спосіб формування і розповсюдження	стаціонарні	формуються і використовуються в інформаційних організаціях за допомогою їх систем і мереж, у том числі й через Інтернет (споживач “рухається” до ресурсу)
		мобільні	формуються як спеціальні інформаційні продукти,

			переважно як банки даних (ресурс “рухається” до споживача)
12	Вартість	платні, безплатні	
13	Рівень взаємодії	*динамічні*	оперативний моніторинг противника, навігації,АСУ військами та зброєю, моделювання ситуацій і поточних розрахунків для підтримки оперативних рішень
		статичні	спеціалізовані архіви, БД, бази знань, бібліотечні фонди, керівні документи, документація військової техніки та технологій подвійного призначення
		комунікативні	обриси, думки, уявлення;продукція мас-медіа,програмні продукти загального характеру для комп’ютерних систем
14	Вид джерел та сфера їх використання	науково-технічної інформації, спільного користування, соціально-економічні, освітянські, інші	
15	Форма ІР (як відчужуваних знань, що стають повідомленнями)	*активні*	модель, алгоритм, програма, проект, бази знань
		пасивні	книги, статті, патенти, бази даних

Також інформаційні ресурси класифікують за такими ознаками:

Ресурси інформаційні за видом інформації – ресурси інформаційні, що можуть містити інформацію таких видів: правова; науково-технічна; політична, економічна (фінансово-економічна); статистична; про стандарти і регламенти; метрологічна; соціальна; про охорону здоров’я; про надзвичайні ситуації; особиста інформація (персональні дані); кадастри (земельний, містобудівний, лісовий, майновий та ін.) тощо.

Ресурси інформаційні за видом носія – ресурси інформаційні, інформація в яких може бути записана на папері, на машиночитаних носіях, у вигляді зображення на екрані ЕОМ, в пам’яті ЕОМ, в каналах зв’язку, на інших носіях.

Ресурси інформаційні за режимом доступу – ресурси інформаційні, що містять інформацію відкриту (без обмежень) або ресурси інформаційні обмеженого доступу, що містять інформацію обмеженого доступу (ІОД): державну таємницю, конфіденційну інформацію, комерційну таємницю, професійну таємницю, службову таємницю, особисту (персональну) таємницю.

1.3 Загроза інформаційній безпеці

Інформаційна загроза – це потенційна можливість певним чином порушити інформаційну безпеку. Під інформаційною безпекою розуміють захищеність даних та інфраструктури, що її підтримує, від будь-яких випадкових або зловмисницьких дій, результатом яких може стати нанесення шкоди безпосередньо даним, їхнім власникам або інфраструктурі, що підтримує інформаційну безпеку.

Стандартною моделлю безпеки даних може слугувати модель із трьох категорій: Конфіденційність – стан даних, за якого доступ до них здійснюють тільки ті особи, що мають на нього право.

Цілісність – уникнення несанкціонованої зміни даних та існування даних у неспотвореному вигляді.

Доступність – уникнення тимчасового або постійного приховування даних від користувачів, котрі мають права доступу.

Відповідно до розглянутої моделі безпеки даних є три різновиди загроз:

- загроза порушення конфіденційності полягає у тому, що дані стають відомими тому, хто не має права доступу до них;

- загроза порушення цілісності передбачає будь-яку умисну зміну даних, що зберігаються в комп’ютерній системі чи передаються з однієї системи в іншу;

- загроза відмови служб виникає щоразу, коли в результаті навмисних дій, які виконує інший користувач або зловмисник, блокується доступ до деякого ресурсу комп’ютерної системи.

Загрози, які можуть завдати шкоди інформаційній безпеці організації, можна розділити на кілька категорій, які представлені на рисунку 1.3.

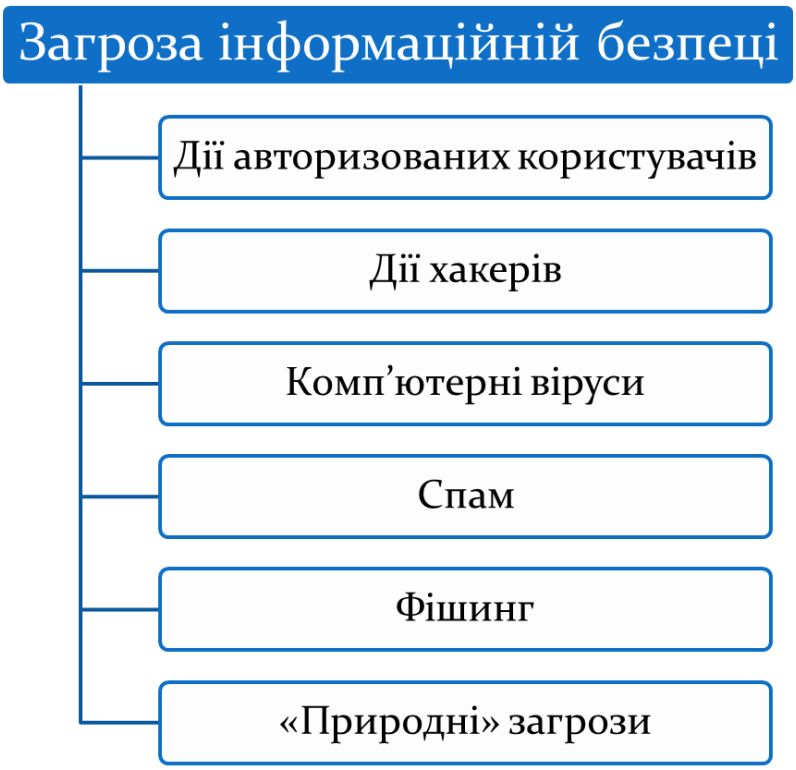

Рисунок 1.3 – Загроза інформаційній безпеці

До категорій дій, що здійснюються авторизованими користувачами, належить: цілеспрямована крадіжка або знищення даних на робочій станції чи сервері; пошкодження даних користувачами в результаті необережних дій.

Хакер – кваліфікований IT-фахівець, який знається на комп'ютерних системах і втручається в роботу комп'ютера, щоб без відома власника дізнатися деякі особисті відомості або пошкодити дані, що зберігаються в комп'ютері.

Окрема категорія електронних методів впливу – комп'ютерні віруси та інші шкідливі програми. Вони становлять реальну небезпеку, широко використовуючи комп'ютерні мережі, Інтернет і електронну пошту.

Спам – небажані рекламні електронні листи, повідомлення на форумах, телефонні дзвінки чи текстові повідомлення, що надходять без згоди користувача.

Фішинг – один з найпопулярніших і прибуткових (для тих, хто його реалізує) видів атак. Зловмисник створює сайт, який у точності копіює дизайн і можливості сайта будь-якого банку, інтернет-магазину або платіжної системи. Мета – збір конфіденційної інформації – паролі, коди тощо.

Морально-етичні основи захисту даних передбачають норми поведінки, які традиційно склались або складаються з поширенням комп'ютерів та мереж: соціальна й персональна відповідальність, рівноправність партнерів по комунікації, точне й сумлінне виконання обов'язків тощо.

Поряд із загальнолюдськими етичними нормами є такі базові права, як:

- загальнодоступність – гарантує право на комунікацію й передбачає доступність державних інформаційних ресурсів;

- таємниця приватного життя – дотримання конфіденційності довірених даних;

- недоторканість приватної власності – основа майнового порядку, дотримання права власності на дані й норм авторського права.

У прийнятих в Україні законодавчих нормах, зазначено, зокрема, що захисту підлягає:

- відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрити інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами;

- конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених Законом України «Про доступ до публічної інформації»;

- службова інформація;

- інформація, яка становить державну або іншу передбачену законом таємницю;

- інформація, вимога щодо захисту якої встановлена законом.

Правовий захист інформації передбачає:

- наявність прав на інформацію – сертифікацію, ліцензування, патентування;

- реалізацію прав – захист інтелектуальної власності, захист авторських прав;

- контроль за процедурами реалізації прав – систему адміністративного, програмного, фізико-технічного захисту інформації.

Власник авторських прав може використовувати знак охорони авторського права, що складається з трьох елементів:

- латинської літери «С» (початкова буква англійського слова copyright – авторське право), взятої в коло ©;

- імені власника виключних авторських прав;

- року першого опублікування твору.

1.3.1 Джерела загроз інформаційній системі

Джерелами загроз (рис.1.4) можуть бути як суб’єкти (особа), так і об’єктивні прояви. Джерела загроз можуть бути як всередині організації – внутрішні джерела, так і зовні її – зовнішні джерела. Поділ джерел на суб’єктивні та об’єктивні виправданий, виходячи з попередніх міркувань стосовно вини або ризику збитку інформації, а поділ на внутрішні та зовнішні джерела виправданий тому, що для однієї й тієї ж загрози методи відбиття для внутрішніх і зовнішніх загроз можуть бути різними.

Оскільки інформація яка підлягає захисту, це насамперед персональні дані громадян, які зберігаються і обробляються у базі даних на сервері. Ці дані потрібно захистити від загроз доступності (блокування інформації, знищення інформації та засобів її обробки), від загроз цілісності (модифікація (спотворення) інформації, заперечення дійсної інформації, нав’язування фальшивої інформації), від загроз конфіденційності (викрадення (копіювання) інформації та засобів її обробки, утрата (ненавмисна втрата, витік) інформації та засобів її обробки).

Рисунок 1.4 – Класифікація джерел загроз безпеці інформації

Поняття загрози інформації є основним в теорії і практиці захисту інформації. Аналіз загроз є початковим і одним з основних етапів при розробці системи захисту інформації і проводиться на основі моделі загроз. Він має виявити можливі загрози інформації, а також показати, з якого боку і в якій точці АСУ слід чекати атаки.

Модель загроз – це абстрактний формалізований або неформалізований опис методів і способів здійснення загроз. Нижче розглянуто формальний опис основних класів загроз інформації, каналів доступу та послуг, реалізація яких дозволяє їм протистояти.

Під загрозами слід розуміти шляхи реалізації дій, що вважаються небезпечними. Наприклад, загроза знімання інформації і перехоплення випромінювання з дисплею може привести до втрати таємності або конфіденційності, загроза пожежі може привести до порушення цілісності та доступності інформації, загроза розриву каналу передачі інформації може реалізувати втрату доступності.

Існує багато підходів щодо класифікації загроз, проте, як здається, найбільш придатною для аналізу є визначення та класифікація загроз за результатом їх дії на інформацію, а точніше, на її основні (фундаментальні) властивості – конфіденційність, цілісність, доступність.

Тоді з цієї точки зору в АСУ розрізняються наступні класи загроз інформації:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності або відмова в обслуговуванні;
- порушення спостереженості або керованості.

Нова інформація від фахівців з безпеки з AV-Test свідчить, що в минулому році кількість випадків виявлення шкідливого ПЗ зросла на 72% порівняно з 2022 р. У загальній складності антивірусами AV-Test було виявлено 143 млн подібних випадків. Причому це абсолютно нові шкідливі програми, які раніше не потрапляли на очі тим, хто забезпечує комп’ютерну безпеку. Таким чином, можна зробити висновок, що кіберзлочинці стають розумнішими і амбітними.

Легкість, з якою хакери можуть перебудовувати шматочки коду і створювати нову загрозу, означає, що антивірусним компаніям стало ще складніше йти в ногу з постійно еволюціонуючими потенційними небезпеками. Лідерство серед країн, відповідальних за поширення спаму, займає США – ця країна перебувала на вершині спамерського античарту, а всього на неї припадає 9,2% спаму. Крім США, в п’ятірці лідерів В’єтнам (7,2%), Аргентина (5,9%), Іспанія (5,8%) і Німеччина (5,6%).

У літературі, присвячених проблемам безпеки інформації, наводилося досить багато фактів несанкціонованого доступу до інформації, що захищалася, і інших зловмисних дій, що мали місце. Причому, за оцінками фахівців, до 85% випадків несанкціонованих проникнень в АСУ взагалі залишаються нерозкритими. З урахуванням введеного фахівцями Стенфордского інституту (США) коефіцієнта розкриття загальне число несанкціонованого проникнення в ПЕОМ урядових установ цієї країни складає більше 450 в рік, а загальний збиток – більше 200 млн. доларів. Аналогічна картина спостерігається і в комерційних системах, де щорічно реєструється близько 400 випадків розкрадання інформації.

Значне місце серед злочинів проти АСУ займають напади на системи і саботаж. Так, у Німеччині нерідкі випадки вандалізму (вибухи, руйнування, виведення із ладу сполучних кабелів, систем кондиціонування і тому подібне). Більше 40 терористичних актів на обчислювальні центри щорічно реєструється в Італії. Широке поширення отримали злочини, пов’язані з порушенням технологічного процесу автоматизованої обробки інформації, причому такі злочини завдають ще більшого збитку.

Особливо широкий розмах отримали злочини в АСУ, обслуговуючих банківські установи і установи торгівлі. За оцінками фахівців, в США, наприклад, збитки від несанкціонованого проникнення тільки в ці АСУ оцінюються в десятки мільйонів доларів.

Своєрідне джерело загроз безпеки інформації представляють спеціальні шкідливі програми, що таємно (приховано) і навмисно впроваджувані в різні функціональні програмні системи. Вказані програми після одного або декількох запусків роблять передбачені при їх створенні деструктивні дії, руйнуючи програмне забезпечення АС, дані, що обробляються, зберігаються або передаються, виводячи з ладу апаратуру і навіть чинячи небезпечну психофізіологічну дію на оператора. На тепер відомі декілька різновидів шкідливих програм, основними з яких є електронні віруси, «комп’ютерні черв’яки» і «троянські коні».

Електронні віруси – це такі шкідливі програми, які не лише здійснюють несанкціоновані дії, але мають здатність до саморозмноження, через що представляють особливу небезпеку для обчислювальних мереж. Відомо декілька визначень програм-вірусів, що підкреслює їх різноманітність. Проте найбільшу популярність здобуло визначення, дане доктором Фредеріком Козном: «комп'ютерний вірус є програмою, яка здатна заражати інші програми, модифікуючи їх так, щоб вони включали копію вірусу (чи його різновид)». Процес життя і розмноження електронного (комп'ютерного) вірусу багато в чому схожий з аналогічними процесами усім нам знайомого біологічного вірусу, що підкреслюється спільністю їх назв.

До «комп'ютерних черв'яків» віднесені шкідливі програми, подібні по своїй дії електронним вірусам. «Черв'як» – це програма, яка поширюється в системах і мережах по лініях зв'язку Як і віруси «комп'ютерні черв'яки» заражають інші програми, проте на відміну від вірусів вони не мають програми-носія. Для розмноження «черв'як» зазвичай використовує додатковий вхід в операційну систему, який створюється для зручності її «відладки» і який нерідко забувають прибрати після закінчення «відладки».

Раніше інших з'явилися і використовувалися в зловмисних цілях шкідливі програми, що дістали назву «троянських коней».

Відомості про них відносяться ще до 70-их рр., причому найбільш поширеною несанкціонованою процедурою було зчитування інформації з областей запам'ятовуючого пристрою, що виділяються законним користувачам. «Троянський кінь» – це програма, яка призводить до несподіваних (зазвичай небажаним) дій на систему.

Відмінною характеристикою «троянського коня» є те, що користувач звертається до цієї програми, вважаючи її корисною. Такі програми мають можливість розкрити, змінити або знищити файли даних і програм. «Троянські коні» зустрічаються в програмах широкого використання (обслуговування мережі, електронна пошта та ін.).

Вже огляду шкідливих програм досить, щоб переконатися у великій небезпеці їх як джерел загроз безпеки інформації в сучасних автоматизованих системах. Таким чином, при обробці інформації засобами обчислювальної техніки виникає велика кількість загроз як прямого несанкціонованого доступу до інформації, що захищається, так і непрямого її отримання коштами технічної розвідки. Упродовж усього періоду регулярного використання обчислювальної техніки для вирішення практичних завдань робилися спроби класифікувати джерела загроз безпеки інформації і самі загрози з метою подальшої стандартизації засобів і методів, вживаних для захисту інформації.

У відомій монографії Л. Дж. Хоффмана «Сучасні методи захисту інформації" було виділено 5 груп різних загроз: розкрадання носіїв, запам’ятовування або копіювання інформації, несанкціоноване підключення до апаратури, несанкціонований доступ до ресурсів ЕОМ, перехоплення побічних випромінювань і наведень. У книзі "Захист інформації в персональних ЕОМ" зроблена спроба класифікації загроз по джерелу можливої небезпеки (людина, апаратура і програма).

До групи загроз, в реалізації яких основну роль відіграє людина, віднесені: розкрадання носіїв, читання інформації з екрану, читання інформації з роздруків; до групи, де основним засобом виступає апаратура: підключення до пристроїв, перехоплення випромінювань; до групи, де основний засіб – це програма: несанкціонований програмний доступ, програмне дешифрування зашифрованих даних, програмне копіювання інформації з носіїв.

Аналогічний підхід пропонується і групою авторів навчальних посібників по захисту інформації від несанкціонованого доступу. Ними виділено три класи загроз: природні (стихійні лиха, магнітні бурі, радіоактивне випромінювання і наведення), технічні (відключення або коливання напруги мережі електроживлення, відмови і збої апаратно-програмних засобів, електромагнітні випромінювання і наведення, витоки через канали зв’язку), створені людьми, причому в останньому випадку розрізняють неумисні і умисні дії різних категорій осіб.

Ще один вид джерел загроз безпеки інформації, пов’язаний з її розкраданням, досить детально класифікований в монографії С.П. Расторгуева «Програмні методи захисту інформації в комп’ютерах і мережах». Автор виділяє чотири способи розкрадання інформації:

- по каналам побічних електромагнітних випромінювань;

- за допомогою негласного копіювання, причому виділено два різновиди копіювання: - «ручне» (виведення інформації на друк або на екран оператором) - «вірусне» (виведення інформації за допомогою вбудованої в ЕОМ радіозакладки);

- розкрадання носіїв інформації;

- розкрадання персональної ЕОМ.

Класифікують за відношенням джерела загрози до АС (зовнішні і внутрішні загрози), по виду джерела загрози:

- фізичні – відбивають фізичні дії на систему;

- логічні – засоби, за допомогою яких людина дістає доступ до логічної інформації системи; в) комунікаційні – відносяться до процесів передачі даних по лініях зв’язку;

- людські – є найважче контрольованими і безпосередньо пов’язаними з фізичними і логічними загрозами), по мірі злого наміру (випадкові і умисні) тощо.

Умисні загрози, у свою чергу, можуть бути підрозділені на активні (несанкціонована модифікація даних або програм) і пасивні (несанкціоноване копіювання даних або програм).

Цікавою є класифікація загроз безпеки інформації за способами їх можливої негативної дії. Така класифікація підтримується переважною більшістю фахівців в області захисту інформації і передбачає підрозділ загроз на інформаційні, програмно-математичні, фізичні і організаційні.

Інформаційні загрози реалізуються у вигляді:

- порушення адресності і своєчасності інформаційного обміну;

- протизаконного збору і використання інформації;

- здійснення несанкціонованого доступу до інформаційних ресурсів і їх протиправного використання;

- розкрадання інформаційних ресурсів з банків і баз даних;

- порушення технології обробки інформації. Програмно-математичні загрози реалізуються у вигляді:

- впровадження в апаратні і програмні вироби компонентів, що реалізовують функції, не описані в документації на ці вироби;

- розробки і поширення програм, що порушують нормальне функціонування інформаційних систем або їх систем захисту інформації.

Фізичні загрози реалізуються у виді:

- знищення, ушкодження, радіоелектронного пригнічення або руйнування засобів і систем обробки інформації, телекомунікації і зв'язку;

- знищення, ушкодження, руйнування або розкрадання машинних і інших носіїв інформації;

- розкрадання програмних або апаратних ключів і засобів криптографічного захисту інформації;

- перехоплення інформації в технічних каналах зв'язку і телекомунікаційних системах;

- впровадження електронних пристроїв перехоплення інформації в технічні засоби зв'язку і телекомунікаційні системи, а також в службові приміщення;

- дії на парольно-ключові системи захисту засобів обробки і передачі інформації. Організаційні загрози реалізуються у вигляді:

- невиконання вимог законодавства в інформаційній сфері;

- протиправної закупівлі недосконалих або застарілих інформаційних технологій, засобів інформатизації, телекомунікації і зв'язку.

На закінчення відмітимо, що в результаті реалізації загроз безпеки інформації може бути нанесений серйозний збиток життєво важливим інтересам країни в політичній, економічній, оборонній і інших сферах діяльності держави, причинний соціально-економічний збиток суспільству і окремим громадянам.

Реалізація загроз може утруднити прийняття найважливіших політичних, економічних і інших рішень, підірвати державний авторитет країни на міжнародній арені, порушити баланс інтересів особи, суспільства і держави, дискредитувати органи державної влади і управління, порушити функціонування системи державного управління, кредитно-фінансової і банківської сфери, а також систем управління військами і зброєю, об’єктами підвищеної небезпеки.

Наслідком реалізації загроз може стати істотний економічний збиток в різних сферах громадського життя і у сфері бізнесу, зниження темпів науково-технічного розвитку країни, підривання оборонного потенціалу.

1.4 Моделі загроз і потенційного порушника

Захист інформації повинен забезпечуватись на всіх її стадіях життєвого циклу в АС, на всіх технологічних етапах обробки інформації та в усіх режимах функціонування АС.

Основними завданнями захисту можуть бути:

- організація і координація робіт із захисту інформації, яка обробляється та передається засобами АС;

- визначення, класифікація ресурсів АС, що підлягають захисту;

- забезпечення визначених конфіденційності, цілісності, доступності інформації під час створення та експлуатації АС, недопущення витоку інформації з обмеженим доступом (ІзОД) та втрати її матеріальних носіїв;

- створення механізму та умов оперативного реагування на загрози для безпеки інформації;

- ефективне попередження, своєчасне виявлення та знешкодження загроз для ресурсів АС, причин та умов, які спричиняють або можуть привести до порушення її функціонування;

- організація служби захисту інформації;

- організація та впровадження системи допуску особового складу (користувачів) до роботи з інформацією, яка потребує захисту;

- керування засобами захисту інформації, керування доступом користувачів до ресурсів АС, контроль за їхньою роботою з боку персоналу служби захисту інформації, оперативне сповіщення про спроби НСД до ресурсів АС;

- створення умов для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними та несанкціонованими діями порушників, зменшення негативного впливу наслідків порушення безпеки на функціонування АС;

- забезпечення режиму секретності під час обробки секретної інформації;

- розробка організаційно-розпорядчої і робочої документації, що визначає вимоги і порядок захисту та обробки ІзОД;

- організація обліку, зберігання, обігу інформації, яка потребує захисту, та її матеріальних носіїв;

- реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;

- здійснення контролю за забезпеченням захисту ІзОД та за збереженням її матеріальних носіїв.

Модель загроз складається для конкретної АС та повинна враховувати особливості функціонування, склад АС, технологію обробки інформації та ін. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз (загрози об’єктивної природи, випадкові та навмисні загрози суб’єктивної природи).

Необхідно визначити перелік суттєвих загроз, класифікувати їх за результатом впливу на інформацію та описати методи і способи їхнього здійснення. Перелік загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити:

- на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення

конфіденційності, цілісності, доступності інформації, а також порушення спостереженості та керованості АС);

- джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу); в) можливі способи здійснення загроз.

Модель потенційного порушника. Розглянемо тепер модель порушника. Згідно з ЗУ порушник – це користувач, який здійснює НСД до інформації.

Оскільки під порушником розуміється людина, то цілком зрозуміло,що створення його формалізованої моделі – дуже складне завдання. Тому, звичайно, мова може йти тільки про неформальну або описову модель порушника. Отже, нижче подається опис можливого для даного класу ІСБ порушника.

Порушник – це особа, яка може отримати доступ до роботи звключеними до складу АС засобами. Вона може помилково, унаслідок необізнаності, цілеспрямовано, свідомо чи несвідомо, використовуючи різні можливості, методи та засоби, здійснити спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Зрозуміло, що в кожному конкретному випадку для кожного об'єкта визначаються імовірні загрози і моделі потенційних порушників – «провідників» цих загроз, включаючи можливі сценарії їх здійснення. Цей етап дуже складний, оскільки від служби безпеки вимагається для кожного об'єкта вибрати з кількох можливих типів один, на який і буде орієнтована ІСБ, що проектується.

Модель порушника – це абстрактний формалізований або неформалізований опис порушника.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо. При розробці моделі порушника визначаються:

–припущення щодо категорії осіб, до яких може належати порушник; – припущення щодо мотивів дій порушника (цілей, які він має);

–припущення щодо рівня кваліфікації та обізнаності порушника і його технічної оснащеності (щодо методів та засобів, які використовуються при здійсненні порушень);

–обмеження та припущення щодо характеру можливих дій порушників (за часом та місцем дії та інші).

Припускається, що за своїм рівнем порушник – це фахівець вищої кваліфікації, який має повну інформацію про систему. Зазвичай розглядаються 5 типів порушників. Спочатку їх поділяють на дві групи: зовнішні і внутрішні порушники. Серед зовнішніх порушників виділяють такі:

- добре озброєна й оснащена силова група, що діє і ззовні швидко і напролом;

- поодинокий порушник, що не має допуску на об’єкт і намагається діяти потайки й обережно, оскільки він усвідомлює, що сили реагування мають над ним переваги.

Серед потенційних внутрішніх порушників можна відзначити:

- допоміжний персонал об’єкта, що допущений на об’єкт, але недопущений до життєво важливого центру (ЖВЦ) АСУ;

- основний персонал, що допущений до ЖВЦ (найбільш небезпечний тип порушників);

- співробітників служби безпеки, які часто формально і не допущені до ЖВЦ, але реально мають достатньо широкі можливості для збору необхідної інформації і вчинення акції.

Має також розглядатися можливість змови між порушниками різних типів, що ще більше ускладнює задачу формалізації моделей порушника. Але слід відзначити, що такий поділ є дуже загальним, а також не всі групи мають важливе значення для всіх АС.

Серед внутрішніх порушників можна виділити такі категорії персоналу:

- користувачі (оператори) системи;

- персонал, що обслуговує технічні засоби (інженери, техніки);

- співробітники відділів розробки та супроводження ПЗ (прикладні та системні програмісти)

- технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти АС);

- співробітники служби безпеки;

- керівники різних рівнів та посадової ієрархії. Сторонні особи, що можуть бути порушниками: а) клієнти (представники організацій, громадяни); б) відвідувачі (запрошені з якого-небудь приводу);

- представники організацій, що займаються забезпеченням життєдіяльності організації (енерго-, водо-, теплопостачання і т. д.);

- представники конкуруючих організацій (іноземних служб) або особи, що діють за їхнім завданням; д) особи, які випадково або навмисно порушили пропускний режим (не маючи на меті порушити безпеку); е) будь-які особи за межами контрольованої зони.

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

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

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

Усіх порушників можна класифікувати за рівнем знань про АС:

- знає функціональні особливості АС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

- має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговуванням;

- має високий рівень знань у галузі програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;

- знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (методами та засобами, що використовуються):

- застосовує суто агентурні методи отримання відомостей;

- застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонент системи);

- використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути потайки пронесені через пости охорони;

- застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).

За часом дії:

- у процесі функціонування (під час роботи компонент системи);

- у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування і ремонтів і т.д.);

- як у процесі функціонування, так і в період неактивності компонент системи.

За місцем дії:

– без доступу на контрольовану територію організації;

– з контрольованої території без доступу до будівель та споруд;

– усередині приміщень, але без доступу до технічних засобів;

– з робочих місць кінцевих користувачів (операторів);

– з доступом у зону даних (баз даних, архівів тощо);

– з доступом у зону управління засобами забезпечення безпеки.

Враховуються також наступні обмеження і припущення про характер дій можливих порушників:

- робота з підбору кадрів і спеціальні заходи ускладнюють можливість створення коаліцій порушників, тобто об’єднання (змови)і цілеспрямованих дій з подолання системи захисту двох і більше порушників;

- порушник, плануючи спробу НСД, приховує свої несанкціоновані дії від інших співробітників;

НСД може бути наслідком помилок користувачів, системних адміністраторів, а також хиб прийнятої технології обробки інформації тощо.

Визначення конкретних характеристик можливих порушників є значною мірою суб’єктивним. Модель порушника, що побудована з урахуванням особливостей конкретної предметної галузі і технології обробки інформації, може бути подана перелічуванням кількох варіантів його образу. Кожний вид порушника має бути схарактеризований згідно з класифікаціями, наведеними вище. Всі значення характеристик мають бути оцінені (наприклад, за 5бальною системою) і зведені до відповідних форм.

Однак при формуванні моделі порушника на її виході обов’язково повинні бути визначені: імовірність реалізації загрози, своєчасність виявлення і відомості про порушення. Слід звернути увагу на те, що всі злочини, зокрема і комп’ютерні,здійснюються людиною. Користувачі АС є її складовою, необхідним елементом. З іншого ж боку, вони є основною причиною і рушійною силою порушень і злочинів. Отже, питання безпеки захищених АС фактично є питанням людських відносин та людської поведінки.

На підставі викладеного для вибору вихідної моделі поводження потенційного порушника доцільний диференційований підхід. Оскільки

кваліфікація порушника - поняття досить відносне і наближене, можна взяти за основу чотири класи безпеки:

1-й клас – для захисту життєво важливої інформації, витік, руйнування або модифікація якої можуть призвести до втрат для користувача. Міцність розрахована на порушника – професіонала.

2-й клас – використовується для захисту важливої інформації при роботі декількох користувачів, що мають доступ до різних масивів даних або формуючих свої файли, недоступні іншим користувачам. Міцність розрахована на порушника високого класу, але непрофесіонала.

3-й клас рекомендується для захисту щодо важливої інформації, постійний НСД до якої шляхом її нагромадження може привести до витоку і більш важливої інформації. Міцність захисту при цьому повинна бути розрахована на відносно кваліфікованого порушника – непрофесіонала.

4-й клас рекомендується для захисту іншої інформації, що не представляє інтересу для серйозних порушників.

Однак його необхідність диктується дотриманням технологічної дисципліни обліку й обробки інформації службового користування з метою захисту від НСД.

Реалізація перерахованих рівнів безпеки повинна забезпечуватися набором відповідних засобів захисту, що перекривають визначену кількість можливих каналів НСД відповідно до очікуваного класу потенційних порушників. Рівень безпеки захисту усередині класу забезпечується кількісною оцінкою міцності окремих засобів захисту й оцінкою міцності контуру захисту від навмисних засобів захисту й оцінкою міцності контуру захисту від навмисного НСД.

Рисунок 1.5 – Види загроз

1.4.1 Модель порушника

Під порушником розуміється особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим наміром або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Модель порушника визначається сукупністю відомостей, що відображають його практичні та потенційні можливості, апріорні знання, час та місце дії тощо;

– припущення щодо категорії осіб, до яких може належати порушник;

– припущення щодо мотивів дій порушника;

– припущення щодо рівня кваліфікації та обізнаності порушника та його технічної оснащеності (щодо методів та засобів, які використовуються при здійсненні порушень);

– обмеження та припущення щодо характеру можливих дій порушника (за часом та місцем дії та ін.).

Модель порушника, яку побудовано з урахуванням особливостей даної автоматизованої системи, технологій обробки інформації, складу технічного персоналу та користувачів характеризується сукупністю значень перелічених характеристик, що зведені до таблиць 4.1–4.5. Сукупність цих характеристик визначає профіль можливостей порушника.

Графа «Рівень загроз» зазначених таблиць визначає відносну оцінку можливих збитків, які може заподіяти порушник за умов наявності відповідних характеристик. Рівень збитків характеризується наступними категоріями: 1 – незначні, 2 – середні, 3 – значні, але здебільшого припустимі, 4 – дуже значні.

Таблиця 4.1 – Класифікація порушників щодо можливостей доступу до технічних засобів АС

Позначення	Визначення категорії	Рівень загрози
ПВ1	Адміністратор безпеки	4
ПВ2	Системний адміністратор	4
ПВ3	Користувач	0

Таблиця 4.2 – Класифікація порушників щодо мотивів здійснення порушень

Позначення	Мотив порушення	Рівень загрози
М1	Безвідповідальність	2
М2	Самоствердження	3
М3	Корисний інтерес	4

Таблиця 4.3 – Класифікація порушників щодо кваліфікації та обізнаності, щодо АС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи	1
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем	2
К4	Знає структуру, функції та механізми дії	3

	спеціалізованих засобів захисту, їх недоліки	
К5	Знає недоліки та вади механізмів захисту, які вбудовано у системне програмне забезпечення та його не документовані можливості	З

Таблиця 4.4 – Класифікація порушників щодо можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загрози
З1	Використовує тільки відомості, що були отримані від авторизованих користувачів системи внаслідок їх необережності або безвідповідальності (ідентифікатори доступу та ін.).	2
З2	Використовує лише штатні засоби АС та недоліки в проектуванні системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів).	3
З3	Використовує для НСД як штатні засоби АС так і способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, впровадження і використання спеціального ПЗ збору, пересилання або блокування даних, дезорганізації систем обробки інформації тощо).	4

На основі припущень щодо характеристик порушника, наведених на початку розділу розроблені профілі можливостей порушника.

Найбільш суттєвими припущеннями, які зроблені при розробці профілів порушників, є те, що мотивація дій внутрішніх порушників обмежується безвідповідальністю користувачів. За цих умов виключається можливість цілеспрямованих дій щодо порушення політики безпеки порушника з числа адміністраторів, які є найбільш небезпечними щодо безпеки інформації.

Профілі можливостей порушників всіх категорій наведені в таблиці 4.6. У графі «Ефективний рівень загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 4.5 – Профілі можливостей порушників

Позначення	Визначення категорії	Характер дії порушника				Ефективний рівень загроз
		Мотив порушення	Класифікація	Можливості	Час дії	
ПВ1	Адміністратор безпеки	М1	К3	З3	Ч1-Ч4	4
ПВ2	Системний адміністратор	М1	К3	З3	Ч1-Ч4	4
ПВ3	Користувач	М2	К1	З2	Ч3	2

1.4.2 Модель загроз

При описі загроз суттєвих для АС використовується загальна класифікація загроз за такими ознаками:

За результатом впливу на інформацію та систему її обробки загрози згідно з нормативними документами системи ТЗІ (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) поділяються на чотири класи:

– порушення конфіденційності інформації (отримання інформації користувачами або процесами всупереч встановленим правилам доступу);

– порушення цілісності інформації (повне або часткове знищення, викривлення, модифікація, нав’язування хибної інформації);

– порушення доступності інформації (часткова або повна втрата працездатності системи, блокування доступу до інформації);

– втрата спостереженості або керованості системи обробки (порушення процедур ідентифікації та автентифікації користувачів та процесів, падання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).

1. За джерелом всі загрози поділяються на природні та техногенні (рис.1.6).

– природні загрози спричиняються стихійними природними явищами та об’єктивними фізичними процесами;

– техногенні загрози є наслідком діяльності людини, технічних засобів і систем.

2. За мотивами походження техногенні загрози поділяються на випадкові та навмисні:

– випадкові загрози спричиняються помилками проектування автоматизованої системи та системи захисту інформації, помилками у програмному забезпеченні, збоями та відмовами апаратури та систем забезпечення, помилками персоналу тощо;

– навмисні загрози зумовлені цілеспрямованими діями людей (порушників). Навмисні загрози здійснюються, як правило, при проникненні в приміщення, де розташовані засоби обробки та збереження інформації.

3. За типом основного засобу, який використовується для реалізації загрози, всі джерела загроз поділяються на наступні групи:

– людина;

– апаратура;

– програма; фізичне середовище.

Рисунок 1.6 – Класифікація загроз безпеці інформації

Однією з найбільш суттєвих ознак наведеної вище класифікації з точки зору можливостей порушника, що виконує спробу реалізації такої загрози, та засобів захисту, що повинні бути застосовані, є розміщення джерела загрози. Нижче наведений неформалізований опис техногенних загроз, що вважаються найбільш актуальними для АС.

2 ОСНОВНІ ПОЛОЖЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Поняття інформаційної безпеки

Перш ніж говорити про інформаційну безпеку необхідно визначитися з поняттям “інформація”. Це поняття сьогодні вживається дуже широко і різнобічно. Важко знайти таку галузь знань, де б воно не використовувалося. Повсякденно під час здійснення різних видів діяльності користуються таким поняттям:

Інформація – нові дані про людей, предмети, факти, події, явища і процеси незалежно від форми їхнього представлення.

У галузі інформаційних систем рекомендується таке означення інформації:

Інформація – це відомості, які є об’єктом зберігання, передавання і оброблення.

Відомо, що інформація може мати різну форму, зокрема, дані в комп’ютерах, листи, пам'ятні записи, досьє, формули, креслення, діаграми, моделі продукції, дисертації, судові документи й ін.

Як і всякий продукт, інформація має споживачів, що потребують її, і тому володіє певними споживчими якостями, а також має і своїх власників або виробників.

Відповідно до різноманітності поняття інформації, словосполучення “інформаційна безпека” в різних контекстах може мати різний сенс. Так, у Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” наводиться таке поняття інформаційної безпеки:

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Спеціальне законодавство в галузі безпеки інформаційної діяльності представлено низкою законів. У їхньому складі особливе місце належить базовому Закону “Про інформацію, інформатизацію і захист інформації”, що закладає основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

- інформації та інформаційних систем;

- суб’єктів – учасників інформаційних процесів;

- правовідносин виробників – споживачів інформаційної продукції;

- власників інформації – обробників і споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян і держави.

Інформаційна безпека (ІБ) – це стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб’єктам інформаційних відносин, зокрема, власникам і користувачам інформації та інфраструктури.

Таким чином, правильний з методологічної точки зору підхід до проблем ІБ починається з виявлення суб’єктів інформаційних відносин та інтересів цих суб'єктів, пов’язаних з використанням інформаційних систем (ІС). Загрози інформаційній безпеці – це зворотна сторона використання інформаційних технологій.

Забезпечення захисту інформації в АС є однією з головних характеристик його функціонування. У випадку виникнення можливості реалізації будь-якої з перелічених вище загроз, має бути вжито усіх заходів щодо усунення такої можливості. У випадку неможливості попередити витік інформації, вживаються заходи щодо припинення обробки інформації та евакуації обладнання АС, що містить носії даних з інформацією.

Політика безпеки інформації реалізується шляхом впровадження комплексу організаційних, технічних заходів, відповідних програмних засобів, а також заходів контролю за виконанням встановлених правил політики безпеки.

Безпосередня реалізація політики безпеки інформації покладається на адміністратора безпеки АС.

Організаційні заходи захисту інформації - це комплекс адміністративних та обмежуючих заходів, регламентуючих діяльність персоналу та порядок функціонування засобів забезпечення інформаційної діяльності та засобів захисту інформації. Вони містять в собі:

–впровадження періодичної зміни паролів (раз на місяць - у всіх користувачів, а в разі виявлення адміністратором безпеки передумов компрометації паролів – негайно у користувача, стосовно якого ці передумови виникли);

- планування та проведення занять з підвищення професійної підготовки співробітників, задіяних в експлуатації АС;

- розробку Інструкції на випадок надзвичайних ситуацій, яка повинна передбачати:

- порядок оповіщення посадових осіб;

- дії персоналу у кожній надзвичайній ситуації;

- порядок відкриття приміщень, в яких розміщені технічні засоби та резервні копії програмного забезпечення, інформаційних масивів АС у випадку надзвичайних ситуацій;

- черговість та порядок евакуації технічних засобів та машинних носіїв з ІзОД, визначення місць їх подальшого зберігання;

- порядок допуску на територію робітників аварійних служб;

- порядок знищення конфіденційної та службової інформації у надзвичайних ситуаціях.

Програмні засоби захисту – це сукупність програмних засобів, призначених для реалізації політики безпеки. Структура комплексу засобів захисту зображено на рис. 2.1.

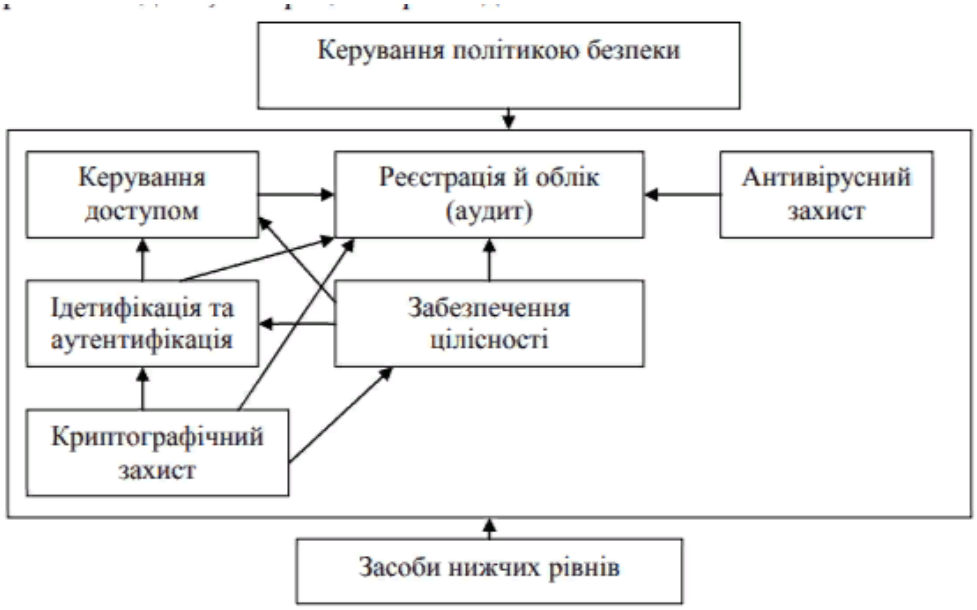

Рисунок 2.1 - Структура комплексу засобів захисту

Ці засоби вирішують завдання:

– ідентифікації та автентифікації користувачів, що намагаються отримати доступ до АС;

– надання користувачам доступу до об’єктів та процесів АС у відповідності до їх повноважень;

– спостереження дій користувачів в журналі аудиту КЗЗ, де фіксуються події, важливі з точки зору забезпечення безпеки оброблюваної інформації. Доступ до журналу аудиту наданий тільки адміністратору безпеки АС.

2.1.1 Основні задачі інформаційної безпеки

Інформаційна безпека – це багатогранна галузь діяльності, в якій успіх може принести тільки систематичний, комплексний підхід.

Основними задачами інформаційної безпеки є:

- забезпечення доступності інформації;
- забезпечення цілісності інформації;
- забезпечення конфіденційності інформації;
- забезпечення вірогідності інформації;

- забезпечення юридичної значимості інформації, представленої у вигляді електронного документа;

- забезпечення невідстежуваності дій користувача.

Доступність – це властивість інформаційного об’єкта щодо одержання його користувачем за прийнятний час.

Інформаційні системи створюються для отримання певних інформаційних послуг. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це, очевидно, завдає збитку всім суб’єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент інформаційної безпеки.

Особливо яскраво основна роль доступності виявляється в різного роду системах управління виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки – і матеріальні, і моральні – може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіа-квитків, банківські послуги тощо).

Цілісність – це властивість інформаційного об’єкта зберігати свою структуру і/або зміст у процесі передавання і зберігання.

Розрізняють цілісність статичну (тобто незмінність інформаційних об’єктів) і динамічну (стосується коректного виконання складних дій (транзакцій). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі по-току фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.

Цілісність є найважливішим аспектом ІБ в тих випадках, коли інформація служить “керівництвом до дії”. Рецептура ліків, зміст медичних процедур, набір і характеристики комплектуючих виробів, хід технологічного процесу – все це приклади інформації, порушення цілісності якої може призвести до небажаних наслідків. Неприємно і спотворення офіційної інформації, будь то текст закону або сторінка Web-сервера якої-небудь урядової організації.

Конфіденційність – це властивість інформації бути доступною тільки обмеженому колу користувачів інформаційної системи, в якій циркулює дана інформація.

Конфіденційність – найбільш опрацьований у нашій країні аспект інформаційної безпеки. На жаль, практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем пов’язана із серйозними труднощами. По-перше, відомості про технічні канали витоку інформації є закритими, тому більшість користувачів позбавлено можливості мати уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії, як основного засобу забезпечення конфіденційності, стоять численні законодавчі перепони і технічні проблеми.

Вірогідність – це властивість інформації, яка полягає у строгій приналежності об’єкту, що є її джерелом, або тому об’єкту, від якого ця інформація прийнята.

Юридична значимість – це властивість інформації, представленої у вигляді електронного документа, мати юридичну силу.

З цією метою суб’єкти, що мають потребу в підтвердженні юридичної значимості переданого повідомлення, домовляються про прийняття деяких атрибутів інформації, що описують її здатність бути юридично значимою. Дана властивість інформації особливо актуальна в системах електронних платежів, де здійснюється операція з пересилання коштів.

Невідстежуваність – це здатність користувача робити деякі дії в інформаційній системі непомітно для інших об'єктів.

Актуальність даної вимоги виникла завдяки появі таких понять, як електронні гроші та Internet-banking. Так, для авторизації доступу до електронної платіжної системи користувач повинен надати деякі відомості, що однозначно його ідентифікують. У процесі розвитку даних систем може з’явитися реальна небезпека, що, наприклад, усі платіжні операції будуть контролюватися, тим самим виникнуть умови для тотального стеження за користувачами інформаційних систем.

Існує кілька шляхів вирішення проблеми неможливості стеження:

- заборона за допомогою законодавчих актів будь-якого тотального стеження за користувачами інформаційних систем;

- застосування криптографічних методів для підтримки неможливості слідкування.

Інформаційна безпека може розглядатися не тільки стосовно деяких конфіденційних відомостей, але і стосовно здатності інформаційної системи виконувати задані функції.

Інформаційна безпека в рамках забезпечення працездатності ІС повинна забезпечувати захист від:

- порушення функціонування інформаційної системи шляхом впливу на інформаційні канали, канали сигналізації, керування і віддаленого завантаження баз даних, комутаційного устаткування, системне і прикладне програмне забезпечення;

- несанкціонованого доступу до інформаційних ресурсів і від намагань використання ресурсів мережі, що призводять до витоку даних, порушення цілісності мережі й інформації, зміни функціонування під-систем розподілу інформації, доступності баз даних;

- руйнування засобів захисту, що вбудовуються, і зовнішніх засобів;

- неправомірних дій користувачів і обслуговуючого персоналу мережі.

Пріоритети серед перерахованих задач інформаційної безпеки визначаються індивідуально для кожної конкретної ІС і залежать від вимог, що висуваються безпосередньо до інформаційних систем.

Якщо повернутися до аналізу інтересів різних категорій суб’єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, на першому місці стоїть доступність. Практично не поступається їй за важливістю цілісність – який сенс в інформаційній послузі, якщо вона містить спотворені відомості?

З погляду державних структур захисні заходи в першу чергу покликані забезпечити конфіденційність, цілісність і доступність інформації.

Комерційним структурам, ймовірно, важливіше всього цілісність і доступність даних і послуг. На відміну від державних, комерційні організації більш відкриті і динамічні, тому ймовірні загрози для них відрізняються не тільки кількістю, але і якістю.

Для розв'язання задач забезпечення безпеки в інформаційних системах необхідно:

- захистити інформацію під час її зберігання, оброблення і передавання мережею;

- підтвердити дійсність об'єктів даних і користувачів (автентифікація сторін, що встановлюють зв'язок);

- знайти і попередити порушення цілісності об'єктів даних;

- захистити технічні пристрої і приміщення;

- захистити конфіденційну інформацію від витоку і від вбудованих електронних пристроїв знімання інформації;

- захистити програмні засоби від під'єднання програмних закладок і вірусів;

- захистити від несанкціонованого доступу до інформаційного ресурсу і технічних засобів мережі, зокрема, до засобів керування, щоб запобігти зниженню рівня захищеності інформації і самої мережі в цілому;

- організувати заходи, що спрямовані на забезпечення збереження конфіденційних даних.

Конкретна реалізація загальних принципів забезпечення інформаційної безпеки може полягати в організаційних або технічних заходах захисту інформації.

2.1.2 Важливість і складність проблеми інформаційної безпеки

Інформаційна безпека є одним з найважливіших аспектів інтегральної безпеки, на якому б рівні ми не розглядали останню – національному, галузевому, корпоративному або персональному.

Для ілюстрації цього положення наведемо кілька прикладів.

- з'явилася інформація про те, що планується терористична атака на Нью-Йоркську біржу. Ціллю терористів є комп'ютерні системи, що зберігають і працюють з інформацією про торгові операції в США та Європі. Наслідки такої операції можуть призвести до кризи світового масштабу. (З інтерв'ю з М. Дюре, директором Центру інформації та документації НАТО в Україні);

- американський ракетний крейсер "Йорктаун" був змушений повернутися в порт через численні проблеми з програмним забезпеченням, що функціонувало на платформі Windows NT. Таким виявився побічний ефект програми ВМФ США з максимально широкого використання комерційного програмного забезпечення з метою зниження вар-тості військової техніки;

- у лютому 2001 року двоє колишніх співробітників компанії Commerce One, скориставшись паролем адміністратора, видалили з сервера файли, що складали крупний (на декілька мільйонів доларів) проект для іноземного замовника. На щастя, була резервна копія проекту, тому реальні втрати обмежилися витратами на слідство і засоби захисту від подібних інцидентів в майбутньому. У серпні 2002 року злочинці постали перед судом.

- британський спеціаліст з інформаційних технологій Максвелл Парсонс отримав 2,5 року ув'язнення за злам банкоматів за допомогою MP3-плеєра і спеціального програмного забезпечення. Таким чином він отримував конфіденційну інформацію про банківські рахунки клієнтів для клонування кредитних карток;

- американські військові оголосили про створення Командного центру кіберпростору ВВС США (U.S. Air Force Cyberspace Command) для захисту країни від онлайнових загроз з Інтернету;

- невідомі "жартівники" скористалися принципами роботи онлайнової енциклопедії Wikipedia для розповсюдження шкідливого програмного забезпечення – нової модифікації вірусу Blaster;

- одна студентка втратила стипендію в 18 тисяч доларів в Мічиганському університеті через те, що її сусідка по кімнаті скористалася їх загальним

системним входом і відправила від імені своєї жертви електронний лист з відмовою від стипендії.

При аналізі проблематики, пов’язаної з інформаційною безпекою, необхідно зважати на специфіку даного аспекту безпеки, яка полягає в тому, що ІБ є складовою частиною інформаційних технологій, – галузі, що розвивається безпрецедентно високими темпами.

На жаль, сучасна технологія програмування не дозволяє створювати безпомилкові програми, що не сприяє швидко-му розвитку засобів забезпечення ІБ. Слід виходити з того, що необхідно конструювати надійні системи ІБ із залученням ненадійних компонентів (програм). У принципі, це можливо, але вимагає дотримання певних архітектурних принципів і контролю стану захищеності протягом усього життєвого циклу ІС.

Наведемо ще декілька цифр.

- у березні 1999 року був опублікований черговий, четвертий річний звіт «Комп'ютерна злочинність і безпека-1999: проблеми і тенденції» (Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey). У звіті наголошувалося на різкому зростанні кількості звернень у правоохоронні органи з приводу комп'ютерних злочинів (32% з кількості опитаних); 30% респондентів повідомили про те, що їх інформаційні системи були зламані зовнішніми зловмисниками; атакам через Internet піддавалися 57% опитаних; у 55% випадках наголошувалося про порушення з боку власних співробітників. Примітно, що на питання “чи були зламані ваші Web-сервери і системи електронної комерції за останні 12 місяців? ” 33% респондентів відповіли “не знаю”.

- у аналогічному звіті, опублікованому в квітні 2002 року, цифри змінилися, але тенденція залишилася такою самою: 90% респондентів (переважно з крупних компаній і урядових структур) повідомили, що за останні 12 місяців в їх організаціях мали місце порушення інформаційної безпеки; 80% респондентів констатували фінансові втрати від цих порушень; 44% (223 респонденти) змогли та/або захотіли оцінити втрати кількісно (загальна сума склала більше 455 млн.

доларів). Найбільшого збитку завдали крадіжки і фальсифікації (більше 170 і 115 млн. доларів відповідно).

Збільшення кількості атак – це не найбільша неприємність. Гірше те, що постійно виявляються нові вразливі місця в програмному забезпеченні і, як наслідок, з'являються нові види атак.

У таких умовах системи ІБ повинні мати можливість протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, атакам автоматизованим і скоординованим. Іноді напад триває частки секунди, а інколи пошук вразливих місць розтягується на години і підозріла активність практично непомітна. Метою зловмисників може бути порушення всіх складових ІБ – доступності, цілісності і конфіденційності.

2.1.3 Об'єктно-орієнтований підхід до інформаційної безпеки

У теперішній час ІБ є відносно замкнутою дисципліною, розвиток якої не завжди синхронізований із змінами в інших галузях інформаційних технологій. Зокрема, в ІБ поки не знайшли віддзеркалення основні положення об'єктно-орієнтованого підходу, що став основою для побудови сучасних інформаційних систем.

Спроби створення великих систем ще в 60-х роках минулого століття розкрили численні проблеми програмування, головна з яких є складність створюваних і супроводжуваних систем. Результатами досліджень у галузі технології програмування стали спочатку структуроване програмування, потім об'єктно-орієнтований підхід.

Об'єктно-орієнтований підхід є основою сучасної технології програмування, випробуваним методом боротьби зі складністю систем.

Складність має двояку природу. По-перше, складні не тільки апаратно-програмні системи, які необхідно захищати, але і самі засоби безпеки. По-друге, швидко зростає складність сімейства нормативних документів, таких, на-приклад, як профілі захисту на основі "Загальних критеріїв", мова про які попереду. Ця

складність менш очевидна, але нею також не можна нехтувати – необхідно спочатку будувати сімейства документів за об’єктним принципом.

Будь-який розумний метод боротьби зі складністю спи-рається на принцип “Divide et impera” – “розділяй і володарюй”. У даному контексті цей принцип означає, що складна система інформаційної безпеки на верхньому рівні повинна складатися з невеликої кількості відносно незалежних компонентів. Потім декомпозиції піддаються виділені на першому етапі компоненти, і так далі – до заданого рівня деталізації. Результатом є система у вигляді ієрархії з декількома рівнями абстракції.

Об’єктно-орієнтований підхід використовує об’єктну декомпозицію, тобто, поведінка системи описується в тер-мінах взаємодії об’єктів.

Об’єкти реального світу володіють, як правило, декількома відносно незалежними характеристиками. Стосовно об’єктної моделі такі характеристики називаються гранями. Ми вже стикалися з трьома основними гранями ІБ – доступністю, цілісністю і конфіденційністю.

Поняття рівня деталізації важливе не тільки для візуалізації об’єктів, але і для систематичного розгляду складних систем, представлених в ієрархічному вигляді. Саме по собі воно дуже просте: якщо черговий рівень ієрархії розглядається з рівнем деталізації $n>0$, то наступний – з рівнем $(n-1)$. Об’єкт з рівнем деталізації 0 вважається атомарним.

Поняття рівня деталізації показу дозволяє розглядати ієрархії потенційно нескінченні заввишки, варіювати деталізацію як об’єктів у цілому, так і їх граней.

Покажемо яким чином можна застосувати об’єктно-орієнтований підхід до питань інформаційної безпеки.

Фактично три грані ІБ вже було введено: це доступність, цілісність і конфіденційність. Їх можна розглядати відносно незалежно, і вважається, що якщо всі вони забезпечені, то забезпечена і ІБ у цілому.

Таким чином, ми структурували нашу мету. Тепер потрібно структурувати засоби її досягнення. Введемо такі грані:

- законодавчі заходи забезпечення інформаційної безпеки;

- адміністративні заходи (накази та інші дії керівництва організацій, пов’язаних з інформаційними системами, що захищаються);

- організаційні (процедурні) заходи (заходи безпеки, орієнтовані на людей);

- інженерно-технічні заходи.

Виходячи з цього, маємо таке поняття.

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

Далі кожна з виділених граней буде розглядатися детальніше. Тут же відзначимо, що, в принципі, їх можна розглядати і як результат варіювання рівня деталізації. Тому в подальшому будуть вживатися словосполучення “законодавчий рівень”, “адміністративний рівень” і т.п.).

Закони і нормативні акти орієнтовані на всіх суб’єктів інформаційних відносин незалежно від їх організаційної приналежності (це можуть бути як юридичні, так і фізичні особи) в межах країни, адміністративні заходи – на всіх суб‘єктів у межах організації, процедурні – на окремих людей (або невеликі категорії суб’єктів), інженерно-технічні – на устаткування і програмне забезпечення.

Продемонструємо тепер, як можна розглядати систему захисту ІС, варіюючи рівень деталізації.

Нехай інтереси суб’єктів інформаційних відносин концентруються навколо ІС певної організації, яка має у своє-му розпорядженні два територіально рознесені виробничі майданчики, на кожному з яких є сервери, що обслуговують своїх і зовнішніх користувачів. Один з майданчиків обладнаний зовнішнім підключенням (тобто має вихід в Internet).

Нульовому рівню деталізації відповідає інформаційна система в цілому. Вже тут необхідно врахувати закони, за-стосовні до організацій, що мають в своєму розпорядженні інформаційні системи. Можливо, яку-небудь інформацію не можна зберігати і обробляти на комп’ютерах, якщо ІС не була атестована на відповідність певним вимогам.

На адміністративному рівні можуть декларуватися цілі, заради яких створювалася ІС, загальні правила закупівель, впровадження нових компонентів, експлуатації і т.п.

На процедурному рівні потрібно визначити вимоги до фізичної безпеки ІС і шляхи їх виконання, правила проти-пожежної безпеки тощо.

На інженерно-технічному рівні можуть бути визначені переважні апаратно-програмні платформи тощо.

На першому рівні деталізації визначаються сервіси і користувачі, або, інакше кажучи, здійснюється поділ на клієнтську і серверну частину (рис. 2.2).

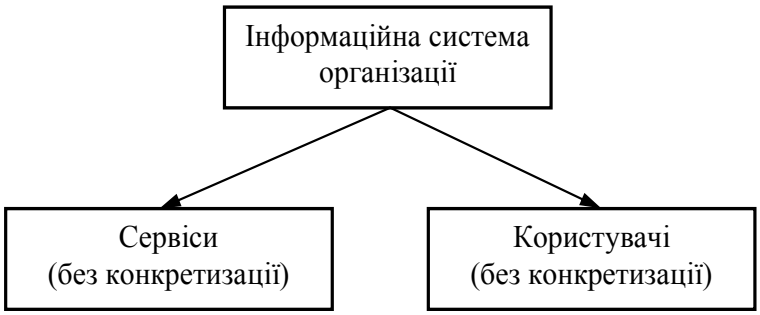

Рисунок 2.2 – ІС при розгляді з рівнем деталізації 1

На цьому рівні потрібно сформулювати вимоги до сервісів (до їх наявності, до доступності, цілісності і конфіденційності інформаційних послуг, що надаються), викласти способи виконання цих вимог, визначити загальні прави-ла поведінки користувачів, необхідний рівень їх попередньої підготовки, методи контролю їх поведінки, порядок заохочення і покарання тощо. Можуть бути сформульовані вимоги і переваги щодо серверних і клієнтських платформ.

На другому рівні деталізації (рис.2.3) ще не описується внутрішня структура ІС організації і деталі Internet. Констатується тільки існування зв’язку між цими мережами, наявність в них користувачів, а також внутрішніх та зовнішніх сервісів без опису їхнього змісту.

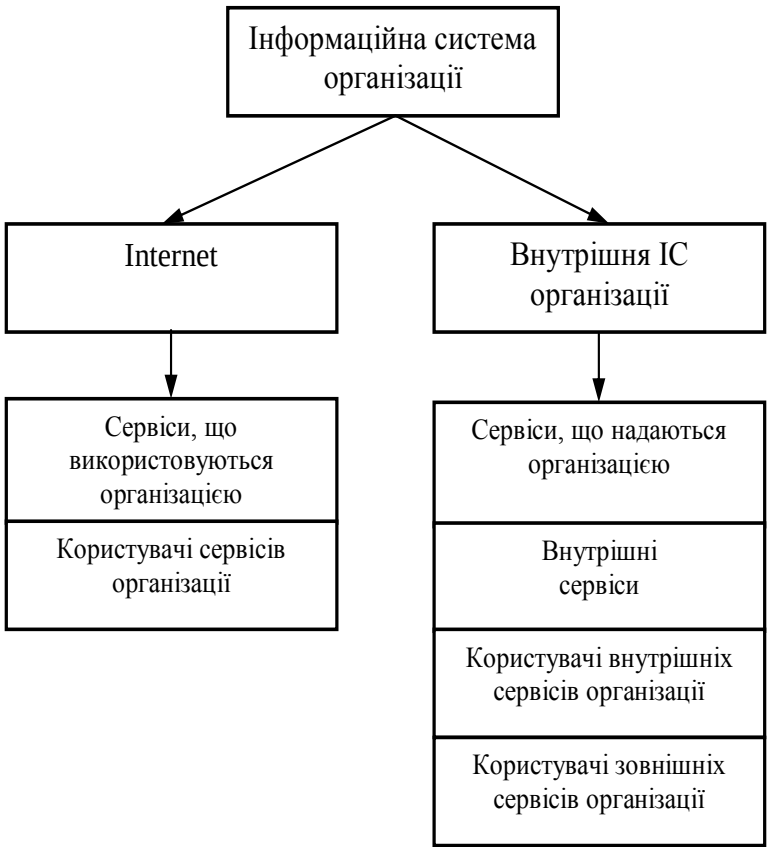

Рисунок 2.3 – ІС при розгляді з рівнем деталізації 2

Для рівня деталізації 2, повинні враховуватися закони, застосовні до організацій, ІС яких забезпечені зовнішніми підключеннями. Мова йде про допустимість такого підключення, про його захист, про відповідальність користувачів, що звертаються до зовнішніх сервісів, і про відповідальність організацій, що відкривають свої сервіси для зовнішнього доступу. Конкретизація аналогічної спрямованості, з урахуванням наявності зовнішнього підключення, повинна бути виконана на адміністративному, процедурному і інженерно-технічному рівнях.

2.1.4 Контроль виконання вимог безпеки

Метою контролю є забезпечення в процесі обробки конфіденційної та службової інформації з використанням АС вимог політики безпеки та плану захисту інформації.

Зазначений контроль здійснюється за такими основними формами: щорічний, щоквартальний, щомісячний, щотижневий, щоденний.

Крім цього, у разі необхідності може проводитись позаплановий контроль.

Контроль здійснюється адміністратором безпеки із залученням, у разі необхідності, співробітників інших підрозділів.

2.1.5 Правила розмежування доступу

Аналізуючи ризики для АС, що потребує захисту, які можуть виникнути в процесі її використання можна сформувати наступні правила розмежування доступу:

– виконання правил розмежування доступу забезпечується застосуванням КЗЗ та організаційними заходами;

– усі особи, які беруть участь в обробленні ІзОД в АС, повинні бути зареєстровані як користувачі АС;

– надання доступу до ІзОД здійснюється з урахуванням наданих згідно зі службовою необхідністю повноважень, за умови достовірного розпізнавання користувачів АС встановленим КЗЗ. КЗЗ забезпечує можливість своєчасного доступу зареєстрованих користувачів АС до ІзОД;

– кожний користувач АС може мати носії ІзОД, які закріплені за ним персонально;

На підставі розглянутих у попередніх розділах моделей загроз та можливого порушника та враховуючи вимоги до політики безпеки та параметрів КСЗІ можна запропонувати наступну структуру КСЗІ на підприємстві, сфера діяльності якого – надання адміністративних послуг. Компоненти КСЗІ показані на рис.2.4.

Рисунок 2.4 – Компоненти комплексної системи захисту інформації

2.2 Поняття системи захисту інформації

Існуючий на теперішній час значний практичний досвід у сфері захисту інформації показує, що потрібна прозора і цілеспрямована організація процесу захисту інформацій-них ресурсів. Причому в цьому повинні активно брати участь професійні фахівці, адміністрація, співробітники і користувачі, що і визначає підвищену значимість організаційної сторони питання.

Відповідно до цього захист будується на основі системного підходу до інформаційної безпеки.

Система захисту інформації – це організована сукупність спеціальних установ, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

Досвід показує, що забезпечення безпеки інформації не може бути одноразовим актом. Це неперервний процес, який полягає в обґрунтуванні і

реалізації найбільш раціональних методів, способів і шляхів удосконалення та розвитку системи захисту, неперервному контролі її стану, виявленні її вузьких і слабких місць, а також протиправних дій.

Безпека інформації може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту в усіх структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації. Найбільший ефект досягається тоді, коли всі використовувані засоби, методи і заходи поєднуються в єдиний цілісний механізм – систему захисту інформації (СЗІ). При цьому функціонування системи повинно контролюватися, обновлятися і доповнюватися залежно від зміни зовнішніх і внутрішніх умов.

Ніяка СЗІ не може забезпечити необхідного рівня без-пеки інформації без належної підготовки користувачів і до-тримання ними всіх установлених правил, спрямованих на її захист.

2.2.1 Вимоги до захисту інформації

З позицій системного підходу до захисту інформації висуваються певні вимоги. Захист інформації повинен бути:

- неперервним. Ця вимога виникає з того, що зловмисники тільки і шукають можливість, як би обійти захист інформації, що цікавить їх;
- плановим. Планування здійснюється шляхом розробки кожною службою детальних планів захисту інформації у сфері її компетенції з урахуванням загальної мети підприємства (організації);
- цілеспрямованим. Захищається тільки те, що повинно захищатися в інтересах конкретної мети, а не все підряд;
- конкретним. Захисту підлягають конкретні дані, що об’єктивно вимагають охорони, втрата яких може заподіяти організації певний збиток;
- активним. Захищати інформацію необхідно з доста-тнім ступенем наполегливості;

- надійним. Методи і форми захисту повинні надійно перекривати можливі шляхи неправомірного доступу до охоронюваних секретів, незалежно від форми їхнього представлення, мови вираження і виду фізичного носія, на якому вони закріплені;

- універсальним. Вважається, що залежно від виду каналу витоку або способу несанкціонованого доступу його необхідно перекривати, де б він не про-явився, розумними і достатніми засобами, незалежно від характеру, форми і виду інформації;

- комплексним. Для захисту інформації повинні застосовуватися всі види і форми захисту в повному обсязі. Неприпустимо застосовувати лише окремі форми чи технічні засоби. Комплексний характер за-хисту виникає з того, що захист – це специфічне явище, що є складною системою нерозривно взаємо-пов'язаних і взаємозалежних процесів, кожний з яких, у свою чергу, має безліч різних сторін, властивостей, тенденцій.

Закордонний і вітчизняний досвід показує, що для забезпечення виконання багатогранних вимог безпеки система захисту інформації повинна задовольняти такі умови:

- охоплювати весь технологічний комплекс інформаційної діяльності;

- бути різноманітною за використовуваними засобами, багаторівневою з ієрархічною послідовністю доступу;

- бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;

- бути нестандартною, різноманітною. Вибираючи засоби захисту не можна розраховувати на непоінформованість зловмисників щодо її можливостей;

- бути простою для технічного обслуговування і зручною для експлуатації користувачами;

- бути надійною. Будь-які несправності технічних засобів є причиною появи неконтрольованих каналів витоку інформації;

- бути комплексною, мати цілісність, що означає, що жодна її частина не може бути вилучена без втрат для всієї системи.

До системи безпеки інформації висуваються також певні вимоги:

- чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;
- надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;
- зведення до мінімуму кількості спільних для декількох користувачів засобів захисту;
- облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;
- забезпечення оцінювання ступеня конфіденційної інформації;
- забезпечення контролю цілісності засобів захисту і негайне реагування на вихід їх з ладу.

2.2.2 Види забезпечення системи захисту інформації

Система захисту інформації як будь-яка система повинна мати певні види власного забезпечення, спираючись на які вона буде виконувати свою цільову функцію. Враховуючи це, СЗІ повинна мати:

- правове забезпечення. Сюди входять нормативні документи, положення, інструкції, посібники, вимоги яких є обов'язковими в рамках сфери їх дій;
- організаційне забезпечення. Мається на увазі, що реалізація захисту інформації здійснюється певними структурними одиницями – такими, як служба захисту документів; служба режиму, допуску, охорони; служба захисту інформації технічними засобами; інформаційно-аналітична діяльність і ін.;
- апаратне забезпечення. Передбачається широке використання технічних засобів як для захисту інформації, так і для забезпечення діяльності власне СЗІ;
- інформаційне забезпечення. Воно містить у собі відомості, дані, показники, параметри, які лежать в ос-нові розв’язання задач, що забезпечують функціонування системи. Сюди можуть входити як показники доступу, обліку,

зберігання, так і системи інформаційного забезпечення розрахункових задач різного характеру, пов’язаних з діяльністю служби забезпечення безпеки;

- програмне забезпечення. До нього належать різні інформаційні, облікові, статистичні і розрахункові програми, що забезпечують оцінювання наявності і небезпеки різних каналів витоку і шляхів несанкціонованого проникнення до джерел конфіденційної інформації;

- математичне забезпечення. Припускає використання математичних методів для різних розрахунків, пов’язаних з оцінюванням небезпеки технічних засобів зловмисників, зон і норм необхідного захисту;

- лінгвістичне забезпечення. Сукупність спеціальних мовних засобів спілкування фахівців і користувачів у сфері захисту інформації;

- нормативно-методичне забезпечення. Сюди входять норми і регламенти діяльності органів, служб, засобів, які реалізують функції захисту інформації, різного роду методики, що забезпечують діяльність користувачів при виконанні своєї роботи в умовах жорстких вимог захисту інформації.

Задовольнити сучасні вимоги до забезпечення безпеки підприємства може тільки система безпеки.

Система безпеки – це організована сукупність спеціальних установ, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз.

Як і будь-яка система, система інформаційної безпеки має свої мету, задачі, методи і засоби діяльності, що узгоджуються за місцем і часом, залежно від умов.

Антивірус – програмний засіб, призначений для боротьби з вірусами. Виходячи з визначення, основними завданнями антивірусу є:

- перешкоджання проникненню вірусів у комп’ютерну систему;

- виявлення наявності вірусів у комп’ютерній системі;

- усунення вірусів з комп’ютерної системи без нанесення ушкоджень іншим об’єктам системи;

- мінімізація збитку від дій вірусів.

Технології, застосовувані в антивірусах, можна розбити на дві групи:

- технології сигнатурного аналізу;

- технології імовірнісного аналізу.

Сигнатурний аналіз – метод виявлення вірусів, що полягає в перевірці наявності у файлах сигнатур вірусів. Сигнатурний аналіз є найбільш відомим методом виявлення вірусів і використається практично у всіх сучасних антивірусах. Для проведення перевірки антивірусу необхідний набір вірусних сигнатур, що зберігається в антивірусній базі. Антивірусна база – база даних, у якій зберігаються сигнатури вірусів.

Через те, що сигнатурний аналіз припускає перевірку файлів на наявність сигнатур вірусів, антивірусна база має потребу в періодичному відновленні для підтримки актуальності антивірусу. Сам принцип роботи сигнатурного аналізу також визначає границі його функціональності – можливість виявляти лише вже відомі віруси – проти нових вірусів сигнатурний сканер неспроможний.

З іншого боку, наявність сигнатур вірусів припускає можливість лікування інфікованих файлів, виявлених за допомогою сигнатурного аналізу. Однак, лікування припустиме не для всіх вірусів – трояни й більшість хробаків не піддаються лікуванню по своїх конструктивних особливостях, оскільки є цільними модулями, створеними для завдання збитків. Грамотна реалізація вірусної сигнатури дозволяє виявляти відомі віруси зі стовідсотковою ймовірністю. Технології імовірнісного аналізу у свою чергу підрозділяються на три категорії:

- евристичний аналіз;

- поведінковий аналіз;

- аналіз контрольних сум.

Евристичний аналіз – технологія, заснована на імовірнісних алгоритмах, результатом роботи яких є виявлення підозрілих об’єктів. У процесі евристичного аналізу перевіряється структура файлу, його відповідність вірусним шаблонам. Найбільш популярною евристичною технологією є перевірка вмісту файлу на предмет наявності модифікацій уже відомих сигнатур вірусів й їхніх комбінацій. Це допомагає визначати гібриди й нові версії раніше відомих вірусів без

додаткового відновлення антивірусної бази. Евристичний аналіз застосовується для виявлення невідомих вірусів, і, як наслідок, не припускає лікування. Дана технологія не здатна на 100% визначити вірус перед нею чи ні, і як будь—який імовірнісний алгоритм грішить помилковими спрацьовуваннями.

Поведінковий аналіз – технологія, у якій рішення про характер об'єкта, що перевіряє, приймається на основі аналізу виконуваних їм операцій. Поведінковий аналіз досить вузько застосуємо на практиці, тому що більшість дій, характерних для вірусів, можуть виконуватися й звичайними додатками. Найбільшу популярність одержали поведінкові аналізатори скріптів і макросів, оскільки відповідні віруси практично завжди виконують ряд однотипних дій. Наприклад, для впровадження в систему, майже кожен макровірус використає той самий алгоритм: у який—небудь стандартний макрос, що запускається автоматично середовищем Microsoft Office при виконанні стандартних команд (наприклад, «Save», «Save As», «Open», і т.д.), записується код, що заражає основний файл шаблонів normal.dot і кожен документ, що відкриває знову. Засоби захисту, що вшивають в BIOS, також можна віднести до поведінкових аналізаторів. При спробі внести зміни в MBR комп'ютера, аналізатор блокує дія й виводить відповідне повідомлення користувачеві. Крім цього поведінкові аналізатори можуть відслідковувати спроби прямого доступу до файлів, внесення змін у завантажувальний запис дискет, форматування жорстких дисків і т.д.

Поведінкові аналізатори не використають для роботи додаткових об'єктів, подібних до вірусних баз й, як наслідок, нездатні розрізняти відомі й невідомі віруси – всі підозрілі програми апріорі вважаються невідомими вірусами. Аналогічно, особливості роботи засобів, що реалізують технології поведінкового аналізу, не припускають лікування. Як й у попередньому випадку, можливе виділення дій, що однозначно трактуються як неправомірні – форматування жорстких дисків без запиту, видалення всіх даних з логічного диска, зміна завантажувального запису дискети без відповідних повідомлень й ін. Проте, наявність дій неоднозначних – наприклад, макрокоманда створення каталогу на

жорсткому диску, змушує також замислюватися про помилкові спрацьовування й, найчастіше, про тонке ручне настроювання поведінкового блокатора.

Аналіз контрольних сум – це спосіб відстеження змін в об’єктах комп’ютерної системи. На підставі аналізу характеру змін – одночасність, масовість, ідентичні зміни довжин файлів – можна робити вивід про зараження системи. Аналізатори контрольних сум (також використається назва «ревізори змін») як і поведінкові аналізатори не використають у роботі додаткові об’єкти й видають вердикт про наявність вірусу в системі винятково методом експертної оцінки. Більша популярність аналізу контрольних сум пов’язана зі спогадами про однозадачні операційні системи, коли кількість вірусів бути відносно невеликим, файлів було небагато й мінялися вони рідко. Сьогодні ревізори змін втратили свої позиції й використаються в антивірусах досить рідко. Частіше подібні технології застосовуються в сканерах при доступі – при першій перевірці з файлу знімається контрольна сума й міститься в кеші, перед наступною перевіркою того ж файлу сума знімається ще раз, рівняється, і у випадку відсутності змін файл уважається незараженим.

Підводячи підсумки огляду технологій, застосовуваних в антивірусах, відзначимо, що сьогодні практично кожен антивірус використає трохи з перерахованих вище технологій, при цьому використання сигнатурного й евристичного аналізу для перевірки файлів і саме в цьому порядку є повсюдним. Надалі засоби, що реалізують комбінацію сигнатурного й евристичного аналізу, ми будемо називати антивірусними сканерами.

Друга група технологій більше різнорідна, оскільки жоден із застосовуваних підходів не дає гарантії виявлення невідомих вірусів. Очевидно, що й спільне використання всіх цих технологій не дає такої гарантії. На сьогоднішній день кращим способом боротьби з новими погрозами є максимально швидке реагування розроблювачів на появу нових екземплярів вірусів випуском відповідних сигнатур. Також, з огляду на наявність активних шкідливих програм, необхідно не менш швидко реагувати на виявлення нових вразливостей в операційних системах і встановлювати відповідні латки безпеки. Антивірусні

програми за своїм призначенням поділяються на детектори, фаги, ревізори, фільтри та вакцини.

Криптографічний захист (шифрування) інформації (рис.2.5) – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. На відміну від тайнопису, яке приховує сам факт передавання повідомлення, зашифровані повідомлення передаються відкрито, приховується їхній зміст.

Рисунок 2.5 – Криптографічний захист

Методи криптографії поділяють на дві групи – підставлення (заміни) і переставлення. Підстановний метод передбачає, що кожна літера та цифра повідомлення замінюється за певним правилом на інший символ. Зокрема, для визначення порядку підставлення може використовуватись певне слово або фраза – ключ. У загальному випадку у криптографії ключ – це послідовність бітів, що використовуються для шифрування та розшифрування даних.

Подібний шифр дуже швидко можна розкрити, вивчивши повторюваність символів та короткі слова «і», «або», «за» і т. ін. У разі використання

перестановного алгоритму змінюються не символи, а порядок їх розміщення в повідомленні.

Залежно від доступності ключів розрізняють:

- симетричне шифрування – для шифрування і розшифрування використовується один ключ. Такі системи із закритим ключем реалізовані, наприклад, в архіваторах даних. Це зручно для шифрування приватної інформації, але під час передавання повідомлення по каналах зв'язку слід забезпечити таємне передавання ключа, щоб одержувач міг здійснити розшифрування. У принципі, якщо можна таємно передати ключ, то можна передати і таємну інформацію, тоді відпадає необхідність у шифруванні, а якщо такої можливості немає, шифрування даремне;

- асиметричне – для шифрування використовується один, відкритий (публічний, загальнодоступний) ключ, а для дешифрування – інший, закритий (секретний, приватний). Це робить непотрібним таємне передавання ключів між кореспондентами. Відкритий ключ безплідний для дешифрування, і його знання не дає можливості визначити секретний ключ. Єдиним недоліком моделі є необхідність адміністративної роботи – ключі (і відкриті, і закриті) треба десь зберігати і час від часу оновлювати. Сьогодні існує достатня кількість криптографічних алгоритмів. Найбільш поширеними з них є стандарт шифрування даних DES (Data Encryption Standart) та алгоритм RSA, названий за пер¬шими літерами прізвищ розробників (Rivest, Shamir, Adleman), розроблені у 1970—х роках. Обидва алгоритми є державними стан¬дартами США. DES є симетричним алгоритмом, а RSA – асиметричним. Ступінь захищеності під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується.

Криптографічні алгоритми використовуються як для шифрування повідомлень, так і для створення електронних (цифрових) підписів (ЦП) – сукупностей даних, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, що його підписала.

Цифровий підпис передбачає вставляння в повідомлення сторонньої зашифрованої інформації. При цьому, якщо не застосовується додаткове шифрування, сама інформація, що передається, ніяк не захищається. Сторонньою інформацією може бути контрольна сума (наприклад, CRC, Cyclic Redundancy Check, циклічний надлишковий код) – значення, яке автоматичне обчислюється за певним алгоритмом і широко використовується для перевірки цілісності інформації. Вимогою до відповідного алгоритму є неможливість створення відмінних текстів з однаковою сумою.

Більш поширеним методом є створення ЦП за допомогою асиметричного шифрування. При цьому накладання підпису виконується за допомогою закритого ключа, а перевірка підпису – за допомогою відкритого (відмінність створення ЦП від шифрування інформації). Публічний ключ та додаткові відомості (ім’я відправ¬ника, серійний номер ЦП, назва уповноваженої фірми та її ЦП) передається разом з підписом. Таким чином, послати зашифроване повідомлення і перевірити підпис може будь—хто, а розшифрувати або підписати повідомлення – тільки власник відповідного секретного ключа.

Криптографічний захист може бути організований як програмно, так і з використанням апаратно—програмних і апаратних засобів. Сьогодні фактичним стандартом для електронного листування в усьому світі завдяки своїй популярності й безплатному поширенню стала програма Філіпа Циммермана «Pretty Good Privacy» (PGP). У PGP застосовується так звана модель рівної довіри – відправник знає одержувача і довіряє йому ключ шифру, звідки і пішла назва «pretty good» (у буквальному перекладі – досить гарна). Перевагами PGP є висока надійність (єдиний метод зламування – «лобова атака»), потужний механізм обробки ключів, велика швидкодія. PGP можна інтегрувати в усі популярні поштові програми. Загалом для забезпечення належного рівня захищеності інформації потрібна криптографічна система (криптосистема) – сукупність засобів криптографічного захисту, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (зокрема й такої, що визначає заходи безпеки). Уразливість криптографічних систем пов’язана з тим, що вони

базуються на задачах, які визнані умовно нерозв’язуваними – для жодної з них не знайдено ефективного розв’язання, але й не доведено, що воно не існує. Від добору ключа методом перебирання криптосистема захищена поки що недостатнім рівнем швидкодії комп’ютерів. А численність типів можливих атак на криптографічні системи («на спосіб реалізації», «на паролі», «на користувача», «на моделі довіри» і т. ін.) підтверджує той факт, що захист є надійним і безпечним доти, доки не розпочинаються спроби його зламування. І нарешті, головним обмеженням криптосистем є те, що при одержанні повідомлення зашифрованого парним ключем, не можна взнати напевне, хто саме його відправив.

Останній недолік можна виправити за допомогою засобів біометричного захисту та методом двофакторної аутентифікації «Я маю» + «Я знаю» (використовується й однофакторна аутентифікація, але вона є менш надійною). Наприклад, користувач повинен мати пластикову картку (картку з магнітною смужкою або смарт—картку) і знати PIN—код.

Отже, розвиток криптосистем і підвищення надійності цифрових підписів створює необхідні передумови для заміни паперового документообігу електронним і переходу до здійснення електронних операцій.

Системи біометричного захисту (рис. 2.6) використовують унікальні для кожної людини вимірювані фізіологічні характеристики для перевірки особи індивіда. Цей процес називається електронною аутентифікацією. Його суть – визначити, чи справді індивід є тією особою, якою він або вона себе називає. Це відрізняє аутентифікацію від ідентифікації та авторизації. Мета ідентифікації – перевірити, чи відомий індивід системі, наприклад перевіркою пароля, а авторизація полягає в наданні користувачеві доступу до певних ресурсів залежно від його особи.

Рисунок 2.6 – Біометричні технології аутентифікації

Біометричні системи забезпечують найбільш точну аутентифікацію, оскільки перевіряють параметри, які дуже важко або неможливо змінити або підробити. Їхні переваги очевидні, оскільки традиційні системи захисту не здатні з'ясувати, наприклад, хто саме вводить код або вставляє смарт—картку.

Слід зазначити, що біометричні технології мають один суттєвий недолік. Вони спрацьовують завдяки тому, що системі відомі унікальні, конфіденційні характеристики кожної конкретної людини. Однак прибічники біометрії стверджують, що насправді вона забезпечує вищий рівень секретності, оскільки під час аутентифікації не залучається інформація про адресу людини, домашній телефон, банківський рахунок тощо.

Донедавна біометрія вважалась атрибутом фантастичних романів і військових систем, але сьогодні відповідні технології доросли до загального

застосування і далі швидко розвиваються. З удосконаленням біометричних пристроїв можна очікувати їх застосування не тільки у промисловості, а й у приватному секторі – проведення онлайнових операцій, доступ до банкоматів і засобів роздрібної торгівлі, вхід та вихід до будинків та багато іншого.

Протягом тривалого часу здійснювались спроби вибрати різні фізичні характеристики як індивідуальний штамп, що його можна було б постійно розпізнавати з високою точністю. Результати таких спроб втілено в сучасних технологіях:

- розпізнавання відбитків пальців. Основою цієї технології, започаткованої у кримінології в XIX столітті, є сканування візерунку пальців людини і порівняння їх з тими, що були попередньо записані у систему. Засоби захоплення варіюються від стандартних сканерів до складних пристроїв, які вимірюють дрібні заряди між складками шкіри. З огляду на зрілість цієї технології за допомогою подібних пристроїв можна досягнути високої точності. Подальший розвиток технології вимагає врахування можливих змін поверхні шкіри і навіть погодних умов. Для користувачів ця технологія приваблива через її простоту і швидкість;

- розпізнавання голосу. Цей підхід використовує стандартні засоби для запису модуляцій індивідуального мовлення. Рівень точності при цьому дещо нижчий, оскільки залежить від акустичного середовища та якості пристрою аудіозапису;

- аналіз геометрії руки передбачає вимірювання фізичних характеристик руки і пальців користувача. Рівень точності ідентифікації прямо пропорційний до кількості точок у записаному зразку. Новітні пристрої дають можливість створити тривимірну карту руки користувача;

- сканування сітківки ока. Ця технологія передбачає сканування системи кровоносних судин на сітківці. Точність розпізнавання дуже висока, на рівні розпізнавання відбитків пальців;

- сканування райдужної оболонки. Основою цього підходу є порівняння унікальних рисунків райдужної оболонки ока. Сканування виконується за

допомогою спеціальної камери. На сьогодні точність ідентифікації не дуже висока, але очікується її збільшення з удосконаленням технології;

- розпізнавання обличчя. Для запису тривимірної геометричної карти обличчя людини застосовується стандартна цифрова камера. Залежно від конкретного варіанта технології рівень точності розпізнавання коливається від низького до середнього;

- розпізнавання динаміки підпису. Під час аналізу підпису, який робиться спеціальною ручкою з перетворювачем прискорення по осях X і Y, враховується не тільки написання літер, а й швидкість і ступінь натискування;

розпізнавання стилю набирання символів на клавіатурі. Під стилем тут розуміється швидкість натискання на клавіші, ритм ударів і тиск, який здійснюється на клавіши.

3 СИСТЕМАТИЗАЦІЯ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ

З прискоренням інформаційного процесу комп'ютерна інформаційна система та мережа стали важливою соціальною інфраструктурою. На основі вивчення базової теорії, технології та застосування реагування на надзвичайні ситуації у сфері безпеки комп'ютерних мереж, ця дипломна робота зосереджується на відповідних стратегіях, спрямованих на створення ефективного механізму реагування на надзвичайні ситуації у сфері безпеки комп'ютерних мереж, аналізує склад стратегії, об'єкт функції та процес дії системної структури, а також розробляє структуру системи стратегії реагування на надзвичайні ситуації у сфері безпеки комп'ютерних мереж.

3.1 Концепція реагування на надзвичайні ситуації

Початок реагування на надзвичайні ситуації пов'язаний з виникненням "інцидентів". Так звані "інциденти" або інциденти безпеки відносяться до тих неналежних дій, які впливають на безпеку комп'ютерних систем і мереж. Збитки, спричинені інцидентами мережевої безпеки, часто є величезними, і часто за дуже короткий проміжок часу. Тому ключовими факторами в боротьбі з мережевими подіями є швидкість і ефективність. Зміст технології реагування на інциденти включає в себе класифікацію подій, опис подій та звіт про події.

3.1.1 Об'єкти реагування на надзвичайні ситуації

У цій роботі під об'єктом реагування на інциденти мережевої безпеки розуміються всі події, пов'язані з безпекою інформації, що обробляється комп'ютером і мережею. Суб'єктом події може бути природа, людина, збій або вірус і черв'як. Крім традиційної класифікації на конфіденційність, цілісність і доступність, до об'єктів аварійного реагування також відносяться сканування та інші порушення безпеки, які також називаються об'єктами аварійного реагування.

Як правило, в процесі реагування на надзвичайні ситуації є щонайменше три ролі: ініціатор, жертва та персонал. Ми називаємо їх "зловмисники", "жертви" та "ті, хто реагує".

3.2 Система стратегії реагування на інциденти безпеки комп'ютерних мереж

3.2.1 Принципи побудови системи стратегії реагування на надзвичайні ситуації

Процес формулювання стратегії є поступовим і безперервним процесом вдосконалення, оскільки неможливо сформулювати стратегію, яка може повністю відповідати і адаптуватися до середовища і потреб мережевої системи, а можна лише постійно наближатися до мети. Розробка системи стратегії реагування на надзвичайні ситуації повинна відповідати наступним принципам:

Керівний принцип: стратегія в системі стратегій реагування на надзвичайні ситуації не є технічним рішенням. Це має бути керівний документ, що описує методи роботи з мережевою безпекою

Згідно з принципом цілісності, стратегія реагування на надзвичайні ситуації повинна бути комплексною профілактикою в межах всієї мережі. У загальній системі перевезень будь-яка недбалість будь-якої ланки може призвести до вразливості всієї системи реагування на надзвичайні ситуації. Розробка всієї системи стратегії реагування на надзвичайні ситуації повинна враховувати як управлінські, так і технологічні аспекти. У той же час, формулюючи стратегію управління, необхідно враховувати здатність реагування, яку може забезпечити технологія, і інвестувати достатньо енергії в управління.

Принцип динамічності, складність інцидентів безпеки унеможливлює досягнення досконалості у формулюванні конкретних стратегій реагування на надзвичайні ситуації. Сформульовані стратегії завжди орієнтовані на поточну ситуацію, тоді як інформаційна безпека є динамічною, і стратегії інформаційної

безпеки потребують постійного розвитку. Тому необхідно постійно вдосконалювати стратегії, тобто реалізовувати ідею життєвого циклу безпеки.

3.2.2 Структура системи стратегії реагування на надзвичайні ситуації

Відповідно до принципів розробки стратегії реагування на надзвичайні ситуації та фактичних характеристик поточної комп'ютерної мережі, структура системи стратегії реагування на інциденти безпеки комп'ютерних мереж, розробленої в цій дипломній роботі, показана на рисунку 3.1.

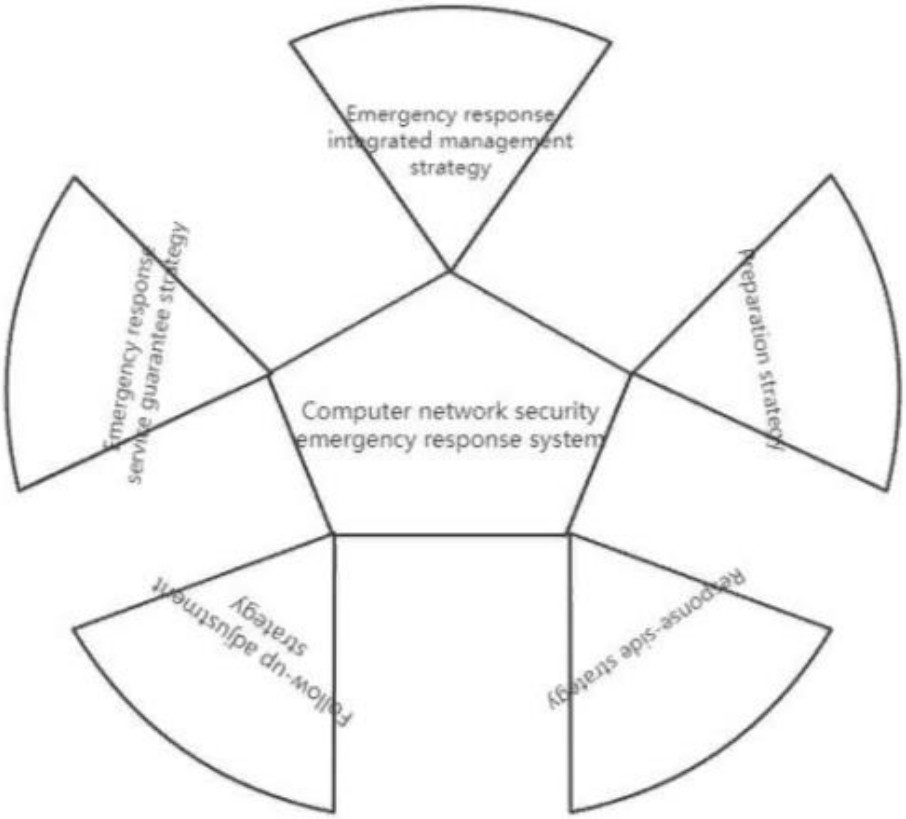

Рисунок 3.1 - Структура стратегії реагування на інциденти безпеки комп'ютерних мереж

Інтегрована стратегія управління реагуванням на надзвичайні ситуації. Стратегія в основному використовується для надання рекомендацій щодо створення організацій реагування на всіх рівнях в рамках інтегрованої побудови

системи реагування на надзвичайні ситуації в галузі мережевої безпеки. Вона в основному включає: відповідно до поточної структури адміністративної системи кожного відділу підрозділу, надається метод створення організації реагування на надзвичайні ситуації в галузі мережевої безпеки; вивчаються характеристики географічного розподілу та вимоги безпеки підрозділу; і формулюється стратегія обміну інформацією для сприяння впровадженню інтегрованого реагування на надзвичайні ситуації.

Стратегія підготовки використовується для того, щоб допомогти співробітникам служби реагування на надзвичайні ситуації здійснити необхідну підготовку до різних інцидентів мережевої безпеки, які можуть статися в майбутньому. Вона в основному включає: правильну оцінку ризиків у мережевій інформаційній системі Департаменту, визначення важливих інформаційних ресурсів у мережі, а також регулярну організацію відповідного персоналу для проведення симуляційних навчань з реагування на надзвичайні ситуації.

Стратегія реагування. Ця стратегія є ключем до реагування на надзвичайні ситуації, який в основному використовується для надання рекомендацій щодо вирішення проблем в процесі реагування на надзвичайні ситуації: як виявити, чи є подія безпеки; як обмежити масштаби атаки; як відновити всі зламані системи та мережеві пристрої до нормального стану, наскільки це можливо.

Стратегія коригування. Стратегія в основному використовується для керівництва роботою після обробки інциденту безпеки, включаючи перегляд і сортування різної релевантної інформації про інцидент мережевої безпеки і підсумовування етапів звіту, а також схему управління документами і доказами події.

Стратегія підтримки служби реагування на надзвичайні ситуації. Ця стратегія в основному використовується для того, щоб визначити, як забезпечити необхідну гарантію обслуговування для реалізації вищезгаданих стратегій, включаючи технічне обслуговування системи, навчання персоналу, технічні консультації, технічні дослідження і розробки, повідомлення про безпеку і юридичну підтримку.

3.2.3 Об'єкти стратегії реагування на надзвичайні ситуації

У цій роботі в системі стратегій, розробленій відповідно до характеристик різних інформаційних мереж, кожен складовий елемент відіграє різну роль у процесі реагування на надзвичайні ситуації з мережевою безпекою і має різні об'єкти дії, як показано на рисунку 3.2.

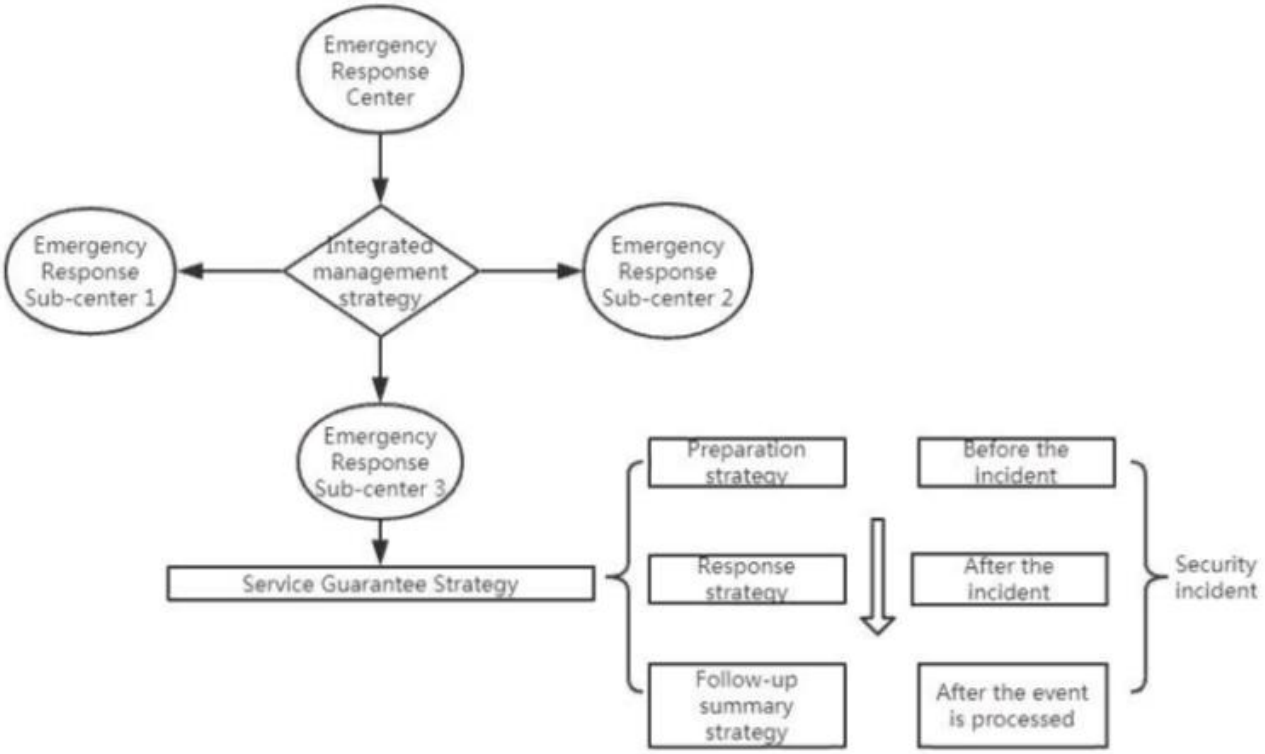

Рисунок 3.2 - Об'єкти стратегії

Перш за все, стратегія підготовки до реагування на надзвичайну ситуацію, стратегія реагування та підсумкова стратегія реалізуються послідовно відповідно до часової послідовності. Реалізація стратегії підготовки до інциденту безпеки є передумовою та основою стратегії реагування. Адекватність реалізації стратегії підготовки безпосередньо вплине на ефективність реалізації стратегії реагування; Стратегія реагування в разі виникнення інциденту відіграє важливу роль у боротьбі з інцидентами мережевої безпеки. Вона є ядром всієї системи стратегії

реагування на надзвичайні ситуації. Вона є не тільки продовженням стратегії підготовки, а й об'єктом опису стратегії підбиття підсумків. Після того, як стратегія узагальнення подій діє на інцидент безпеки, вона є ланкою передачі інформації між стратегією підготовки та стратегією реагування, після того, як стратегія узагальнення подій може повернути дефекти стратегії реагування на надзвичайні ситуації до стратегії підготовки, що робить ці три утворюють замкнутий цикл.

По-друге, стратегія підтримки реагування на надзвичайні ситуації відіграє важливу роль у всьому процесі реалізації вищезазначених стратегій, забезпечуючи гарантію надання послуг для реалізації стратегії. Формулювання комплексної стратегії підтримки може ефективно гарантувати реагування на надзвичайну ситуацію роботи з реагування. Вона є ключовим фактором для безперешкодної реалізації вищезазначених стратегій і важливою допоміжною стратегією для вищезазначених стратегій. Нарешті, стратегія інтегрованого управління діє на різні центри реагування на надзвичайні ситуації, що є горизонтальним інформаційним каналом, який широко використовується однотипними стратегіями, сформульованими різними центрами реагування на надзвичайні ситуації. З одного боку, це обмежує формулювання вищезазначених стратегій для задоволення потреб інтегрованого управління, з іншого боку, це може сприяти постійному вдосконаленню вищезазначених стратегій.

3.3 Аналіз процесу функціонування системної структури

Кожен компонент системи стратегій реагування на надзвичайні ситуації має відносно незалежні функції та чітко визначену сферу або об'єкт дії. Політики формують відносини взаємної залежності та сприяння, і спільно слугують для реагування на надзвичайні ситуації в сфері мережевої безпеки. Процес реагування на надзвичайні ситуації у сфері мережевої безпеки показано на рисунку 3.3.

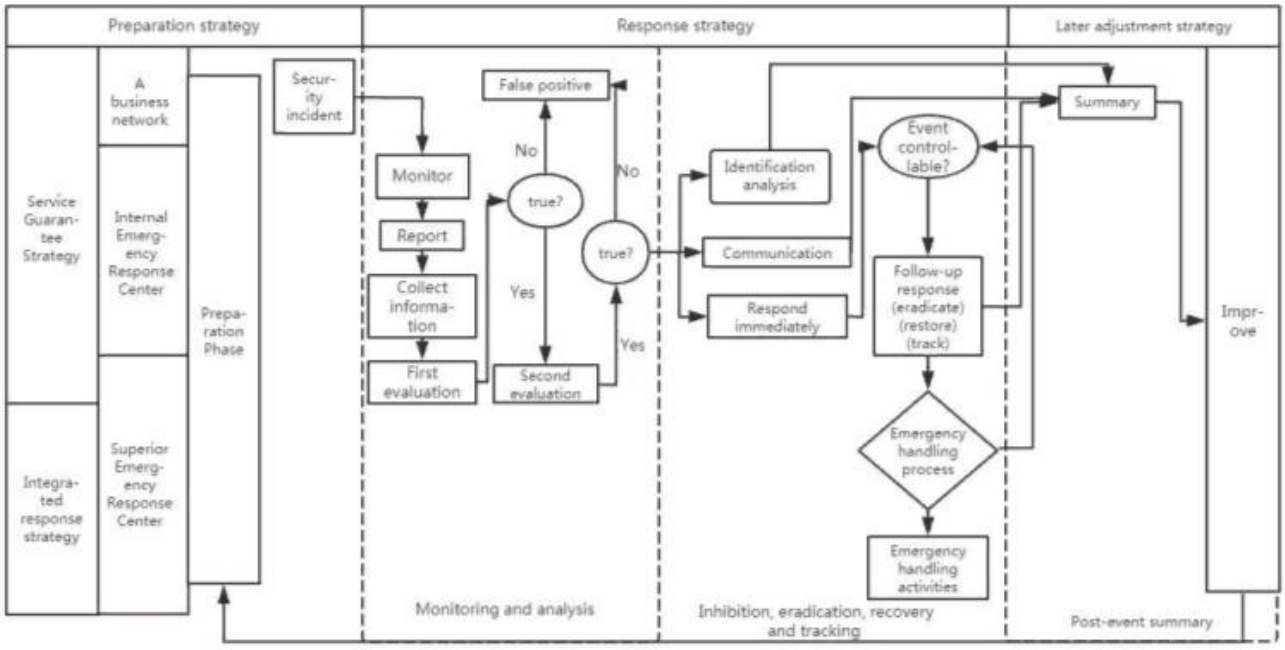

Рисунок 3.3 - Процес розробки стратегії

Перед виникненням інцидентів мережевої безпеки персонал служби реагування на надзвичайні ситуації активно виконує підготовчі роботи з реагування на надзвичайні ситуації. Цей етап відноситься до підготовчого етапу, а підготовчі роботи керуються стратегією попередньої підготовки. Мережа, в якій реалізована стратегія підготовки, повинна мати можливість виявлення вторгнення подій мережевої безпеки, а також здійснювати моніторинг ситуації з мережевою безпекою в будь-який час. Коли відбувається інцидент безпеки, ненормальну ситуацію в системі зазвичай першими виявляють співробітники служби управління мережевою безпекою і користувачі мережевих терміналів.

Обробка надзвичайної ситуації переходить на етап виявлення та аналізу, і процес обробки на цьому етапі керується стратегією реагування на інциденти. Коли оператори мережі виявляють підозрілі ситуації, вони повинні спочатку провести оцінку, щоб визначити, чи є це подією безпеки. Якщо визначено, що це подія безпеки або причина невизначеної події, він повинен своєчасно повідомити про ситуацію в центр реагування на надзвичайні ситуації з мережевої безпеки Департаменту. Внутрішній центр реагування на надзвичайні ситуації проводить повторну оцінку відповідно до фактичної ситуації. Коли це буде визначено як

інцидент мережевої безпеки, він вживатиме необхідних заходів для його негайного вирішення за допомогою аналізу автентичності та зв'язку відповідно до плану реагування на надзвичайні ситуації на етапі попередньої підготовки.

Після обробки інциденту безпеки робиться необхідний підсумок роботи з ліквідації наслідків надзвичайної ситуації. У цей час процес реагування на інцидент переходить у стадію коригування підсумків після події. Робота на цьому етапі повинна виконуватися відповідно до стратегії коригування підсумків після події. Завдяки ретельному узагальненню можна знайти дефекти в роботі з ліквідації наслідків надзвичайної ситуації та своєчасно скоригувати стратегію підготовки та реагування в процесі. Крім того, протягом усього процесу реагування на надзвичайні ситуації, необхідна сервісна підтримка, яка виконується під керівництвом стратегії сервісної підтримки реагування на надзвичайні ситуації.

Через природні, технічні та людські фактори вразливості мережі неминучі, а інциденти мережевої інформаційної безпеки неминучі. Аварійне реагування є останньою лінією оборони в системі активної оборони та оборони в глибину, і являє собою необхідні засоби та заходи для забезпечення живучості мережевої інформації. Побудова системи аварійного реагування - це складний системний інжиніринг. Життєдіяльність системи аварійного реагування полягає у взаємозв'язку різних заходів безпеки. Тому необхідно повністю розуміти її ієрархічну структуру, а потім з'ясувати основні проблеми, які необхідно вирішити. Система реагування на надзвичайні ситуації дуже складна і величезна. У цій дипломній роботі розроблено структуру системи стратегії реагування на надзвичайні ситуації в галузі безпеки комп'ютерних мереж, але глибока структура основного органу та функціональної одиниці є недостатньою, що потребує вдосконалення.

ВИСНОВКИ

З прискоренням інформаційного процесу комп’ютерна інформаційна система та мережа стали важливою соціальною інфраструктурою. Базуючись на вивченні базової теорії, технології та застосування реагування на надзвичайні ситуації безпеки комп’ютерної мережі, цей диплом зосереджений на відповідних стратегіях для управління створенням ефективного механізму реагування на надзвичайні ситуації безпеки комп’ютерної мережі, аналізує склад стратегії, об’єкт функції та процес дії структуру системи та розробляє структуру системи стратегії реагування на надзвичайні ситуації безпеки комп’ютерної мережі.

Через природні, технічні та людські фактори вразливості мережі неминучі та інциденти безпеки інформації в мережі неминучі. Реагування на надзвичайні ситуації є останньою лінією захисту в системі активної оборони та є необхідними засобами та заходами для забезпечення стійкості інформаційної мережі. Побудова системи реагування на надзвичайні ситуації є комплексною інженерною системою. Працездатність системи реагування на надзвичайні ситуації полягає у зв'язці різноманітних заходів безпеки. Тому необхідно повністю зрозуміти його ієрархічну структуру, а потім з’ясувати основні проблеми, які необхідно вирішити. Система реагування на надзвичайні ситуації дуже складна і велика.

ПЕРЕЛІК ПОСИЛАНЬ

1. Abdulbasit Ahmed, Alexei Lisitsa, and Clare Dixon. A misuse-based network intrusion detection system using temporal logic and stream processing. 2021 5th International Conference on Network and System Security, 2021.
2. Pedro Casas, Johan Mazel, and Philippe Owezarski. Coping with 0-day attacks through unsupervised network intrusion detection. 2022 International Wireless Communications and Mobile Computing Conference (IWCMC), 2022.
3. Zhang Chao-Yang. Dos attack analysis and study of new measures to prevent. 2018 International Conference on Intelligence Science and Information Engineering, 2018.
4. Jeremy Seth Davis. Sony psn downed; hacking group claims ddos attack | sc media, Jul 2018.
5. Kristof Elst. Deep q-learning in the physical world, 2015.
6. Asha Girija Girija, Deepa Rao, and Prathibha Gowda. Cmpe 232 – component- based and reuse-oriented sw engineering.
7. D. Zhang M. Zhang H. Li, Y. Wang and E. Y. Chang. “pfp: parallel fp-growth for query recommendation,” in proceedings of the 2018 acm conference on recommender systems - recsys ’18, lausanne, switzerland, 2018, p. 107.
8. Jparaiso. “cisco - netranger intrusion detection system.”, Dec 2018.
9. Christopher V. Kopek, Errin W. Fulp, and Patrick S. Wheeler. Distributed data parallel techniques for content-matching intrusion detection systems. MILCOM 2007 - IEEE Military Communications Conference, 2017.
10. C. Kruegel, F. Valeur, G. Vigna, and R. Kemmerer. Stateful intrusion detection for high-speed networks. Proceedings 2012 IEEE Symposium on Security and Privacy.
11. Pavel Laskov, Patrick Düssel, Christin Schäfer, and Konrad Rieck. Learning intrusion detection: Supervised or unsupervised?, 09 2015.
12. Li and Yuxi. Deep reinforcement learning: An overview, Sep 2017.

13. Tadashi Ogino. Evaluation of machine learning method for intrusion detection system. International Journal of Machine Learning and Computing, 5(2):137–141, 2015.

14. Tadashi Ogino. Evaluation of machine learning method for intrusion detection system on jubatus. International Journal of Machine Learning and Computing, 5(2):137–141, 2015.

15. OpenAI. A toolkit for developing and comparing reinforcement learning algo- rithms.

16. Iman Sharafaldin, Amirhossein Gharib, Arash Habibi Lashkari, and Ali A. Ghorbani. Towards a reliable intrusion detection benchmark dataset. Software Networking, 2017(1):177–200, 2017.

17. W.d. Smart and L. Pack Kaelbling. Effective reinforcement learning for mo- bile robots. Proceedings 2012 IEEE International Conference on Robotics and Automation (Cat. No.02CH37292).

18. Tran and Huy Nhut. A dynamic scalable parallel network-based intrusion de- tection system using intelligent rule ordering, Aug 2017.

19. S. Velliangiri and J. Premalatha. Intrusion detection of distributed denial of service attack in cloud. Cluster Computing, Apr 2017.

20. Gülsüm Yiğit and Merve Arnavutoğlu. Sql injection attacks detection preven- tion techniques. International Journal of Computer Theory and Engineering, 9(5):351–356, 2017.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ