МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____ Михайло СТЕПАНОВ
«____»_____ 2023 р.

На правах рукопису
УДК 004.056.5:510.22(043.3)

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Методи управління станом захисту інформаційних ресурсів в умовах кіберпливу

Виконавець: Владислав ТКАЧЕНКО

Керівник: д.т.н., професор Сергій ТОЛЮПА

Консультант розділу «Охорона навколишнього середовища»: к.т.н., доцент Тетяна ДМИТРУХА

Нормоконтролер: д.т.н., професор Сергій ТОЛЮПА

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Магістр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____ Михайло СТЕПАНОВ

«___» _____ 2023 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

здобувача вищої освіти Ткаченка Владислава Сергійовича

1. Тема: Методи управління станом захисту інформаційних ресурсів в умовах кіберзагрози затверджена наказом ректора від «15» вересня 2023 № 1814/ст.

2. Термін виконання з 16.10.2023р. по 31.12.2023р.

3. Вихідні дані: Вхідним значенням є: $X = XH \cup XM \cup XL$ – параметри вхідного трафіку; $XM = \{x_i(t), i = \overline{1,18}\}$ – множина параметрів трафіку, що характерні зовнішнім кібератакам; $XH = \{x_h(t), h = \overline{1,15}\}$ – множина параметрів трафіку, що характерні внутрішнім кібератакам;

4. Зміст пояснювальної записки: нормативно-правова складова кібербезпеки. атаки та системи їх виявлення, загальна характеристика сутності сучасних кібератак; аналіз систем управління захищеними інформаційними ресурсами, аналіз вразливостей та атак на інформаційні ресурси, що обробляються в інформаційних системах, обґрунтування та оцінка методів управління станом захищеності інформаційних ресурсів в інформаційних системах, оцінка ефективності.

5. КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

№ з/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	16.10.2023	Виконано
2.	Аналіз літературних джерел		Виконано
3.	Обґрунтування вибору рішення		Виконано
4.	Збір інформації		Виконано
5.	Нормативно-правова складова кібербезпеки.		
6.	Загальна характеристика сутності сучасних кібератак та систем їх виявлення		Виконано
7.	Аналіз систем управління захищеними інформаційними ресурсами		Виконано
8.	Аналіз вразливостей та атак на інформаційні ресурси, що обробляються в інформаційних системах		
9.	Практична реалізація методу та оцінка ефективності		Виконано
10.	Апробація роботи		Виконано
11.	Перевірка на антиплагіат		Виконано
12.	Оформлення і друк пояснювальної записки		Виконано
13.	Оформлення презентації		Виконано
14.	Отримання рецензій	22.12.2023	Виконано

6. Консультант з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона навколишнього середовища	Дмитруха Т.І.		

7. Дата видачі завдання: «16» жовтня 2023 р.

Здобувач вищої освіти (підпис) Владислав ТКАЧЕНКО

Керівник кваліфікаційної роботи (підпис) Сергій ТОЛЮПА

РЕФЕРАТ

Магістерська кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має 94 сторінок основного тексту, 30 рисунків, 3 таблиці, 2 додатків. Список використаних джерел містить 53 найменування. Загальний обсяг роботи 105 сторінок.

Мета і завдання дослідження. Метою досліджень є підвищення ефективності управління станом захищеності ІР від зовнішніх та внутрішніх кібератак на ІС.

Завдання магістерської кваліфікаційної роботи полягає в виборі методів управління станом захищеності ІР від зовнішніх та внутрішніх кібератак на ІС з використанням методів ідентифікації, динамічного програмування та опорних векторів.

Часткові взаємопов'язані задачі дослідження:

аналіз функціонування ІС обробки ІР, вразливостей ІС та атак на ІР;

аналіз методів прийняття рішень з забезпечення захищеності ІС та методів управління станом їх захищеності;

дослідження можливості розподілу системи управління станом захищеності ІС на основі множини проведення зовнішніх та внутрішніх кібератак;

розроблення методу управління станом захищеності при проведенні зовнішніх кібератак на ІС;

удосконалення існуючих методів управління станом захищеності при проведенні внутрішніх кібератак на ІС; оцінювання ефективності розроблених методів управління станом захищеності ІС з використанням комп'ютерного моделювання.

Об'єкт дослідження – процес функціонування ІС обробки ІР в умовах впливу кібератак.

Предмет дослідження – методи управління станом захищеності ІР на основі даних про кібератаки.

Методи дослідження. Для вирішення сформульованого завдання в роботі використано такі методи: теорія ймовірностей та математична статистика – для вивчення закономірностей випадкових явищ, подій, їхніх функцій, властивостей та операції над ними; динамічне програмування – для розбиття складних задач на більш прості, встановлення структурних зв'язків між елементами досліджуваної системи; моделювання – для побудови моделі ІС, що використовувалася для дослідження процесу управління станом захищеності ІР з використанням розроблених методів.

Новизна. Запропонований метод управління станом захищеності від зовнішніх кібератак на ІС на основі розподільчої ідентифікації та динамічного програмування, який дає можливість збільшення достовірність прийняття управлінського рішення.

Практична цінність заключається в збільшенні достовірності прийняття управлінського рішення щодо оцінки стану захищеності ІР в ІС на 12–16%. Може бути використаний в системах виявлення вторгнень на об'єктах критичної інфраструктури.

Ключові слова: кібератака, кіберрозвідка, інформаційна система, загроза, інформаційні ресурси, захищенність.

Апробація

Сергій Толюпа, Владислав Ткаченко**.** УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЙНИХ РЕСУРСІВ В УМОВАХ ВПЛИВУ КІБЕРАТАК. Збірник матеріалів доповідей та тез VI міжнародної науково-практичнної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» м. Київ, 27 квітня 2023 року. – К.: ВПЦ "Київський університет", 2023. – С. 47-48.

ЗМІСТ

ВСТУП

У зв’язку з широкомасштабним вторгненням росії в Україну від 24 лютого 2022 року в Україні запроваджений воєнний стан. Водночас російські військові здійснюють агресію проти України й у кіберпросторі. Кількість атак на державні інформаційні системи та об’єкти критичної інформаційної інфраструктури зросла втричі. 90% атак здійснюють військові хакери рф та білорусі, діяльність яких фінансується владою.

Через воєнні дії багато установ перенесли свої дані – хтось в інші, більш спокійні регіони країни, хтось – у хмару на території України, хтось – у хмару за кордон. Внесено відповідні зміни до законодавства, які дозволили це робити навіть державним установам.

Проте, як і раніше, всі інформаційні системи, вимоги до захисту яких закріплені в законодавстві України, мають бути захищені за чинними стандартами. Зокрема, комплексною системою захисту інформації (КСЗІ), а в деяких випадках допустиме використання європейських стандартів ISO/IEC 27 серії. Саме системи захисту інформації є першим кордоном, що стримує ворога від знищення нашої країни в інформаційне середовище.

Під час дії воєнного часу вимоги щодо захисту інформації в інформаційно-комунікаційних системах не змінюються. Вони визначені в Законі України «Про захист інформації в інформаційно-комунікаційних системах».

Ще до початку війни українські інформаційні системи зазнали потужних атак російських хакерів. Від початку широкомасштабної відкритої агресії рф інтенсивність атак не знижується. Російські хакери намагаються отримати доступ до персональних даних українців, а також завдати шкоди українським інформаційним системам. Ці атаки координуються з атаками на критичну інфраструктуру і є частиною воєнної агресії рф.

Витік персональних даних українців загрожує тим, що військові рф та спецслужби ворога використовують їх проти нашого населення, зокрема на тимчасово окупованих територіях, де українці найбільш вразливі до агресії російських загарбників. Крім того, витік чутливих даних загрожує роботі органів влади та критичної інфраструктури, якщо він буде використаний ворогом для подальших атак. Тож під час війни та протистояння російській агресії питання захисту даних в інформаційних системах постає більш гостро.

З метою захисту інформації, а також захисту державних інформаційних ресурсів, Кабінетом Міністрів України прийнято постанову від 12 березня 2022 р. № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану», відповідно до якої на період дії воєнного стану міністерства, інші центральні та місцеві органи виконавчої влади, державні та комунальні підприємства, установи, організації, що належать до сфери їх управління, для забезпечення належного функціонування інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, публічних електронних реєстрів, володільцями (держателями) та/або адміністраторами яких вони є, та захисту інформації, що обробляється в них, а також захисту державних інформаційних ресурсів, можуть зупиняти, обмежувати роботу інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів.

Аналіз ведення сучасних гібридних війн у світі та проведення кібернетичних операцій, свідчить про розвиток форм, способів та методів, які застосовуються для проведення атак на систему управління інформаційним ресурсом (ІР) та інформаційні системи (ІС). Для ефективного функціонування ІТС доцільно використовувати у складі системи управління ІР відповідну підсистему забезпечення безпеки з можливістю проведення

оцінювання та управління станом захищеності ІС в режимі реального часу та в умовах постіно змінюючій природі атак.

До основних особливостей ІС відносяться: різна розмірність мереж, територіально рознесені складові ІС, вихід елементів ІТС за межі контрольованої зони, для доступу до оброблюваних ресурсів застосовуються обчислювальні можливості системи, мають які мають високі вимоги до доступності інформаційних ресурсів, конфігурація ІС змінюється (змінюється склад користувачів та їхні привілеї, оновлюються версії програм, з'являються нові сервіси, нова апаратура і т.п.).

Зазначені особливості ІС роблять їх привабливими з точки зору організації та впровадження швидкої взаємодії між територіально-рознесеними підрозділами державних установ, однак, можуть бути використані зловмисниками для здійснення атак з метою вчинення деструктивних дій по відношенню до неї і системи управління ІР в цілому. Звичайно, функціонування ІС в інформаційне середовище залежить від множини природних, техногенних та антропогенних чинників, які порушують процес передачі інформації. Але найбільшу шкоду ІС може завдати навмисні атаки та вплив на існуючі вразливості системи безпеки, які можуть здійснюватися на різних рівнях базової еталонної моделі взаємодії відкритих систем.

Виходячи з вказаного, одним з найважливіших питань, які необхідно вирішити в процесі експлуатації ІС є гарантування інформаційної, програмної та апаратної безпеки, а для управління станом захищеності ІР необхідне застосування спеціального обладнання, алгоритмів та методів, що забезпечують безпечну роботу вузлів, компонентів, та ІТС в цілому.

На сьогодні вирішення питань забезпечення безпеки в ІС та управління станом захищеності ІС описується в роботах вітчизняних та закордонних дослідників, а саме: Субача І.Ю., Бурячка В.Л., Гнатюка С.О., Корченко О.Г., Юдіна О.К., Бучика С.С., Євсеєва С.П., Дудикевича В.Б., Казмирчук С.В., T. Ptaceka, G. Elmasry, P. Albers, O. Camp та інших.

Однак, запропоновані на сьогодні методи управління станом захищеності ІС не враховують особливостей проведення атак внутрішнім і зовнішнім зловмисниками, а також мають низьку достовірність прийняття управлінського рішення щодо оцінювання стану захищеності ІС та застосування засобів захисту. Водночас, основними вимогами, які пред'являються до методів управління станом захищеності ІР в ІС є: робота в режимі реального часу; врахування загроз характерних інформаційно-телекомунікаційним системам; адаптивне функціонування системи захисту інформації з самоорганізацією; децентралізація управління та ієрархічно-розподільча структура; збільшення достовірності та повноти прийняття управлінського рішення; зменшення математичної складності та ресурсної обтяжливості методів; гнучкість математичного апарату; застосування спеціальних вибірок про стан захищеності ІС; можливість застосовування в системах з високою динамікою зміни топології; децентралізація управління та наявність ієрархічно-розподільної структури; мінімальне завантаження мережі службовою інформацією.

Таким чином, сьогодні спостерігається невідповідність між вказаними можливостями існуючих методів управління станом захищеності ІС та вимогами до методів управління станом захищеності ІР в ІС, для усунення якого поставлене завдання, а саме: розроблення методів управління станом захищеності ІР від зовнішніх та внутрішніх атак на ІС з використанням методів ідентифікації, динамічного програмування та опорних векторів.

Мета і завдання дослідження. Метою досліджень є підвищення ефективності управління станом захищеності ІР від зовнішніх та внутрішніх атак на ІТС.

Завдання магістерської кваліфікаційної роботи полягає в розробленні методів управління станом захищеності ІР від зовнішніх та внутрішніх атак на ІС з використанням методів ідентифікації, динамічного програмування та опорних векторів.

Часткові взаємопов'язані задачі дослідження:

аналіз функціонування ІС обробки ІР, вразливостей ІС та атак на ІР;

аналіз методів прийняття рішень з забезпечення захищеності ІС та методів управління станом їх захищеності;

дослідження можливості розподілу системи управління станом захищеності ІС на основі множини проведення зовнішніх та внутрішніх атак;

розроблення методу управління станом захищеності при проведенні зовнішніх атак на ІС;

удосконалення існуючих методів управління станом захищеності при проведенні внутрішніх атак на ІТС; оцінювання ефективності розроблених методів управління станом захищеності ІТС з використанням комп'ютерного моделювання.

Об'єкт дослідження – процес функціонування ІС обробки ІР в умовах впливу атак.

Предмет дослідження – методи управління станом захищеності ІР на основі даних про атаки.

Методи дослідження. Для вирішення сформульованого завдання в роботі використано такі методи: теорія ймовірностей та математична статистика – для вивчення закономірностей випадкових явищ, подій, їхніх функцій, властивостей та операції над ними; метод опорних векторів – для розпізнавання образів, пошуку закономірностей даних та класифікації за ознаками; динамічне програмування – для розбиття складних задач на більш прості, встановлення структурних зв'язків між елементами досліджуваної системи; моделювання – для побудови моделі ІС, що використовувалася для дослідження процесу управління станом захищеності ІР з використанням розроблених методів.

РОЗДІЛ 1.
НОРМАТИВНО-ПРАВОВА СКЛАДОВА БЕЗПЕКИ. АТАКИ ТА СИСТЕМИ ЇХ ВИЯВЛЕННЯ.

1.1. Захищений кіберпростір - запорука успішного розвитку країни. Нормативно-правове забезпечення безпеки.

Забезпечення безпеки є одним із основних напрямків у системі національної безпеки держави. Реалізація зазначеного напрямку буде здійснюватися шляхом покращення спроможностей національної системи безпеки для протидії загрозам у сучасному інформаційному середовищі.

Питома вага загроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур керування як національних, так і транснаціональних формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу у інформаційне середовище, посилюється їх бажання за рахунок такого поділу покращити реалізацію власних геополітичних інтересів.

Інформаційний простір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Набирає сили створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури (КІІ) від атак, а й проведення превентивних наступальних операцій у інформаційне середовище, що включає виведення з ладу критично важливих ОІ противника шляхом руйнування інформаційних мереж, які управляють такими об'єктами.

Російська Федерація залишається основним джерелом загроз національній та кібербезпеці, активно реалізує концепцію протиборства,

базовану на поєднанні егативних дій у інформаційному середовищі та інформаційно-психологічних операцій, дії якої активно застосовуються у гібридній війні проти нашої держави. Така негативна активність створює реальну загрозу здійснення актів кібертероризму та кібердиверсій стосовно ОКІ.

Прогнозується зростання міждержавного протиборства і розвідувально-підривної діяльності у інформаційному просторі. Розширюється коло країн, які намагаються побудувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної дії у інформаційному просторі, посилюють контроль за сегментами мережі Інтернет. При цьому розширюється інструментарій, що передбачає зростання великих масивів даних щодо поведінки людини, певних груп та використання перспективних досягнень у сфері штучного інтелекту. Зростає тенденція здійснення підривної діяльності у інформаційному просторі шляхом підключення спецслужбами окремих країн, насамперед Російської Федерації, хакерських угруповань для реалізації кібервпливу.

Підвищується технічний рівень реалізації загроз, постійно вдосконалюються й впрваджуються нові інструменти і напрямки атак. Зростає тенденція відносно використання атак як інструменту спеціальних операцій, маніпулювання суспільною думкою населення, впливу на виборчі процеси. Структурно систему безпеки держави представлена на рисунке 1.1.

Рисунок 1.1. –Загальна структура національної системи безпеки

Глобального масштабу досягає використання кіберпростору організаціями терористів. Пріоритетними цілями яких залишаються об'єкти КІ тощо.

Нові загрози несе з собою перехід на 5G-мережі, функціонування яких залежить від коректної роботи програмного продукту, що за рахунок перспективних технології може мати нові загрози.

Поширення кібервпливу на усі сфери діяльності та покращення інструментарію їх реалізації дає необхідність зміни стратегії і тактики протидії ним. Набуває впливу максимально швидке виявлення кібервпливів і атак, реагування та розповсюдження інформації про них для мінімізації можливої шкоди.

Цифровий світ потребує формування більш збалансованої національної системи безпеки, яка дасть можливість адаптуватися до змін кібербезпекового середовища, гарантуючи безпечне функціонування національного сегмента інформаційного простору, передбачивши можливості для цифровізації всіх сфер суспільного життя.

Україна повинна бути здатною забезпечити свій соціально-фінансовий розвиток у навколишньому світі, що вимагає спроможності ефективно нівілювати деструктивні дії в кіберсередовищі, досягнення кіберстійкості та взаємодії всіх суб'єктів безпеки, яка ґрунтується на довірі.

У такій ситуації актуальним є нова Стратегія безпеки України, яка визначає національні інтереси у сфері безпеки, наявні та можливі загрози, цілі та напрямки забезпечення безпеки України для безпечного функціонування кіберпростору, його використання в інтересах суспільства і держави.

Стратегія ґрунтується на Конституції України, законів України "Про НБ України" та "Про основні засади забезпечення кібербезпеки України" (рис. 1.2), Конвенції про захист прав людини і основоположних свобод, Конвенції про кіберзлочинність, Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392, Концепції боротьби з тероризмом в Україні, затвердженої Указом Президента України від 5 березня 2019 року № 53, інших нормативно-правових актів. Перспективні напрямки розвитку системи безпеки показані на рисунке 1.3.

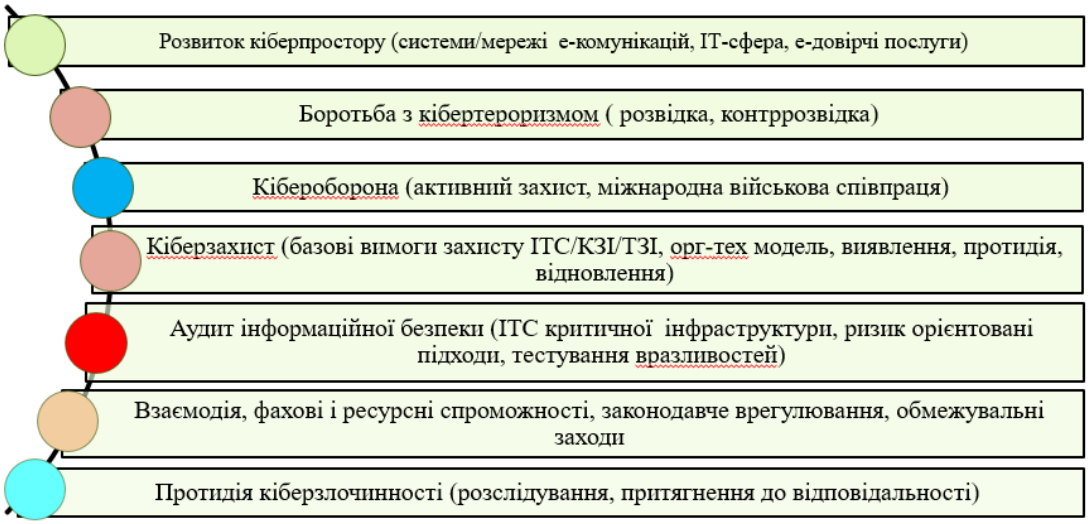


Рисунок 1.2. – Основні напрямки реалізації закону

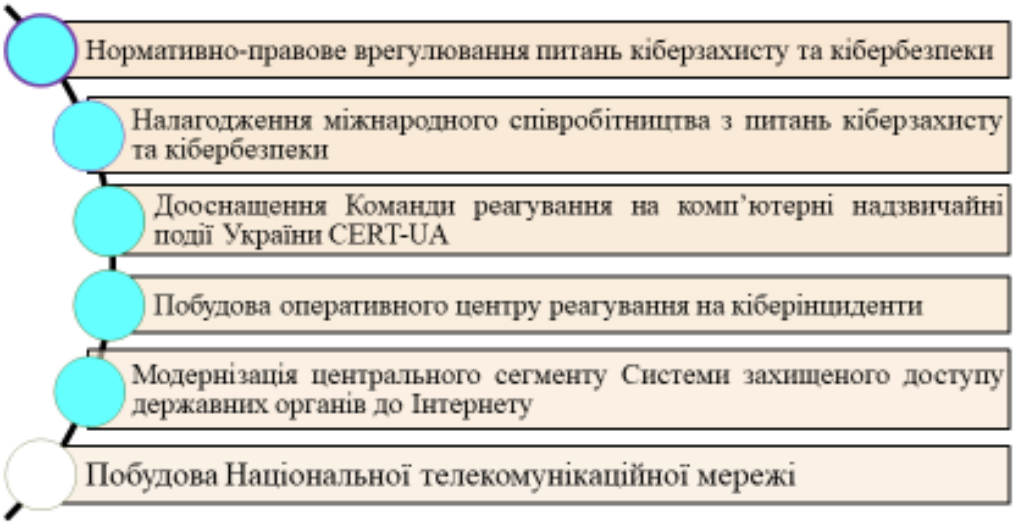


Рис. 1.3. – Перспективні напрямки розвитку системи кіберзахисту

Перша Стратегії кібербезпеки України затверджена Указом Президента України від 15.03.2016 року, що стало ключовим кроком у запровадженні підходів планування в цій сфері.

За роки першої Стратегії безпеки України, було докладено багато зусиль до розвитку національної системи безпеки. Важливим при цьому стало прийняття Закону України "Про основні засади забезпечення кібербезпеки України", який визначив правові основи забезпечення захисту інтересів людини і громадянина, суспільства та держави (рис 1.4).

Рисунок 1.4. – Складові системи безпеки

Удосконалено нормативн-правове забезпечення з питань кіберзахисту ОКІІ, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту.

Розбудовується Національна ТКМ, утворюється Національний центр резервування державних інформаційних ресурсів, забезпечується ефективна дія системи виявлення кібервпливу і реагування на інциденти та атаки, діє урядова структура реагування на надзвичайні події України CERT-UA.

З метою поліпшення координації діяльності суб'єктів безпеки і оборони, які підтримують кібербезпеку, утворено орган Ради національної безпеки і оборони держави - Національний координаційний центр безпеки.

Активно здійснюється співпраця у сфері безпеки з країнами партнерами (США, Велика Британія і Ірландія, ФРН, Нідерландами, Японією тощо), поглиблюється співробітництво з ЄС та НАТО, постійно проводяться ефективні кібернавчання за участю інших держав.

Однією з помітних проблем стала недостатня структуризація визначених пріоритетів забезпечення безпеки держави, значна частина яких не мала кінцевої мети та була не конкретною. Негативним був рівень планування напрямків з реалізації Стратегії безпеки держави, заплановані заходи не завжди співпадають із визначеними завданнями. Реалізація даної Стратегії була покращена відсутністю цілісного бачення розвитку спроможностей основних суб'єктів безпеки держави, обмеженістю матеріального забезпечення цієї системи, відсутністю державної підтримки розвитку.

Не були розроблені індикатори виконання Стратегії безпеки держави, що ускладнило процес оцінки її результативності та визначених незавершених поблем. Участь у формуванні Стратегії переважно брали участь суб'єкти сектору безпеки і оборони, не активно залучалися інші органи, наукові інститути, громадськість.

Надзвичайно критичні для розвитку національної системи безпеки напрямки Стратегії безпеки держави, не були враховані, зокрема: не

сформовано перелік ІКІІ, не створено модель приватного партнерства з державою. Розвиток цифрової грамотності відбувався без чіткої національної програми, кібернавчання здійснювалися епізодично.

Нова Стратегія безпеки держави, яка була затверджена Указом Президента Держави від 26 серпня 2021 року № 447/2021, враховує напрацьований досвід і завдання, стан кібербезпекового простору на державному та міжнародному рівні, а також напрямки Стратегії безпеки ЄС на цифровий простір, стратегій безпеки держав - членів ЄС та членів НАТО.

Викликами для Держави у сфері безпеки (рис. 1.5) є:

Рисунок 1.5. – Виклики та загрози національному кіберпростору

активне впровадження кіберзасобів у міжнародній конкуренції;

змагальний характер розвитку безпеки в умовах прогресуючих змін ІК технологій, зокрема хмарних, 5G-мереж, глобальних даних, штучного інтелекту тощо;

мілітаризація інформаційного простору та розвиток кіберзброї, що дає можливість проводити атаки для бойових дій і підривної діяльності у інформаційному середовищі;

вплив COVID-19 на фінансову діяльність та людську поведінку, що спричинив трансформацію і організацію певного сегмента суспільних відносин у онлайн режимі з широким залученням електронних сервісів та ІКС;

упровадження новітніх технологій, цифрових послуг для електронної взаємодії громадян з державою, що проводиться безсистемно в частині заходів з безпеки та оцінки ризиків.

Загрозами кібербезпеці держави є (рис 1.6):

Рис. 1.6. – Системні кібезагрози національній безпеці

гібридна агресія росії проти держави у інформаційному середовищі. Держава-агресор постійно нарощує потенціал кіберзброї агресивного призначення, використання якої може призвести до невиправних руйнівних наслідків. Атаки росії спрямовані на ІКС державних органів держави та ОКІІ з метою виведення їх з ладу, отримання несанкціонованого доступу і контролю, здійснення розвідувально-підривної діяльності. Атаки також активно запроваджуються державою-агресором як елемент інформаційних операцій з метою впливу на населення, втручання у виборчі процеси та спотворення української державності;

кіберзлочинність, завдає шкоди інформаційним складовим, суспільним процесам, особисто населенню, знижує довіру населення до інформаційних процесів та призводить до певних матеріальних втрат. Набуває поширення застосування кіберпростору для проведення злочинів проти основ безпеки держави, а також протиправних правопорушень, які пов'язані із легалізацією доходів, одержаних злочинним шляхом, незаконним викориистанням зброї, незаконним обігом наркотиків, психотропних речовин, їх, які загрожують життю та здоров'ю людей тощо;

організовані урядами інших держав атаки, що тісно пов'язані з викраденням у політичних колах, економічних або силових цілях інформації (кібершпигунство) та здійсненням розвідувально-підривної дії. Особливостями таких атак є їх велика тривалість, складність, адаптивність та прихований характер, що ускладнює їх виявлення та нейтралізацію;

застосування терористичними організаціями кіберпростору для вчинення актів тероризму, фінансової та терористичної діяльності.

Ураховуючи виклики та кіберзагрози, що постали перед державою у інформаційному середовищі.

Чинники та передумови, які формують зазначені загрози:

висока залежність держави від іноземних виробників продукції ІКТ, відсутність сертифікації оцінки відповідності даної продукції вимогам з безпеки, що підвищує рівень уразливості інформаційної структури від незадекларованих функцій та зменшує спроможності протидії загрозам;

нормативно-правова база у сфері безпеки є недосконалою, а також її застарілість у СЗІ, повільне впровадження положень європейського законодавства, недостатня погодження цифрової складової розслідування кримінальних злочинів, а також низький рівень нормативно-правової відповідальності за порушення вимог законодавства;

відсутність у державі відповідних підрозділів, кадрового забезпечення та належного контролю за кібербезпекою, здійснення фінансування робіт із кібербезпеки за принципом, що залишилося;

відсутність незалежного аудиту ІБ та механізмів надання інформації про вразливості при динамічній цифровізації державного управління та життєдіяльності держави;

підвищення кваліфікації фахівців з питань безпеки та кіберзахисту, невідповідність сучасним вимогам рівня підготовки та неефективні механізми їх стимулювання діяльності в державному секторі;

відсутність законодавчого акта про КІ держави та її захист, що значно погіршує формування системи кіберзахисту такої структури;

організаційно-технічної моделі кіберзахисту впроваджена не в повному обсязі, яка відповідатиме загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку безпеки;

низький рівень обізнаності суспільства щодо загроз та кіберзахисту, відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в інформаційне середовище,;

відсутність дієвої системи ІАЗ безпеки;

недостатня захищеність від атак ДІР та ОКІ;

невідповідність вимогам законодавства стану захисту ІКС державних органів та суб'єктів функціонування, в яких обробляється велика частина інформації з обмеженим доступом.

Держава прагне побудувати максимально відкритий, стабільний і безпечний кіберпростір в інтересах прав і свобод людини, соціального, політичного і фінансового розвитку держави. Дорожна карта розбудови кіберпростору представлена схематично на рис. 1.7.

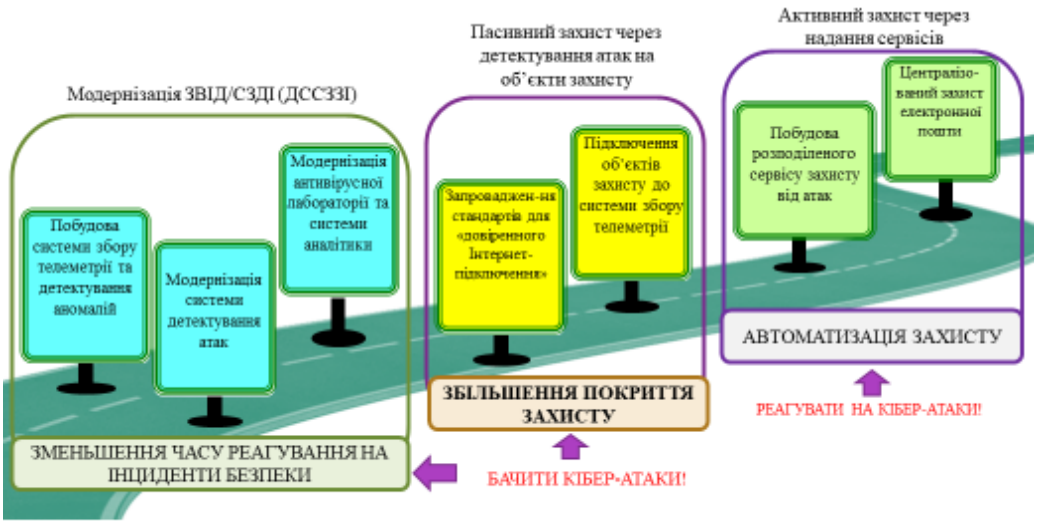


Рис. 1.7. Дорожна карта розбудови кіберпростору

Для розбудови національної системи безпеки в сфері кіберстримування, кіберстійкості, взаємодії необхідним є:

нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та тероризму, посилення спроможності системи безпеки для унеможливлення силової агресії проти держави у інформаційному просторі або з його застосуванням;

набуття можливості швидко адаптуватися до загроз у інформаційному просторі, відновлювати стале функціонування національної інформаційної структури, насамперед ОКІ (кіберстійкість);

розвиток стратегічних відносин у сфері безпеки із іноземними партнерами, передусім з ЕС, США та іншими державами - членами НАТО, забезпечення розвитку комунікації та координації між суб'єктами забезпечення безпеки на державному рівні, співробітництво з іншими державами та організаціями на основі інтересів держави (взаємодія).

Україна, крім основних суб'єктів НСБ, залучить до вирішення завдань безпеки більш широке коло учасників, громадські об'єднання та окремих громадян держави.

Об'єднувальну та координаційну роль при цьому відіграватиме Національний координаційний центр безпеки.

Україна розбудовуватиме державну систему безпеки, ґрунтуючись на:

неухильному захисті національних інтересів Держави у сфері безпеки всеохоплюючому розумінні та постійному аналізі глобальних трендів кібербезпекового середовища,;

удосконалення законодавства у сфері безпеки та оперативності дій щодо його актуалізації відповідно до безпекових умов, що змінюються, перманентності заходів з перегляду та уточнення повноважень і відповідальності суб'єктів забезпечення безпеки держави,;

пріоритетності фінансового і соціального розвитку суспільства;

дотриманні законності, повазі до основоположних цінностей, прав людини і громадянина збалансованому забезпеченні потреб держави і прав громадян;

стимулюванні до обміну інформацією, знаннями і досвідом, ризик-аналізі сильних та слабких сторін моделей безпеки інших країн,орієнтованому підході до забезпечення безпеки чіткому визначенні ролей та механізмів взаємодії під час розв'язання завдань безпеки;

зміцненні довіри, зокрема в рамках державно-приватного партнерства, співпраці та інклюзивному діалозі всіх суб'єктів забезпечення безпеки,;

впровадженні принципів, методів та механізмів державного управління у сфері безпеки;

зоптимальному розподілі матеріальних, фінансових та інших ресурсів;

проактивному підході до виявлення та усунення загроз;

забезпеченні демократичного контролю за функціонуванням державної системи безпеки.

Пріоритетами забезпечення національної системи безпеки є:

захист кіберпростору для суверенітету держави та розвитку суспільства;

захист прав, свобод і інтересів громадян держави у інформаційне середовище;

євроатлантична і європейська інтеграція у сфері безпеки.

Формування нової якості державної системи безпеки потребує чіткого та прозорого визначення цілей, що мають бути виконані протягом терміну реалізації цієї Стратегії.

Закон держави «Про основні засади забезпечення безпеки України» визначає правові основи забезпечення захисту в кіберпросторі, напрями та принципи державної політики у сфері безпеки, національну систему безпеки, основні цілі, повноваження суб'єктів безпеки та засади координації.

Одним із напрямів визначених Законом функціонування та забезпечення державної системи безпеки є впровадження організаційно-технічної моделі (ОТМ). ОТМ кіберзахисту розроблена фахівцями Держспецзв'язку, ґрунтуючись на практиці застосування положень цього Закону, практиці організації роботи у цій сфері та взаємодії з іншими суб'єктами забезпечення безпеки, досвіді розбудови національної системи безпеки, .

Положення про ОТМ визначає саму модель, склад та структуру, цілі та механізм функціонування. В ній визначені дефініції сил та засобів кіберзахисту, команд реагування на комп'ютерні надзвичайні події. ОТМ передбачає багаторівневу архітектуру, яка представляє собою структуровану систему з трьох інфраструктур.

Базовий рівень – базисна інфраструктура – сукупність ОКІ та їх критичних активів, суб'єктів господарювання, громадян держави та об'єднань громадян, інших осіб, які провадять діяльність та/або надають відповідні послуги; ***середній рівень*** – технологічна інфраструктура – сукупність сил та засобів кіберзахисту та їх забезпечення; ***верхній рівень*** – організаційно-керуюча інфраструктура – сукупність суб'єктів забезпечення безпеки, що формують та/або реалізують державну політику у сфері безпеки;

Положенням про ОТМ визначено, що її функціонування направлене на оперативне (кризове) реагування на атаки та кіберінциденти, впровадження

контрзаходів та зниження вразливості комунікаційних систем.

Положення про ОТМ окреслює не суперечливу, цілісну, об‘єднану єдиним задумом систему, місце в ній кожного суб’єкта державної системи безпеки, напрями інформаційного обміну, форми взаємодії між різними суб’єктами одного та інших рівнів моделі, характер зв’язків з іншими суб‘єктами, основні етапи управління кіберінцидентами та базові механізми запобігання, виявлення, ідентифікації, реагування на кіберінциденти і атаки та відновлення після них. Положення про ОТМ чітко сформульовало систему безпеки, де всі її учасники тісно пов’язані між собою, доповнюють діяльність один одного, а характер відносин є здебільшого партнерським.

Положення про ОТМ розроблено на виконання третьої статті Закону «Про основні засади забезпечення безпеки України» та частини першої статті Закону України «Про Державну службу спеціального зв’язку та захисту інформації України».

Підвищення ефективності функціонування державної системи безпеки є основним завданням для сталого і безпечного функціонування державної КІІ в кіберпросорі, для вирішення якого впроваджується ОТМ. Її нормативно-правове визначення - створити умови для об’єднання дій суб’єктів забезпечення безпеки при вирішенні ефективності рівня кіберстійкості КІІ держави, яка охоплює як ОКІ, так і комунікаційно-інформаційні та інші системи, сталість та надійність яких критично важлива для функціонування державних органів, установ, організацій та підприємств всіх форм власності.

ОТМ кіберзахисту є набором заходів, сил і засобів кіберзахисту, які направлені на оперативне реагування на кіберінциденти та атаки, впровадження превентивних контрзаходів, спрямованих на мінімізацію вразливості інформаційних систем. ОТМ кіберзахисту - допоможе об’єднати зусилля суб’єктів кібербезпеки та створити умови для безпечного функціонування кіберпростору, його використання в інтересах суспільства і держави, через реалізацію заходів, спрямованих на захист національних ІР, кіберзахист ОКІІ, забезпечення їх кіберстійкості, стабільного

функціонування інформаційної структури національного та приватного секторів економіки.

Як було визначено ОТМ кіберзахисту складається з організаційно-керуючої, технологічної та базисної інфраструктури кіберзахисту та впроваджується для ефективного забезпечення функціонування державної системи безпеки. Такий опис ОТМ можна навести у вигляді архітектури (див. рис. 1.8.), яка являє собою структуровану систему, що складається з трьох інфраструктур кіберзахисту, які взаємозалежні, взаємопов'язані і взаємодіють між собою для досягнення цілей впровадження ОТМ кіберзахисту.

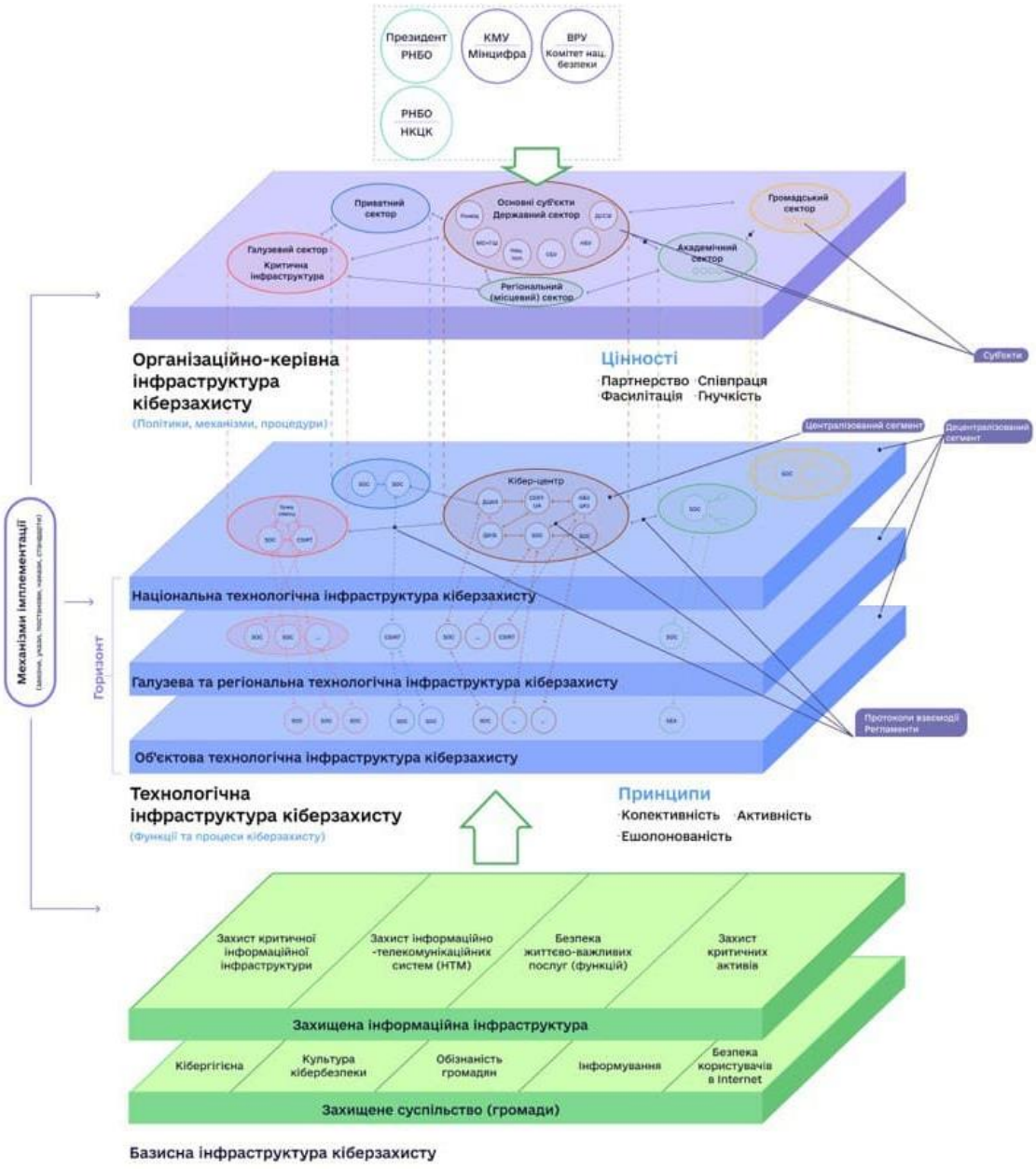


Рисунок 1.8. - Архітектура організаційно-технічної моделі кіберзахисту кіберпростору

1.2. Кавліфікаційні ознаки атак та систем виявлення вторгнень

В даний час, при стрімкому розвитку інтелектуальних технологій і зростаючої інформатизації суспільства на перший план висуваються задачі забезпечення належного рівня захищеності та кіберстійкості інформаційних

систем. Зі збільшенням числа комп'ютерних кіберінцидентів, пов'язаних з безпекою, почали стрімко розроблятися СВА.

Ссистеми виявлення атак (СВА) класифікуються відповідно до двох характеристик: рівня системи на якому здійснюється захист і методу виявлення. Всі розробники СВА і організації, які використовують їх повинні розуміти й вивчати їх класифікацію, щоб оптимізувати кращі рішення для СЗІ. При дослідженні різних аспектів класифікації і застосуванні різних комбінацій ми зможемо досягти оптимального рівня безпеки ІС.

В роботі систематизовані ознаки СВА та розроблена класифікація таких систем, що у повному обсязі відповідає сучасним тенденціям побудови інформаційних мереж та викликам, що ставляться перед СЗІ в цілому.

На сьогодні СВВ і атак являють собою програмні або апаратно–програмні рішення, які процес контролю подій автоматизують, що відбуваються в ІС або мережі, а також самостійно аналізують події в пошуках ознак проблем безпеки. Оскільки кількість різних способів і типів несанкціонованих проникнень в чужі мережі значно збільшилася, СВА стали необхідним компонентом структури безпеки ОІД.

Аналіз останніх публікацій і досліджень дає можливість дійти висновку, що більшість існуючих напрямків поділу СВА дуже абстрактні, не є повними, і потребують доповнень та узагальнень (рис. 1.10).

Аналізуючи класифікацію СВА, стає зрозуміло, що автори включають напрямки моніторингу безпеки, такі як оцінки вразливості. Вони класифікують СВА по п'яти ознакам: парадигмі виявлення і частоті використання; поведінці при виявленні; аудиту місцеположення джерела; методу виявлення.

З часом автори у своїй класифікації представляють, що СВА може функціонувати як автономний централізований або інтегрований додаток, який створює розподілену інформаційну систему.

Але все ж найповніша класифікація, з точки зору відомих ознак, представлена на рис. 1.11. де автори розширюють всі спроби їх попередників

та включають додатково аж дванадцять класифікаційних ознак, проте деякі вимагають відвертої модернізації та суттєвих доповнень у відповідності до реалій сьогодення.

Рисунок 1.11 – Класифікаційні ознаки систем виявлення і запобігання атак

Першою класифікаційною ознакою СВА є класифікація за середовищем моніторингу, тобто у відповідності від того де здійснюється збір інформації: на конкретному комп'ютері чи на певних додатках, що працюють на комп'ютері чи в мережі.

Більшість класифікацій розділяють СВА за даною ознакою на два типи: СВА на рівні вузла та СВА на рівні мережі. Сьогодні наявність одного типу СВА зменшує свою ефективність через відсутність іншого, тому досить популярною стає розробка комбінованих систем які успішно функціонують як на рівні вузла так і на рівні мережі. А зі збільшенням сектору надання

додаткових послуг та появою додатоків (application) виникла необхідність моніторингу безпеки на їх рівні. Тому доцільно класифікувати СВА за середовищем моніторингу таким чином: на рівні додатків, на рівні вузла, на рівні мережі та гібридні (комбіновані).

Другою основою ознакою класифікації СВА є поділ за методом виявлення загроз та вразливостей. Прийнято розділяти СВА на ті, що засновані на методі виявлення сигнатур, і ті, що базуються на застосуванні методу виявлення аномалій (МВА). Сьогодні МВА являються пріоритетними у побудові СВА. Найпопулярнішими є чотири підгрупи, а саме: виявлення на основі машинного навчання, виявлення засноване на інтелектуальному аналізі даних, статичне виявлення аномалій, виявлення засноване на існуючих знаннях. Слід відмітити, що в більшості класифікацій відсутні гібридні методи, які на даний час стрімко досліджуються і є комбінаторікою сигнатурного методу і МВА.

Наступною класифікаційним типом є поділ за архітектурою. В залежності від структури СВА виділяють системи, за якими спостерігають (target) та системи, на якій виконується програмне забезпечення (host). Раніше СВА, виконувалися на тих же системах, які вони захищали проте з появою РС і ПК у більшості архітектур СВА передбачається їх виконання на окремій системі, розділяючи системи host і target. Це підвищує безпеку функціонування СВА.

За характером відповіді СВА поділяють на активні та пасивні, тобто СВА може реагувати на вторгнення в пасивній чи активній формі. Пасивні системи частіше всього представляють собою звіт СВА, зроблений для фахівців. Коли СВА активно реагує на вторгнення вона може змінити динамічний стан об’єкту, що піддався атаці, або, в деяких випадках, змінити стан порушника. Активні заходи об’єкта, що піддався атаці, має автоматичне втручання в іншу систему.

Іншою ознакою класифікації СВА є розподіл за принципом функціонування на статичні та динамічні. Не кожна сучасна класифікація

СВА має подібну класифікаційну ознаку, так як більшість науковців вважають статичні СВА морально застарілими. Проте існують ІС які не несуть в собі важливої інформації та не підлягають нападу зі сторони порушника, тому й не потребують механізмів реалізації динамічних СВА.

Статичні СВА роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, помилки в конфігураціях, перевіряють версії прикладних програм на наявність відомих вразливостей і слабких паролів, розшукуючи вразливе програмне забезпечення, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів.

Динамічні СВА здійснюють аналіз у реальному часі всіх дій, що відбуваються в СВА, аналізуючи файли аудиту або мережні пакети, що передаються за визначений проміжок часу. Динамічні IDS здійснюють аналіз у реальному часі і дозволяють стежити за безпекою системи постійно.

Слідуючою ознакою є розподіл за часом реакції. Багато ранніх СВА були пакетного типу, тобто вони повністю залежали від інформації записів аудита в ОС. СВА пакетного типу не виконують ніяких активних дій на виявлені атаки.

Доцільно класифікувати СВА за джерелом аудиту. СВА виявляють вразливості на основі аналізу даних, які зібрані на основі різних джерел аудиту. Зібрані дані представляють інформаційну систему, додатки і ста функціонування мережі. Успішне виявлення вразливостей залежить від повноти даних з джерел аудиту, швидкості збору та їх обробки.

Дані з журналів аудиту ІС несуть в собі інформацію про діяльність в системі. У разі успішної атаки, відбуваються зміни, тому дані актуальні лише до моменту атаки.

Ще однією ознакою класифікації СВА є розподіл за технологіями побудови. При побудові СВА важливо знати, які технології впроваджуються в побудові ІС. Адже проводові мережі, порівняно з безповодовими, використовують специфічні і різні методи безпечної передачі, наприклад,

кодування, шифрування. Тому фізична мережа передачі відіграє важливу роль у проектуванні СВА.

Проводові мережі, як правило, швидші і дешевші, ніж безпроводові. Деякі з мережевих функцій, таких як, інтенсивність трафіку і структура топології мережі, можуть бути задіяні для виявлення вторгнень у мережах зв'язку. Мобільні бездротові мережі представляють собою набір мобільних сигментів, що автоматично переналаштовуються без допомоги фіксованої інфраструктури або управління. Вони бувають: мобільні агенти, ієрархічні, автономні та розділенні. Ієрархічні СВА застосовуються для багатошарових мережевих інфраструктур, коли мережа розподіляється на кластери.

Також СВА поділяються на ті що оцінюють переходи між станами і ті що оцінюють стан. Система виявлення описує, як СВА оцінює вторгнення і може бути двох типів: перший тип оцінює стан щоб дізнатись чи є він безпечним, другий тип оцінює переходи міг станами, а саме перехід з безпечного стану в незахищений.

Ще однією з класифікаційних ознак СВА є розподіл за режимом збору даних. Дані аудиту можуть бути отримані в розподіленому режимі з різних джерел, або зібрані централізовано від одного джерела.

Окремо слід відмітити СВА основаних на методах інтелектуального розподілу даних Data Mining.

Узагальнений вигляд класифікації СВА представлений на рис. 1.12.

Взагалі кажучи, сучасні СВВ і атак далекі від ергономічних і ефективних, з точки зору безпеки управлінських рішень. Підвищення ефективності слід ввести не тільки в області виявлення протиправних дій на інфраструктуру ОІД, але і з врахуванням повсякденної експлуатації цих засобів, а також економії інформаційних ресурсів даної системи захисту.

Якщо говорити про модулі обробки даних, то, кожна сигнатура атаки в системі обробки даних про атаку є базовою інформацією для розпізнавання більш загальних дій – фази атаки (етапи її реалізації). Саме поняття сигнатури компонується до деякого вирішального правила. Таким чином

кожна атака розбивається на набір етапів її проведення. Чим простіша атака, тим більш простіше її виявити і з'являється більше можливостей щодо її аналізу.

Сценарій атаки це граф переходів. А фази атак можна представити, наприклад, наступним чином: застосування експлойтів; управління через бекдори; пошук встановлених троянів; ідентифікація програмних і апаратних засобів; випробування портів; збір банерів; дезорганізація функціоналу мережі за допомогою атак на відмову в обслуговуванні; пошук проксі–серверів; видалення слідів присутності і т. д.

Переваги такого підходу лежать на поверхні і очевидні – у разі роздільної обробки етапів атаки з'являється можливість розпізнавати атаку ще в процесі її формування і підготовки, а не на стадії її вразливості, як це відбувається в існуючих СВА. Елементною базою для розпізнавання може бути як сигнатурний аналіз, так і виявлення певних аномалій, використання експертних методів та інтелектуальних систем, довірчих та інших інформаційних стосунків, вже відомих і реалізованих, мережевих і локальних примітивів оцінки того, що відбувається в інформаційному середовищі потоку подій. Узагальнюючий підхід до моніторингу дозволяє визначати розподілені загрози у логічному та в фізичному просторі. Загальна схема обробки подій також дозволяє здійснювати моніторинг розподілених атак шляхом відповідної агрегації даних з відомих джерел і конструювання дані про відомі інциденти.

СВА, як і більшість сучасних програмних продуктів, повинні задовольняти ряду вимог. Це й орієнтування на особливості сучасних інформаційних мереж і сучасні технології розробки та відповідна сумісність з іншими програмами. Щоб зрозуміти, як правильно використовувати СВА, потрібно чітко знати, як вони функціонують і які їх вразливі місця.

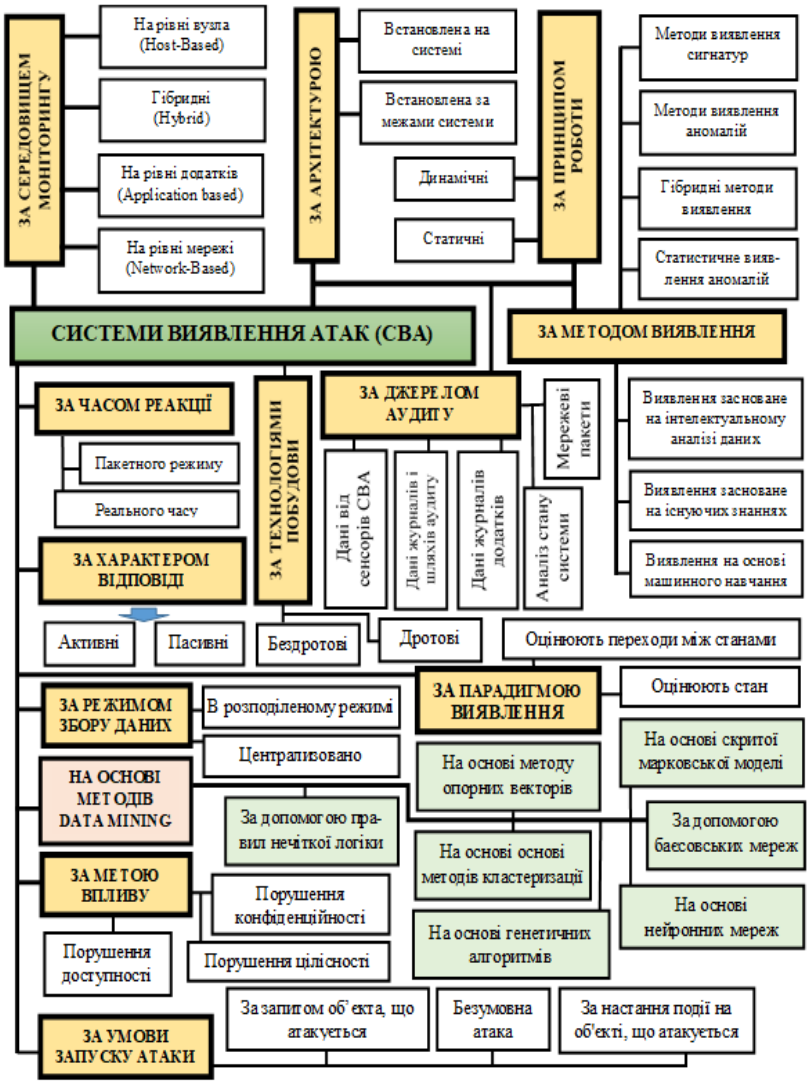


Рисунок 1.12 – Узагальнений вигляд класифікації систем виявлення вторгнень та атак

Нині достеменно невідомо, скільки видів атак (сукупність узгоджених за метою, змістом і часом дій або заходів, так званих кібератакцій, спрямованих на певний об’єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережності та/або авторства циркулюючої в ньому інформації, а також порушення роботи його ІС) та методів їх застосування з моменту виникнення цього поняття і до цього часу розробило людство. Комплексні статистичні дослідження з цього приводу до останнього часу не проводилися. Фахівці описуючи математичні основи вірусної технології, довели, що оскільки кількість злоякісних кодів, які є підмножиною множини

атак, нескінченна, то й кількість самих атак, загальну структуру яких подано на рис. 1.13, є також нескінченна.

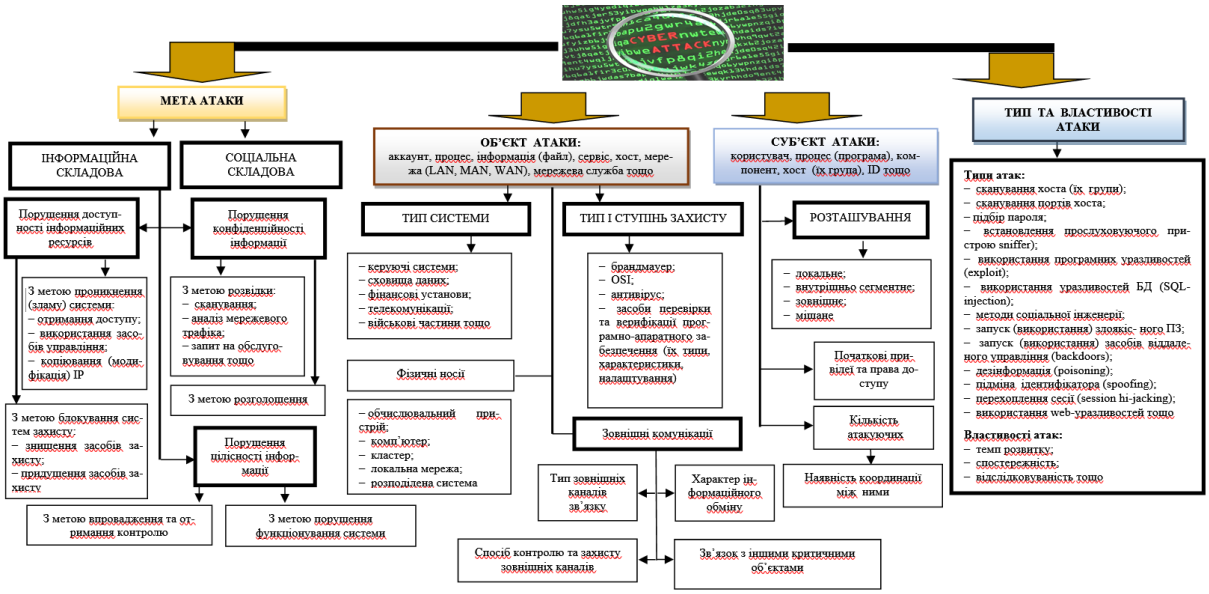


Рисунок 1.13 – Загальна структура кібернетичної атаки

Сучасні атаки класифікують за такими ознаками:

за метою впливу на об’єкт атаки, що може бути спрямований, наприклад, на порушення цілісності (integrity) або конфіденційності (confidentiality) інформації, її захищеності від несанкціонованого доступу (authentication), а також забезпечення живучості (survivability) системи та надійності (availability) її функціонування. Закордонний і вітчизняний досвід показує, що вирішення цих завдань використовують методи криптографії в поєднанні з перевіреним і ліцензованим програмним забезпеченням (ПЗ), а також надійні інтелектуальні носії важливої інформації (матеріал ключа). При цьому саме живучості (здатності системи вчасно виконувати свої функції в умовах фізичного руйнування, часткової втрати ресурсів, відмов і збоїв елементів, несанкціонованого втручання в систему управління), яка визначає мобілізаційну готовність збройних сил, промисловості, економіки, народного господарства й суспільства в цілому як до ведення війни, так і до ліквідації наслідків терористичних актів, стихійних лих і техногенних катастроф, приділяють останнім часом найбільшу увагу;

за принципом впливу на об’єкт атаки:

використання прихованих каналів (шляхів передачі інформації, що дозволяють двом процесам обмінюватися нею у спосіб, який порушує політику безпеки);

використання прав суб’єкта системи (користувача, процесу) до об’єкта (файлів даних, каналів зв’язку тощо);

за характером впливу на об’єкт атаки:

активний вплив (користувач виконує деякі дії, що виходять за рамки його обов’язків і порушують наявну політику безпеки, наприклад, розкриття пароля тощо);

пасивний вплив (користувач прослуховує лінії зв’язку між двома вузлами мережі тощо);

за способом впливу на об’єкт атаки, зокрема на систему дозволів (захоплення привілеїв), а також безпосередній доступ до даних, програм, служб, каналів зв’язку з використанням привілеїв;

за засобами впливу на об’єкт атаки, що передбачають використання або стандартного ПЗ, або спеціально розроблених програм;

за об’єктом атаки: напад може здійснюватися саме на систему в цілому; на дані і програми, що знаходяться на зовнішніх (дисководи, мережеві пристрої, термінали) або внутрішніх (оперативна пам’ять, процесор) пристроях системи, а також у каналах передачі даних; на процеси і підпроцеси системи за участю користувачів. Метою таких атак є або прямий вплив на роботу процесу (його припинення, зміна привілеїв і характеристик), або зворотний вплив (використання зловмисником привілеїв, характеристик тощо іншого процесу у своїх цілях);

за станом об’єкта: безпосередньо під час атаки інформація в ньому може зберігатися, передаватися або оброблятися. Наприклад, у ході передавання інформації лініями зв’язку між вузлами мережі або всередині вузла можливий доступ до фрагментів переданої інформації шляхом перехоплення пакетів на ретрансляторі мережі, або ж прослуховування з використанням прихованих каналів;

за використовуваною системою захисту, за кількістю атакуючих, за джерелами атак, за розміщенням атакуючого об’єкта відносно до атакованого, за наявністю зв’язку з атакованим об’єктом, за рівнем еталонної моделі OSI об’єкта, на який здійснюється вплив тощо. При цьому помилки системи захисту інформації (СЗІ) можуть бути зумовлені, наприклад, помилками адміністративного управління, помилками в алгоритмах програм, а також у зв’язках між ними, помилками кодування тощо.

Зважаючи на те, що нині переважну кількість атак на практиці не застосовують, більш життєздатною вважається класифікація, запропонована П. Нойманом, який пропонує сконцентрувати увагу на двадцяти шести

основних типах таких дій (табл. 1.1), які можуть бути спрямованими проти розподілених ІТС.

Найбільш розповсюдженими способами їх здійснення є mailbombing, sniffer пакетів та IP–спуфінг, DoS і DDoS атаки, парольні атаки, атаки типу Man–in–the–Middle та/або Side Channel Attack, атаки на рівні додатків типу логічних бомб і троянських коней, вірусні атаки, атаки з використанням мережевих черв'яків та так звані ін'єкції.

Наприклад, mailbombing, як спосіб здійснення атаки, за розумінням П. Ноймана та інших фахівців полягає в бомбардуванні ПК протиборчої сторони електронною поштою. Сьогодні mailbombing практично не використовується.

Сніфер пакетів – програма, яка використовує мережевий інтерфейс є у так званому нерозбірливому (promiscuous mode) режимі, перехоплює мережевий трафік, призначений для інших вузлів, та здійснює його подальший аналіз. Результати застосування дають можливість виявити паразитний, вірусний і закільцьований трафік; виявити в мережі шкідливе і несанкціоноване ПЗ (мережеві сканери, флудери, троянські програми тощо); перехопити будь–який, призначений для користувача, незашифрований, а деколи і зашифрований трафік з метою отримання паролів та іншої інформації; локалізувати несправність мережі або помилку конфігурації мережевих агентів).

Таблиця 3.1

Основні типи кібернетичних атак відповідно до класифікації П.Ноймана

Тип атаки		Спосіб здійснення	Результат
Зовнішні		Візуальне спостереження	Спостереження за клавіатурою або монітором
		Омана	Омана операторів або користувачів
		Вилучення сміття	Вилучення інформації із сміттєвих корзин
Апаратні		Логічне відновлення	Вилучення інформації з викрадених носіїв
		Прослуховування	Перехоплення даних
		Втручання	
		Фізична атака	Руйнування або ушкодження обладнання, джерел живлення
		Фізичне видалення	Вилучення обладнання або сховищ даних
Маскувальні		Імітування	Використання хибних ідентифікаторів
		Узурпація ліній зв'язку або хостів	
		Атака з підміною параметрів	
		Заплутування мереж	Маскування фізичного місця розташування або маршруту
Злоякісні програмні коди		Троянські коні	Упровадження злоякісного коду
		Логічні бомби	Різновид троянських коней
		Черв'яки	Заволодіння розподіленими ресурсами
		Віруси	Прикріплення до програм та розповсюдження
		Обхід	Обхід механізмів безпеки
		Експлуатація уразливостей	
		Зламування паролів	
Зловживання	Активне	Інкрементальні атаки	Поступова ескалація привілей, повільне просування до мети
		Відмова в обслуговуванні	Здійснення масованих атак
	Пасивне	Огляд	Випадковий або вибірковий пошук
		Збір та виведення даних	Використання баз даних та аналіз трафіку
		Приховані канали	Використання прихованих каналів або інших способів витоку інформації

1.4 Напрямки вирішення поставленної задачі

Аналіз ведення сучасних гібридних війн у світі та проведення кібернетичних операцій, свідчить про розвиток форм, способів та методів, які застосовуються для проведення атак на систему управління ІР та ІС. В свою чергу ефективність ІС, залежить від інфраструктури, робота якої ґрунтується на застосуванні множини відповідних підсистем, які забезпечують функціонування ІС, в тому числі підсистеми захисту програмних та апаратних інформаційних ресурсів. Застосування ІС вимагає урахування особливостей, якими вони характеризуться під час функціонування. Ці особливості обумовлюють множину вразливостей, які можуть бути використані для здійснення впливу в ІС з метою порушення безпеки або для організації атак на ІС. Тому метою магістерської роботи є підвищення ефективності управління станом захищеності ІР від зовнішніх та внутрішніх атак на ІС.

В цілому постановка завдання дисертаційного дослідження зазначена на рис. 1.14.

Ри

сунок 1.14 – Постановка завдання дисертаційного дослідження

Необхідно збільшити достовірність прийняття управлінського рішення щодо оцінки стану захищеності державних інформаційних ресурсів за умов, що час прийняття управлінського рішення буде не більше ніж у існуючих методів:

$$\begin{cases} D \to \max; \\ D > D_{isn} \\ T \le T_{isn} \end{cases}.$$

РОЗДІЛ 2. ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ, ЩО ОБРОБЛЯЮТЬСЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

2.1 Аналіз систем управління захищеними інформаційними ресурсами

Реформування та розвиток системи забезпечення державної безпеки країни, спеціальних ІС та захисту інформації, як складової системи забезпечення національної кібербезпеки, залишається одними з ключових питань. Система забезпечення національної безпеки грунтується на державних інтересах та формується з урахуванням реальних загроз та викликів безпеці.

Сукупність ресурсів, що розподіляються між кінцевими точками ІС та надають користувачам певні послуги (або їх набір) називають базовою платформою надання цих послуг. До ресурсів зберіганнят та обробки даних відносять продуктивність мікропроцесорів та обсяги пам’яті ПК, які працюють у мережі, а також час, протягом якого вони застосовуються.

Інформаційні ресурси використовуються і формуються на основі певних процесів та різних методів організації суспільно важливої діяльності. Процеси реалізації та перетворення знань через використання інформаційного ресурсу отримують впровадження за рахунок інформаційних технологій, а для збереження і отримання переваг в умовах конкуренції кожна дія в кіберпросторі має великий вплив у світі фізичних ресурсів: фінансових та предметних. Це розподіляється в мережевих банках даних, з якими працюють користувачі ІС. Ці ресурси визначають цінність ІС, тому їх необхідно: постійно створювати та поповнювати; вчасно архівувати та оновлювати; користування мережею повинно забезпечувати можливість отримання оптимальної інформації саме тоді, коли в ній виникає потреба.

До програмних ресурсів додається мережеве ПЗ, а саме:

– мережеві ОС, серверне ПЗ, ПЗ користувачів;

– прикладне спеціалізоване ПЗ;

– інструментальні засоби: аналізатори проходження трафіку, засоби мережевого контролю, програми додаткових функцій, обслуговування мережевих електронних поштових скриньок, утиліти, автентифікація, криптозахист інформації,

Ресурси ІС дозволяють здійснювати обробку інформації, забезпечувати ефективний моніторинг її в будь-якому місці ІС, зберігати й накопичувати дані. Сукупність мережевих ІР забезпечують можливість передачі в просторі інформаційних повідомлень, взаємодію ІС, виробництво нових послуг та інформації.

ІР представляють собою необхідну інформацію, що є доступною за допомогою ІТ, а саме інформаційних процесів, що використовують засоби ПК та забезпечують необхідну швидкість обробки інформації, швидкий пошук її, розосередження інформаційних даних, доступ до джерел даних незалежно від їх розташування. ІР включають відкриту інформацію, конфіденційну інформацію та таємну інформацію. В свою чергу інформаційні технології класифікують:

– за способом можливої реалізації;

– за ступенем задач управління;

– за класом технологічних операцій;

– за типом інтерфейсу користувача;

– за топологією мережі;

– за сферами обслуговування.

Однією з найпоширеніших ІТ є ІС, що представляє собою сукупність інформаційних технологій, які у процесі обробки даних діють як єдине ціле. ІС відіграють важливу роль в інтеграції ІР у сферах життєдіяльності людини та суспільства.

Під ІС як фізичним об’єктом слід розуміти набір територіально розрізнених користувальних систем, які об’єднані ІС, що забезпечує

взаємодію прикладних процесів в кінцевих системах та їх колективний доступ до ресурсів ІС.

ІС відображає інформаційні процеси, які відбуваються в мережі в результаті взаємодії кінцевих пристроїв, під'єднаних до ІС. Вона передбачає розгляд мережі в сукупності зі взаємоповязаними за допомогою неї об'єктами [19]. У такому розумінні ІС являє собою навантажену мережу.

Робота в ІС виконується перефирією, тобто в кінцевих пристроях мережі, а ІС виконує функції транспортування (рис. 2.1).

Рисунок 2.1 – Структура інформаційної системи

Параметри оцінки ефективності ІС визначаються рівнем продуктивності її, як системи розподільчих ресурсів, та складаються з:

- реакції мережі в часі;
- інформаційна затримка передачі даних;
- типи затримки даних;
- відкритість.

ІС є комплексом пристроїв користувачів, кінцевих систем та універсальної платформи надання послуг, які відповідають вимогам користувачів до їх типу та якості (рис. 2.2).

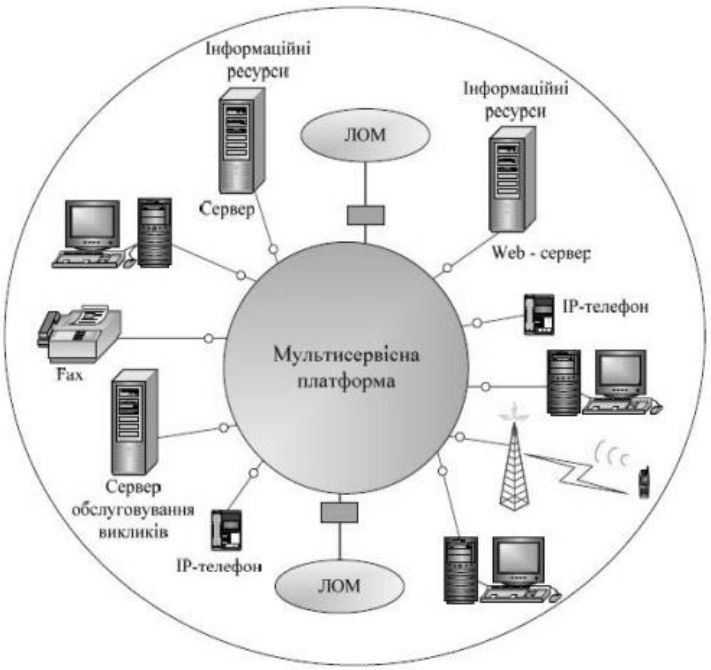


Рисунок 2.2 – Структура інформаційної мережі

Таким чином ІС дозволяє вирішувати такі актуальні завдання:

– надання можливості обміну повідомленнями різного типу (мова, відео, дані);

– своєчасне отримання необхідної інформації з будь-якого джерела в мережі;

– автоматизація накопичення, обробки, зберігання великих обсягів даних в мережі.

До ІС входять наступні елементи: бази даних та системи управління базами даних, канали зв'язку, обчислювальна техніка, система доступу до каналів зв'язку, системи захисту. Узагальнена структура ІС показана на рис. 2.3.

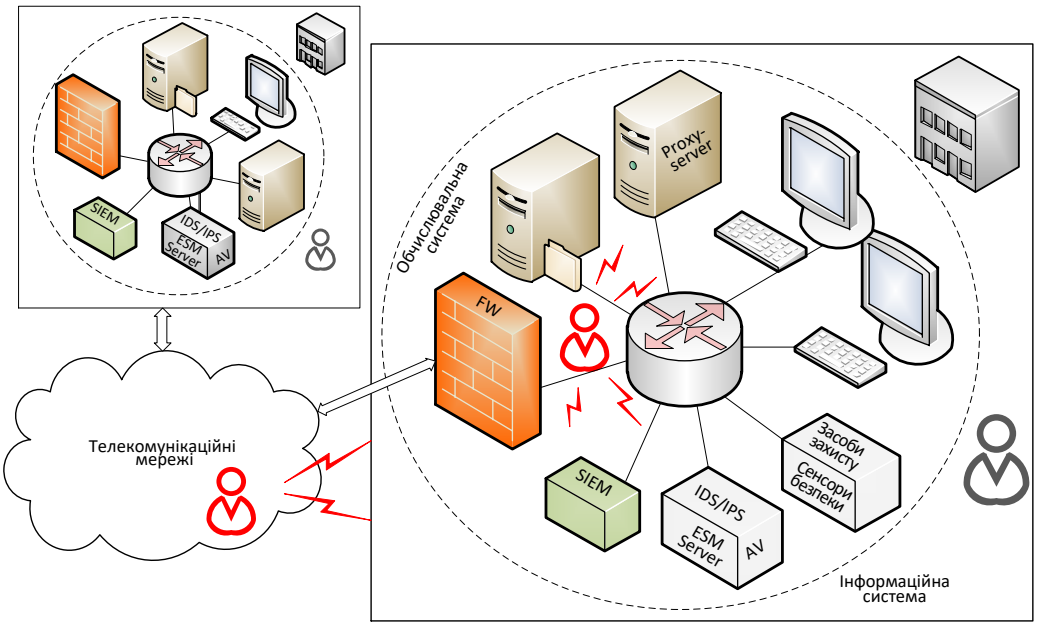


Рисунок 2.3 – Узагальнена структура ІС

Для забезпечення безпеки кіберпростору необхідне впровадження КСЗІ, а саме систем:

– розмежування доступу;
– застосування міжмережних екранів;
– криптозахист інформації;
– віртуальні приватні інформаційні мережі;
– антивірусного захист ІС;
– СВА та СВВ;
– автентифікації, ідентифікація і аудиту;
– контроль цілосності даних;
– управління інциндентами та подіями.

З проведеного аналізу видно, що сучасним ІС присуща велика кількість вразливостей рис. 2.4.

Приклади частих уразливостей, що виникають при організації захищених ІС і можуть бути використані для реалізації НСД, наведено на рис. 2.4.

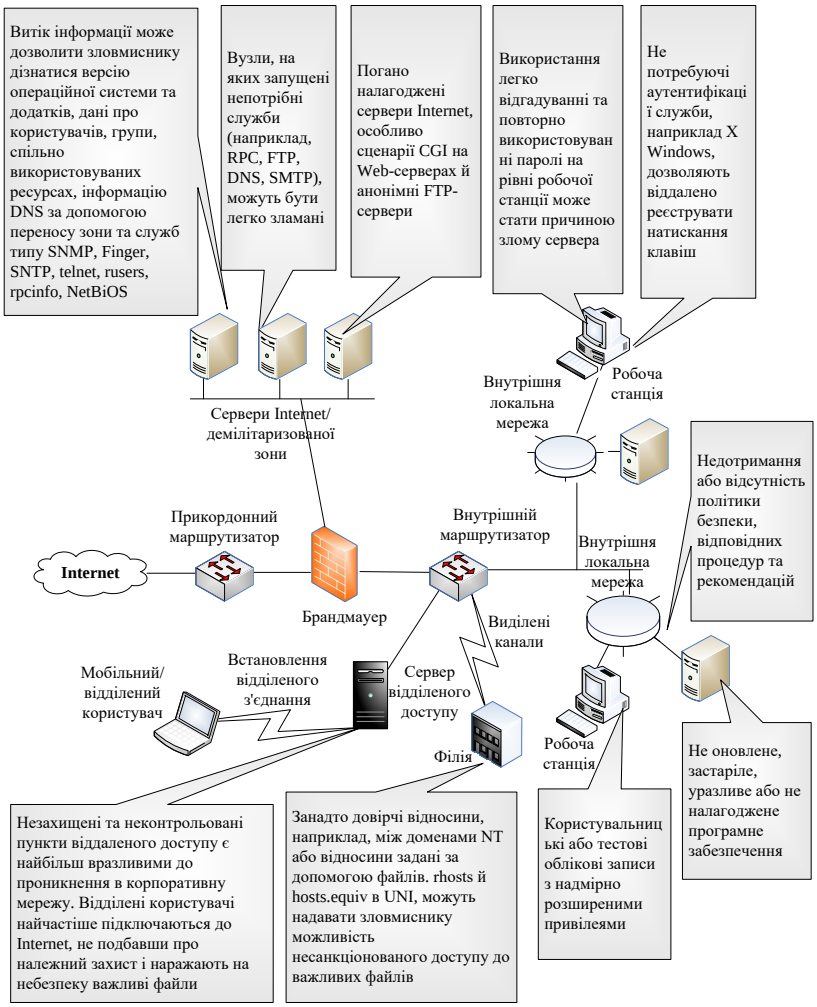


Рис. 2.4. Приклади уразливості в інформаційних мережах

В основному ефективність захисту ІС визначається кіберстійкістю ІС до атак та роботі при наявності дестабілізуючих факторів. Тому з метою оцінки функціонування ІР за умов викликів безпеці та загроз необхідно провести детальний моніторинг вразливостей ІС, загроз ІР та атак.

Враховуючи особливості процесу обробки ІР засобами передачі, під ІР слід розуміти взаємопов’язану сукупність інформації, що належить організації, носіїв інформації, засобів передачі та персоналу, що захищається системою захисту.

Слід відмітити, що існуючі сучасні ІС відображають складову кіберпростору та призначені для функціонування ІР. Для забезпечення безпеки ІР необхідно аналізувати сучасні вразливості та їх кваліфікаційні властивості, а також механізми захисту.

2.2 Аналіз вразливостей та атак на інформаційні ресурси, що обробляються в інформаційних системах

На фоні системи забезпечення безпеки значущою стає вимога забезпечення безпеки ІР в інформаційному середовищі та спроможності системи управління та підсистеми забезпечення безпеки (ПЗБ) здійснювати достовірне та оптимальне визначення загроз на стан безпеки ІР на основі оцінки значень множини відповідних показників. Доленосним питанням для прийняття управлінських рішень в ПЗБ є питання визначення достовірного впливу загроз на стан безпеки ІР.

Одним з факторів розвитку ІТ є об'єднання програмних продуктів, спеціалізованих технічних засобів (СТЗ) та систем передачі даних. Таке поєднання надає сучасним СТЗ нові можливості у користуванні та управлінні. Зворотною стороною таких переваг є вразливості програмно-керованих СТЗ. Крім відомих ТКВІ слід враховувати загрози віддаленого НСД технічних засобів, а також впровадження шкідливого ПЗ та програмних й технічних закладок. Зазначені загрози можуть функціонувати з метою порушення цілісності, конфіденційності, достовірності та доступності інформації, яка обробляється технічними засобами, а також порушення конфіденційності інформації.

Сучасне місце користувача обладнане рядом технічних засобів, які у процесі технологічного розвитку перейшли від «звичайних» технічних засобів (ТЗ) до спеціалізованих технічних засобів. До них можна віднести системи телебачення, зв'язку, відеонагляду, мультимедійні системи, ІС тощо. ТЗ пропонованих систем мають у своїй структурі модулі або інтерфейси ПД,

які за відповідних умов можуть застосовуватися в якості можливих каналів несанкціонованого управління ТЗ. Використання СТЗ, які мають у своїй структурі модулі та інтерфейси передачі інформації, потребує впровадження додаткових заходів із ЗІ, враховуючи існуючі загрози [25].

З позиції теорії систем, ПЗБ відносяться до класу складних систем, строге моделювання яких становить актуальне завдання. Ситуація ускладнюється тим, що різні ОІД кіберзахисту відносяться до відповідності різних суб'єктів державної системи безпеки та мають індивідуальну направленість до використання нормативних документів.

Порушення захисту у сфері застосування ІС розподіляються на такі види:

– НСД до функціонування мереж, баз даних;

– збут або поширення шкідливих ПЗ або ТЗ;

– НСД до інформації з обмеженим;

ІТ дають можливість отримати важливий ефект регулювання інформаційного впливу залежно від користувача.

Зараз в усьому світі гостро постає проблема щодо захисту ІР у зв'язку з наданням доступу до ІР через відкритий інформаційний простір. Кількість комп'ютерних злочинів постійно збільшується, збільшилась ймовірність загрози атак на більш високому рівні для реалізації політичної і економічної мети.

ІС та ІР мають великі можливості надання впливу на формування громадської думки, прийняття економічних, військових і політичних рішень, впливу на ІР зловмисника і поширення у мережі дезінформації.

Поняття інформаційна зброя (ІЗ) включає електронний і людський аспекти.. Основними завданнями застосування ІЗ у мережі є:

– порушення цілісності та доступності, конфіденційності інформації;

– проходження комплексних систем захисту;

– обмеження доступу легальних користувачів, дезорганізація роботи ТЗ, комп'ютерних систем.

Види ІЗ у глобальних мережах [27]:

– програми типу “комп’ютерні віруси”;

– вразливі програми типу “троянський кінь”;

– вразливі програми типу “логічна бомба”;

– “люк” – це залишені розробником функції через які можна здійснити НСД та обминути механізми захисту;

– засоби порушення інформаційного обміну;

– засоби локалізації тестових програм;

–помилки, які вводяться порушником до ПЗ;

– електромагнітний вплив на техніку з метою знищення даних, виведення обладнання з ладу, модифікації налаштування та створення умов для НСД до ІР.

Ці засоби надають можливості зловмиснику завдавати інформаційних впливів на систему.

Прихованість, багатоваріантність, універсальність, форм програмно-технічної реалізації, достатній вибір часу і місця застосування, радикальність впливу, економічність роблять ІЗ надзвичайно небезпечною: вона може маскуватися під засоби ТЗ тп ПЗ.

Для запобігання або усунення наслідків використання ІЗ необхідно впровадити наступні заходи:

– захист ОІД, що складають фізичну основу ІР;

– забезпечення стійкого функціонування баз і банків даних;

– перекручування або знищення, захист інформації від НСД;

– збереження цілосності інформації.

Атаки реалізуються хакерами для порушення цілісності конфіденційності або доступності ІР, що обробляється, зберігається та циркулює в ІС. З цією ціллю використовують вразливості ІС, тобто неможливість системи протидіяти реалізації певної загрози або сукупності загроз. Структура реалізації атак представлена на рис. 2.5.

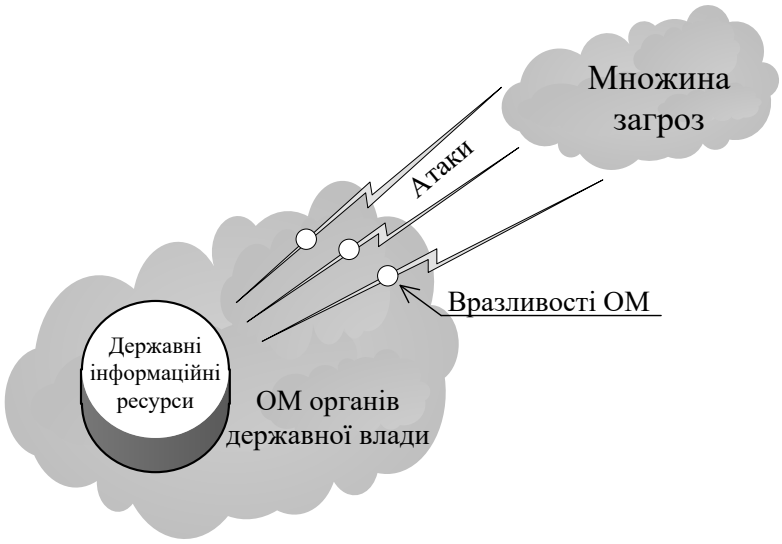


Рисунок 2.5 – Загальна структура реалізації атак

Для одержання даних про можливі вразливості на інформацію, вимога щодо захисту якої регламентується законодавством, інформаційні наслідки цього прояву, а також виявлення небезпечних атак застосовують модель (рис. 2.6), де КБА – можливі комбінації атак, S – можливі підмножина станів ІС, ВФ – виконання необхідних функцій ІР, ІНПІС – переход ІС, МСЗІР – модель СЗ ІР.

Здійснено аналіз характеристик безпеки ІР, таких як: вразливості ІР, кібервплив ІС та вторгнень на ІР. Розглянуто бази даних, які включають опис вразливстей атак та загроз.

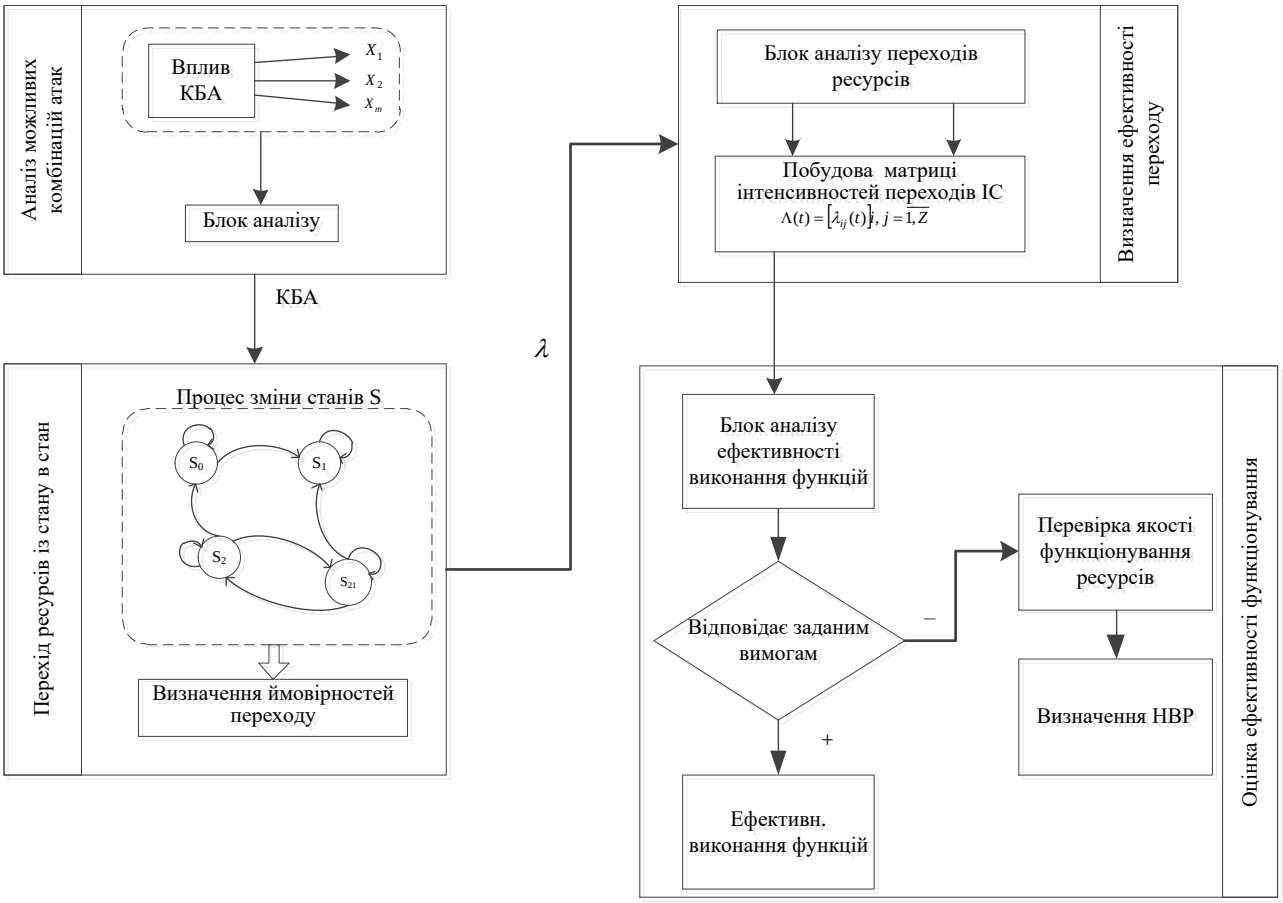


Рисунок 2.6 – Модель поводження системи при впливі атак

Розглянемо детально деякі бази вразливостей:

– CVE – пошуково-довідкова система позначень та посилань вразливостей. Відмінною складовою є CVE ідентифікатори – які надаються кожній вразливості в сфері ІБ. Система містить 88000 записів про відповідні вразливості. Основна відмінність відзначається в тому, що вона є повною та систематизованою, тому застосовують як основу для відповідності записів вразливостей в інших базах.

Під порушенням безпеки розуміємо НСД в ІС, в результаті діяльності, що порушують безпекову політику або обходять СЗІ. Під певною атакою слід розуміти спробу винекнинння загрози. Відповідно загроза є обставина або подія, що є причиною порушення функціонування ІС, апаратним та програмним складовим мережі, нанесення збитків, політиці безпеки, тощо.

Існуючі типи атак на ІС представлені (таблиця 1.2), та їх параметри. З точки зору атаки важливим є взаємне розташування об’єкта атаки та суб’єкта, тобто де вони знаходяться в різних чи в однакових сегментах. При внутрисегментній атаці, суб’єкт і об’єкт атаки знаходяться в одному сегменті. При межсегментній атаці суб'єкт і об’єкт атаки розташовані в різних мережевих сегментах. Ця ознака дає можливість судити про “ступінь віддаленості” атаки.

Внутрисегментну атаку можна здійснити простіше, ніж міжсегментну (зовнішню). Також зовнішня атака представляє більшу небезпеку, ніж атака внутрішня. Це пояснюється тим, що при внутрішній атаці її об’єкт і субєкт перебувають на відстані тисяч кілометрів один від одного, що перешкоджає заходам по протидії атакам.

Таблиця 1.2 - Класифікація атак

Таблиця 1.2 – Класифікація атак

Ознака атаки	Тип атаки	Характеристика атаки
За характером впливу	пасивні	Атаки, що не мають безпосереднього впливу на роботу системи, але можуть порушувати її політику безпеки. Важко виявити. Після атаки не залишається ніяких слідів. Приклад: прослуховування каналу зв'язку в мережі.
	активні	Атаки, що безпосередньо впливають на роботу системи (зміна конфігурації ІС, порушення працездатності і т. д.) і порушують прийняту в ній політику безпеки. Практично всі типи віддалених атак є активними. Існує можливість виявлення, так як в результаті здійснення атаки в системі відбуваються певні зміни.
За метою впливу	порушення конфіденційності	Перехоплення інформації. Приклад: прослуховування каналу в мережі.
	порушення цілісності	Спотворення інформації. Прикл.: впровадження помилкового об'єкта в ІС.
	порушення доступності	Не відбувається НСД (зберігається цілісність і конфіденційність), проте доступ до інформації легальних користувачів неможливий. Приклад: відмова в обслуговуванні.
За умовою початку здійснення впливу	атака на запит від об'єкта, що атакується	У разі запиту атакуючий очікує передачі від потенційної мети атаки запиту певного типу, який і буде умовою початку здійснення впливу. Ініціатором здійснення початку атаки є об'єкт, що атакується. Приклад: DNS- і ARP-запити в стеці TCP / IP.
	атака по настанню події, що очікується на об'єкті	У разі настання події, атакуючий здійснює постійне спостереження за станом операційної системи віддаленої цілі атаки і при виникненні певної події в цій системі починається вплив. Ініціатором здійснення початку атаки є об'єкт, що атакується. Приклад: переривання сеансу роботи користувача з сервером в мережевих операційних системах без видачі команди LOGOUT.
	безумовна атака	У разі безумовної атаки початок її здійснення безумовно по відношенню до мети атаки, тобто атака здійснюється негайно і безвідносно до стану системи і атакується об'єкта. Ініціатором здійснення початку атаки є атакуючий.
За наявністю зворотного зв'язку з об'єктом, який атакується	зі зворотним зв'язком	Атака зі зворотним зв'язком – атака, під час якої атакуючий отримує відповідь від об'єкта на частину своїх дій. Ці відповіді потрібні, щоб мати можливість продовжити атаку і/або здійснювати її більш ефективно, реагуючи на зміни, що відбуваються в системі.
	без зворот-ного зв'язку (односпрямована атака)	Атака без зворотного зв'язку – атака, яка відбувається без реакції на поведінку системи, що атакується. Приклад: відмова в обслуговуванні.
За кількістю атакуючих	розподілена	Атака, вироблена двома або більше атакуючими на одну і ту ІС, об'єднаними єдиним задумом і в часі.
	нерозподілена	Нерозподілена атака проводиться одним атакуючим.
По розта-шуванню атакуючого щодо ата-куємого об'єкта	внутрисег-ментна	Атака, при якій суб'єкт і об'єкт атаки знаходяться всередині одного сегменту мережі (сегмент – фізичне об'єднання станцій за допомогою комунікаційних пристроїв не вище канального рівня).
	міжсегментна	Міжсегментна атака – атака, при якій суб'єкт і об'єкт атаки знаходяться в різних сегментах мережі.

Проаналізувавши вразливості та атаки на ІР, що обробляються в ІС, показав велику кількість підходів до побудови баз даних вразливостей, кожен має свої недоліки та переваги, але найбільш значущим є орієнтованість задекларованих баз вразливистей для застосування в експертних системах. Сучасні ІС обробки та зберігання ІР мають значну кількість внутрішніх і зовнішніх вразливостей, а реалізація яких здійснюється у відповідності множини різнонаправлених та цільових атак. Розповсюдження вразливостей певного вузла ІС може призвести до появи додаткових вразливостей безпеці ІР, що в ній функціонує. Таким чином для визначення множини інформаційних параметрів при оцінці захищеності ІР повному обсязі та виявлення нових атак, доцільно здійснювати функціонування СУ подіми ІБ з урахуванням запропонованих вимог, параметрів даних та особливостей сучасних СУ ІР.

2.3. Аналіз методів управління безпекою інформаційних ресурсів інформаційних систем

Технологія безпеки надає інформацію про моніторинг подій безпеки з мережевих пристроїв і програм подія управління (SIEM). SIEM визначається як програми, пристрої або служби , а також використовується для збору даних і створення звітів. Сегмент систем управління безпекою, пов’язаний із моніторингом у реальному часі, кореляцією подій, сповіщеннями та відображенням на кінцевих пристроях, зазвичай називають керуванням подіями. Друга область, яка називається керуванням зберіганням даних, забезпечує довгострокове зберігання, аналіз і звітування про зібрані дані. Оскільки попит на додаткові функції зростає, функціональність цієї категорії продуктів постійно розширюється та доповнюється.

Концепція управління інцидентами інформаційної безпеки, описує здатність продукту збирати, аналізувати та подавати інформацію з мережевих і захисних пристроїв, ідентифікацій (керування ідентифікацією) і програм контролю доступу, а також підтримувати політика безпеки інструментів і моніторинг уразливостей, операційні системи, журнали баз даних і програм, а також інформація про зовнішні загрози.

Керує параметрами користувачів і послуг, службами каталогів та іншими змінами конфігурації, а також перевіряє та переглядає журнали, а також реагуйте на події. Система збирає дані, аналізує їх (і генерує сповіщення), зберігає в базах даних і аналізує поведінку (і генерує попередження) на основі попередніх спостережень. На практиці схема реалізується за допомогою таких компонентів: агенти (збирають дані з різних джерел); сервери збору (збір даних від агентів); сервер бази даних (сховище даних); кореляційний сервер (аналіз даних). Вхідними даними для системи SIEM можуть бути різноманітні дані.

Функціональність :

- збір даних: інформація збирається з різних джерел: мережевих пристроїв і служб, датчиків системи безпеки, серверів, баз даних, програмного забезпечення; забезпечує консолідацію даних для виявлення критичних інцидентів. керування журналами даних; кластеризація.

технологія дозволяє використовувати різні методи для інтеграції інформації з різних джерел для перетворення необроблених даних у значущу інформацію. Кореляція є типовою ознакою управління інцидентами безпеки.

- повідомлення: автоматичний аналіз корельованих подій і створення звітів (оповіщень) про поточні проблеми. Повідомлення можна відображати в панелі програми і відправляти на інші сторонні канали: електронну пошту, GSM-шлюз і т.д.

- інструменти візуалізації (дошка): відображають діаграми, які допомагають визначити шаблони, які відрізняються від стандартної поведінки.

- відповідність (трансформація): автоматизація збору даних, створення звітів для адаптації зібраних даних до поточних процесів управління інформаційною безпекою та аудиту.

- сховище даних: довгострокове зберігання даних в історичному порядку для зв'язування та трансформації даних з часом. Довгострокове зберігання даних має важливе значення для комп'ютерної та технічної криміналістики, оскільки розслідування мережевих подій зазвичай відбувається після моменту злому.

- експертний аналіз: можливість пошуку багатьох журналів за різними кнопками; можна зробити в рамках програмно-технічної експертизи.

Документ [27] визначає такі випадки використання SIEM:

може виявляти вразливості нульового дня та поліморфні віруси. Перш за все, це пов'язано з низьким рівнем виявлення антивірусів проти шкідливих програм, що швидко змінюються.

- автоматичний аналіз журналу, нормалізація та класифікація можуть виконуватися автоматично. Незалежно від типу комп'ютера чи мережевого пристрою пристрій може реєструвати події.

- візуалізація з SIEM, а також використання журналів подій безпеки та збоїв можуть допомогти визначити шаблони.

- журнал помилок може вказувати на неправильну конфігурацію або проблему безпеки. Що SIEM може знайти за допомогою розпізнавання шаблонів, сповіщень і аналітики.

- SIEM може виявляти секретні, шкідливі повідомлення та зашифровані канали.

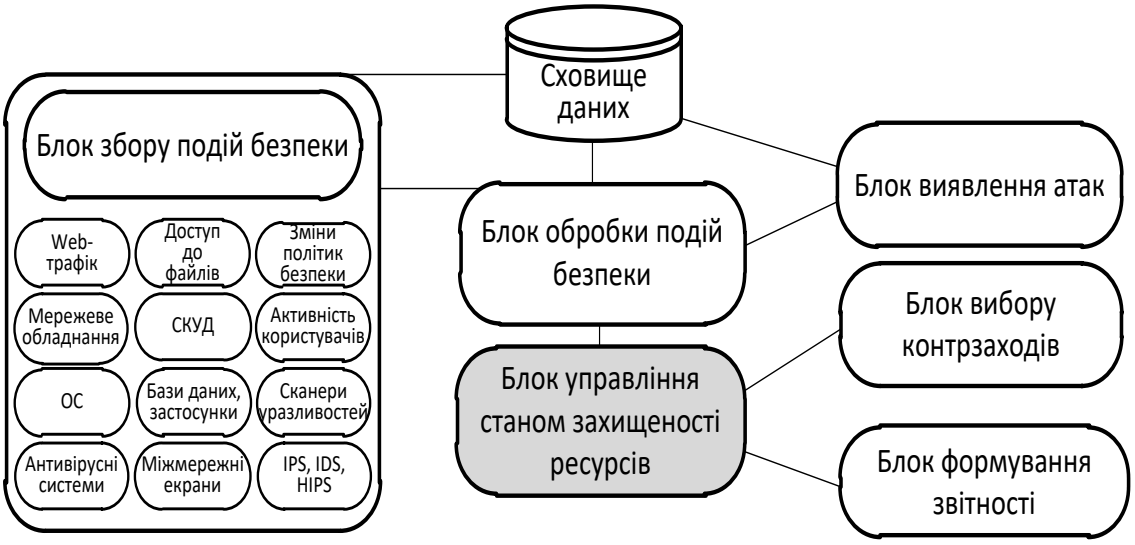
- атака може бути виявлена з точністю, що дозволяє SIEM ідентифікувати як атаку, так і жертву .

SIEM є ядром центру контролю кібербезпеки та, загалом, системи захисту, розробленої будь-яким державним органом. Вони збирають інформацію з різних систем безпеки , таких як брандмауери, IPS і антивірус, і дозволяють виявляти підозрілі та потенційно небезпечні ситуації.

Перші рішення SIEM з'явилися близько десяти років тому в системах керування журналами подій. Необхідність таких рішень пов'язана зі збільшенням кількості загроз, схожих на «сніжки», їх складністю та появою цілеспрямованих атак, у тому числі з використанням різних векторів проникнення. SIEM може бути реалізований у формі апаратного чи програмного забезпечення (віртуальний пристрій) і може бути розміщений на території замовника або в хмарі. Робоча схема SIEM наведена на рис. 2.7 .

SIEM збирає дані з усіх мережевих вузлів і різних пристроїв безпеки (інтернет-екранів, систем виявлення та запобігання вторгненням, антивірусів робочих станцій тощо), співвідносить їх у реальному часі та сповіщає співробітників про порушення встановлених правил. Ці правила можна скоригувати відповідно до потреб організації, щоб визначити пріоритетність ризиків і зменшити помилкові спрацьовування. Оскільки атаки стають все

більш витонченими, зростає потреба у вдосконаленні механізмів їх виявлення.



Ry сонок 2.7 є в наявності інформації безпеки подія управління до робити системи структурний діаграма

Атака – це навмисна дія в інформаційному середовищі, яка включає електронні комунікації (включаючи дані, програмне забезпечення, апаратне забезпечення, інші технічні чи технологічні засоби та обладнання) і спрямована на одну або декілька з наступних цілей: конфіденційність, цілісність, доступність IP;. отримання НСД за вказані ресурси; порушення захищеності, стабільного, надійного режиму роботи ІБ; використання ІС, її ресурси і виконувати для електронних комунікацій для здійснення атак на інші об’єкти кіберзахисту.

Забезпечення безпеки ІС оброки IP пов’язано з вразливостями ІС, які зумовлені передачею інформації в інформаційне середовище, масштабованістю, необхідністю збору значної кількості службової інформації про стан системи для функціонування методів та протоколів на різних рівнях мережевої моделі OSI [22]. Зазначені вразливості можуть бути використані зловмисником для здійснення вторгнень або атак на ІС з метою порушення властивостей IP, або організації деструктивного впливу на сам процес функціонування ІС.

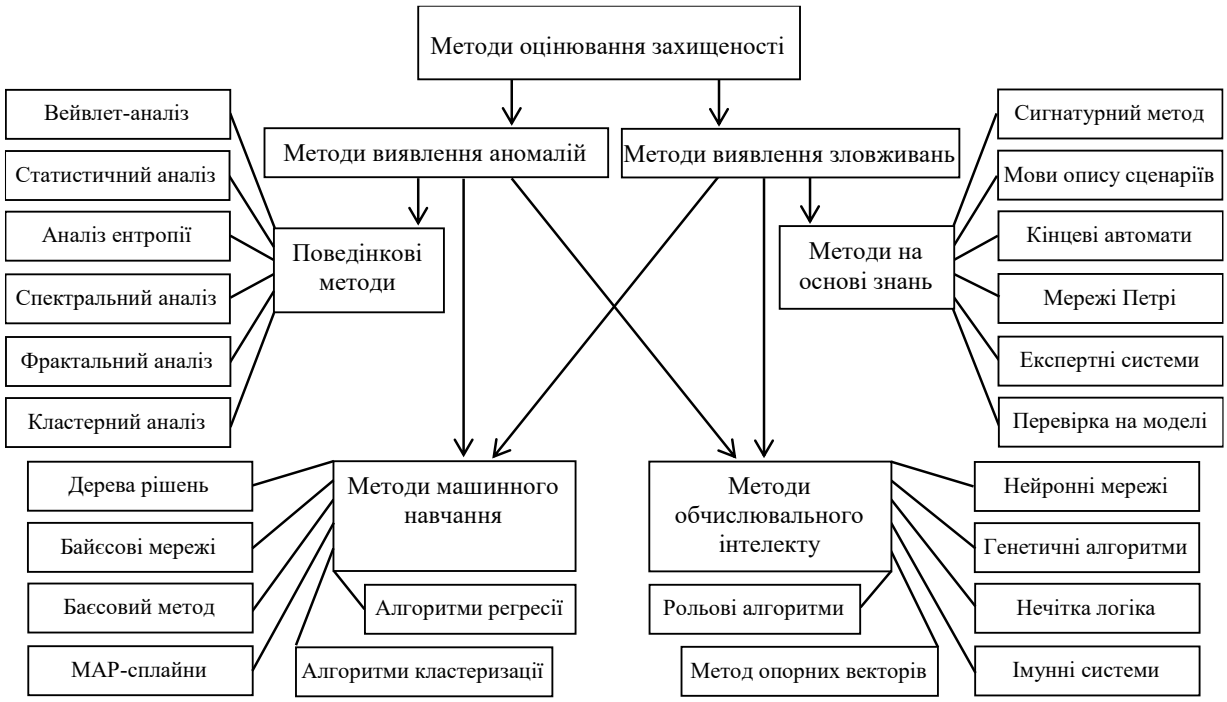
Не менш важливим завданням є управління безпекою, яке визначає безпеку ІБ та адекватність реалізованих заходів безпеки.

Безпека ІР – це сукупність станів, що забезпечують безпеку ІР, тобто їх конфіденційність, цілісність і доступність. Процес управління станом захищеності ІС передбачає перевірку можливості порушення таких станів доступними зловмиснику способами. Виконання цієї процедури вимагає вирішення наступних завдань: збір інформації про компоненти ІС; обробка цієї інформації і побудова прийнятної моделі ІС на основі отриманих результатів для подальшого використання при оцінці ризиків ІС. В свою чергу забезпечення безпечного функціонування ІС представляє собою безперервний процес прийняття рішення з оцінювання стану захищеності ІС, ефективності реалізованих засобів захисту, дестабілізуючих факторів та визначення оптимального набору засобів захисту.

Методи управління станом безпеки, які ґрунтуються на ймовірнісному підході або перевірці відповідності вимогам, встановленим на етапі технічного завдання, не враховують реальну захищеність ІБ, а дають лише приблизну оцінку на основі інформації, отриманої експертами.

Першим кроком в управлінні безпекою ІБ є оцінка поточного стану ІБ, який можна реалізувати відповідними методами. Класифікація методів оцінки безпеки наведена на рис. 2.8.

Розглянуті методи здебільшого використовуються в системах з такими характеристиками: необмежені ресурси, час прийняття рішень, точність прийняття рішень, застосовність у невизначеному середовищі та відкрита структура не враховуються. не адаптована. розділяти функціональні можливості тощо. Тому необхідно встановити комплекс вимог до методів управління станом безпеки ІБ, а саме: функціонування в режимі реального часу; розгляд загроз ІБ; адаптивна робота СЗІ з самоорганізацією; децентралізація управління та ієрархічна структура розподілу; підвищення достовірності та повноти прийняття управлінських рішень; зниження математичної складності та ресурсоємності методів.



2.8. Рисунок – Класифікація методів оцінки безпеки

Як зрозуміло з аналізу, для врахування запропонованого набору вимог рекомендується вдосконалити методи управління станом безпеки, які працюють для вищезазначених характеристик СЗІ.

Таким чином проведено аналіз методів управління станом захищеності та прийняття рішень з застосування ЗЗ в ІС та встановлено, що застосування розглянутих сучасних методів не в повній мірі відповідає висунутим вимогам для методів забезпечення захищеності ІР в ІС. Для забезпечення безпеки ІР, що циркулюють в ІС, а також оцінювання реалізованих сервісів і механізмів безпеки в СЗІ, доцільно проводити комбінування та удосконалення розглянутих методів виходячи з вимог до СЗІ та функціонування ІС.

Висновки до розділу 2

У другому розділу магістерської роботи було проаналізовано стан функціонування ІР в ІС. Розглянуто роботу СУ станом захищеності в ІС та визначено основні проблеми щодо функціонування підсистеми оцінювання

як складової СЗІ. Здійснено моніторинг основних типів атак на IP, вразливостей ІС які застосовуються при проведені атак, а також засоби та методи керування станом захищеності IP в ІС. Можна ствердждувати, що існуючі методи можуть оцінювати рівень захисту на застосуванні повної вибірки характеристичних параметрів атак, але нажаль не враховують особливості функціонування ІС, що нажаль не враховує можливості визначення нових типів атак, визначення управлінських рішень, які направлені на підтримання стану захисту системи, та призводить до зменшення достовірності і збільшення часу прийняття управлінських рішень. Запропоновано при розробці методів керування станом захисту IP в ІС здійснити розподіл на основі визначеної множини параметрів, що притаманні внутрішнім і зовнішнім атакам та необхідно удосконалити існуючі методи керування станом захисту IP в ІС, за рахунок використання методів ідентифікації та опорних векторів.

РОЗДІЛ 3
ОБҐРУНТУВАННЯ МЕТОДІВ УПРАВЛІННЯ СТАНОМ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

2.1 Модель порушення захищеності державних інформаційних ресурсів, що обробляються в інформаційних системах

У зв’язку з тим, що СЗІ ІС обробки ІР має забезпечувати реалізацію прийнятої політики безпеки, керувати розмежуванням доступом, сигналізувати про небезпечні подій, виявляти атаки на ІР, проводити оцінку захищеності системи та вживати заходи щодо управління станом захищеності ІР в ІС, то СЗІ має відслідковувати весь трафік, що циркулює в ІС. Для цього СЗІ забезпечує своє функціонування на всіх рівнях базової еталонної моделі взаємодії відкритих систем (моделі OSI), здійснюючи: контроль з’єднань, аналіз структури та вмісту мережевих пакетів, контроль трафіку, оцінку станів функціонування елементів системи та ін.

При використанні ІС, метою порушення захищеності ІР може бути приховане управління кінцевими та мережевими ресурсами або вплив на інформаційні, програмні та апаратні засоби ІС. Реалізація зазначеної мети досягається використанням методів, що направлені на вразливості ІС. В свою чергу це може призвести до втрати ІР внаслідок віддаленого керування кінцевим або мережевим обладнанням. Відомі підходи до моделювання забезпечення захисту і порушення захищеності ІР використовують різний математичний апарат, враховують питання доступу суб’єктів до об’єктів, вартості захисту ІР, організації процесу захисту, тощо, але не розглядають вплив різних типів атак на імовірність реалізації порушення зовнішнім або внутрішнім зловмисником.

Під вразливістю розуміємо властивості ІС (архітектурний, програмний, організаційний або інший недолік), які можуть бути використані для здійснення деструктивних впливів. В свою чергу вразливість являє собою характеристику захищеності ІС, а будь-яка вразливість ІС несе в собі загрозу впливу на ресурси системи за допомогою атаки. Класифікацію загроз безпеці інформаційним ресурсам при вторгненні в ІС представлено на рис. 3.1.

Загрози безпеці інформаційним ресурсам																																
За ступенем наміру дії		За характером дії		За джерелом загрози		За впливом на властивості інформації			За технічною реалізацією			За способом дії на об'єкт			За розміром нанесеного збитку				За способом реалізації		За досягнутою метою		За кінцевим результатом								
навмисні	ненавмисні	активні	пасивні	внутрішні	зовнішні	конфіденційність	цілісність	доступність	сканування	відмова в обслуговуванні	вторгнення	безпосередні	на ІТС управління	опосередковані	загальні	локальні	часткові	імітаційні	вплив однієї загрози	вплив множини загроз	проміжні	кінцеві	віддалений контроль	блокування	захоплення						

Рисунок 3.1 – Класифікація загроз безпеці ІР в ІС

Вказані загрози впливають на ІС та її компоненти, які забезпечують передачу інформації у відповідності з функціональними особливостями кожного об'єкта системи. Загальна структура ІС обробки інформаційних ресурсів представлена на рисунку 3.2.

З рисунку видно, що ІС складається з множини взаємопов'язаних функціональних систем, серед яких є СЗІ. В свою чергу СЗІ містить ряд підсистем. Важливе місце в СЗІ займає підсистема управління станом захищеності, яка функціонує в тісній взаємодії з іншими підсистемами. В основу роботи підсистеми управління станом захищеності ІС покладені відповідні методи оцінювання поточного стану захищеності ІС та методи прийняття управлінських рішень про застосування механізмів і засобів захисту. Підсистема управління станом захищеності ІС отримує дані з

суміжних підсистем СЗІ, аналізує поточний стан ІС та ефективність реалізованих ЗЗ та приймає управлінське рішення щодо достатності вжитиз захисних засобів або необхідність підвищення стану захищеності.

Рисунок 3.2 – Структура ІС обробки ІР

Узагальнена архітектура підсистеми управління станом захищеності ІС та взаємодія її елементів представлені на рис. 3.3.

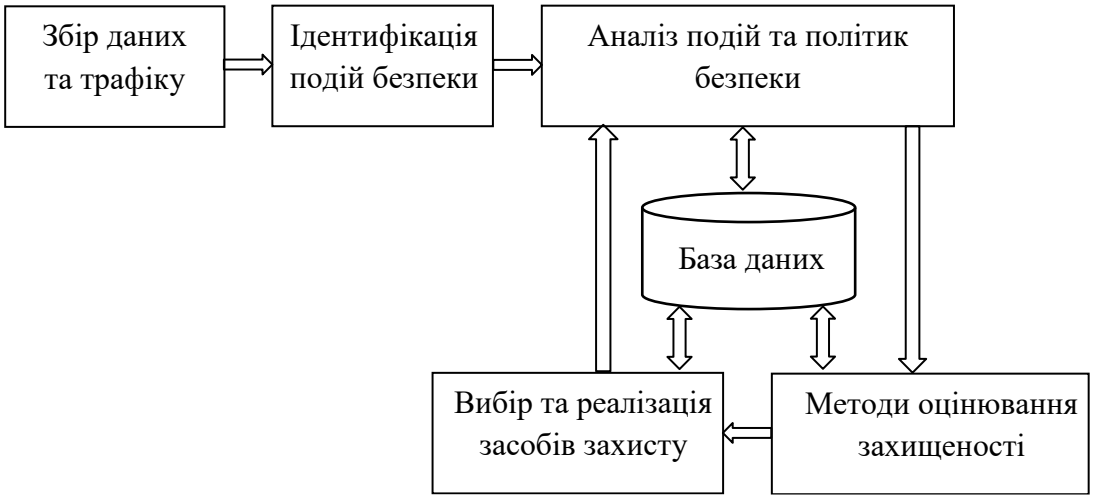


Рисунок 3.3 – Узагальнена схема підсистеми управління станом захищеності

В цілому можливо відмітити, що для ефективного функціонування СЗІ, підсистема управління станом захищеності повинна проводити власну оцінку виходячи із даних про реалізації основних типів атак, направлених на систему із зовні (зовнішні) або на елементи системи перебуваючи вже в середині системи (внутрішні) та з урахуванням множини стратегій порушення захищеності системи.

Атаки реалізуються множиною способів (вплив загрози на один чи декілька об'єктів; вплив множини загроз на один об`єкт чи декілька об`єктів, тощо). Вказані способи направлені на досягнення проміжної або кінцевої мети, в наслідок чого відбувається: відмова в обслуговуванні, віддалене контролювання, блокування або захоплення частини системи або ІС в цілому.

Розглядаючи практичне здійснення порушень або атак на інформаційні, програмні та апаратні засоби ІС, варто зазначити, що об'єктами атак є правила і технічні процедури, які здійснюють з'єднання і обмін даними в ІС.

Показники реалізації порушення захищеності ІР та здійснення атак на ІС залежать від: кваліфікації того хто реалізує порушення, обладнання яке застосовується для реалізації, покладених задач, стратегії здійснення порушення та інше. Зловмисник, в свою чергу, розраховує на вразливості об'єкту порушення та низький рівень забезпечення безпеки ІС. Також зловмисник має множину інструментів для реалізації порушень/атак, які в свою чергу впливатимуть на імовірність успішного їх здійснення.

Модель СЗІ ІР повинна відображати основні процеси, які протікають в системі з метою оптимізації процесів захисту інформації. Такі процеси в загальному вигляді можуть бути представлені як процеси розподілу і використання ресурсів, які виділяються на захист інформації. Сьогодні існує велика кількість засобів та способів забезпечення захисту ІР, що обробляються в ІС. Удосконалення СЗІ потребує побудови моделі протидії

порушенням захищеності ІР в ІС, враховуючи системний характер впливу на ІС різних за характером, місцем застосування та фізичною природою загроз.

Використання методів моделювання при забезпеченні належного рівня захищеності ІР призвело до розробки множини формальних моделей безпеки, що сприяє підтримання належного рівня захищеності систем на основі об'єктивних і незаперечних постулатів математичної теорії.

Метою моделювання в системі забезпечення безпеки ІС є побудова моделі, яка враховувала б найбільшу кількість чинників впливу і дозволяла б розраховувати ймовірність виникнення вразливості та реалізації загрози, обчислювати час реалізації загрози і можливі збитки, визначати ефективність упровадження засобів захисту та стан захищеності системи.

Захищеність ІС характеризує ступінь адекватності механізмів захисту інформації, які реалізовані в ІС, ризиків, що існують в середовищі та загрози безпеці. Взаємодію загроз, ресурсів ІС та СЗІ описує узагальнена типова модель процесу захисту з повним перекриттям загроз [63], яку представлено на рис. 3.4.

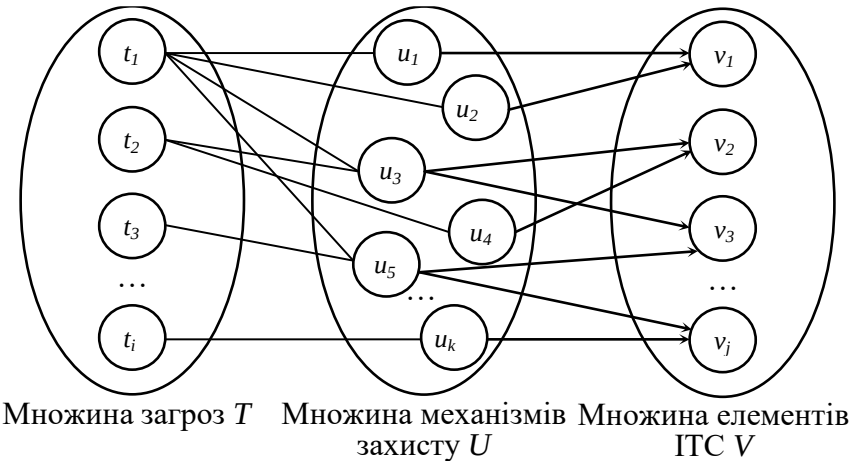


Рисунок 3.4 – Типова модель процесу захисту інформації з повним перекриттям

В даній моделі вважається, що кожній загрозі СЗІ протистоїть певний механізм захисту. Побудована за таким принципом СЗІ не дозволяє впливати загрозам на області, які захищаються. Основним положенням захисту з повним перекриттям є теза про те, що ІС повинна мати хоча б один ЗЗ на

кожному можливому шляху впливу загроз на ресурси ІС. Дану модель доцільно використовувати в поєднанні з іншими типами моделей СЗІ. При синтезі систем забезпечення безпеки в ІС такий підхід дозволяє мінімізувати витрати ресурсів ІС для забезпечення заданого рівня захищеності ІР.

Розглянуті моделі повинні використовуватися на етапі проектування систем захисту інформації, коли ще не сформована архітектура системи, і необхідно дати попередню оцінку ефективності СЗІ, яка проектується.

На основі проаналізованих уразливостей ІС обробки ІР та з метою оцінки ефективності СЗІ і оцінювання стану захищеності ІР, що в них циркулює, доцільно побудувати модель протидії порушенням захищеності ІР в ІС.

Сутність моделі полягає у зміні структури функціонування елементів моделі у порівнянні з вищезазначеним прикладом. На стан захищеності елементів ІС та ІР в цілому впливає в певний момент часу множина зовнішніх і внутрішніх загроз які направлені на порушення цілісності, доступності, конфіденційності елементів СЗІ та ІС або проведення деструктивного впливу на програмну, апаратну, інформаційні складові самої системи. Також на стан захищеності ІС впливає множина механізмів захисту, які реалізовані в ІС та направлені на забезпечення безпеки. У ІС механізми захисту реалізуються на основі алгоритмів навчання з учителем на етапі розробки самої ІС, та алгоритму навчання без учителя, якій реалізується у процесі функціонування ІС. Саме перетин зазначених множин та наявність інструментів захищеності ІС в цілому визначає поточний стан захищеності самої ІС. Що в свою чергу дозволяє запропонувати управлінське рішення для підтримки належного стану безпеки та визначити механізми протидії на кожну окрему загрозу виходячи із цільової функції або мети управління безпекою.

Розпізнавання станів захищеності ІС здійснюється наступним чином. Є деяка множина станів, які відносяться до p різних класів. Компонентами вектора є окремі загрози безпеці ІР. Необхідно, використовуючи інформацію

про стани ІС та їх класифікацію, знайти таке правило, за допомогою якого можна було б з мінімальним числом помилок класифікувати нові стани за даними про отримані параметри атак.

Узагальнену типову модель, що описує взаємодію загроз, засобів захисту ІС та множину станів захищеності ІС представлено на рис. 3.5.

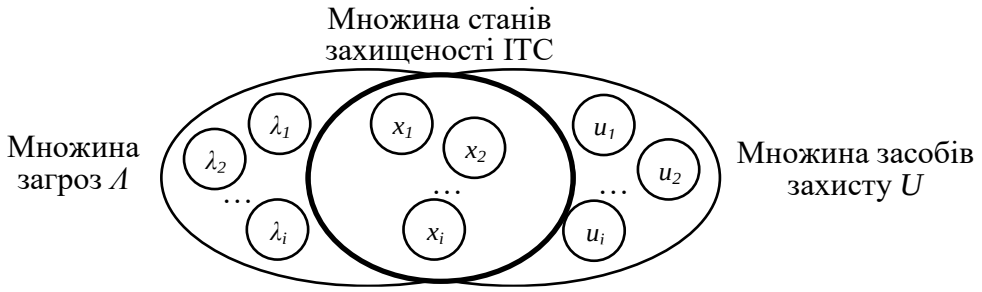


Рисунок 3.5 – Типова модель протидії порушенням захищеності ІР в ІС

Класами можуть бути стани захищеності ІС. Приклад для двох класів: стан захищеності ІС погіршується; стан захищеності ІС покращується. Приклад для трьох класів: стан захищеності ІС погіршується; стан захищеності ІС залишається без змін; стан захищеності ІС покращується. Очевидно, що кількість класів може бути довільною та визначатися умовою однозначної класифікації поточної ситуації.

Отже, зміна стану захищеності ІР як процес протікає в певній фізичній системі, яка не може бути представлена детермінованою системою.

Математична модель протидії порушенням захищеності інформаційних ресурсів в ІС визначається в результаті послідовного розв’язання наступних завдань:

– визначення початкової множини загроз, об’єднаної в конкретний момент часу в вектор загроз, та зміни координат вектора за певний період спостереження;

– оцінка чисельних значень рівнів загроз на обраних часових зрізах фазового простору моделі;

– пошук оптимального направляючого вектора розділяючої гіперплощини для множини векторів зміни рівнів загроз.

Розглянуті вирази, свідчать про те, оцінювання стану захищеності ІС залежатиме від швидкості адаптації існуючих СЗІ до нових загроз, коректної ідентифікації вхідного трафіку та виявлення параметрів атак за внутрішнім або зовнішнім ознакам.

Запропонована модель протидії порушенням захищеності ІР в ІС на відміну від подібних існуючих на сьогодні моделей, які призначені для оцінювання впливів можливих атак і загроз різного рівня та прийняття обґрунтованого рішення щодо реалізації СЗІ ІС, надає можливість оперативно оцінювати поточний стан захищеності ІС за умов забезпечення працездатності формальних методів за короткими обмеженими вибірками про параметри засобів захисту ІС та параметри загроз, що впливають на елементи ІС. Застосування запропонованої моделі дозволить отримувати поточні оцінки стану захищеності ІР, надати додатковий час на підготовку та проведення заходів реагування на загрози з метою посилення безпеки ІР.

2.3 Вибір математичного апарату розробки методів управління станом захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах

Забезпечення ефективного функціонування ІР в ІС можливе лише за наявності системи управління, здатної приймати управляючі рішення в умовах впливу атак. Функціонування ПЗБ не можливе без системи управління станом захищеності, основним завданням якої є оцінюваня поточного стану системи та приймання управлінських рішень для підтримання належного рівня безпеки ІР в ІС на основі аналізу трафіка ІС.

На сьогоднішній день системи управління подіями інформаційної безпеки інтенсивно розвиваються в напрямку інтелектуалізації, при цьому істотно змінюється технологія прийняття управлінських рішень.

Одним із шляхів підвищення ефективності заходів захисту ІР в ІС є забезпечення умови своєчасної оцінки їх стану. Значущою виявляється умова

своєчасного виявлення змін у стані захищеності ІР та безпеки ІС і здатності враховувати вплив зовнішніх і внутрішн іх атак. Ця задача вирішується через оцінювання стану безпеки ІС та рівня захищеності ІР на основі алгоритмів ідентифікації та розподілу параметрів тафіку, динамічного програмування та методу опорних векторів.

Відомі методичні підходи до управління станом захищеності ІР в ІС та безпеки її складових [69-74] використовують методики багатовимірного порівняльного аналізу, які в основному ґрунтуються на методах таксономії з елементами факторного аналізу.

Для зменшення обсягу вхідних даних при управлінні станом захищеності ІР і підвищення достовірності та оперативності оцінювання пропонується наступний апарат. Здійснимо визначення порядку математичного аналізу вхідних даних, якими виступають оцінки рівнів загроз безпеці ІС, з метою встановлення стану захищеності ІР. При цьому математичний апарат оцінки повинен бути гнучким до переліку загроз безпеці ІР за умови забезпечення оперативного оцінювання поточного стану рівня захищеності ІР. За таких умов важливою є вимога забезпечення працездатності формальних методів за короткими обмеженими вибірками даних спостереження.

Метод ДП широко застосовується для оптимізації дискретних систем. Переваги методу ДП:

1) ДП являє собою засіб рішення задач, які можуть бути вирішені й іншими методами. Цінність методу полягає в тому, що багатокроковий процес прийняття рішення заміняється послідовністю однокрокових процесів ухвалення рішення.

2) ДП дає математичний апарат для рішення задач, які раніше не вміли вирішувати. Зокрема, варіаційні задачі з обмеженнями типу нерівностей, рішення яких пов'язане зі значними труднощами, вирішуються методом ДП.

3) ДП має велику загальність і може застосовуватись для широкого кола задач.

З метою вирішення наукового завдання, визначимо основні етапи управління станом захищеності IP в IC. Під час побудови етапів управління станом захищеності доцільно врахувати загальну структуру побудови системи управління подіями безпеки до складу якої входть методи оцінювання захищеності від зовнішніх і внутрішніх загроз. В свою чергу, виходячи із проведеного аналізу для побудови методу управління станом захищеності від внутрішніх атак доцільно обрати метод опорних векторів, а для побудови методу управління станом захищеності від зовнішніх атак – метод динамічного програмування. Сутність даних кроків полягає у ідентифікації станів захищеності з урахуванням множини різнорідних параметрів трафіка, що передається в IC.

Структурно–логічна схема системи управління подіями інформаційної безпеки в IC представлено на рис. 3.6.

Основні етапи управління станом захищеності IC складаються з:

1. тримання вхідних даних: множина параметрів вхідного трафіку та параметрів сенсорних індикаторів безпеки; приклад параметрів вхідного трафіка.

2. Розподіл вхідних даних – розподіл параметрів трафіка відповідно до функціональних особливостей методів управління станом захищеності IC (від внутрішніх атак – 15, від зовнішніх атак – 18);

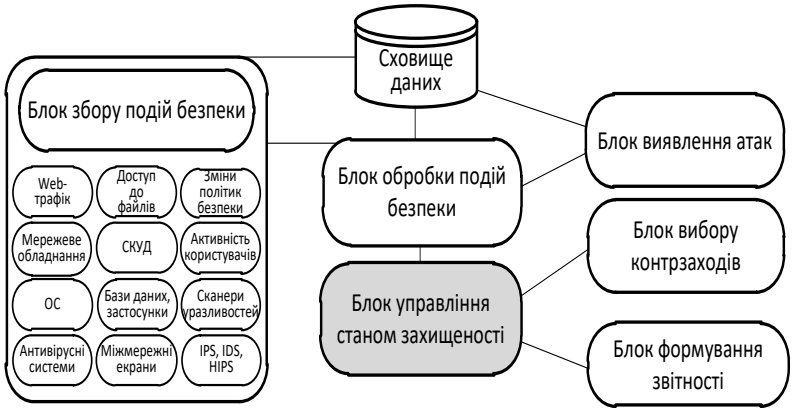
3. Виявлення атак – ідентифікація (*DoS, U2R, R2L, Probe, Side-channel*) категорій атак та нормальної поведінки, які впливають на стан захищеності IC.

4. Перевірка можливості протидіяти виявленим порушенням:

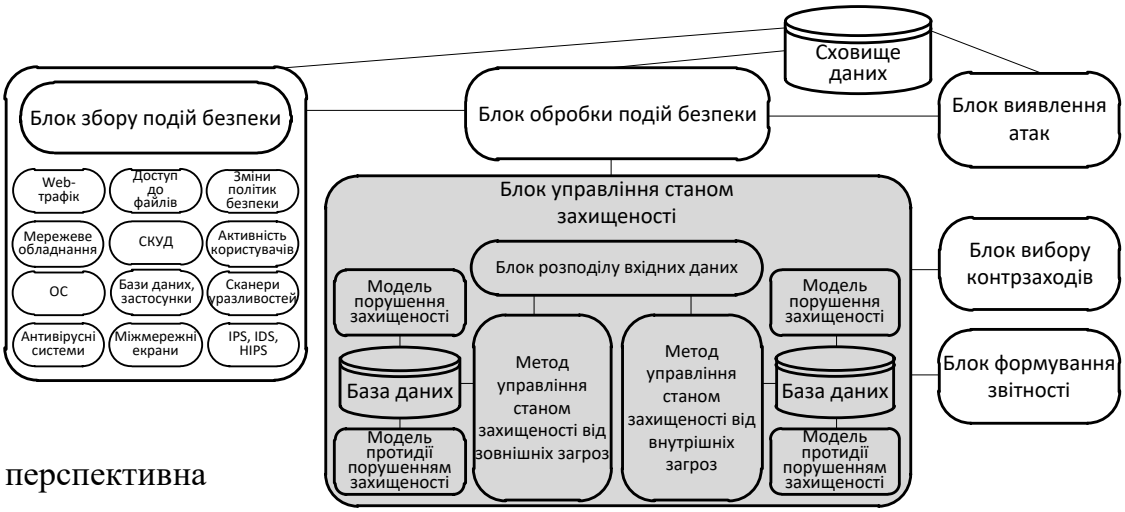
5. Перевірка коректності ідентифікації;

6. Встановлення стану захищеності.

7. Прийняття управлінського рішення – на основі параметрів атак.



а) існуюча



б) перспективна

Рисунок 2.6 – Структурна схема системи управління подіями інформаційної безпеки: а) існуючої; б) перспективної.

3.1 Застосування методу управління станом захищеності від зовнішніх атак на інформаційну систему на основі розподільчої ідентифікації та динамічного програмування

Існуючі системи управління подіями інформаційної безпеки передбачають прийняття рішень щодо виявлення загроз на основі обробки множини різнорідних параметрів даних. Загрози в свою чергу реалізуються різнонаправленими атаками. Інформація, під час проходження системою,

аналізується за відповідними параметрами на предмет виявлення порушень захищеності. У результаті чого на виході блоку управління станом захищеності з'являється ознака щодо наявності зміни стану захищеності ІС та можливості протидіяти загрозам.

В якості навчальної множини підсистеми управління станом захищеності ІС використаємо конкретні різновиди атак, представлені в базах даних NSL-KDD та KYOTO. В цих базах даних міститься більше 8 000 000 записів щодо аномальних з'єднань та близько 2 000 000 відомостей про нормальний тип з`єднання. Кожен запис являє собою образ мережевого з`єднання, включає 41 параметр мережевого трафіка (додаток А), серед яких міститься три типи ознак: символьні, логічні та числові. У загальному вигляді вони містять інформацію про тривалість з'єднання, тип протоколу, кількість спроб реєстрації тощо.

На основі вхідних параметрів трафіка відбувається перевірка на наявність порушень захищеності та маркування їх як „порушення" або „не порушення". Вказаний запис складається з 42 полів. Перші 41 поле описують ознаки мережевого трафіка, а останнє 42-е поле вказує на тип трафіка, який описується. Вказане поле може приймати значення „normal", якщо дане мережеве з`єднання відноситься до „нормального" стану трафіка, або найменування типу атак (наприклад, „ipsweep").

Вирішуючи задачу класифікації атаки (наприклад по її сигнатурі) підсистема управління станом захищеності ставить у відповідність наведеним вище параметрам мережевого трафіка 29 типів найбільш часто застосованих атак. Відкласифіковані параметри вхідних даних (атак) співвідносяться до множини управлінських рішень щодо варіантів реагування на кожен окремий тип атаки. В наслідок чого відбувається управління станом захищеності ІС.

З огляду на вищезазначене розробляємий метод управління станом захищеності від зовнішніх атак враховує наступні особливості ІС:

– різна розмірність мереж;

– територіально рознесені складові ІС;

– вихід елементів ІС за межі контрольованої зони;

– для доступу до оброблюваних ресурсів застосовуються не тільки ПК;

– мають високі вимоги до доступності інформаційних ресурсів;

– конфігурація ІС змінюється (змінюється склад користувачів та їхні привілеї, оновлюються версії програм, з'являються нові сервіси, апаратура і т.п.);

– взаємозв'язок та взаємозалежність елементів ІС.

Позначення вхідних даних: Розглядається ситуація знаходження системи у стані рівноймовірнісного протікання порушень захищеності ІС. В один і той же час відбуваються як порушення захищеності від зовнішніх атак на ІС так і пошук варіантів протидій на виявлені зміни стану захищеності. Для моделювання такої ситуації будується навчальна вибірка, яка має в собі 20 % нормальних інформаційних повідомлень та 80 % аномальних інформаційних повідомлень, які містять типи атак. Також будується база з варіантами протидій на множину виявлених порушень. Так як кожна фаза атаки характеризується множиною технік проведення і реалізується внутрішнім або зовнішнім зловмисником, тому для проведення управління станом захищеності від зовнішніх атак відбувається ідентифікація типів порушень на основі параметрів даних, що характерні саме зовнішнім атакам. Загальна кількість параметрів x_i = 18.

Під час виявлення атак буде застосовуватись механізм логічного виводу для опису бази вхідних параметрів. На підставі співставлення вхідних параметрів, у системі формуватиметься рішення, щодо їх класифікації. В наслідок чого відбувається співвідношення стану захищеності ІС до можливих видів порушень та наявних засобів захисту та приймається управлінське рішення щодо підтримки належного стану захищеності ІС.

Вхідним значенням є: $X = XH \cup XM \cup XL$ – параметри вхідного трафіку;

$XM = \{x_i(t), i = \overline{1,18}\}$ – множина параметрів трафіку, що характерні зовнішнім атакам;

$XH = \{x_h(t), h = \overline{1,15}\}$ – множина параметрів трафіку, що характерні внутрішнім атакам;

XL – множина параметрів трафіку, що не задіяні при реалізації методу.

Обмеження та допущення: Ідентифікуються типи атак: DoS, U2R, R2L, Probe, Side. Аномальна поведінка ідентифікується, як нововиявлений стан захищеності. Процес управління станом захищеності є квазістаціонарним на інтервалі часу $(t_0 ... T)$.

Необхідно: збільшити достовірність прийняття управлінського рішення щодо оцінки стану захищеності IP D від зовнішніх атак за умов, що час прийняття управлінського рішення буде не більше ніж у подібних методів:

$$\begin{cases} D \to \max; \\ D > D_{isn} \\ T \le T_{isn} \end{cases}.$$

Сутність методу полягає у: використанні розподільчої ідентифікації параметрів зовнішніх атак з проведенням вибору щодо застосування заходів із захисту системи при повному описі ІС та врахуванням стратегій впливу на неї на основі динамічного програмування.

Управління станом захищеності ІС від зовнішніх загроз може відбуватись при проведенні ідентифікації параметрів порушень, які реалізуються множиною різнонаправлених та різних за своїм змістом атак.

Тому проведемо ідентифікацію вхідних даних (параметрів даних) трафіка.

І. Під ідентифікацією розумітимемо знаходження оптимальної в деякому сенсі моделі, побудованої за результатами спостережень над вхідними та вихідними змінними об’єкта, а саме набором параметрів трафіку. Завданням ідентифікації є зворотне завдання системного синтезу.

При побудові моделі оцінки захищеності за експериментально отриманими даними поширеною є ситуація, для якої практично вся інформація, що використовується обробником для розв’язання поставленої задачі, обмежується вибіркою вихідних даних. Тому для розв’язання задачі параметричної ідентифікації використовують методи, орієнтовані виключно на інформацію про невідповідність між виходами об`єкта та моделі.

В загальному випадку для довільної моделі відомої структури рівень невідповідності між виходами об’єкта та моделі залежить від вибору параметрів моделі. Тому, якщо ввести показник якості параметричної ідентифікації, який інтегрує в собі всю інформацію про рівні нев’язок і містить відомості про залежність рівня невідповідності між виходами об’єкта та моделі від значень параметрів моделі, то мінімізація цього показника дозволить визначити оптимальні параметри моделі.

Структуру алгоритму реалізації методу управління станом захищеності від зовнішніх атак на ІС на основі алгоритму розподільчої ідентифікації та динамічного програмування представлено на рис. 3.2.

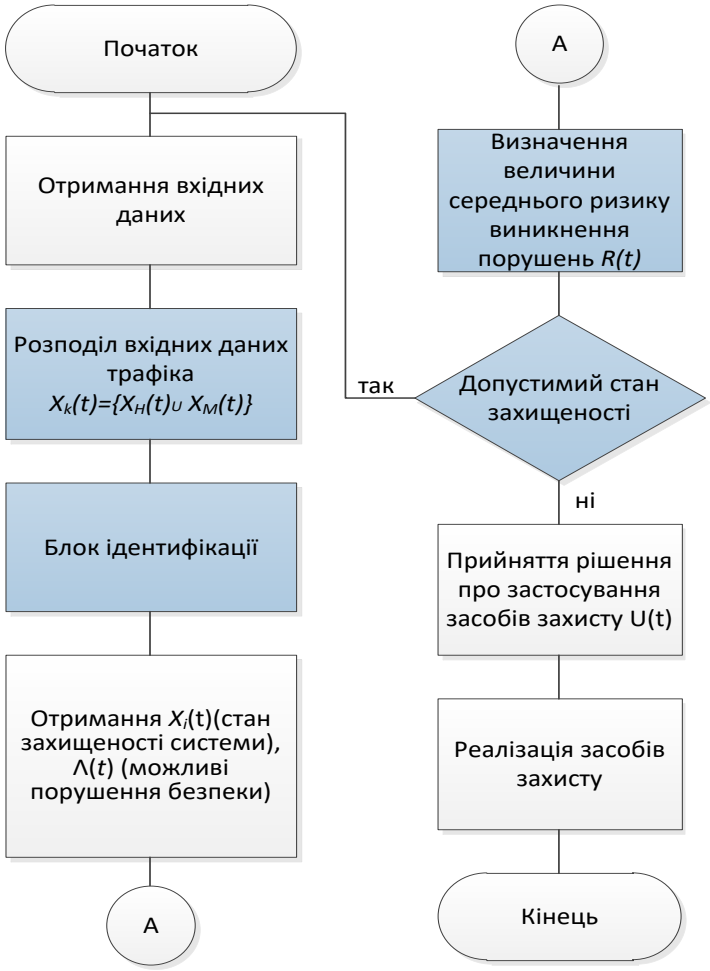


Рисунок 3.2 – Структура алгоритму реалізації методу управління станом захищеності від зовнішніх атак

Структурна схема управління станом захищеності ІС від загроз, характерних зовнішньому зловмиснику представлено на рис. 3.3.

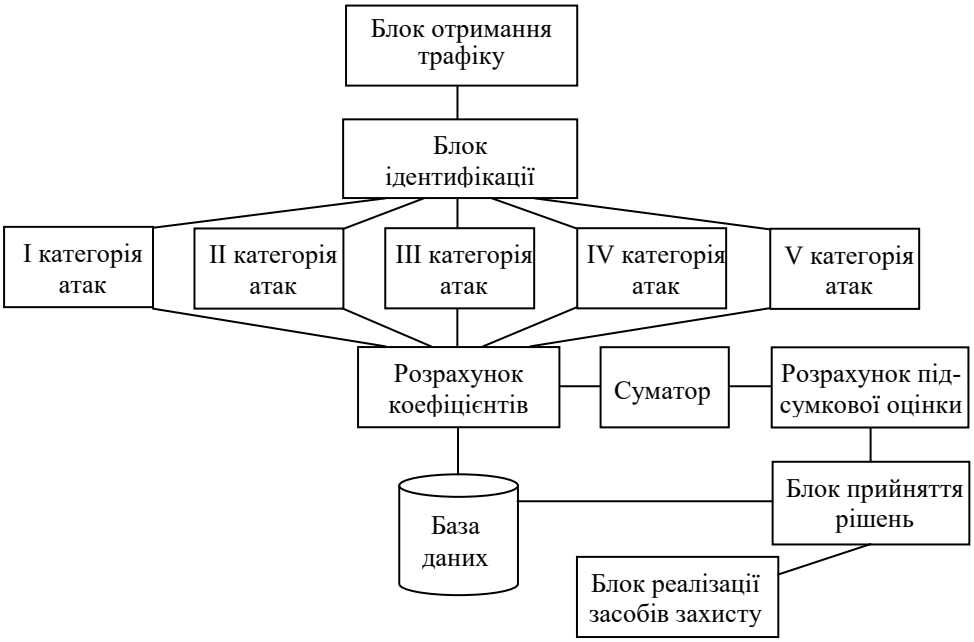


Рисунок 3.3 – Схема реалізації управління станом захищеності від зовнішніх загроз

Метод управління станом захищеності від зовнішніх атак на ІС, на відміну від подібних методів, приймає управлінське рішення щодо стану захищеності ІР при множині вхідних параметрів зовнішніх атак на основі паралельно-розподільчої ідентифікації та динамічного програмування.

Під час розробки програмної компоненти управління станом захищеності ІР в ІС прийнято рішення стосовно вибору та використання мов програмування, технологій реалізації та додаткових інструментів реалізації програмної компоненти. В якості мови програмування обрано JavaScript, яка найчастіше використовується для написання веб-додатків, через можливість створення сценаріїв для взаємодії користувача на клієнтській стороні з веб-застосунком та асинхронно обмінюватися даними з сервером. При розробці програмної компоненти використано бібліотеку JavaScript jQuery. Дана бібліотека легко отримує доступ до будь-яких елементів DOM.

Для реалізації програмної компоненти управління станом захищеності на стороні сервера застосовано мову програмування PHP. Вона є одною з найпоширеніших мов, що використовуються для написання веб-застосунків.

Для роботи користувача з програмним компонентом використано безкоштовний Apache HTTP Server та сервер бази даних MySql. Для налаштування роботи PHP та підняття Apache HTTP Server та бази даних MySQL прийнято рішення про використання OpenServer. Даний програмний продукт є серверною платформою та дозволяє розробляти, виконувати налагодження, тестувати проекти.

До того ж, цей локальний сервер дозволяєте в налаштуваннях вибрати один з декількох варіантів Apache, PHP, MySQL та інших компонентів.

Програмний компонент управління станом захищеності IP в IC надає можливість проводити оцінювання ефективності розглянутих методів та отримати інформацію щодо його результатів.

Фрагмент тексту програмного компоненту управління станом захищеності представлено в Додатку Б.

Існуючі методи управління станом захищеності IP в IC показують, що їх побудова ґрунтується на застосуванні програмних та апаратних засобів, які забезпечують практичне виявлення уразливих місць IC.

Використовуючи запропоновану програмну компоненту управління станом захищеності IC від зовнішніх і внутрішніх атак було отримано результати, що наведено в таблиці 3.1. та таблиці 3.2.

Таблиця 4.1 – Управління станом захищеності IC від зовнішніх атак

Значення / Відрізки	X (мс.)	Y (%)	1/X	$1/X^2$	Y/X
100	168	96,1	0,005952381	0,000035	0,57202381
150	173	97,2	0,005780347	0,000033	0,561849711
200	178	95,3	0,005617978	0,000032	0,535393258
250	184	96,2	0,005434783	0,000030	0,522826087
300	186	96,4	0,005376344	0,000029	0,51827957
350	190	96,1	0,005263158	0,000028	0,505789474
400	195	95,3	0,005128205	0,000026	0,488717949
450	205	95,1	0,004878049	0,000024	0,463902439
500	215	93,2	0,004651163	0,000022	0,433488372
Сер. знач.	188	95,6	0,005319149	0,000028	0,508510638

де значення b_0 = 84,46; b_1 = 2094,02

На рис. 4.5 та рис. 4.6 зображені результати оцінки ефективності управління станом захищеності IP від зовнішніх атак розробленим методами та подібними у вигляді залежностей достовірності прийняття управлінського рішення від кількості інформаційних повідомлень.

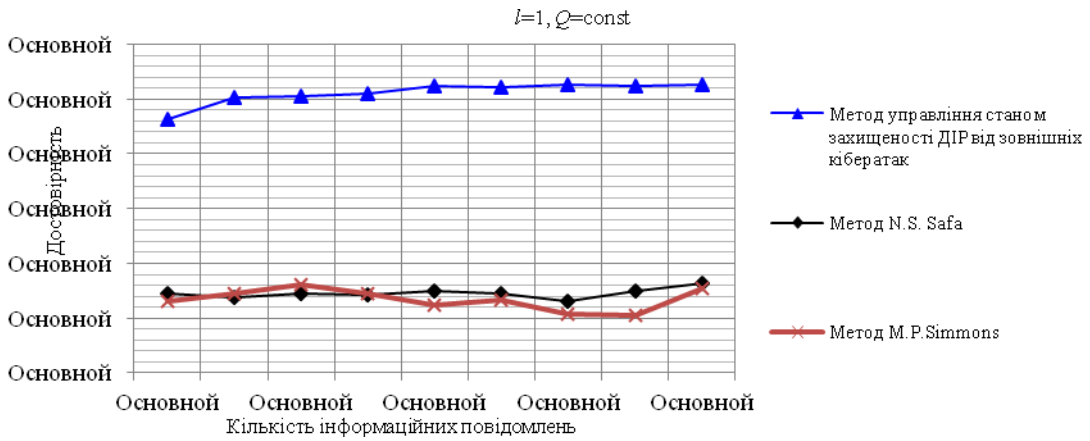


Рис. 4.5. Залежність достовірності прийняття управлінського рішення від кількості інформаційних повідомлень

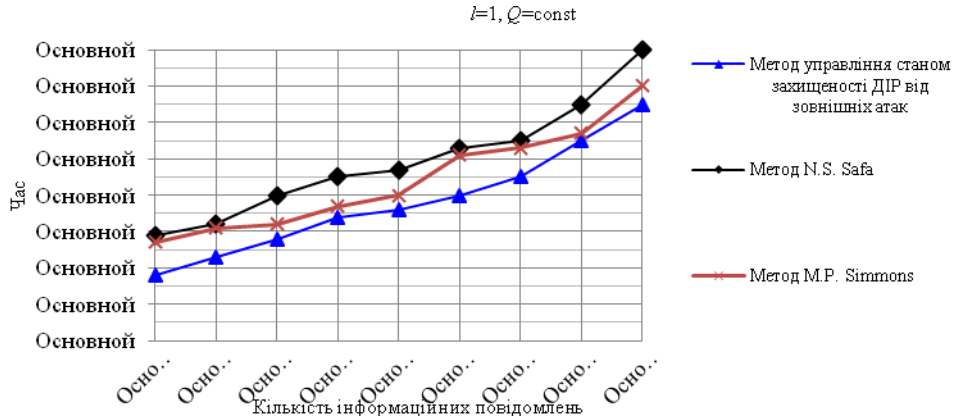


Рис 4.6. Залежність часу прийняття управлінського рішення від кількості інформаційних повідомлень

Таблиця 3.2 – Оцінювання стану захищеності ІС від внутрішніх атак

Значення / Відрізки	X (мсек.)	Y (%)	1/X	$1/X^2$	Y/X
5	145	98,1	0,006896552	21025	0,676551724
10	148	96,9	0,006756757	21904	0,65472973
15	152	97,2	0,006578947	23104	0,639473684
20	158	96,4	0,006329114	24964	0,610126582
25	162	95,1	0,00617284	26244	0,587037037

30	161	95,9	0,00621118	25921	0,595652174
35	164	96,4	0,006097561	26896	0,587804878
40	169	95,3	0,00591716	28561	0,563905325
45	175	95,1	0,005714286	30625	0,543428571
Сума	159	96,2	0,006277464	25376,49	0,603892028

де значення b_0 = 96,26; b_1 = 654,38

З графіків видно, що при збільшені кількості інформаційних повідомлень, які передаються в ІС, значення показників оцінок змінюється у бік покращення в наслідок застосування ідентифікації, динамічного програмування та побудови опорних векторів. Значення оціночних показників удосконалених методів оцінювання мають виграш у порівнянні з існуючими та подібними методами, які лежать в основі сучасних систем управління подіями інформаційної безпеки, а саме:

– достовірності прийняття управлінського рішення щодо оцінювання захищеності та застосування ЗЗ (рис. 4.5 та 4.7) розробленим та удосконаленим методами, в порівнянні з існуючими та подібними, збільшується за рахунок застосування розподільчої ідентифікації, динамічного програмування та побудови опорних векторів;

– час прийняття управлінського рішення (рис. 4.6 та 4.8) розробленим та удосконаленим методами, в порівнянні з існуючими, зменшується за рахунок застосування розподільчої ідентифікації параметрів трафіку.

Висновки до розділу 3

У третьому розділу магістерської роботи запропоновано метод управління станом захищеності від зовнішніх атак на ІС на основі розподільчої ідентифікації та динамічного програмування. Сутність методу полягає у використанні розподільчої ідентифікації параметрів зовнішніх атак з проведенням вибору щодо застосування заходів із захисту системи при повному описі ІС та врахуванням стратегій впливу на неї на основі динамічного програмування. На відміну від подібних методів, запропонований метод приймає управлінське рішення щодо стану захищеності ІР при множині вхідних параметрів зовнішніх атак на основі паралельно-розподільчої ідентифікації та динамічного програмування. Метод дозволяє збільшити достовірність прийняття управлінського рішення щодо оцінювання стану захищеності ІР в ІС, за умов часу прийняття управлінського рішення щодо оцінювання стану захищеності не більше ніж у подібних методів.

Висновки

В магістерській кваліфікаційній роботі запропоновано методику оцінки ефективності методів управління станом захищеності ІР в ІС, яка основана на моделюванні процесу оцінювання. При застосуванні методики до розроблених методів управління станом захищеності від зовнішніх атак на ІС на основі розподільчої ідентифікації та динамічного програмування було зафіксовано збільшення достовірність прийняття управлінського рішення щодо оцінки стану захищеності ІР в ІС на 12–16%.

ДОДАТОК А

Параметри мережевого трафіка

№ з/п	Параметр	Опис	Тип атаки
Основні ознаки			
1.	*duration*	Тривалість з'єднання (у секундах)	зовнішня
2.	*protocol_type*	Тип протоколу (TCP, UDP, etc.)	внутрішня, зовнішня
3.	*service*	Сервіс атакованого рівня	внутрішня
4.	*flag*	Статус з'єднання	внутрішня
5.	*src_bytes*	Вхідний потік, байт	внутрішня, зовнішня
6.	*dst_bytes*	Вихідний потік, байт	внутрішня, зовнішня
7.	*land*	Співпадіння адрес, 1 якщо з'єднання від/до того самого вузла	внутрішня, зовнішня
8.	*wrong_fragment*	Кількість неправільних фрагментів	внутрішня, зовнішня
9.	*urgent*	Кількість термінових пакетів	внутрішня, зовнішня
Статистичні ознаки			
10.	*count*	Кількість з'єднань з співпадаючим вузлом в поточній сесії.	внутрішня
11.	*serror_rate*	% з'єднань що мали помилки „SYN”	внутрішня, зовнішня
12.	*rerror_rate*	% з'єднань що мали помилки „REJ” та з`єнання з однаковим вихідним вузлом	внутрішня
13.	*same_srv_rate*	% з'єднань з однаковим сервісом	внутрішня, зовнішня
14.	*diff_srv_rate*	% з'єднань на різні сервіси	внутрішня
15.	*srv_count*	Кількість з'єднань на такий самий сервіс.	зовнішня
16.	*srv_serror_rate*	% з'єднання з помилкою „SYN” в пакеті	внутрішня, зовнішня
17.	*srv_rerror_rate*	% з'єднання, що мають помилки „REJ”	внутрішня, зовнішня
18.	*srv_diff_host_rate*	% з'єднаннь з різними вузлами	внутрішня, зовнішня
Ознаки окремого з`єднання			
19.	*hot*	Кількість „гарячих” індикаторів	зовнішня
20.	*num_failed_logins*	Кількість невдалих спроб входу	зовнішня
21.	*logged_in*	Вдалий вхід в систему - 1, невдалий - 0	внутрішня
22.	*num_compromised*	Кількість „компроментуючих” умов	внутрішня, зовнішня
23.	*root_shell*	Доступ з адміністративними повноваженнями - 1; інакше 0	внутрішня
24.	*su_attempted*	1, якщо виконувалась „su root”; інакше 0	внутрішня
25.	*num_root*	Кількість спроб доступа з правами користувача	внутрішня
26.	*num_file_creations*	Кількість операцій створення файлів	внутрішня
27.	*num_shells*	Кількість спроб використання запитів на надання	внутрішня

		доступу	
28.	*num_access_files*	Кількість операцій с файлами контролю доступу	зовнішня
29.	*num_outbound_cmds*	Кількість вихідних команд для FTP сесії	зовнішня
30.	*is_hot_login*	1, якщо логін належав до „гарячого” списку	зовнішня
31.	*is_guest_login*	1, якщо „гостьовий” вхід	зовнішня
Додаткові ознаки			
32.	*dst_host_count*	Кількість з`єднань до вузла, встановлених віддаленою стороною та використовуючих різні служби	зовнішня
33.	*dst_host_srv_count*	Кількість з`єднань до вузла, встановлених віддаленою стороною та використовуючих одну службу	зовнішня
34.	*dst_host_same_srv_rate*	% з`єднань до вузла, встановлених віддаленою стороною та використовуючих одну службу	зовнішня
35.	*dst_host_diff_srv_rate*	% з`єднань до вузла, встановлених віддаленою стороною та використовуючих різні служби	зовнішня
36.	*dst_host_same_src_port_rate*	% з`єднань до вузла з поточним джерелом	зовнішня
37.	*dst_host_srv_diff_host_rate*	% з`єднань до вузла з різним джерелом	зовнішня
38.	*dst_host_serror_rate*	% з`єднань з помилкою типу SYN для даного приймача	зовнішня
39.	*dst_host_srv_serror_rate*	% з`єднань з помилкою типу SYN для служби приймача	зовнішня
40.	*dst_host_rerror_rate*	% з`єднань з помилкою типу REJ для даного приймача	зовнішня
41.	*dst_host_srv_rerror_rate*	% з`єднань з помилкою типу REJ для служби приймача	зовнішня

ДОДАТОК Б

Фрагмент тексту програмного компоненту управління станом захищеності ДІР в ІТС.