РОЗРОБКА ТА ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

Шевченко В.М.

Науковий керівник - доц. каф. “Комп’ютерні системи та мережі”, канд. техн. наук Шендрик Є.В.

Ступінь впровадження бездротових технологій в сфери діяльності сучасної людини неухильно зростає з кожним днем. Бездротові мережі використовуються як складова частина корпоративних систем, і в малих офісах підприємств, як домашня мережа. Багато мобільних пристроїв, від звичайних телефонів до портативних комп’ютерів, мають бездротові мережні інтерфейси, що забезпечує обмін даними практично в будь-якому місці.

Незважаючи на стрімке зростання різних бездротових технологій, основним, на сьогоднішній день, є стандарт 802.11 і його різновиди. Обумовлено це тим, що покриття таких мереж постійно зростає, нарівні з падінням цін на карти бездротового доступу.

Враховуючи особливості фізичного рівня бездротових мереж, а саме, низька стійкість до перехоплення сигналу, а також неконтрольоване зростання бездротових вузлів мереж, виникає гостра потреба в організації заходів безпеки передачі даних в таких мережах. Щодня користувачі мережі використовують особисті паролі для отримання доступу до тих чи інших соціальних систем, обмінюються конфіденційними даними і т. п. Для запобігання крадіжки або спотворення інформації існують різні підходи, які, як правило, слід використовувати в комплексі:

– особисті запобіжні заходи (нерозголошення паролів, відмова від сумнівного змісту вузлів, грамотне користування операційними системами);

– програмні засоби локального застосування (антивіруси, фаєрволи, спеціальне програмне забезпечення і т. п.);

– мережеві програмні засоби (мережні агенти, системи моніторингу тощо);

– протоколи передачі даних, криптографічні системи і т. д.

Для вирішення проблем безпеки бездротових мереж необхідно вести розробку і розвиток методів захисту даних в бездротовій середовищі, а також методик їх застосування.

Виходячи з даних, отриманих при аналізі безпровідних систем і їх загроз, можна запропонувати три групи об'єктів, що належать конкретній системі:

- довірені об'єкти - об'єкти системи, достовірність яких заздалегідь відома;

- підозрілі об'єкти - об'єкти системи діяльність яких викликає підозру, які вимагають додаткового контролю;

- порожні об'єкти - об'єкти, що не належать конкретній системі, але дії, що знаходяться в її зоні.

Довіреними об'єктами можуть бути абонентські станції які обслуговують систему персоналу, співробітники організації, а також комунікаційне устаткування системи - точки доступу і маршрутизатори, мережеві принтери і т.п.

Підозрілі об'єкти - об'єкти, які проявляли істотну підозрілу активність на мережевому і логічному рівнях мережі. Такі абоненти надалі схильні до щільнішого контролю систем безпеки і схильні до гостріших реакцій системи на протиправні дії.

Порожніми об'єктами системи можуть бути не аутентіфіцированниє об'єкти системи, або що дійсно не належать цій системі. Такі абоненти, по-перше, не мають доступу до ресурсів системи по-друге схильні до суворого контролю на логічному рівні безпровідної мережі.

Таким чином, об'єкти системи можна представити таким чином:

$$K=\{\{T\},\{D\},\{E\}\}, \text{ де}$$

$T = \{t_1, t_2,\ldots,t_n\}$, безліч довірених об'єктів,

$D = \{d_1,d_2,\ldots,d_m\}$, безліч підозрілих об'єктів,

$E = \{e_1,e_2,\ldots,e_k\}$, безліч порожніх об'єктів.

Необхідно врахувати, що при настанні певної події, і -й об'єкт кожного з множин може переходити з однієї множини в інше.

Довірений об'єкт, що вчинив роз'єднання з системою автоматично повинен потрапити у безліч порожніх об'єктів. Якщо ж дії довіреного об'єкту в системі несуть за собою достатню кількість подій, класифікованих як зловмисні, відбувається його перехід у безліч підозрілих об'єктів.

Підозрілий об'єкт, при настанні певних подій має можливість переходу в групу довірених об'єктів.

Для визначення умов переходу об'єктів між множинами, необхідно визначити ряд правив для кожної множини що характеризують події що впливають на включення тієї або іншої великої кількості.

- Для об'єктів безлічі T і D можливі переходи в самих себе, якщо при аналізі їх активності була доведена правомірність дій відповідних об'єктів.
- Для об'єктів безлічі T можливі переходи за наступними критеріями:
- перехід у безліч D, якщо діяльність об'єкту визначена як підозріла активність;
- перехід у безліч E можливо при реалізації двох сценаріїв – абонент сам припинив сеанс зв'язку або сеанс розірваний системою як наслідок протиправних дій.

Для об'єктів безліч D можливі переходи за наступними критеріями:

- перехід у безліч E у разі припинення сеансу об'єктом або розриву зв'язку системою;
- перехід у безліч T, якщо об'єкт з часом показав сприятливу статистику активності або був переведений в цю групу адміністратором системи.

Для об'єктів безліч E можливі переходи в інші множини у разі, коли об'єкт аутентифіцірувався і довів свою приналежність системі, або якщо об'єкт став новим абонентом системи.

Для і-го елементу однієї з множин може бути можливим наступні переходи:

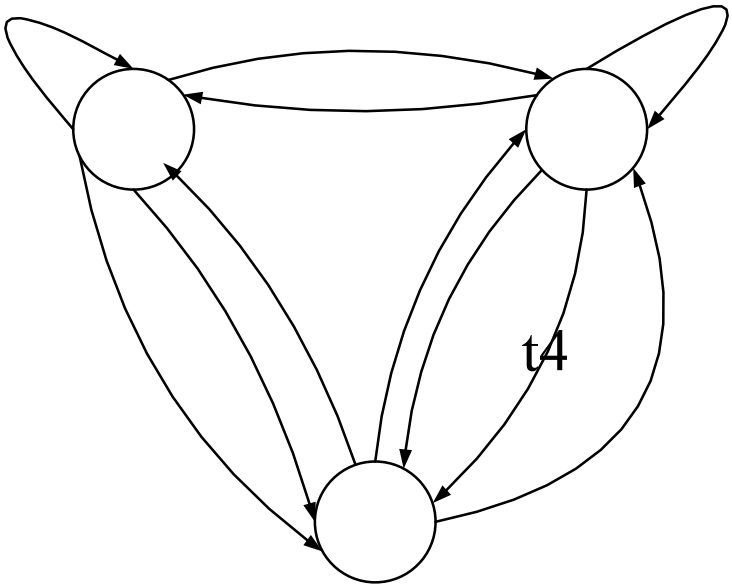

Рис. 1.1 Організація переходів між множинами

t1 – підозріла активність.

t2 – порушення правил безпеки.

t3 – завершення сеансу зв’язку з об’єктом.

t4 – правомірні дії.

t5 – позитивна статистика активності.

t6 – аунтифікація об’єкта .

t7 – реєстрація нового об’єкта мережі.

t6

t3

t2

Параметри об'єкту формуються з метою визначення відхилень характеристик, що описують об'єкт, від заданих, або відстежування активності об'єкту в мережі, з метою виявлення аномалій.

Характеристика положення об'єкту:

- Визначення місця розташування об'єкту в зоні дії безпровідної мережі можна визначити двома способами:
- за допомогою вектору напряму;
- за допомогою системи координат.

Для зручності, в розробці використовується визначення положення об'єкту за допомогою тривимірної системи координат. Існує ряд програмних утиліт об'єктів, що відстежують положення, в мережі. Одним з головних недоліків таких систем є неточність. Відомо що визначення місця розташування мобільних пристроїв має певну погрішність. Як правило, розкид складає від п'яти до двадцяти метрів, залежно від характеристик довкілля. У зв'язку з цим запропоновано в набір параметром місця розташування ввести також коефіцієнт невизначеності, що набуває значення від нуля до одиниці, і що визначає вірогідність того, що об'єкт знаходиться саме по координатах, що визначилися.

Отже, місце розташування об'єкту в мережі визначатимуть чотири параметри - координати і коефіцієнт невизначеності.

Характеристика активності об'єкту:

Характеристики активності визначає параметри, що описують події в мережі визначувані діяльність цього об'єкту.

Внаслідок того, що більшість мережевих атак розпочинаються з логічного рівня мережі, параметри об'єкту також характеризуватимуть його діяльність на логічному рівні. Отже, в першу чергу, необхідно здійснювати контроль за фреймами, які посилає об'єкт в мережу.

Саме у посилці помилкових і неправильних фреймів полягають багато атак, спрямованих на підміну об'єктів або глушення каналу зв'язку.

Основними параметрами контролю активності мережевого об'єкту виступатимуть наступні характеристики:

– кількість фреймів;

– розмір фрейма;

– тип фрейма;

– порядковий номер фрейма;

- значення ідентифікатора мережі в тілі фрейма.

Відстежуючи ці параметри, можна буде судити про дії об'єкту і події, що викликаються цими діями.

У результаті кожен об'єкт безпровідної мережі можна описати таким чином:

$$A_i = \{\{P\}\{F\}\}, \text{ де}$$

P = {{x, y, z},k} – множина, що описує положення об'єкту, де

{x, y, z} – координати положення об'єкту, k - коефіцієнт невизначеності,

F = {n, s, t, j, e}, множина описує активність об'єкту, де

n – кількість фреймів;

s – розмір фрейма;

t – тип фрейма;

j – порядковий номер фрейма;

e – значення ідентифікатора мережі в тілі фрейма.

Якщо у безпровідній мережі сталася подія, що характеризує аномальну активність або бездіяльність в мережі, або підозрілі дії об'єктів мережі, необхідно забезпечити адекватну систему реакцій на ці події.

Класифікувати реакцію на подію можна таким чином:

- порожня реакція (бездіяльність системи);
- попередження системи;
- перенесення об'єкту з однієї множини в іншу;
- обмеження доступу;
- розрив з'єднання.

При ухваленні рішень про відповідну реакцію на події важливо врахувати адекватність рішення до тих дій, які сталися.

Найзручніше представляти процес реалізації реакції на події, що сталися, за допомогою графів або граф-схем алгоритмів.

3.6.1 Визначення реакцій на дії об'єктів мережі

Для опису процесу контролю над положенням об'єкту потрібно чотири стани і три переходи. Припустимо що:

s1 – стан «вхід об'єкту»;

s2 – стан переходу об'єкту у безліч D;

s3 – стан перевірки достовірності об'єкту;

s4 – стан «припинення сеансу зв'язку»

t1 – перехід, якщо параметри положення об'єкту прагнуть до граничних;

t2 – перехід, якщо параметри об'єкту перевищили граничні;

t3 – перехід до розриву зв'язку.

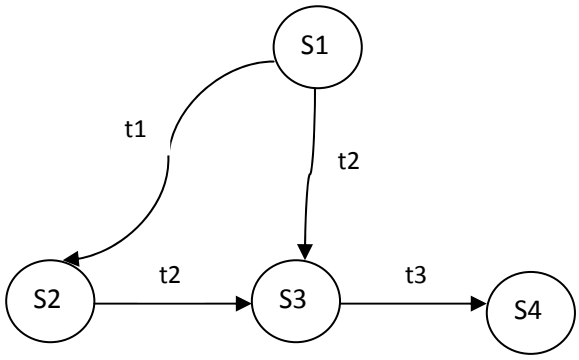

Рис. 1.2 Граф реакції на зміну параметрів положення об'єкту

Відбувається порівняння параметрів місця розташування об'єкту, в результаті якого можливі дві події - параметри прагнуть до граничних, або параметри перевищили граничні. У першому випадку зміна параметрів класифікується як підозріле, а об'єкт вимагає додаткового контролю, вірогідність перебування його в заданій точці падає. У такому разі об'єкт слід перенести у безліч об'єктів D.

У другому випадку вимагається віднести об'єкт до безлічі D і повторити процедуру аутентифікації для визначення достовірності, вірогідність знаходження в заданій точці падає. У разі підтвердження недостовірності об'єкту необхідно зробити припинення сеансу зв'язку з об'єктом.

Детальніше ці процедури представлені в граф-схеме алгоритму реакції на аномалії.

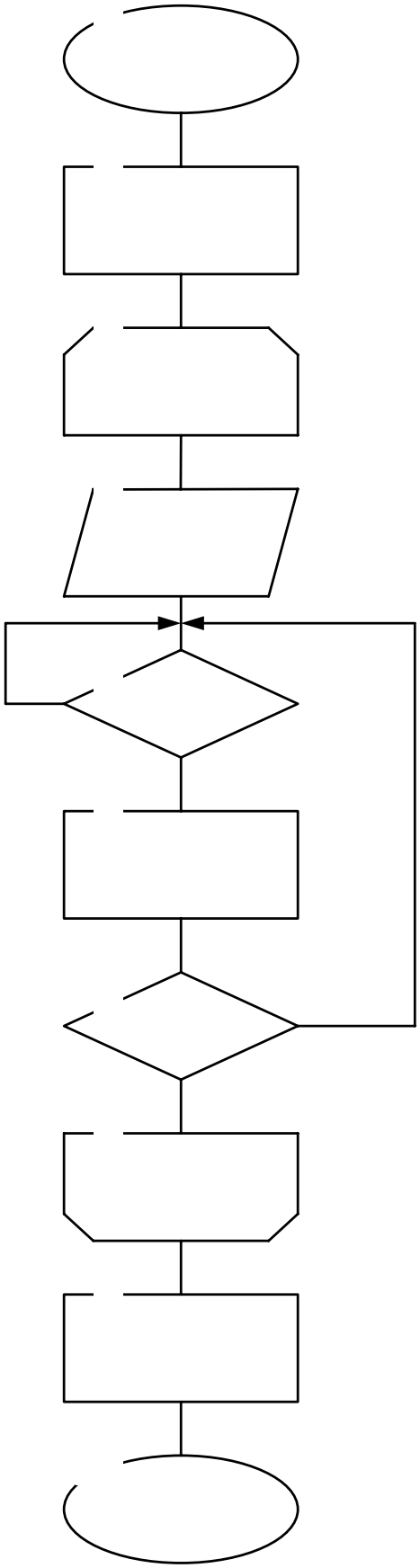

Рис. 1.3 Алгоритм контролю місця розташування об'єкту

Контроль параметрів фреймів, циркулюючих в системі, виглядає таким чином:

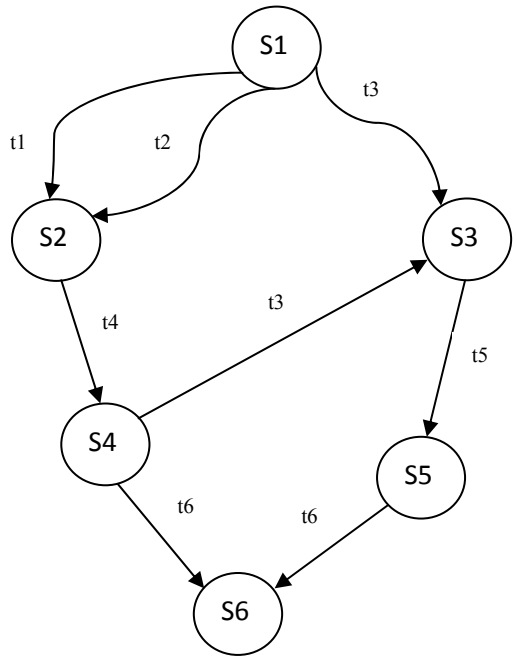

Рис. 1.4 Граф реакції на відхилення в параметрах фреймів

В цій схемі представлені наступні елементи:

s1 – вступ фрейма.

s2 - вірогідність помилки по параметрах n_i и e_i

s3 - критична помилка в параметрах.

s4 - перенесення об'єкту в групу D.

s5 - повторна реєстрація об'єкту.

s6 - припинення сеансу зв'язку.

t1 - наближення кількості фреймів до критичної межі.

t2 - помилка в ідентифікаторі мережі.

t3 - критична помилка в параметрах si, ti, ji.

t4 - збільшення міри контролю за об'єктом.

t5 - перевірка відповідності об'єкту мережі.

t6 - повторне порушення параметрів.

Алгоритм цієї процедури представлений на малюнку 3.5.

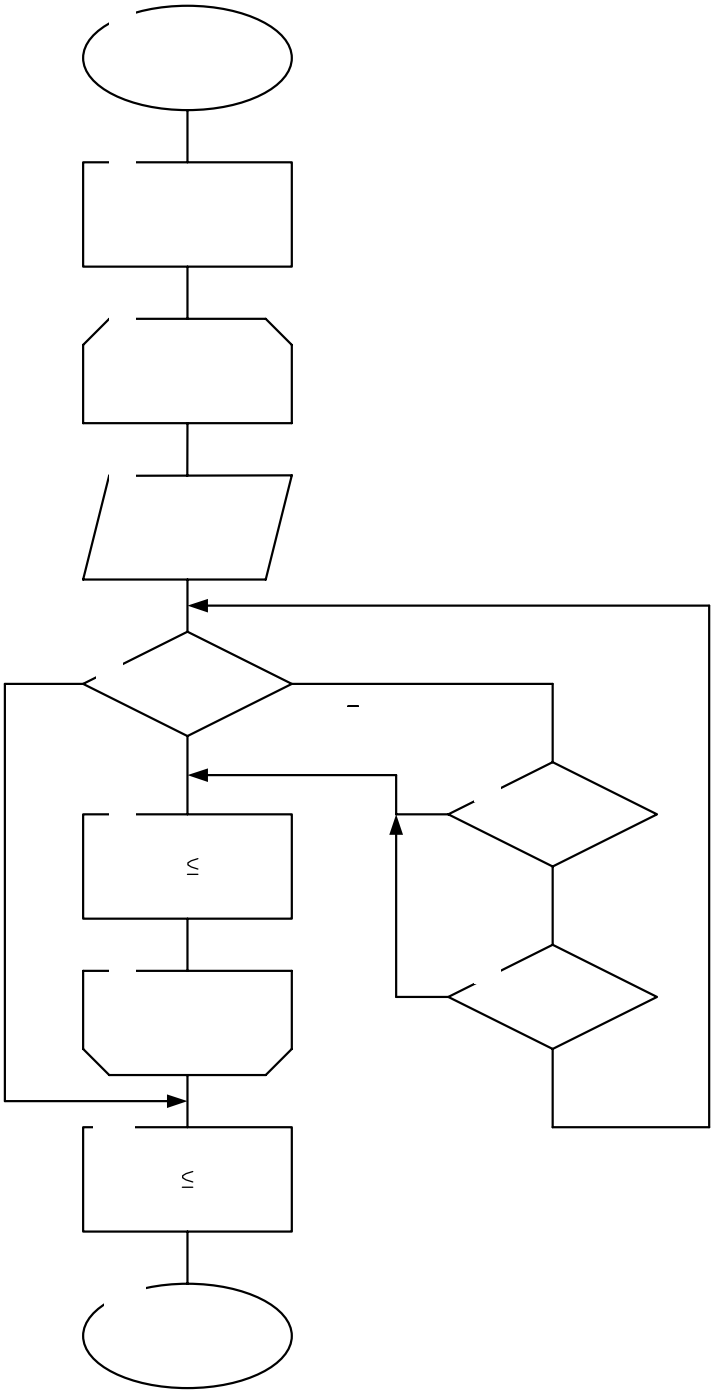

Рис. 1.5 Процедура контролю об'єкту по параметрах його активності

Параметри, що перевіряються, характеризують кількість фреймів в одиницю часу і ідентифікатор мережі, можуть мати деяку погрішність, яка викликає подію, пов'язану зі збільшенням контролю, а не розривом з'єднання. Якщо кількість фреймів прагне до граничного значення, але не досягає його, слід детальніше розглянути цей об'єкт. Невірний ідентифікатор мережі може

бути вкладений помилково, отже перш ніж закривати сеанс, слід також спершу перевірити об'єкт.

Параметри характеризують тип, розмір і номер фрейма має жорсткіші рамки контролю, оскільки є строго визначеними для заданої мережі. Отже, при виникненні виняткової події, необхідно перевірити достовірність об'єкту мережі і якщо результат негативний, припинити сеанс зв'язку.

Контроль поведінки безпровідної мережі і реакція на події здійснюється на третьому рівні ієрархії.

Контроль мережі ведеться по трьох параметрах - два параметри пакету і параметр логічних зв'язків і адресного простору. Процедура представлена наступним графом зв'язності подій.

У цьому графові прийняті наступні позначення:

S1 - перевірка характеристик каналу.

S2 - розмір пакету не відповідає заданому.

S3 - заголовок пакету модифікований.

S4 - характеристики логічного каналу і адреси не відповідають заданим.

S5 - перевірка достовірності джерела пакету

S6 - перенесення об'єкту в групу ризику.

S7 - підтвердження об'єкту.

S8 - перевірка логічних портів і адресного простору.

S9 - якщо перевірка дала негативний результат, триває перебування об'єкту в мережі в групі ризику.

S10 - якщо перевірка дала позитивний результат, процедура передає управління процедурі контролю за об'єктами.

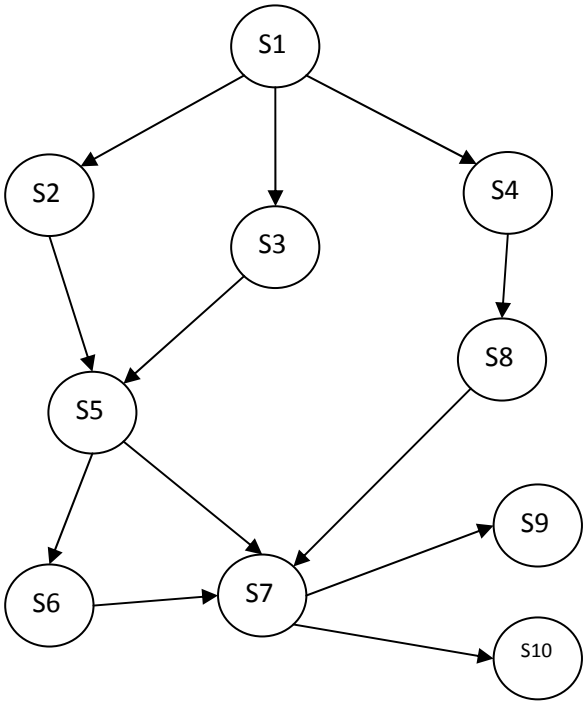

Рис. 1.6 Граф зв'язності подій в мережі

Оскільки параметри передаваних в мережі пакетів є жорстко регламентованими, виявлення аномалій піддається сигнатурному методу контролю над поведінкою мережі. Аналіз логічних каналів і адресного простору є нетривіальним завданням і вимагає імовірнісного підходу до контролю системи. Під контроль потрапляє система розподілу динамічних адрес а також процес відкриття логічного порту при аутентифікації мережевого об'єкту і виділення логічного каналу зв'язку з об'єктом. Детальна процедура здійснення контролю і реакції представлена алгоритмом на рис.1.7.

Визначивши основні елементи забезпечення безпеки безпровідної мережі можна визначити процедурні етапи реалізації виявлення вторгнення і реакції на цю подію.

На першому етапі необхідно сформувати безліч об'єктів безпровідної мережі і визначити властивість приналежності однієї з трьох груп, запропонованих в розробці. Слід зазначити, що під об'єктами системи розуміється уся безліч комунікаційних облаштувань мережі.

На другому етапі необхідно визначити властивості мережевих об'єктів, схильних до контролю. На початковому етапі кількість властивостей має бути мінімальною, але достатньою для адекватного опису параметрів об'єкту. З часом можна збільшувати цю кількість проте зі збільшенням кількості параметрів контролю, може сповільнитися час реакції на аномалії, а також збільшитися навантаження на канал зв'язку.

На третьому етапі формуються параметри поведінки мережі, схильні до контролю. Параметри поведінки мережі характеризують третій рівень моделі взаємодії мережі. Параметри об'єктів характеризують логічний рівень взаємодії.

На четвертому рівні формуються правила для реакцій на виникнення аномалій в поведінці об'єктів або усієї мережі. У загальному випадку при виникненні подій, пов'язаних з вторгненням в систему або можливим вторгненням передбачено три сценарії подій - перенесення об'єктів в групу ризику, повторне підтвердження об'єкту або розривши зв'язки з об'єктом.

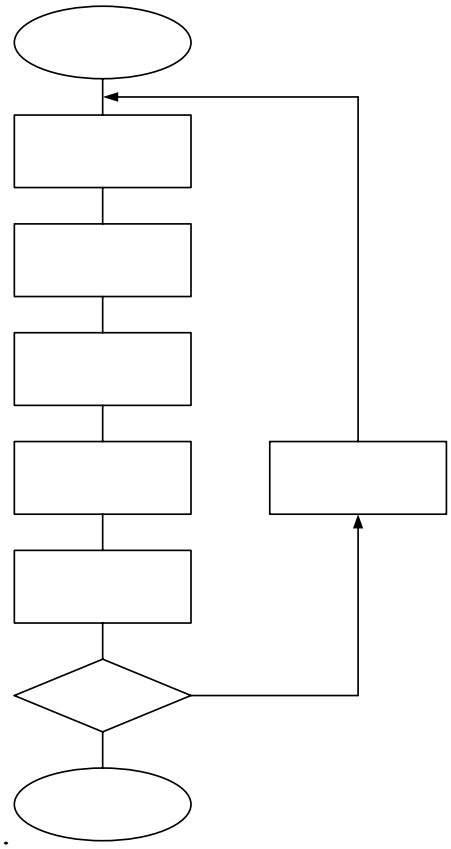

Рис. 1.8 Метод організації безпеки БС

На п'ятому етапі проводиться аналіз подій, що сталися. В результаті аналізу повинно бути визначено, чи було це вторгнення або ні, і, якщо підтверджено вторгнення, необхідно відновити дані про об'єкти і мережу. Якщо ж подія сталася по помилковому або помилковому спрацьовуванню, і загрози мережі немає, то процес організації безпеки закінчений.

Для реалізації системи безпеки безпровідних мереж запропонована абстрактна структура цієї системи.

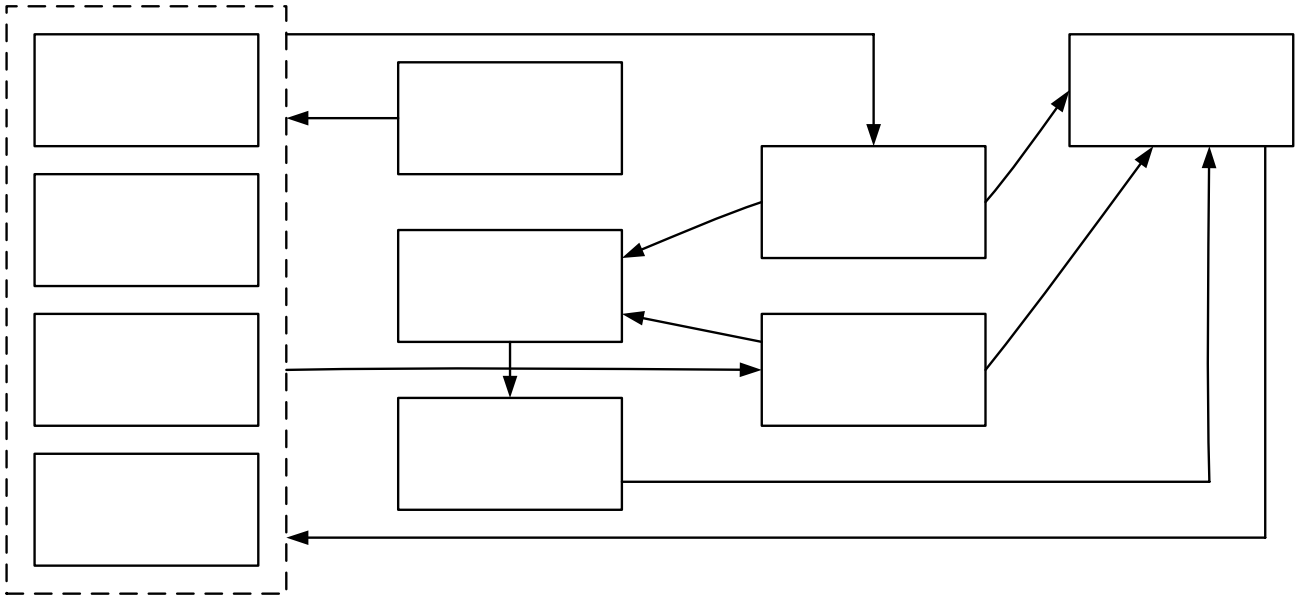

Рис. 1.9 Структура абстрактної системи безпеки БС

У структуру системи входять сім блоків.

Бази даних. У цей блок включено чотири бази даних. База цих загроз включає сигнатури відомих методів атак. База об'єктів містить в собі відомі об'єкти мережі і їх властивості. База сценаріїв містить розроблені сценарії реакцій на вторгнення. База цих аномалій містить журнал подій, які не були пізнані як вторгнення, але викликали нетипову активність в мережі.

Блок формування об'єктів. Визначає об'єкти мережі, а також формує їх властивості, з точки зору контролю над їх активністю з мережі. Формує базу цих об'єктів.

БД загроз

Блок формуванн об'єктів

БД об’єктів

Блок початкс реакції

БД сценаріїв

Блок прийня

Блок початкової реакції. Генерує сигнали тривоги на аномальну активність і веде журнал подій.

Блок виявлення зловмисної активності. Блок реагує на відомі вторгнення, оповіщаючи блок початкової реакції.

Блок виявлення аномальної активності. Блок реагує на підозрілі дії об'єктів мережі або на поведінку в мережі в цілому. Також оповіщає блок початкової реакції.

Блок ухвалення рішень. Блок визначення дій на події, що відбуваються в мережі.

Блок аналізу загроз. Блок аналізу і класифікації подій. Формує бази цих загроз і підозрілої активності.