УДК 004.621.3:681.14

**Чернишев О.М.**

# СИСТЕМА ПІДТРИМКИ ПРИЙМАННЯ РІШЕНЬ ДЛЯ ЗАСОБІВ МОНІТОРИНГУ

У статті запропонована система підтримки прийняття рішень для систем моніторингу безпеки інформаційних мереж, що забезпечує гнучку реакцію засобів захисту на дії порушників і дозволяє підвищити захищеність користувацьких і системних даних за рахунок виконання прогнозування дій зловмисників в автоматичному режимі.

*Вступ.* Моніторинг безпеки являє собою комплекс мір та заходів (організаційних, технічних і правових), які направлені на реалізацію спостереження, аналізу і прогнозування станів безпеки інформаційних мереж (ІМ). Класична сучасна система моніторингу безпеки (СМБ) характеризується принципом виявлення, областю застосування і методами виявлення, які використовуються [1]. В межах одної мережі можуть використовуватись декілька СМБ, що відповідають за виконання задач захисту інформації різного плану. При цьому в існуючих СМБ для аналізу дій суб'єктів використовуються експертні оцінки, що знижує коректність прийняття рішень по подальшим контр мірам по відношенню до порушників.

Таким чином, є актуальним створення систем підтримки прийняття рішень (СППР) для СМБ, які дозволяють мінімізувати людський фактор і генерують адекватні коректні рішення для рішення питань безпеки.

*Основна частина.* З економічної точки зору система моніторингу безпеки ІМ направлена, перш за все, на виявлення несанкціонованих дій з інформацією і інформаційними ресурсами. До переліку інформації, що представляє цінність і потребує захисту, відносять конфіденційну управлінську, науково-технічну, торгівельну і іншу інформацію, що використовується при досягненні переваги над суперниками. Витік цих даних може нанести шкоду її власникам у вигляді прямих втрат інформації і т. і.

Для більш коректного і адекватного використання СМБ необхідно, виходячи із вимог і потреб конкретної системи, яка захищається, виробити стратегію захисту на основі якої будуть взаємодіяти всі захисні механізми. Виділяються наступні три стратегії захисту [2]:

- оборонна – захист від вже відомих загроз, здійснюється без надання суттєвого впливу на інформаційно-керуючу систему і мережу;
- наступальна – захист від всієї множини потенційно можливих загроз, при якому в архітектурі і технології функціонування інформаційно-керуючої системи і мережі враховуються умови, що продиктовані потребами захисту;
- випереджувальна – створення інформаційного середовища, в якому загрози інформації не мали б умов для виникнення.

Використання СМБ необхідно і ефективно лише при реалізації наступальної чи випереджувальної стратегії, а також їх комбінації.

В практичних застосуваннях потрібне вироблення політики безпеки ІМ, яка базується на використанні різноманітних способів керування доступом, визначаючим порядок використання ресурсів суб'єктами.

Управління доступом може здійснюватись за допомогою наступних методів визначення прав на використання інформації [3]:

- вибірковий метод, при якому формується матриця прав доступу, яка містить відомості про суб'єктів, ресурси і права доступу до них;
- повноважний метод, який передбачає зіставлення мітки критичності для кожного об'єкту (інформаційної цінності) і рівня прозорості суб'єкту (його рівень доступу до інформації).

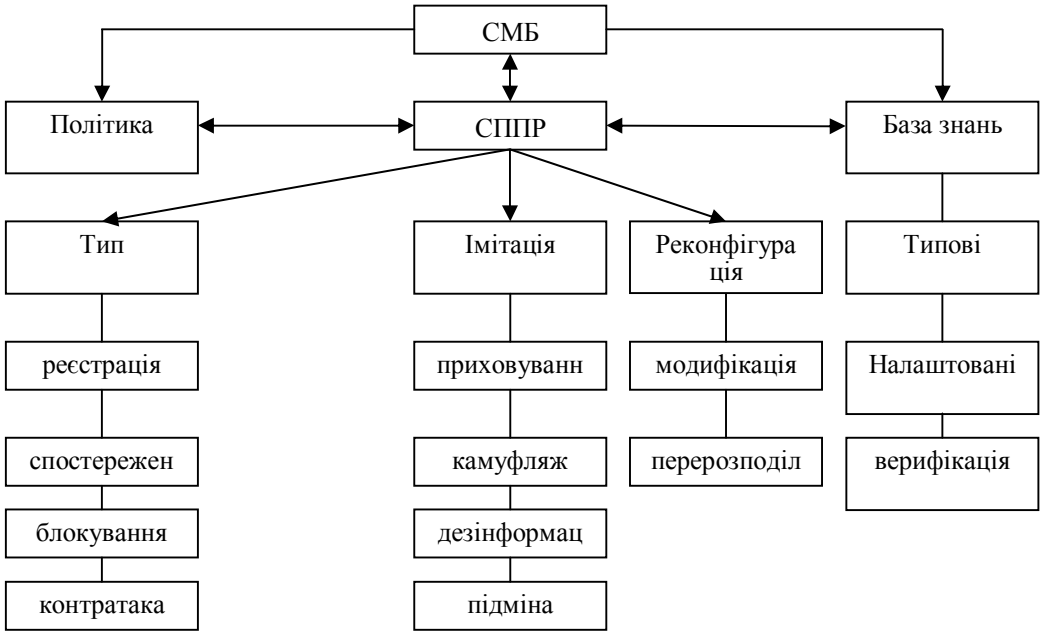


Рис.1. Узагальнена структура СППР для системи моніторингу безпеки

Використання СППР для СМБ дозволяє більш коректно організувати роботу всієї системи захисту інформації в цілому і адміністратора безпеки окремо.

При цьому зменшується час реакції засобів захисту на позаштатні ситуації і підвищується рівень захищеності ІМ. На рис. 1. показана загальна схема реалізації СППР, яка при побудові можливих варіантів відповідних дій для системи захисту інформації в ІМ використовує дані, отримані при аналізі інформації системою моніторингу безпеки. СМБ аналізує існуючі причинно-наслідкові зв'язки, що вказують на взаємозв'язок між вторгненнями, диференційованими за часом, місцем, способом атаки і задіяними засобами.

Імплікація параметрів різноманітних вторгнень в єдину оцінку проводиться шляхом конкретизації цілей або на основі збору інформації про дії визначеного суб'єкта. Потім проводиться автоматичне ранжування за рівнями небезпеки загроз дії порушника на основі аналізу можливих збитків інформаційній мережі.

При цьому пріоритетною задачею СМБ є формування ймовірностей вторгнень зловмисників в ІМ і визначення потенційних цілей порушників, а також прогнозування їх подальших дій.

СППР, на підставі виробленої стратегії захисту і політиці безпеки в ІМ, що використовується, пропонує адміністратору безпеки різноманітні варіанти поведінки і реагування на інциденти, що виникають в системі.

В базу знань СППР, що використовується для навчання системи, закладені типові конфігурації, що визначаються шаблонними моделями поведінки відносно порушників. Так, на підставі статистичної інформації о подіях, що відбулися в ІМ і відповідних їм контрзаходам, формуються значення відповідних дій, що застосовуються за замовчуванням. Подальше навчання СППР і СМБ відповідно, а також керування правами доступу для політики безпеки, здійснюється за допомогою налаштування відповідних параметрів в базі знань.

Крім того, через деякий конкретний проміжок часу виконується верифікація рішень, що були прийняті як адміністратором за допомогою СППР або без її застосування, так і СМБ самостійно. На підставі отриманих оцінок правильності прийнятих рішень розробляються більш коректні правила поведінки СМБ у позаштатних ситуаціях.

Основні типи дій, що пропонуються СППР адміністратору безпеки, можуть бути представлені трьома наступними групами:

- запропонована реакція СМБ на події, що відбуваються в ІМ;

- імітація відповіді, що отримує порушник, при спробі здійснити несанкціоновану дію;
- ре конфігурація системи захисту, що виконується за необхідністю.

Типи реакції системи захисту, на загрози безпеці, що виникають, представлені у вигляді блоків на рис. 1, впорядковані за ступенем збільшення керуючих дій. Розглянемо їх більш детально.

Під реєстрацією розуміється запис виявлених позаштатних ситуацій в журнали реєстрації СМБ і повідомлення адміністратору безпеки. Спостереження – це тимчасова відсутність реакції на дії порушника для виявлення його подальших планів і збору доказів. Блокування являє собою завершення з'єднання з атакуючим вузлом чи блокування облікового запису суб'єкту до виконання повного аналізу ситуації, що склалась. Контратака – це виконання аналогічних або переважаючих за силою дій, направлених на нейтралізацію зловмисників. Використання контратаки повинно бути суворо регламентовано.

Імітація відповіді використовується для дезінформування порушника,змушує його робити помилки і виконувати некоректні дії, збільшуючи при цьому рівень захищеності [4]. При цьому визначають наступні варіанти імітації відповіді:

- приховування – наприклад, приховування топології за допомогою мережевого екрану;
- камуфляж – наприклад, використання інтерфейсу Unix в операційній системі Windows;
- дезінформація – наприклад, повернення програмою The Bat заголовків, які характерні для Outlook;
- підміна – наприклад, існування двох складних зовнішніх баз даних.

Крім того широко використовуються методи стеганографії, які дозволяють приховати сам момент передачі інформації і використовувати приховані і змінні трафіки.

Реконфігурація системи захисту інформації застосовується для цілеспрямованої зміни структури системи захисту, заснованої на використанні залежності захищеності об'єктів ІМ і інформаційної системи від їх інформаційної цінності [5]. При цьому ре конфігурація реалізується як:

- модифікація, яка виконується як для забезпечення заданого рівня захищеності ІМ так і для зниження витрат і вартості системи захисту інформації;
- перерозподіл, коло забезпечення вимог по захищеності об'єктів інформаційної мережі здійснюється за рахунок перерозподілу засобів захисту з об'єктів, що мають мінімальну інформаційну цінність, або засобів з об'єктів, які на даний момент не під впливом атаки.

*Висновки*

1. Ефективність застосування систем моніторингу безпеки, в інформаційних мережах багато в чому визначається коректністю її реалізації. Одним із найважливіших елементів системи моніторингу, є алгоритм формування керуючих впливів і визначення типу реакції засобів захисту на потенційно небезпечні дії в системі.
2. Запропонована в роботі система підтримки прийняття рішень дозволяє забезпечити гнучку реакцію системи моніторингу безпеки на дії порушника, а також підвищити захищеність користувацьких системних даних за рахунок виконання прогнозування дій зловмисників, імітації відповідей на їх запити і ре конфігурації системи захисту, що виконується в автоматичному режимі.

## ЛІТЕРАТУРА

1. Азаренко Ю.Ю. Мониторинг информации в компьютерных сетях// Азаренко Ю.Ю., Чернышев А.Н., Смычков Е.Е., Хорошко В.А.// Збірник наукових праць СНУЯЕ та П, №2(22), 2007.-с.187-197.
2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.// Домарев В.В. – Киев: ТИД «ДС», 2001.-688с.
3. Голубенко О.Л. Політика інформаційної безпеки// Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Яремчук Ю.Є. – Луганськ: Вид.СНУ ім. Даля, 2009.-300с.

4. Лукацкий А.В. Обнаружение атак// Лукацкий А.В. – СПб.: «БВХ-Петербург». 2003.-608с.
5. Ленков С.В., Методы и средства защиты информации. В 2-х томах// Ленков С.В., Перегудов Д.А., Хорошко В.А. – Киев: Арий, 2008.

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Хорошко В.О.р