дорівнює визначнику матриці M з рівняння (20). Тільки цей знаменник і необхідно визначити.

Результати експериментів з визначення асимптотичної стійкості одноконтурного параметричного підсилювача, проведених за описаним методом на основі знаменника функції $G(s,\xi)$ кола, наведені у [8].

1. *Солодов А.В., Петров Ф.С.* Линейные автоматические системы с переменными параметрами.-М.:Наука, 1971.-620 с.
2. *Бриккер И.Н.* О частотном анализе линейных систем с переменными параметрами//Автоматика и телемеханика, № 8, 1966.-с.43-54.
3. *Шаповалов Ю.І.* Особливості оцінки асимптотичної стійкості лінійних параметричних кіл частотним символьним методом. // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип.55. – К.: 2010. – с. 126-133.
4. *Шаповалов Ю.І., Смаль Д.Р.* "Оцінка асимптотичної стійкості лінійних параметричних кіл за допомогою рядів Фур'є". Вісник НУ „Львівська політехніка".-№680.-2010.- с. 18-21.
5. *Шаповалов Ю.І.* «Формування символьних рівнянь лінійних параметричних кіл методами виключення змінних». // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип.48. – К.: 2008. – С. 111-119.
6. *Шаповалов Ю.І.* «Про можливість застосування матричних та топологічних методів до моделювання лінійних параметричних кіл». // Зб. наук. пр. ІПМЕ НАН України. – Вип.48. – К.: 2008. – С. 125-135.
7. *Шаповалов Ю., Мандзій Б.* Символьний аналіз лінійних параметричних кіл: стан питань, зміст і напрямки застосування. // Теоретична електротехніка. 2007. Вип. 59 с.3-9.
8. *Ю.И. Шаповалов, Б.А. Мандзий, С.В. Маньковский* «Об оценке устойчивости линейных параметрических цепей при частотном символьном анализе», Журнал «Известия вузов. Радиоэлектроника», т.53, №9, 2010,с.11-17.

Поступила 20.09.2010р.

УДК 621.372

С.О. Нікулін, м. Київ

РОЗРОБКА СТРУКТУРИ СИСТЕМИ ТИПУ HONEYPOT ДЛЯ ЗАХИСТУ ДОСТУПУ В СПЕЦІАЛІЗОВАНУ СИСТЕМУ УПРАВЛІННЯ

Система захисту (SZ), що ґрунтується на основі *honeypot* має ряд особливостей, якими остання відрізняється від іншого типу системи захисту. До таких особливостей можна віднести наступні:

- більш широкі можливості по виявленню та визначенню небезпек, що являються потенціальними ініціаторами атак проти системи або об'єкту, який охороняється (OZ),

- розширені можливості по реалізації процедур протидії атакам, що активізувалися відповідними небезпеками, що являються зовнішніми по відношенню до OZ,
- здатність відповідних систем захисту (SZH) до реалізації спеціальних процедур по відношенню до OZ, які пов'язані зі збільшенням рівня безпеки OZ,
- високий рівень універсальності структур елементів захисту (Zh), які формуються в рамках SZH, що дозволяє використовувати Zh_i розв'язку задач різних типів,
- можливість створення розподілених систем захисту, елементи яких можуть переміщатися в рамках відповідної розподіленої системи управління.

Біль широкі можливості по виявленню та визначенню небезпек ґрунтуються на тому, що на відміну від стандартних засобів, наприклад, firewall, IDS чи системи захисту доступу мають можливість перехоплювати атаки з OZ на себе і втручатися в процес реалізації атаки, що ініціюється зовнішньою небезпекою. Таким чином, щоб отримати максимально можливу кількість інформації про ZN та іншу інформацію, яка може бути використана для розв'язку задачі збільшення рівня захисту OZ. Особливістю цієї можливості є необхідність SZH маскувати себе по відношенню до ZN. Таким чином, щоб остання сприймала SZH як реальний об'єкт, що атакується ZN. Це приводить до необхідності в рамках SZH розв'язувати наступні задачі, які не є типовими для стандартних засобів захисту OZ, що переважно використовувати в системах захисту. До таких задач можна віднести наступні:

- задача ідентифікації об'єкту захисту по відношенню до якого ініційована атака,
- задача захисту у ідентифікованих OZ базових характеристик, що можуть бути відомими і можуть використовуватися для формування атак на відповідні об'єкти,
- задача обміну активними даними між OZ_i і SZH, незалежно від того, чи OZ_i атакований на момент ініціації зі сторони SZH чи ні,

Приведені вище задачі є зрозумілими, оскільки Zh_i і SZH в цілому є системами адаптивними і повинні враховувати усі зміни, які в процесі функціонування OZ в ньому відбуваються.

Розширені можливості в протидії атакам, які активізувалися, обумовлюються тим, що для виявлення окремих атак на визначення можливих способів протидії активізованим атакам у SZH є значно більше часу та можливостей, оскільки атака, якщо вона перехоплена, не діє на OZ, а співпрацює з окремим елементом Zhi. Відомо, що для того, щоб можна було активно та успішно протидіяти атаці, необхідно мати наступну інформацію:

- інформацію про загрозу, яка використовується атакою в процесі реалізації,

- ціль реалізації атаки,
- спосіб реалізації атаки,
- інформацію про рівень небезпеки, який може обумовлюватися відповідною атакою,
- інформацію про міру універсальності атаки.

Якщо атака була ініційована ZN і почала функціонувати по відношенню до OZ, то це означає, що у OZ існує загроза, яка не є відомою для системи SZ. Тому виявлення відповідної загрози є першочерговою задачею SZH_i. Очевидно, що по відношенню до відомих загроз, які існують в OZ, SZH забезпечує необхідні методи їх нейтралізації на етапі виявлення атак, що тільки зароджуються в OZ. В даному випадку доцільно прийняти, що атаки існують або функціонують в межах OZ. Всі фактори, що спричиняють можливість виникнення атак, будемо розглядати як деякі зовнішні фактори, що сформовані небезпеками. В рамках OZ доцільно розглядати атаку, яка представляє собою певний процес, що складається з послідовності подій. Останні розділимо на наступні етапи реалізації атаки:

етап зародження атаки,

етап зародження атаки, або другий етап,

етап завершення атаки, або третій етап.

На першому етапі атака взаємодіє з загрозою і здійснює дії, що пов'язані з проникненням атаки в середовище OZ. Слід відмітити, що послідовність подій, які описують або реалізують відповідний етап в рамках засобів OZ можуть бути розділеними у просторі OZ. У зв'язку з цим досить важко ідентифікувати сукупність певної послідовності подій, як таку, що відповідає реалізації окремої атаки.

Це означає, що окрема загроза, яка існує в OZ, може бути розділеною в середовищі OZ, що суттєво ускладнює виявлення відповідної загрози. Слід відмітити, що загрози можуть виникати та модифікуватися в процесі функціонування OZ. Тому задача виявлення можливих загроз не є тривіальною. Відповідно, виявлення атаки на етапі зародження є досить складним.

На етапі розвитку атаки остання реалізує процеси або окремі події, безпосередньо пов'язані з досягненням цілі атаки, тому для засобів типу Zh особливо важливим є здатність розпізнавання цілі атак. Якщо притримуватися традиційних уявлень про розпізнавання образів [3], то основою для цих процесів служить наявність еталонних образів, які необхідно розпізнавати. У даному випадку такими еталонами можуть служити описи відомих цілей або описами самих атак. Очевидно, що використання такого підходу недоцільне, тому що всі атаки є відомими та різновидність можливих атак є досить велика. Більш ефективним є підхід, що ґрунтується на описі еталонів, цілі функціонування OZ, оскільки будь-яка система створюється для виконання тих чи інших задач, які окреслюють ціль функціонування OZ. Такий підхід використовується при створенні системи

IDS. Один із принципів діагностики інтрузів в таких системах полягає у діагностиці або у виявлені ненормальної поведінки системи [2]. Якщо описи допустимого функціонування системи звести до опису цілей, що є визначеними для OZ або цілей для досягнення яких система була спроектована, то всі ті цілі, які не відповідають описаним цілям, для реалізації яких проектувалась система, є цілями атак. Опис цілей є в повному і точному описі для складних систем в багатьох випадках є досить складною задачею, і ідентифікувати ціль як таку, що відповідає певній атаці, є неможливим. В рамках стандартних підходів це обумовлено тим. Що проектна ціль функціонування системи в багатьох випадках не може бути описана достатньо точно. Така ціль уточнюється значенням параметрів, що описують сформульовані цілі. У випадку систем управління, в рамках яких розв'язуються спеціальні задачі, ситуація дещо відмінна від ситуації в традиційних інформаційних системах. Це обумовлюється тим, що в таких системах, що спеціалізуються на використанні інформаційних систем, цілі функціонування співпадають з цілями управління об'єктом. Останній дозволяє суттєво звузити можливі варіанти способів та результатів управління, що дозволяє більш точно описувати ціль функціонування відповідної інформаційної системи. Уявлення по ціль, і тим більше, її опис, в цьому випадку є досить широким. Виходячи з того, що будь-який об'єкт чи подія, яку можна було інтерпретувати як ціль, описується тими чи іншими параметрами. Для інформаційних систем є характерними досить складні цілі, які в багатьох випадках на етапі проектування описати неможливо. Тому розглянемо наступні ситуації, що безпосередньо зв'язані з описом цілей функціонування інформаційної системи управління цілей та атак на відповідні системи, які по суті, є атаками на об'єкти управління.

Першою, найбільш ідеальною ситуацією, що відповідає можливості адекватного опису цілей, є ситуація, коли весь процес реалізації певної цілі управління описується у вигляді однозначних детермінованих подій, які визначають окрему ціль функціонування. Тоді будь-які зміни однозначності та детермінованості подій, що приводять до виникнення кінцевої події, яка інтерпретується як ціль, може розглядатися як прояв атаки OZ з ціллю, що полягає у недопущенні відповідної кінцевої події, у формі, яка передбачена проектом відповідної системи. Наступною ситуацію, яку можна було б виділити, є ситуація, при якій окрема ціль функціонування інформаційної системи управління (IZU) може бути ідентифікована лише в результаті використання відповідної цілі об'єктом управління. Наприклад, якщо ціллю управління є забезпечення оптимального способу функціонування в певним чином заданих межах, часових чи будь-яких інших. Тоді факт досягнення цілі IZU може бути ідентифікований лише на основі аналізу процесу функціонування або після завершення відповідного інтервалу функціонування, або після завершення відповідного інтервалу функціонування відповідного об'єкту управління. Зрозуміло, що описана ситуація представляє собою крайній випадок по відношенню до першого

випадку однозначної і детермінованої поведінки IZU. Тому необхідно для реальних систем IZU використовувати підхід, який по своїй суті, був би синтезом двох вище зазначених крайніх підходів. Це означає, що системи захисту повинні в найбільшій мірі відображати результат відповідного синтезу.

Наступний підхід буде представляти собою синтез двох зазначених вище підходів. Умовами реалізації такого синтезу є наступні:

використання окремих компонент в рамках IZU для розв'язку задач захисту,

оцінка доцільності їх використання повинна ґрунтуватися не на кількості виявлених і усунених атак, а на мірі безпечності функціонування IZU,

функціональна активність системи захисту в середовищі повинна бути взаємозв'язана з необхідною мірою забезпечення безпеки IZU.

Розглянемо структурну схему системи захисту, що ґрунтується на використанні засобів захисту, які побудовано на принципах технологій honeypot. Схема, що відображає основний склад такої системи та взаємозв'язки між окремими компонентами системи, приведена на рис. 4.1.

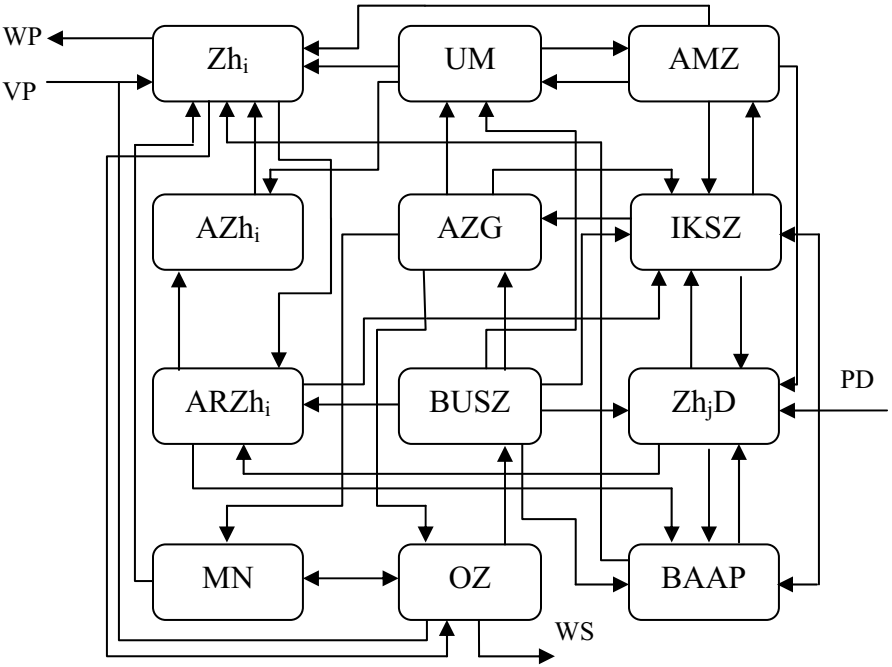

Рис. 4.1. Структурна схема системи захисту

На рисунку 4.1. прийнято наступні скорочення:

- WP — вихідний пакет з системи захисту,
- VP — вхідний пакет, що попадає в систему захисту та в систему, що захищається,
- WS — вхідний пакет системи, що захищається,
- Zhi — засіб захисту типу honeypot,
- UM — управління міграцією Shi,
- AMZ — активізація мігруючого засобу захисту,
- AShi — аналіз роботи Shi,
- ARZhi — аналіз загроз об'єкту захисту,
- MN — модель безпеки,
- PD — запит доступу до OZ,
- AZG — аналіз загроз об'єкту захисту,
- BUSZ — блок управління системного захисту,
- OZ — об'єкт, що захищається,
- IKSZ — інформаційні компоненти системи захисту,
- ZhjD — засіб захисту доступу,
- BAAP — базові алгоритми подій, що пов'язані із впливом на рівень безпеки OZ.

Коротко охарактеризуємо кожен функціональний блок системи (SZ). Блок Shi представляє собою мобільний засіб захисту, який функціонує у відповідності з принципами honeypot.

Блок AShi представляє собою засіб, що здійснює модифікацію окремого Shi таким чином, щоб Shi адаптувався до змін зовнішніх факторів, що представляють собою небезпеку. Прикладом реалізації одного з процесів адаптації може служити наступний процес.

Зрозуміло, що однією з функцій Shi є розпізнавання типу атаки. Одна з реалізацій такої функції полягає у використанні певних еталонів атак, описи яких зберігаються в магазині автомату, що описує зовнішній формі відповідний Shi. Досить велика частина атак, що реалізується по відношенню до OZ, мають однакові фрагменти. Переважно такі фрагменти співпадають на початкових стадіях реалізації відповідних атак. В цьому випадку виникає задача вибору чергового опису еталону атаки для розв'язку задачі ідентифікації атаки. Коли початкові фрагменти різних атак співпадають, а дисципліну вибору чергового еталону вибрати послідовною, то може виявитися, що перехід Shi на еталон реальної атаки виникне тільки після того, як будуть перебрані описи початкових фрагментів інших атак, які в даний момент не здійснюються. Щоб мінімізувати такі затрати, модуль AShi реалізує зміну послідовності вибору початкових фрагментів опису еталонів атак, при якій вибирається не послідовно розміщені описи еталонів, а описи еталонів тих атак, які найбільш вірогідні в даному фрагменті мережевого середовища або в даному фрагменті середовища OZ або в певний період часу функціонування OZ. Очевидно, що процеси адаптації реалізуються в тих чи

інших механізмах, які використовуються алгоритмами Shi та різними критеріями оптимізації. Адаптація Shi, які визначає і реалізує модуль $_{AShi}$, здійснюються на основі даних, що формуються у інших блоках системи захисту OZ, що приведена на рисунку 4.1.

Одним з блоків, який визначає механізми та параметри адаптації AShi, є блок аналізу роботи засобу захисту $ARSh_i$. Основною функцією цього блоку є аналіз процесів, що реалізуються в Sh_i. Різні процеси в Sh_i характеризуються досить загальними параметрами. Прикладом таких параметрів можуть служити кількість циклів, що реалізуються в одній процедурі реалізації того чи іншого алгоритму. Об'єм даних, який аналізується в рамках алгоритму, кількість допоміжних операцій, що виявляються необхідними для розв'язку задачі, для яких призначається той чи інший алгоритм в Sh_i та інші. В даному випадку під кількістю допоміжних операцій розуміється не сама операція в класичному розумінні цього слова, а кількість підпрограм чи окремих модулів, які необхідно було використовувати для реалізації рішення окремої задачі відповідним алгоритмом. Кількість циклів, яку потрібно реалізувати для розпізнавання певного інтруза відповідним алгоритмом, визначається по відношенню до даних одного типу. Тип даних в даному випадку може визначатися наступними способами:

- однотипними даними є ті дані, які характеризуються одним і тим же фрагментом алгоритму, який переважно являється циклом,
- об'єм даних, які використовуються в програмі визначаються кількістю різноманітних даних.

Об'єм даних може зменшуватися завдяки тому, що в процесі реалізації алгоритму не виникає необхідності реалізовувати всі процедури, які є можливими в рамках тієї чи іншої програми. Ця зміна може обумовлюватися зміною значень вхідних даних, які використовуються даним алгоритмом.

Блок $ARSh_i$ функціонує на основі аналізу стану Shi або на основі параметрів алгоритмів, що функціонують в Sh_i на деякому інтервалі часу. Наприклад, якщо Sh_i протягом певного інтервалу Δt_i не вивив інтрузів, а останні реалізовували атаки, що виявилися успішними, то на основі реалізації успішних атак, що здійснюються блоком управління BUSZ, $ARSh_i$ ініціює новий аудит, який відповідного інтруза не виявив, і таким чином допустив можливість реалізації успішної атаки. Успішність атаки на OZ може виявитися лише блоком BUSZ, оскільки в залежності від типу атаки остання приводить до зміни стану в OZ або до появи події в OZ, яка не передбачалася в рамках алгоритму функціонування OZ, як подія, яка є допустимою. Тому інформація про це з OZ передається в BUSZ, оскільки останній повинен визначити, якого характеру аналіз в рамках всієї системи SZ необхідно ініціювати для того, щоб можна було протидіяти наслідком суспільної атаки, або які додаткові дії необхідно ініціювати в рамках SZ, щоб уникнути можливості реалізації відповідних атак в наступних циклах функціонування

спеціалізованої системи управління. Блок управління міграцією засобів захисту виконує наступні функції в процесі функціонування системи захисту в цілому:

- визначає нове місце для розміщення вибраного Shi в середовищі OZ,
- переміщає в це місце відповідний засіб,
- займається реконфігурацією в середовищі, що охороняється системою SZ.

Визначення нового місця в середовищі захисту полягає у зміні вхідних параметрів відповідного засобу. Наприклад, такою зміною може бути зміна вхідної адреси засобу, що відповідає підключенню до того чи іншого місця в мережі системи управління. Іншим прикладом зміни місця розміщення Shi в середовищі OZ може служити переорієнтація відповідного засобу захисту напевний тип атаки. Така інтерпретація обумовлюється тим, що в рамках OZ атаки можуть ініціюватися по відношенню до атаки одного типу, які можуть ініціюватися, які орієнтовані в просторі адрес на одну і ту ж саму адресу. Наприклад, в силу її специфіки. Така ситуація є досить відомою, наприклад, по відношенню до адрес електронної пошти [4, 5].

Блок управління міграцією разом з блоком активізації мігруючого засобу AMZ представляє собою систему моніторингу місць розміщення Sh_i в середовищі, яке захищається системою SZ. Коротко розглянемо особливості функціонування AMZ, оскільки вони не зводяться виключно до активізації засобів захисту в безпосередньому значенні цього терміну. Доцільність самої активізації Zh_i і Zh_iD блоком AMZ обумовлюється тим, що активність захисту означає, що останні перехоплюють пакети по адресах, на які останні настроєні. Таких пакетів може бути досить багато, протягом інтервалу часу всі пакети перехоплювати недоцільно, оскільки не всі вони можуть бути носіями інтрузів, а їх аналіз може привести до превантаження відповідних засобів захисту. Тому блок AMZ по суті здійснює управління активністю Zh_i в часі. Таке управління грунтується на даних про інтенсивність атак на OZ, яка міняється в часі, міняється по відношенню до різних адрес, і відповідно, різних фрагментів OZ. На основі закономірностей зміни активності атак в просторі або мережених адрес, відповідні дані про необхідність міграції Zhi в просторі адрес блок активізації засобів захисту передає в блок управління міграцією. Це необхідно через те, що блок UM здійснює просторовий моніторинг системи Zh_i, і тому тільки в ньому знаходяться дані про місце знаходження кожного Zh_i та про міру активності Zh_i кожного. Таким чином, на основі аналізу активності всіх Zhi, що знаходяться в системі SZ, блок UM вибирає необхідного кандидата серед Zh_i на його переміщення. Критерієм вибору Zh_i може служити міра його текучої активності. Іншим прикладом критерію вибору Zh_i для міграції може служити текуче значення пріоритету важності відповідного Zh_i. Цей критерій тісно пов’язаний з мірою безпеки відповідного фрагмента OZ.

1. *Коул Э.* Руководство по защите от хакеров. — М.: Издательский Дом «Вильямс», 2003.
2. *Столлинг В.* Основы защиты сетей. Притложения и стандарты. — М.: Издательский Дом «Вильямс», 2002 — 433 с.
3. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. — М.: Техносфера, 2006 — 1072 с.
4. *Лукацкий А. В.* Обнаружение атак. СПБ БХВ — Петербург, 2001, 624 с.
5. *Мак-Клар С., Шах С, Шах Ш.* Хакинг в web: атаки и защита. — М.: Издательский Дом «Вильямс», 2003, 384 с.

Поступила 29.08.2010р.

УДК 377.1:158.920

Б.В.Дурняк, д.т.н., УАД, М. Поліщук, викл. ВПТУ, Р.А. Федчишин, вик. ВПТУ
Л.С. Сікора, д.т.н., НУ «Львівська політехніка»
Р.Л. Ткачук, к.т.н., ЛДУ БЖД

КОГНІТИВНІ МОДЕЛІ АКТИВІЗАЦІЇ ПРОФЕСІЙНО-ОРІЄНТОВАНОЇ ПІДГОТОВКИ КАДРІВ ДЛЯ КОМП'ЮТЕРИЗОВАНИХ ТА АВТОМАТИЗОВАНИХ ВИРОБНИЦТВ З ІЄРАРХІЧНОЮ ОРГАНІЗАЦІЄЮ

Анотація. Розглянуто когнітивну модель активізації професійно-орієнтованої підготовки учня базуючись на методах інформатики, системного аналізу та психології.

Annotation. This article examines the cognitive model of implementation of professional orientation for students based on methods of information, systemic analysis and psychology.

Ключові слова. Управління, когнітивна модель, ієрархія, система.

Key words. Management, cognitive model, hierarchy, system.

Актуальність. Зростаючі вимоги до персоналу виробничих підприємств, організацій, адміністративно-управлінського персоналу, держаних службовців, які виконують свої обов'язки в ситуації напруженій кризою і конфліктами, вимагають нових підходів до їх взаємодії на всіх рівнях ієрархії техногенно-соціальної та регіональної структур. Це відповідно ставить задачу підвищення професійного рівня підготовки і перепідготовки кадрів для всіх рівнів виробництва і управління [1-2].

