УДК 381.3.06

О.Є. Мазулевський[1], Г.Я. Криховецький[1], О.А. Колотило[2]

[1]*Військовий інститут телекомунікацій та інформатизації НТУУ «КПІ», Київ*
[2]*Національний авіаційний університет, Київ*

РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ КОМПЛЕКСНОЇ МЕТОДИКИ АДАПТИВНОГО КОНТРОЛЮ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Представлені результати проведеного імітаційного моделювання методик вдосконалення контролю захищеності комп'ютерної мережі. Застосування представлених методик дозволяє підвищити оперативність дій адміністратора безпеки під час проведення ним заходів з контролю захищеності комп'ютерної мережі та усуненні виявлених вразливостей.

Ключові слова: *контроль комп'ютерної мережі, адаптація, трафік, навантаження мережі, модель.*

Вступ

При створенні і в ході експлуатації комп'ютерній мережі (КМ) автоматизованої системи управління (АСУ) неминуче встає питання про захищеність її від загроз безпеці інформації. Захищеність комп'ютерної мережі є одним з найважливіших показників ефективності функціонування АСУ, разом з такими показниками як надійність, відмовостійкість, продуктивність [1]. У публікаціях [2, 3] наведены причини низької ефективності контролю захищеності, які негативно впливають на оперативність діяльності адміністратора безпеки:

– епізодичний характер контролю – характеризується запізненням контролю захищеності, який здійснюють сучасні засоби аналізу захищеності (ЗАЗ);

– значний час контролю – час, що витрачається на проведення повного контролю захищеності всієї комп'ютерної мережі;

– відсутність у сучасних ЗАЗ можливості врахування динаміки змін що відбуваються в комп'ютерній мережі і адаптації параметрів процесу контролю до поточного стану вузлів мережі і ліній зв'язку.

Постановка задачі

Аналіз дій адміністратора [4], що виконуються при проведенні контролю захищеності комп'ютерної мережі, показує, що етап перевірки вузлів мережі на наявність вразливостей характеризується великими витратами часу (до 50 % від загального циклу рішення задачі).

Характерною рисою сучасних АСУ є велика швидкодія, що вимагає достатньо швидкого реагування системи безпеки на усі імовірні загрози безпеки, враховуючи сучасні методики вдосконалення контролю захищеності комп'ютерної мережі [5 – 7], які мають, як поліпшення характеристик системи контролю безпеки так і обмежуючі умови використання. Спостерігається ускладнення в процесах підвищення оперативності дій адміністратора безпеки. В такій ситуації **актуальною задачею** є проведення оцінки ефективності наведених методик вдосконалення контролю захищеності комп'ютерної мережі, що дозволить отримати рекомендації щодо підвищення оперативності дій адміністратора безпеки.

Основна частина

1. Показники та критерії оцінки ефективності контролю захищеності комп'ютерної мережі.

Показник ефективності, для оцінки оперативності дій вибраний час роботи адміністратора безпеки комп'ютерної мережі, що витрачається на виконання контролю і усунення вразливостей:

$$T_{адм} = t_{вв} + t_{іп} + t_{пр} + t_{рпр},$$

де $t_{вв}$ – час виявлення вразливостей, $t_{іп}$ – час інформаційної підготовки ухвалення рішення, $t_{пр}$ – час ухвалення рішення, $t_{рпр}$ – час реалізації вирішеного.

У свою чергу $t_{вв}$ включає:

$$t_{вв} = t_{по} + t_{K_\Sigma},$$

де $t_{по}$ – час, який витрачає адміністратор на виконання ручних підготовчих операції; t_{K_Σ} – сумарний час контролю захищеності (час виконання перевірок при контролі захищеності).

Сумарний час контролю захищеності визначається формулою:

$$t_{K_\Sigma} = \sum_{I-1}^{I}\sum_{J-1}^{J} t_{ij}\theta_{ij},$$

де t_{ij} – час контролю і-го вузла $\left(i \in \overline{i,I}\right)$ j-ою перевіркою $\left(j \in \overline{i,J}\right)$, а θ_{ij} – елемент матриці допустимості перевірок, що визначається таким чином:

$\theta_{ij} = 1$, якщо j-а перевірка використовується для і-го вузла

$\theta_{ij} = 0$, якщо j-а перевірка не використовується для і-го вузла.

© О.Є. Мазулевський, Г.Я. Криховецький, О.А. Колотило

2. Моделювання методики організації контролю захищеності комп'ютерної мережі АСУ.

Сутність методики організації контролю захищеності комп'ютерної мережі АСУ полягає в раціональній організації проведення контролю захищеності на основі експертної інформації про параметри вузлів КМ і потенційних уразливостей, а також в усуненні ручних операцій, що виконуються адміністратором за рахунок автоматичної реалізації етапу підготовки проведення контролю.

Моделювання даної методики проводилося в середовищі об'єктно-орієнтованого програмування Delphi 7.0. Як початкові дані для моделювання були узяті параметри найбільш популярного, поширеного і доступного мережного сканера NESSUS 2.0 [8]. Для моделювання методики були вибрані умови, які імітували характеристики найбільш поширених типів комп'ютерних мереж. Так, наприклад, кількість вузлів мережі змінювалася від 150 до 500 з кроком 50 вузлів. Всі комп'ютери мережі залежно від ролі, яку вони виконують, були розподілені на групи [2]: сервери, автоматизовані робочі місця (АРМ) обслуговуючого персоналу, АРМ керівництва, сервери відділів, АРМ обслуговуючого персоналу відділів, АРМ керівника відділу, АРМ службовців відділу. Кількість перевірок, що виявляють уразливості змінювалося в межах від 1000 до 2000 з кроком 250. Трафік, що створюється перевіркою в ході контролю захищеності вузла мережі задавався випадково з математичним очікуванням 910 кбіт/с.

Час виконання перевірки задавався також випадково в межах ±30 % від середньої тривалості перевірки, значення якої для мережного сканера NESSUS 2.0, яке складало 224 мс.

Для підвищення достовірності результатів моделювання для кожної комбінації кількості вузлів і кількості перевірок моделювання проводилося 50 разів, а потім обчислювалося середнє арифметичне значення кожного параметра для кожного експерименту.

2.1. Оцінка ефективності методики організації контролю захищеності.

В ході моделювання визначено час, що витрачається адміністратором безпеки на підготовчі операції $t_{по}$ і спільного часу проведення контролю $t_{кΣ}$. Розглянемо три варіанти проведення контролю захищеності (КЗ) комп'ютерної мережі: перший – це послідовний варіант проведення КЗ в ручному режимі, другий – КЗ по групах вузлів (всі вузли в групі перевіряються одночасно) в ручному режимі і третій – проведення КЗ на основі методики організації КЗ КМ АСУ. Результати моделювання наведені в табл. 1.

Аналіз, значень приведених в табл. 1 показує, що $t_{кΣ}$ для 3-го варіанту майже в 19 разів менше, ніж для 1 варіанту.

Таблиця 1

Порівняльна оцінка
варіантів контролю захищеності

	Варіант 1	Варіант 2	Варіант 3
Час підготовчих операцій $t_{по}$	475 хвилин	40 хвилин	0
Сумарний час контролю $t_{кΣ}$	923 хвилини	47 хвилин	49 хвилин

Невелике збільшення значення $t_{кΣ}$ для 3-го варіанту в порівнянні з 2-м варіантом (2 хвилини) обумовлене тим, що при моделюванні методики організації контролю захищеності $t_{кΣ}$ залежить від пропускної спроможності мережі, яка виділялася для трафіку КЗ. Проте виграш за часом для варіанту 3 (в порівнянні з варіантами 1 і 2) виходить унаслідок усунення $t_{по,}$ тобто в даному випадку час виявлення вразливостей буде рівним $t_{вв}=t_{кΣ}$. Проведене прогнозування, в MS Excel за допомогою трендів, показало, що при збільшенні використовуваною ЗАЗ пропускної спроможності мережі для трафіку контролю $t_{кΣ}$ може скоротитися в 6 разів (рис.1).

Таким чином, $t_{вв}$ для варіанту 1 складає більше 23 годин (з них 34 % часу витрачається адміністратором на підготовчі операції). Для другого варіанту $t_{вв}$ склало в середньому 83 хвилини (при цьому $t_{по}$ склало 46 %), для третього варіанту $t_{вв}$ в середньому склало 49 хвилин (підготовчі операції відсутні). Отже, проведення контролю по розробленій методиці дозволяє зменшити $t_{вв}$ в середньому на 40 %.

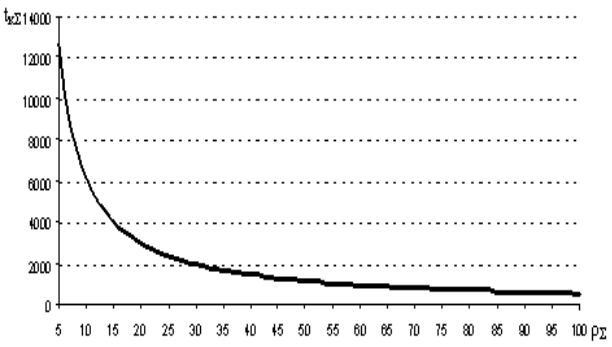

Рис. 1. Прогнозування значення $t_{кΣ}$ залежно від використовуваної смуги пропускання мережі

3. Моделювання методики адаптивного контролю захищеності комп'ютерної мережі

Моделювання методики адаптивного контролю захищеності комп'ютерної мережі проводилося в середовищі математичного моделювання Simulink пакету MatLab 6.5.

Суть даної методики полягає в адаптації параметрів роботи ЗАЗ (трафіку, що створюється перевірками в ході контролю захищеності) до реальних

умов функціонування мережі з метою запобігання можливим перевантаженням мережі. При проведенні імітаційного моделювання необхідно було вирішити наступні завдання:

– визначити структуру і зв'язки між елементами імітаційної моделі;

– визначити початкові дані, які надходять в модель (значення завантаження, яке створюється ЗАЗ, послідовність значень робочої завантаженості вузла мережі і ліній зв'язку по маршруту до цього вузла);

– дослідити зміну $t_{к\Sigma}$ залежно від смуги пропускання мережі, що використовує ЗАЗ.

Результати проведеного раніше експериментально-теоретичного дослідження засобів аналізу захищеності комп'ютерної мережі показали, що найбільш важкі умови для роботи мережі створюються в ході контролю захищеності WEB-серверу на платформі операційної системи Windows'2000 Server [8] із допомогою ЗАЗ NESSUS 2.0. Саме параметри даної перевірки були використані як початкові дані при моделюванні (середній розмір пакету, кількість пакетів відправлених за секунду, загальне число пакетів в перевірці).

В процесі моделювання було враховано, що недоліком мереж побудованих на «спільній шині» є те, що при досягненні певного значення завантаження продуктивність мережі різко падає. Для цього до складу моделі був включений обмежувач. Число верхньої межі обмежувача узято рівним 54 %, згідно [9] із-за застосування алгоритму доступу до середовища передачі такого як «Ненаполегливий ALOHA». Такий тип мережі для імітації вибраний як найбільш важкий для проведення контролю захищеності.

Модель системи управління параметрами КЗ, а саме частини роботи, що відповідає за адаптацію, ЗАЗ до умов функціонування, мережі приведена на рис. 2.

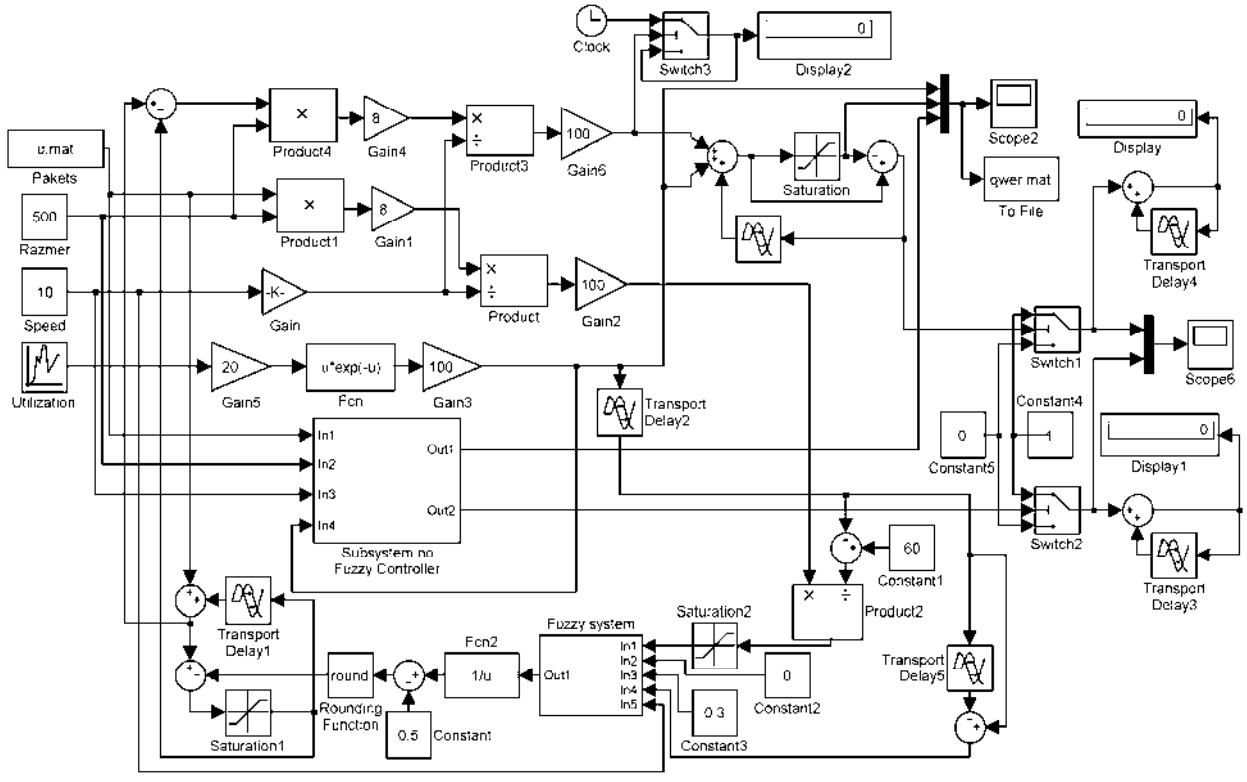

Рис. 2. Модель частини системи адаптивного контролю захищеності

Проведені дослідження на імітаційній моделі показали, що при проведенні адаптивного контролю захищеності комп'ютерної мережі середнє значення завантаження ліній зв'язку на 18,5 % менше, ніж при проведенні контролю без адаптації до умов функціонування мережі. Проте зменшення навантаження на мережу приводить до збільшення $t_{к\Sigma}$ в середньому на 35 %.

Крім того, в результаті моделювання було визначено, що при проведенні адаптивного контролю захищеності число випадків, при яких завантаження досягало гранично допустимого значення завантаження мережі було в середньому на 39 % менше.

Моделювання методики формування плану дій адміністратора не проводилося. Було проведено додаткове дослідження, в ході якого встановлено, що залежно від числа знайдених уразливостей час, що витрачається адміністратором на складання плану дій склало 8 – 12 % від загального робочого часу адміністратора.

Таким чином, при автоматичній реалізації даного етапу виграш в середньому складе 10 %.

Висновки

Проведені дослідження показали, основні залежності етапів дій адміністратора розподіляються таким чином:

$$t_{вв} – 50\ \%,\ t_{іп}+t_{пр} – 25\ \%,\ а\ t_{рпр} – 10\ \%$$

від часу, який витрачає адміністратор безпеки на проведення заходів, пов'язаних з виконанням дій з підвищення рівня захищеності комп'ютерної мережі.

Моделювання методики організації контролю захищеності показало, що час виявлення вразливостей, при її застосуванні, скорочується в середньому на 40 % (виключається час ручних підготовчих операцій). Це означає, що час виявлення вразливостей скоротиться на 20%.

Моделювання методики адаптивного контролю захищеності показує, що сумарний час контролю, із складу часу виявлення вразливостей, збільшиться на 50 %. Це означає, що час виявлення вразливостей зросте на 15%.

Використання методики формування плану дій адміністратора безпеки за результатами контролю, усуває час, що витрачається адміністратором на інформаційну підготовку приймання рішення. Аналіз дій адміністратора безпеки показав [4], що час інформаційної підготовки ухвалення рішення складає 60 % від часу, що витрачається на інформаційну підготовку і саме приймання рішення. Це означає, що час інформаційної підготовки приймання рішення і приймання рішення на 15%.

Таким чином, час роботи адміністратора безпеки при використанні методик вдосконалення КЗ КМ АСУ складе 70 % від часу що витрачається адміністратором на проведення заходів щодо підвищення рівня захищеності комп'ютерної мережі в даний час. Це дозволяє підвищити оперативність дій адміністратора безпеки комп'ютерної мережі в середньому на 30 %.

Список літератури

1. Астахов А. Анализ защищенности корпоративных автоматизированных систем / А. Астахов // Jet Info. – 2002. – № 7(110). – С. 3-28.

2. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. – СПб.: БХВ – Петербург, 2003. – 624 с.

3. Галатенко В.А. Основы информационной безопасности / В.А. Галатенко. – М.: ИНТУИТ.РУ "Интернет-Университет Информационных Технологий", 2003. – 280 с.

4. Шохін Б.П. Вдосконалення контролю за станом захищеності комп'ютерної мережі на основі адаптивного моніторингу / Б.П. Шохін, О.М. Юдін, О.Є. Мазулевський // Зб. наук. пр. ВІТІ НТУУ «КПІ». – 2004. – № 4. – С. 208-217.

5. Мазулевский О.Е. Методика организации контроля защищенности компьютерной сети / О.Е. Мазулевский // Радіоелектронні і комп'ютерні системи. – 2006. – № 5. – С. 122-127.

6. Мазулевський О.Є. Методика адаптивного контролю захищеності комп'ютерної мережі / О.Е. Мазулевський // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. – 2005. – № 10-11. – С. 69-72.

7. Мазулевский О.Е. Методика формирования плана действий администратора безопасности по результатам контроля защищенности / О.Е. Мазулевский // Системи обробки інформації. – 2006. – № 8(57). – С. 80-90.

8. Експериментально-теоретичне дослідження засобів аналізу захищеності комп'ютерної мережі / О.М. Юдін, О.Є. Мазулевський, О.В. Тесленко, С.В. Сомов // Зб. наук. пр. Харківського університету Повітряних Сил. – 2006. – № 4. – С. 68-74.

9. Крылов В.В. Теория телетрафика и ее применение / В.В. Крылов, С.С. Самохвалова. – СПб.: БХВ-Петербург, 2005. – 288 с.

Надійшла до редколегії 3.11.2011

Рецензент: д-р техн. наук, проф. В.І. Гостєв, Державний університет інформаційно-комунікаційних технологій, Київ.

РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ КОМПЛЕКСНОЙ МЕТОДИКИ АДАПТИВНОГО КОНТРОЛЯ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНОЙ СЕТИ

О.Е. Мазулевский, Г.Я. Криховецкий, О.А. Колотило

В статье представлены результаты проведенного имитационного моделирования методик усовершенствования контроля защищенности компьютерной сети. Применение представленных методик позволяет повысить оперативность действий администратора безопасности во время проведения им мероприятий по контролю защищенности компьютерной сети и устранении выявленных уязвимостей.

Ключевые слова: *контроль компьютерной сети, адаптация, траффик, нагрузка сети, модель.*

THE RESULTS OF MODELING OF COMPLEX ADAPTIVE CONTROL TECHNIQUES COMPUTER NETWORK SECURITY

O.E. Mazulevsky, G.Y. Krikhovetsky, O.A. Kolotylo

We present the results of simulation modeling techniques to improve control of computer network security. The application presented techniques can improve the speed of action security administrator at the time of their control activities, protection of computer network and addressing the identified vulnerabilities.

Keywords: *control of computer network, adaptation, traffic, loading of network, model.*