МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
Військовий інститут телекомунікацій та інформатизації
Національного технічного університету України
„Київський політехнічний інститут”

ВОЄННО-НАУКОВО КОНФЕРЕНЦІЯ КУРСАНТІВ (СТУДЕНТІВ)

Факультету інформаційних технологій в системах управління
26 травня 2011 року

(Доповіді та тези доповідей)

Київ – 2011

ББК
Ц4 (4Укр)39
П-768

У збірнику матеріалів воєнно-наукової конференції курсантів (студентів) факультету інформаційних технологій у системах управління опубліковано доповіді та тези доповідей вчених, науково-педагогічних працівників, ад'юнктів, здобувачів, курсантів і студентів Військового інституту телекомунікацій та інформатизації Національного технічного університету України „Київський політехнічний інститут" та інших вищих навчальних закладів, в яких розглядаються пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення.

ЗМІСТ

1. ОРЖЕШКО Д.В. Вступне слово..... 5
2. ЛЮБАРСЬКИЙ С.В. Про роботу наукового гуртка кафедри №21. 6

(Тези доповідей пленарного засідання)

1. **Головко О.О., Хусаінов П.В.** Алгоритм кластеризації вузлів інформаційно-телекомунікаційної мережі..... 8
2. **Кураєв К.О., Сілко О.В.** Методи побудови комбінованих систем виявлення атак..... 9
3. **Судніков Є.О., Сілко О.В., Фесьоха В.В.** Алгоритм ідентифікації користувачів в інформаційній системі супроводу навчального процесу..... 10

(Тези доповідей секційного засідання)

1. **Бартош А.О., Соколов В.В.** Програмування засобами активних динамічних з'єднань..... 12
2. **Березань Ю.В., Нестеренко М.М** Механізми захисту від розподілених атак типу відмова в обслуговуванні на основі систем багатоагентного моделювання..... 13
3. **Горбенко В.І., Діденко О.В.** Процедура дослідження параметрів трафіку робочої станції інформаційної мережі 14
4. **Горбенко В.І., Дмитренко А.Ю.** Процедура визначення ймовірності відмови процесора через співвідношення температури та завантаженості..... 15
5. **Любарський С.В., Костина А.В.** Система оперативного аудиту інформаційної безпеки корпоративної мережі..... 16
6. **Хусаінов П.В., Крушеницький О.П.** Агрегація первинних даних про інфраструктуру інформаційно-телекомунікаційної мережі..... 18
7. **Мащенко О.В., Соколов В.В.** Графічне відображення об'єктів при моделюванні засобами активних динамічних з'єднань..... 19
8. **Сетяєв А.Г., Хусаінов П.В.** Алгоритм формування раціонального плану перевірки вузлів інформаційно-телекомунікаційної мережі..... 20
9. **Шаров М.В., Субач І.Ю.** Інтелектуальна система аналізу стану роботи інформаційної мережі 21
10. **Дурманенко Д.М., Любарський С.В.** Програмне забезпечення захисту інформаційних систем щодо умов ліцензійного використання..... 22

11. **Ткачик С.В., Макарчук О.М.** Класифікація комп'ютерних атак за допомогою нейронних мереж..... 24
12. **Островой М.М., Любарський С.В.** Програмне забезпечення пошуку оптимального рішення на основі генетичних алгоритмів. 25

ВСТУПНЕ СЛОВО

Шановні офіцери, працівники ЗСУ, курсанти та студенти. Сьогодні, відповідно до річного плану воєнно-наукової роботи курсантів (студентів) факультету, ми проводимо наукову конференцію воєнно-наукового товариства.

Конференція проводиться з метою підбиття підсумків наукової роботи курсантів (студентів) за навчальний рік, популяризації кращих робіт і широкого обміну думками стосовно них на факультеті.

Робота воєнно-наукового товариства на факультеті була організована і проводилася відповідно до вимог керівних документів:

Наказ Міністра оборони України № 9 від 13.01.2007 р.;

Наказ НІ № 94 від 11.08.2008 р. „Про організацію підготовки та проведення наукової та науково-технічної діяльності в інституті на 2007-2008 навчальний рік”;

Методичних вказівок про організацію роботи ВНТ курсантів і студентів;

Положення про воєнно-наукове товариство курсантів (студентів) (затверджене Вченою радою інституту. Протокол № 10 від 27.02.2008 р.).

Товариші, кожний із вас у свій час виявив бажання самостійно займатися науковою працею і технічною творчістю, добровільно вступивши до воєнно-наукового товариства ВНТ курсантів (студентів) інституту. На протязі року ви підвищували свою методологічну підготовку, розвивали наукове мислення, набували навичків дослідницької роботи, творчого підходу до вирішення задач бойового застосування з питань автоматизації процесів та інформатизації, а також вивчали основи організації і проведення наукових досліджень.

Пріоритетними напрямками наукової роботи та науково-технічної діяльності роботи факультету є:

– інформаційні технології функціонування комунікаційних систем в мережах;

– статистичне оцінювання процесів, що відбуваються у телекомунікаційних системах та їх застосування на практиці;

– методологія аналізу, синтезу та управління телекомунікаційними мережами;

– системи автоматизації електронного документообігу;

– інформаційні системи та бази даних;

– управління інформаційними мережами;

– захист інформації в інформаційних мережах;

– зменшення працезатрат на технічне обслуговування і ремонт військової техніки зв'язку та автоматизації;

– автоматизація процесів управління технічним забезпеченням зв'язку і АУВ на всіх рівнях підпорядкування;

– оптимізація номенклатури засобів вимірювальної техніки з урахуванням їх морального стану, фізичного старіння та можливостей поставок для забезпечення.

Бажаю вам успіхів під час виступів як на пленарному засіданні так і під час роботи наукових секцій та закликаю до плідної творчої праці.

підполковник Любарський С.В. (ВІТІ НТУУ „КПІ”)

ПРО РОБОТУ НАУКОВОГО ГУРТКА КАФЕДРИ №21

Наукова робота курсантів (студентів) є окремим видом наукової і науково-технічної діяльності, яка проводиться у вищих військових навчальних закладах та військових навчальних підрозділах вищих навчальних закладів під керівництвом науково-педагогічного складу (наукових співробітників).

Метою наукової роботи наукового гуртка кафедри № 21 є підвищення методологічної підготовки, розвиток наукового мислення, набуття навиків дослідницької роботи, творчого підходу до вирішення задач бойового застосування та експлуатації сучасних інформаційних технологій, спеціального програмного та апаратного забезпечення ПЕОМ, вивчення основ організації та проведення наукових досліджень у цьому напрямку.

Залучення курсантів (студентів) до наукової роботи дає також змогу використовувати їх творчий потенціал для вирішення актуальних завдань ВІТІ НТУУ „КПІ”.

Наукова робота нашого гуртка проводиться у тісному зв'язку з навчальним процесом, є його невід'мним продовженням та повинна відповідати завданням навчального процесу та основним напрямам науково-дослідної роботи кафедри.

Пріоритетними напрямками сумісної співпраці науково-педагогічних працівників та курсантів (студентів) є: впровадження та застосування сучасних інформаційних технологій в систему управління військами; методологія аналізу захищеності та забезпечення безпеки комп'ютеризованих систем, моделювання загроз їх безпеці; підтримка прийняття рішень у галузі захисту інформаційних систем; підвищення ефективності підготовки висококваліфікованих кадрів за рахунок оптимізації алгоритмів функціонування сучасних систем навчання; методологія оптимізації шляхів відпрацювання електронних документів; дослідження актуальних проблем і перспектив розвитку військової освіти; удосконалення підготовки та виховання військових фахівців. І у цих напрямках деякі з курсантів (студентів) нашого факультету досягнули певних успіхів. Так за кращу наукову працю серед курсантів та студентів ВІТІ НТУУ “КПІ” заохочені наступні члени наукового гуртка кафедри: курсант Головко О.О., курсант Сетяєв А.Г., курсант Судніков Є.О., студент Пашков В.О., курсант Волощук А.В.

Саме з метою підбиття підсумків наукової роботи курсантів (студентів) за навчальний період, популяризації кращих робіт і широкого обміну думками стосовно них проводиться сьогоднішня воєнно-наукова конференція курсантів(студентів) факультету інформаційних технологій в системах управління.

Бажаю усім присутнім успішного виступу і подальшої творчої наснаги у питаннях розбудови сучасних Збройних Сил України.

Тези доповідей пленарного засідання

к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ")
Головко О.О. (ВІТІ НТУУ „КПІ")

АЛГОРИТМ КЛАСТЕРИЗАЦІЇ ВУЗЛІВ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

В останні роки відмічається посилення зацікавленості, щодо практичних рішень на основі математичного апарату запропонованого сучасним напрямком дискретної математики відомого, як теорія складних мереж (*complex network*). Складні мережі – це реально існуючі в природі мережі (графи), що володіють нетривіальними та важливими топологічними властивостями.

Предмет теорії є науково-практичні задачі, вирішення яких базується визначенні топологічних утворень (групи, кластери та ін.) та динамічних процесів.

Наприклад:

– визначення клік (підгрупа або кластер, в якому вузли пов'язані між собою сильніше, ніж з членами інших клік) в мережі;

– виділення компонент (частин мережі), які пов'язані всередині і не пов'язані між собою;

– знаходження блоків і перемичок (вузол називається перемичкою, якщо при його вилученні мережа розпадається на незв'язані частини);

– виділення угруповань – груп еквівалентних вузлів (які мають максимально схожі профілі зв'язків);

Одним з напрямків застосування теорії складних мереж є дослідження топологічних властивостей (груп, кластерів, дерев та ін.) інформаційно-телекомунікаційної мережі (ІТМ) значної розмірності, де граф складної мережі є її ізоморфним відображенням. Найбільш придатним підходом для аналізу графу ІТМ без наявності апріорної інформації про можливі класифікаційні ознаки є методи кластеризації, особливо в контексті інформаційної боротьби в ІТМ.

У доповіді пропонується покращення алгоритму кластеризації вузлів ІТМ на основі адитивного показника , що дозволяє враховувати декілька параметрів вузлів ІТМ.

$$W=k_1 \bullet v_1+ k_2 \bullet v_2+ k_3 \bullet v_3+ \ldots +k_n \bullet v_n, ,$$

де k_n – коефіцієнти;

v_n – числове значення параметру який оцінюється, а також алгоритм для оцінки текстових параметрів які мають ієрархічну структуру, наприклад доменні імена.

Доменне ім'я – це унікальне алфавітно-цифрове ім'я, що ідентифікує конкретний вузол Інтернет. Доменні імена зазвичай складаються з двох і більше частин, що розділені крапками. Ліва частина доменного імені відповідає кінцевому вузлу мережі (ідентифікує кінцевий вузол мережі). Права частина є більш загальною (визначає країну, область, регіон і т. п.).

Наприклад, для визначення схожості доменних імен пропонується наступний алгоритм:

1. Доменні імена розбиваються на частини за рівнями ієрархії.
2. Кожному рівню привласнюється свій коефіцієнт (1 рівень – 0, 2 рівень – 1 і так далі).
3. Визначається доменне ім'я з максимальним рівнем ієрархії.
4. Якщо доменні імена першого рівня співпадають, то за адитивним показником визначаємо ступінь схожості, причому поточному значенню $v_n=1$, $F=(k_n \bullet v_n+ \ldots + k_2 \bullet v_2+ k_1 \bullet v_1)/(k_n+ \ldots +k_2+k_1)$.
5. Визначення ступеня схожості відбувається до тих пір поки не буде виявлене перше не позитивне співставлення.

Подальший розвиток дослідження планується проводити у напрямку програмної реалізації алгоритму, його тестування та оцінки ефективності.

Кураєв К.О. (ВІТІ НТУУ „КПІ”)
к.т.н. Сілко О.В. (ВІТІ НТУУ „КПІ”)

МЕТОДИ ПОБУДОВИ КОМБІНОВАНИХ СИСТЕМ ВИЯВЛЕННЯ АТАК

В даний час розробкам у галузі забезпечення інформаційної безпеки цифрових інформаційно-телекомунікаційних мереж приділяється підвищена увага. Для забезпечення оперативного контролю та прогнозування стану інформаційних ресурсів необхідне створення нових технологій виявлення ознак віддаленої атаки, що базуються на застосуванні активних і пасивних методів, датчиків стеження.

Існуючі сигнатурні системи виявлення вторгнень не можуть профілювання перехопленого потоку даних розподіленних атак для їх класифікації та відпрацювання сигналу про вторгнення.

Найбільш перспективним напрямком вирішення даної задачі є теорія розпізнавання образів.

Статистичні системи розпізнавання, як системи перевірки складних гіпотез проти складних альтернатив, складаються з модульних логічних елементів, так званих твірних. Будь-яка твірна володіє невіддільними від неї зв’язками, які можуть бути орієнтованими (вхід→вихід) або неорієнтованими.

Системи розпізнавання будуються із зв’язків двох або більшого числа твірних. Кожний зв’язок системи розпізнавання, в залежності від даних, привласнених парі її зв’язків, може знаходитися в одному з двох станів – істинному або хибному. Шляхом замикання або розмикання зв’язок в системі розпізнавання, складеної з орієнтованих твірних, моделюють з’єднання і роз’єднання виходів та входів модулів, з яких складається реальна система.

Логічні і фізичні модулі з входами і виходами можна уявити векторами орієнтованих твірних:

$$a(gi) = a(i, \gamma_{il}, \beta_{im}^{il}, \beta_{ir}^{out}) \qquad (1)$$

У теорії розпізнавання образів показники зв’язки β і атрибути γ вектора (1) трактуються як змінні, що мають відповідні області значень.

Твірними, які визначаються вектором (1), представляють структури реальних модулів в узагальненій формі.

Враховуючи вище викладене, можна зробити висновок, що для винесення припущення про мету та наслідки атаки на ІТМ необхідна розробка системи виявлення вторгнень, профілюючої комбінації сигнатур і мережевих аномалій на підставі заданих ознак. Інструментом для ефективного групування і обробки може стати методика упорядкування даних, які не можуть бути класифіковані за безпосереднім ознаками.

Судніков Є.О. (ВІТІ НТУУ „КПІ”)
к.т.н. Сілко О.В. (ВІТІ НТУУ „КПІ”)
Фесьоха В.В. (ВІТІ НТУУ „КПІ”)

АЛГОРИТМ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ СУПРОВОДУ НАВЧАЛЬНОГО ПРОЦЕСУ

Актуальним вирішенням проблеми захисту від руйнівних інформаційних впливів в інформаційних системах супроводу навчального процесу (ІС СНП) є застосування програмно-апаратного комплексу ідентифікації користувачів з елементами несиметричного шифрування. Такий підхід має підвищити ефективність функціонування підсистеми ідентифікації користувачів та провести удосконалення існуючої системи захисту ІС СНП, оскільки загальновизнано, що проблема встановлення автентичності та авторства без паперової документації вирішується за допомогою криптографічних систем з відкритим ключем в комплексі з криптографічними алгоритмами. Для запобігання порушень пов'язаних з аунтифікаційними даними, які реалізується за допомогою механізму ідентифікації, який дозволяє переконатися в тому, що тільки повноважні користувачі отримують доступ до необхідних їм ресурсів ІС СНП, в той час як неправомірним користувачам доступ заборонений. Рішення задачі з ідентифікації зазвичай включають в себе аутентифікацію, авторизацію та облік, серед іншого, вони визначають правильну ідентифікацію мережних користувачів, вузлів, служб і ресурсів.

Алгоритм ідентифікації користувачів в інформаційній системі супроводу навчального процесу передбачає виконання наступних етапів:

1. Перевірка підключення та відповідності *USB*-приладу (отримання серійного номеру *USB*-пристрою, що є унікальним параметром, на основі якого видається коректна відповідь на запит системи про аутентифікацію):

нехай $F = \{F_1,...,F_b,...,F_u\}$, $b = \overline{1,u}$ – множина варіантів реалізації мережевої розвідки віддаленого вузла ІС СНП. Припустимо, що проведення мережевої розвідки віддаленого вузла є відображенням вигляду:

$$F = f(S,W,G),$$

де $S = \{S_1,...,S_i,...,S_n\}$, $i = \overline{1,n}$ – множина варіантів впровадження в об'єкт інформаційного аналізу;

$W = \{W_1,...,W_j,...,W_r\}$, $j = \overline{1,r}$ – множина варіантів встановлення з'єднання з віддаленим вузлом.

$G = \{G_1,...,G_k,...,G_m\}$, $k = \overline{1,m}$ – множина варіантів реалізації управління віддаленим вузлом.

2. Якщо прилади відсутні або не відповідають дійсності, то алгоритм зупиняє виконання та чекає або закриття, або підключення приладу, який відповідає базі.

3. При позитивному результаті перевірки алгоритм виконує код розшифровування модуля аутентифікації та авторизації користувача. Після цього здійснюється перехід на цей модуль.

Проведений аналіз щодо забезпечення безпеки ІС СНП при їх впровадженні в навчальний процес доводить необхідність застосування додаткового програмного забезпечення для реалізації підсистеми ідентифікації користувачів. Застосування запропонованого алгоритму дозволить підвищити рівень захисту та взаємодіяти з кожним користувачем особисто, що дозволить виявляти та не допускати порушників та здійснювати руйнівний вплив на інформаційну систему супроводу навчального процесу.

Тези доповідей секційного засідання

Бартош А.О. (ВІТІ НТУУ „КПІ”)
к.т.н. Соколов В.В. (ВІТІ НТУУ „КПІ”)

ПРОГРАМУВАННЯ ЗАСОБАМИ АКТИВНИХ ДИНАМІЧНИХ З'ЄДНАНЬ

Для реалізації графічного середовища розробки програмного забезпечення засобами активних динамічних з'єднань прикладом є існуюча система *UML* (англ. *Unified Modeling Language* – уніфікована мова моделювання) – мова графічного опису для об'єктного моделювання в області розробки програмного забезпечення. *UML* є мовою широкого профілю, це відкритий стандарт, який використовує графічні позначення для створення абстрактної моделі системи, званої *UML*-моделю. *UML* був створений для визначення, візуалізації, проектування та документування в основному програмних систем. *UML* не є мовою програмування, але в засобах виконання *UML*-моделей як інтерпретується коду можлива кодогенерація (синтез).

Будемо розглядати об'єкт так:

– вхід – набір властивостей, доступних для зміни ззовні об'єкта, значення яких використаються для обчислення похідних значень (виходу);

– вихід – набір властивостей, доступних тільки для читання ззовні об'єкта, значення яких обчислюються і є похідними від значень входу;

– ядро – головний метод, що реалізує перетворення даних входу в дані виходу.

Рис 1.1. Схема об'єкта.

Коротко концепцію технології активних динамічних з'єднань можна викласти у вигляді наступної системи поглядів на об'єкт:

– об'єкт – це не змінна структурного типу даних, а програмний модуль;

– властивості об'єкта – це локальне статичне середовище модуля, його дані, що зберігають свої значення;

– властивості об'єкта можна розділити на вихідні дані (вхід), вихідні результати (вихід) і проміжні значення;

– методи об'єкта – це операції над даними об'єкта;

– об'єкт може одержувати керування (активуватися) для обробки вихідних даних й одержання результатів шляхом застосування операцій, заданих у вигляді методів, до вихідних даних у певній послідовності (алгоритм ядра);

– об'єкт повинен контролювати відповідність поточних вихідних результатів поточним вихідним даним;

– процес від початку зміни вихідних даних до закінчення обчислення всіх вихідних результатів об'єкта може виконуватися транзакційно, з поверненням змін або без повернення;

– об'єкт може пасивно взаємодіяти з іншими об'єктами будь-яких класів шляхом читання значень їхніх властивостей;

– об'єкт може активно взаємодіяти з іншими об'єктами будь-яких класів шляхом передачі їм керування (активації).

Отже, таким чином необхідно визначити зовнішній вигляд об'єкта, тому що результатом роботи повинно бути графічне середовище розробки програмного забезпечення.

к.т.н. Нестеренко М.М (ВІТІ НТУУ «КПІ»)
Березань Ю.В. (ВІТІ НТУУ «КПІ»)

МЕХАНІЗМИ ЗАХИСТУ ВІД РОЗПОДІЛЕНИХ АТАК ТИПУ ВІДМОВА В ОБСЛУГОВУВАННІ НА ОСНОВІ СИСТЕМ БАГАТОАГЕНТНОГО МОДЕЛЮВАННЯ

Однією з важливих особливостей комп'ютеризованих систем є можливість здійснення блокування інформаційних (програмно-апаратних) ресурсів за допомогою атак типу „відмова в обслуговуванні". У зв'язку з цим актуальним питанням захисту комп'ютеризованих інформаційно-телекомунікаційних мереж є науково–практичні дослідження принципів побудови механізмів захисту від даного типу атак.

Згідно офіційної інформації є всі підстави зтверджувати, що такі атаки на більш менш великі інформаційні ресурси проводяться як мінімум щодня. Ціль атакуючих – зробити недоступним для користувачів той чи інший ресурс корпоративної мережі. Найчастіше це просто блокування доступу, іноді виведення цього ресурсу з ладу (найбільш відомий наслідок дії *DoS*-атаки – синій екран). Іноді *DoS*-атака може бути частиною іншої, більше широкомасштабної та складної акції, що спрямована на злом ресурсу, викрадення конфіденційних даних або знищення важливої інформації.

Метою дослідження є підвищення ефективності аналізу механізмів захисту від розподілених атак типу „відмова в обслуговуванні" на основі системи багатоагентного моделювання.

На практиці досить проблематично здійснити перевірку й оцінку застосування того або іншого механізму захисту. Дослідження на основі реальних мереж важко реалізовано практично внаслідок того, що необхідно або мати у своєму розпорядженні більший виділений фрагмент мережі, де можна проводити експерименти, або використати для експериментів реальні мережі Інтернет-провайдерів але, атаки *DoS* створюють більше навантаження на мережу, навіть до повної відмови в обслуговуванні, що приводить до виходу експерименту з під контролю, і навіть поширенню атак в Інтернет. Через критичність даного класу атак, складності проведення досліджень на реальних мережах, моделювання *DoS*-атак та механізмів захисту від них є дійсно актуальним завданням.

Одним із сучасних способів протидії *DoS*-атакам є імітація зменшення продуктивності роботи сервера шляхом обмеження обробки однотипних запитів та маніпулювання вхідними підключеннями атакуючих таким чином, щоб підвищити навантаження на сам атакуючий вузол.

Винесений на огляд новий спосіб захисту передбачає, що за допомогою нього надається можливість ввести в оману машини ботнета, змушуючи їх вважати, що атака здійснюється на сервер, який, підключений до Інтернету через занадто повільний канал.

Пропонуються маніпулювати вхідними підключеннями атакуючих таким чином, щоб підвищити завантажити сам ботнет. Навмисно ігноруючи частину однотипних запитів, сервер переконує атакуючі комп'ютери в тому, що він не встигає їх обробляти – через цього атакуючі комп'ютери знову й знову намагаються встановити з'єднання. Підсумкова затримка становить приблизно 5 хвилин [1] – протягом цього часу кожний вузол ботнета працює не завантажуючи сервер, що серйозно знижує загальну продуктивність ботнета. У якийсь момент атакуючі комп'ютери будуть змушені здатися.

Особливої уваги заслуговує прийом, що використовується для розпізнавання легітивних запитів до сервера від нескомпроментованих комп'ютерів, за допомогою моделі запит-відповідь на базі сценарію *Javascript* або *Flash*-контента.

к.т.н., доцент Горбенко В.І. (ВІТІ НТУУ «КПІ»)
Діденко О.В. (ВІТІ НТУУ «КПІ»)

ПРОЦЕДУРА ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ТРАФІКУ РОБОЧОЇ СТАНЦІЇ ІНФОРМАЦІЙНОЇ МЕРЕЖІ

На теперішній час інформаційні технології стали невід'ємною частиною життєдіяльності Збройних сил України.

Для підвищення ефективності роботи персональних комп'ютерів їх об'єднують у інформаційні мережі. Поряд із розвитком глобальних мереж зростає необхідність у захисті конфіденційних даних, які зберігаються на носіях, до яких мають доступ мереж різних видів. Тому дослідження параметрів роботи мережі являється невід'ємною частиною заходів по підтримці роботи мережі. Трафік однієї робочої станції складається з: трафіку протоколів TCP, UDP, ICMP, HTTP, FTP та інших.

Моніторинг мережі – це робота системи, яка виконує постійне (збір, аналіз та збереження параметрів трафіку робочої станції) спостереження за інформаційною мережею в пошуках повільних або несправних компонентів і яка при виявленні збоїв повідомляє про них адміністратора за допомогою пошти, пейджера чи інших засобів оповіщення [1]. Ці задачі є підмножиною завдань управління мережею [2].

Під час моніторингу трафіку робочої станції необхідно: збирати інформацію, щодо вхідного та вихідного трафіку і систематизувати її, проводити аналіз отриманих результатів.

Виходячи з цього в доповіді пропонується розглянути методику дослідження параметрів трафіку робочої станції інформаційної мережі за допомогою процедури аналізу завантаженості станції, що дозволить виявити з певною долею ймовірності шкідливий трафік і в подальшому попереджати про активне підвищення трафіку користувача та адміністратора мережі. Наводяться вхідні дані та алгоритм методики і приклад її застосування.

Висновки:

– по-перше, в результаті аналізу вхідного трафіку, щодо протоколів TCP, UDP, ICMP можливо отримати середні статистичні дані щодо активності мережі на робочій станції;

– по-друге, при обробці отриманих даних можливо відслідковувати аномальне підвищення мережевої активності;

– по-третє, системний адміністратор отримає більш широкі можливості, щодо виявлення та запобігання програмних атак через мережеву карту на робочу станцію.

ЛІТЕРАТУРА:

1. Дженнинингс Практическая передача данных: модемы, сети и протоколы/ Пер. с англ. М.: Мир, 1989.

2. Крейг Персональные компьютеры в сетях TCP/IP: Пер. с англ. - К.: Издательская группа BHV, 1997.

к.т.н, доцент Горбенко В.І. (ВІТІ НТУУ "КПІ")
Дмитренко А.Ю. (ВІТІ НТУУ "КПІ")

ПРОЦЕДУРА ВИЗНАЧЕННЯ ЙМОВІРНОСТІ ВІДМОВИ ПРОЦЕСОРА ЧЕРЕЗ СПІВВІДНОШЕННЯ ТЕМПЕРАТУРИ ТА ЗАВАНТАЖЕНОСТІ

Останнім часом гонка за продуктивністю настільних комп'ютерів піднялася на новий рівень. Зростання тактової частоти та обчислювальної потужності, перехід на багатоядерну платформу і впровадження архітектури *IA*64 забезпечує підняття продуктивності обчислювальних засобів мережі. Але при збільшенні тактової частоти, відповідно, збільшується тепловиділення електронних компонентів. Так як у електронних схемах працездатність забезпечується при визначеному діапазоні температур, то існує проблема тепловиділення, що не може зростати нескінченно. Вирішення цієї проблеми можливе декількома шляхами: по-перше, впровадженням нових процесорних архітектур і технологічних процесів, які дозволяють знизити тепловиділення, включно до появи старших процесорів сімейства. По друге удосконаленням системи охолодження процесорів. Саме цим шляхом зараз прямує більшість виробників процесорів. За останні кілька років еволюція систем охолодження пройшла шлях від радіаторів, якими задовольнялися процесори *Intel* 80486 до сучасних систем охолодження на основі теплових трубок. [1]

Нормальна працездатність при високих температурах малоймовірна, оскільки в глибинах процесора мають місце не тільки електричні явища, але і величезна кількість електрохімічних процесів і реакцій, які є за своєю суттю термоактиваційними (їх швидкість виключно залежить від температури). З плином часу вони принципово можуть не тільки ускладнити коректне функціонування процесора, але і навіть призвести до його повної відмови, хоча робочі температури при цьому можуть перебувати в цілком безпечних межах, якщо дивитися з чисто електричної точки зору. [2]

На даному етапі розвитку інформаційних мереж Збройних Сил України актуальною є розробка підсистеми для збору показників датчиків температури та завантаженості процесора, а також підсистеми аналізу та прогнозування подальшої роботи процесора і ймовірності виходу його з ладу. Обчислити ймовірність виходу з ладу процесора дуже складно оскільки вона залежить від великої кількості факторів і потребує суттєвих часових витрат. Тому у доповіді пропонується процедура визначення ймовірності відмови процесора опосередковано через співвідношення температури та завантаженості комп'ютера. Алгоритм роботи підсистеми полягає в тому, що проводиться в заданому інтервалі часу збір випадкових величин показників температури та завантаженості центрального процесора. Після чого здійснюється математичний аналіз даних випадкових величин і отримується ймовірність. Дана підсистема полегшує вирішення проблем ремонту ЕОМ. Наприклад, якщо в період деякого відрізку часу показники завантаженості процесора будуть незмінні, а температура весь час піднімається, то користувач отримує повідомлення про необхідність обслуговування (замані) системи охолодження центрального комп'ютера. [3]

Таким чином:

- по-перше, на даному етапі розвитку інформаційних мереж ЗС України актуальною є розробка підсистеми за допомогою якої буде можливо проаналізувати роботу процесора та прогнозування ймовірності виходу його з ладу;
- по-друге, підсистема аналізу працездатності процесора полегшить вирішення проблем під час ремонту комп'ютера, та прийнятті рішення про їх заміну.

п/п-к Любарський С.В. (ВІТІ НТУУ „КПІ”)
Костина А.В. (ВІТІ НТУУ „КПІ”)

СИСТЕМА ОПЕРАТИВНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ

На сьогоднішній день корпоративні комп'ютерні мережі вже набули широкого поширення в організації роботи організацій та установ будь-якого рівня. В межах даних організацій та установ (у тому числі і спеціального призначення) циркулює велика кількість інформації, що потребу захисту від фальсифікації, викрадення, підміни, всеприлюдного розголошення і т.д. Тому постає важлива проблема, яким же чином забезпечити цю саму цілісність та безпеку інформаційних ресурсів корпорації?

Забезпечення безпеки корпоративних мереж включає організацію протидії будь-якому несанкціонованому вторгненню в процес функціонування, а також спробам модифікації, розкраданню, виводу з ладу або руйнуванню її компонентів, тобто захист всіх компонентів інформаційно-комунікаційних систем та мереж – апаратних засобів, програмного забезпечення, даних та персоналу, тощо.

Предметом дослідження є методи організації оперативного аудиту інформаційної безпеки, що дозволяють оцінити рівень захищеності інформаційної корпоративної мережі.

Завдання проектування (розробки, вдосконалення) системи захисту інформації та її елементів виникає тоді, коли створюється нова організація із закритою (таємною, конфіденційною) інформацією або існуюча система не забезпечує необхідний рівень безпеки інформації.

Проектування системи захисту, що забезпечує досягнення поставлених перед інженерно-технічним захистом інформації і вирішення завдань, проводиться шляхом системного аналізу існуючої та розробки варіантів необхідної.

Побудова нової системи або її модернізація передбачає:

– визначення джерел інформації, що захищається і опис факторів, що впливають на її безпеку;

– виявлення і моделювання загроз безпеці інформації;

– визначення слабких місць існуючої системи захисту інформації;

– вибір раціональних заходів запобігання загроз;

– порівняння варіантів за приватними показниками і загальному критерію, вибір одного або декількох раціональних варіантів;

– обґрунтування обраних варіантів у доповідній записці або в проекті для керівництва організації;

– доопрацювання варіантів або проекту з урахуванням зауважень керівництва.

Так як відсутні формальні способи синтезу системи захисту, то її оптимізація підчас проектування можлива шляхом поступового наближення до раціонального варіанту. А тому для реального і ефективного вирішення питань безпеки корпоративної мережі, потрібно здійснювати аналіз записів аудиту, що є найбільш ефективнішим у представленні моделі Д. Деннінга.

В якості моделі середнього і стандартного відхилень використовуються наступні співвідношення:

$$S = x_1 + x_2 + \cdots + x_n;$$

$$S^2 = x_1^2 + x_2^2 + \cdots + x_n^2;$$

$$m = \frac{s}{n};$$

$$d = sqrt\left(\frac{s^2}{n} - m^2\right).$$

Нове значення вважається аномальним, якщо воно виходить з інтервалу $m + dk$. З нерівності Чебишева випливає, що ймовірність того, що значення потрапить поза інтервалу, не перевищує $1/k^2$. Наприклад, для $k = 4$, $p = 0{,}0625$.

Модель використовує форми шаблонів (зразків), подібних використовуваним в мові *SNOBOL*: *«String»*–рядок знаків;

* – будь-який рядок;

\# – числовий рядок;

IN (list) – будь-який рядок у списку;

P→name – рядок, що містить *p*, асоціюється з name;

$p_1 \vee p_2$ – p_1 або p_2;

$p_1 \wedge p_2$ – p_1 і p_2;

$Notp$ – не *p*.

Аудит дозволяє всебічно дослідити інформаційну систему організації, оцінити поточний рівень інформаційної безпеки, виявити вразливі місця в системі захисту, створити моделі можливих загроз інформаційні системи, перевірити правильність підбору і настройки засобів захисту.

У процесі проведення аудиту виявляються технологічні потоки як електронної, так і паперової інформації, топологія мережі, незахищені або неправильні мережеві з'єднання, проводиться аналіз налаштувань між-мережевих екранів і інших засобів захисту. Результатом проведення аудиту є ряд організаційних документів, які в подальшому можуть стати основою для побудови надійної та ефективної системи захисту.

Результати аудиту дозволяють побудувати оптимальну за ефективністю і витратам систему захисту корпоративної інформації, адекватну поточним завданням і цілям бізнесу.

к.т.н. Хусаінов П.В. (ВІТІ НТУУ "КПІ")
Крушеницький О.П. (ВІТІ НТУУ "КПІ")

АГРЕГАЦІЯ ПЕРВИННИХ ДАНИХ ПРО ІНФРАСТРУКТУРУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Агрегація первинних даних про об'єкти інфраструктури інформаційно-телекомунікаційної мережі є важливим питанням аналізу мережевих ресурсів загалом, та подальшого їх використання. оскільки, в ході досліджень ми можемо отримати інформацію про працездатність будь-якого вузла мережі а також, використовуючи різні параметри сканування, додаткову інформацію що можливо використати в свої цілях.

Інформаційно-телекомунікаційна мережа включає в себе сукупність програмного та апаратного забезпечення, за допомогою якого ми можемо зв'язати та передати (отримати) усю необхідну інформацію між вузлами мережі. Для отримання первинних даних про об'єкти мережі використовують різного типу мережеві сканери, сніфери та мережеві екрани. В загальному випадку всі вони збирають мінімально доступну, або визначену за певними критеріями, інформацію про об'єкти мережі. Ця інформація знаходиться в так званих пакетах даних, що надсилаються в мережу, які деяка програма перехоплює, і робить записи про їх проходження. Після створення запису, вона пересилає пакет далі в мережу, при цьому залишаючись непоміченою. Основна інформація що перехоплюють ці програми повинна містити: ім'я хоста (або його *IP*-адреса), який пересилає інформацію; номер порту, з якого здійснюється передача інформації; ім'я хоста (або його *IP*-адреса), який отримує інформацію; номер порту, в який надсилається інформація; кількість байт інформації що передана; кількість байт інформації що була прийнята. Використовуючи цю інформацію ми можемо проаналізувати та зробити висновок що до зв'язності вузлів мережі між собою та способи передачі інформації між ними, визначити вразливі місця кожного з доступних вузлів та способи впливу на об'єкти мережі.

В результаті отриманих даних про об'єкти мережі, виникає питання про приведення даних до однакової форми, усунення зайвих даних, впорядкування даних за заданою ознакою, з метою зручності використання та подальшого прийняття рішення. Тому в цьому випадку має місце поняття агрегації даних, що являє собою обчислення узагальнених показників для підтримки стратегічного або тактичного керування за допомогою детальних даних. Наприклад, вся інформація що надходить від різних мережевих сканерів до одного масиву даних. Усі записи що ми отримуємо від мережевих сканерів та сніферів мають різні параметри пошуку,тому виникає потреба агрегації первинних даних та усунення зайвої інформацій.

Основними показниками, за якими буде проводитися агрегування інформації, будемо вважати час надходження пакету, розмір пакету та інтенсивність надходження пакетів до певного вузла мережі. Таким чином, використовуючи ці параметри формується масив даних, в якому виникає необхідність оновлення та усунення найменш важливої для нас інформації.

Початковий алгоритм буде формуватися на основі родового типу даних з динамічно змінюючим об'ємом виділеної пам'яті. Це дозволить більш раціонально використовувати доступну пам'яті, а використовуючи процедуру оперативного формування агрегатів, ми зможемо зменшити час на обробку нової інформації та оновлення застарілої.

Слід зазначити що дослідження вже існуючих методів агрегації дає нам змогу зробити висновки що до переваг та недоліків кожного з них і на основі цього використати певні властивості для досягнення оптимальних витрат часу та ресурсів пам'яті, підвищити швидкодію роботи програми та точність побудови мережевої моделі.

к.т.н. Соколов В.В. (ВІТІ НТУУ "КПІ")
Машенко О.В. (ВІТІ НТУУ "КПІ")

ГРАФІЧНЕ ВІДОБРАЖЕННЯ ОБ'ЄКТІВ ПРИ МОДЕЛЮВАННІ ЗАСОБАМИ АКТИВНИХ ДИНАМІЧНИХ З'ЄДНАНЬ

За мірою повноти опису моделі поділяють на повні, неповні та наближені. Повні моделі адекватні об'єкту у просторі та часі. Для неповного моделювання ця адекватність не зберігається. При наближеному моделюванні беруться до уваги тільки найважливіші аспекти системи. Залежно від характеру досліджуваних процесів у системі моделі поділяють на детерміновані та стохастичні, статичні та динамічні, неперервні та дискретно-неперервні. Детерміновані моделі відображають процеси, для яких передбачається відсутність випадкових впливів, а у стохастичних враховуються випадкові процеси та події. Статичне моделювання застосовується для описування стану системи у фіксований момент, а динамічне - для дослідження поведінки системи у часі. Дискретне, неперервне та дискретно-неперервне моделювання застосовуються для опису процесів, які змінюються у часі.

При реальному моделюванні використовують можливість дослідження характеристик на реальному об'єкті чи на його частині. При натурному моделюванні проводять дослідження на реальному об'єкті із подальшим обробленням результатів експерименту на основі теорії подібності. Фізичне моделювання здійснюється через відтворення досліджуваного процесу на моделі, яка в загальному випадку має відмінну від оригіналу природу, але однаковий математичний опис процесу функціонування. Абстрактне моделювання має різноманітні види: наочне, символьне, математичне. При наочному моделюванні на базі уявлень людини про реальні об'єкти створюють наочні моделі, що відображають явища та процеси, які відбуваються в об'єкті. Символьне моделювання являє собою штучний процес створення об'єкта, який замінює реальний та виражає основні його властивості через певну систему знаків та символів.

Графічна модель фіксує існуючий рівень пізнання про досліджуваний об'єкт. Неможливо створити універсальну модель, котра могла б відповісти на всі запитання, що викликають інтерес; кожна з них дає лише наближений опис явища, причому в різних моделях знаходять відображення різні його властивості. До моделювання звертаються тоді, коли досліджувати реальний об'єкт з усією сукупністю його властивостей недоцільно, незручно або неможливо. Графічні моделі дають зовнішнє представлення натури і переважно служать для демонстраційних цілей: показують форму, принцип дії, взаємне розташування частин, процес збірки і оброблення інформації, компоновку об'єкту. Графічні моделі широко застосовують в навчанні військовослужбовців проведення бою, та підготовки до нього.

Наприклад властивості об'єктів будуть містити в собі такі характеристики:

- місце знаходження (координати);
- тактико технічні характеристики бойової одиниці техніки (танки, літаки, ЗРК, та ін.);
- дальність стрільби;
- рухомий об'єкт чи ні.

Сетяєв А.Г. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

АЛГОРИТМ ФОРМУВАННЯ РАЦІОНАЛЬНОГО ПЛАНУ ПЕРЕВІРКИ ВУЗЛІВ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Практична діяльність щодо перевірки працездатності вузлів інформаційно-телекомунікаційної мережі (ІТМ) часто здійснюється в умовах невідповідності часових обмежень значній кількості вузлів, які підлягають перевірці. Одним з підходів до зменшення негативного впливу часових обмежень є формування раціонального плану перевірки на основі показників важливості та витрат часу для перевірки кожного вузла ІТМ. Враховуючи заздалегідь відомі значення цих показників необхідно знайти найкращий раціональний варіант послідовної перевірки працездатності вузлів ІТМ при якому не буде перевищення допустимого часу. Загальне розв’язання даної задачі полягає в скороченні плану перевірки, але обґрунтувань, з використанням певних припущень щодо втрат якості перевірки.

Під якістю перевірки будемо розуміти сумарну важливість всіх вузлів ІТМ, які підлягають перевірці. Якщо внаслідок часових обмежень необхідно скоротити план фактично перевіряємих вузлів ІТМ, то якість перевірки буде зменшена на величину важливості вузлів ІТМ, які не потрапили до плану перевірки.

Формування раціонального плану перевірки вузлів ІТМ полягає у виконанні багатоітераційного алгоритму для роботи якого вважаються заданими наступні вхідні дані:

– допустимий час, що може бути витрачений для перевірки;
– градації значень допустимої важливості для розбиття вузлів ІТМ на підмножини;
– вектор часових витрат на перевірку вузлів ІТМ;
– вектор важливості вузлів ІТМ, які підлягають перевірці.

Результат роботи алгоритму оформлюється у вигляді цілочисельного вектору, який відображає порядок перевірки вузлів ІТМ, де найбільш приорітетним елементом буде елемент з максимальним значенням у векторі перевірки.

Алгоритм передбачає виконання наступних кроків:

1. Вибрати елемент з підмножини градації важливості вузлів з найбільшим значенням, значення у векторі плану перевірки якого рівне 0 та перейти до кроку 2.
2. Вибрати значення відповідного вузла з вектору часових показників, перейти до наступного кроку.
3. Перевірити умову часового обмеження шляхом додавання до попереднього значення суми часових значень, значення даного вузла. Перейти до кроку 4, при невиконанні умови перейти до кроку 5.
4. Поставити відмітку „+1” до значення у векторі плану перевірки в позиції вузла та до всіх ненульових додатних значень вектору та перейти до кроку 1.
5. Поставити відмітку „-1” до значення у векторі плану перевірки в позиції елемента до всіх від’ємних значень вектору та повернутися до кроку 1.
6. При невиконанні умови обмеження часу вузлами однієї градації, необхідно перейти до наступної градації та повторити кроки, починаючи з першого.
7. За умови, що всі елементи було перевірено, необхідно виконати завершення алгоритму.

Подальший розвиток дослідження планується проводити у напрямку програмної реалізації алгоритму, його тестування та оцінки ефективності.

Шаров М.В. (ВІТІ НТУУ „КПІ”)
д.т.н., доцент Субач І.Ю. (ВІТІ НТУУ „КПІ”)

ІНТЕЛЕКТУАЛЬНА СИСТЕМА АНАЛІЗУ СТАНУ РОБОТИ ІНФОРМАЦІЙНОЇ МЕРЕЖІ

В наш час на ринку інформаційних послуг спостерігається стрімке розширення спектру послуг пов’язаних з інтеграцією та розгортанням телекомунікаційних мереж різноманітного призначення. Це пов’язане з розвитком інформаційних технологій (в загальному плані: користувач має сучасне обладнання і бажає отримати й відповідну віддачу, тому і продовжується розвиток цієї ланки ринку інформаційних послуг). Перед адміністратором постають закономірні питання:

- Чи готовий він до обслуговування подібних систем?
- Чи можливо забезпечити їх функціональність та працездатність?
- Чи можливо забезпечити безпеку інформаційних систем?

Саме тому для забезпечення високої якості обслуговування користувачів під час впровадження сучасних інформаційних технологій і забезпечення високотехнологічних інформаційних послуг потрібна система управління та моніторингу інформаційної мережі, у складі якої має функціонувати інтелектуальна підсистема підтримки рішення, що покликана автоматизувати роботу адміністратора даної мережі. Зазначена система має надавати адміністратору можливість проведення моніторингу і швидкої реконфігурації мережі, своєчасно знаходити і усувати несправності, забезпечувати розвиток мережі та оперативне підключення абонентів до нових інформаційних послуг.

Розробка і впровадження засобів організаційно-технічного забезпечення діяльності адміністратора є одним з важливих питань роботи інформаційної системи структурного підрозділу Збройних Сил України. На адміністратора покладається відповідальність за усунення невизначеності та прийняття рішень щодо оцінки негативного впливу на поточний стан інформаційної системи.

Для ефективної діяльності адміністратора інформації потрібна безперервна робота системи моніторингу, а також всебічний контроль системи, яку потрібно захистити з боку адміністратора. У зв’язку з цим накопичується дуже великий обсяг інформації про діяльність самої системи та її користувачів, який в майбутньому і в найкоротший термін потрібно обробити. З досвіду можна сказати, що об’єм інформації, який потрібно обробити адміністратору, значно перевищує оптимальний об’єм, який адміністратор в змозі обробити. З цього випливає, що час реакції адміністратора системи на певну проблему в мережі не дає змогу ефективно реагувати на події, що відбуваються в мережі. Тобто потрібно автоматизувати рутинні операції обробки великої кількості подій щодо реагування на певні нестандартні події.

Одним із способів вирішення даної задачі є використання системи підтримки прийняття рішень в інформаційній мережі моніторингу даних. Використання інтелектуальних технологій дасть змогу фахівцям інформаційних технологій аналізувати процеси функціонування комп’ютерних систем, виявляти приховані семантичні залежності у даних, отримувати моделі, що дозволяють оцінювати та прогнозувати виникнення можливих проблем з метою їх запобігання і, таким чином, підвищити рівень працездатності комп’ютерної системи в цілому.

Дурманенко Д.М. (ВІТІ НТУУ „КПІ”)
к.т.н. Любарський С.В. (ВІТІ НТУУ „КПІ”)

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ЩОДО УМОВ ЛІЦЕНЗІЙНОГО ВИКОРИСТАННЯ

Аналіз існуючих методів захисту інформаційних систем щодо умов ліцензійного використання показав низький рівень захищеності в першу чергу це пов’язано з економічним фактором. Програмний продукт є товаром, який має автора, ціну, гарантії якості. Цей товар можна купити, продати, обміняти тощо і як будь-який товар, він може бути об’єктом крадіжки та незаконного використання. Підробкою програмного забезпечення займаються багато людей, тому що це дуже вигідний бізнес.

Експерти підрахували, що 75% від усіх порушень авторських прав у галузі програмного забезпечення складає нелегальне копіювання програм.

Найбільш поширеними формами незаконного копіювання програм є

– установка на жорсткий диск комп’ютера неліцензійної копії програми;

– копіювання програм на комп’ютери у кількості, що перевищує умови ліцензійних угод.

Існує два види захисту прав виробників програмних продуктів – юридична та технічна. Нас цікавить саме технічний захист програмного забезпечення. Технічний захист спрямована на те, щоб технічними засобами утруднити чи зробити неможливим використання програмного продукту незаконним користувачем.

Технічними засобами захисту програмних продуктів можна реалізувати кілька підходів до даної проблеми:

1) протидіяти копіювання програми на інший диск;

2) дозволивши власне копіювання програми, протидіяти спробам запуску і/або виконання незаконної копії;

3) не протидіяти ні копіювання, ні виконання програми, але, супроводжує її прихованою інформацією про управління правами, у разі потреби мати достовірну доказ, що підтверджує авторство і незаконне використання.

У відповідності з різними підходами до захисту прав творців комп’ютерних програм, захист програмного забезпечення можна класифікувати таким чином:

– захист від власне незаконного копіювання;

– захист від незаконного використання;

– захист від дослідження програм;

– ідентифікація програмних продуктів.

Основними документами в області оцінки безпеки інформаційних систем є: „Критерії оцінки надійних комп’ютерних систем” (*Trusted Computer Systems Evaluation Criteria, TCSEC*) США; „Критерії оцінки безпеки інформаційних технологій” (*Information Technology Security Evaluation Criteria, ITSEC*) Франції, Німеччини, Голландії та Великобританії, і, нарешті, „Загальні критерії оцінки безпеки інформаційних технологій”, що є міжнародним стандартом.

Для захисту програмного забезпечення використовується ряд методів:

1. Алгоритми заплутування.
2. Алгоритми мутації.
3. Алгоритми компресії даних.
4. Алгоритми шифрування даних.
5. Гамільтоновий цикл в графі.
6. Нестандартні методи роботи з апаратним забезпеченням.

Розібравши надані методи, а саме Гамільтоновий цикл в графі, надає найбільшу захищеність програмного забезпечення так як він використовує важко оборотний метод.

Розглянемо його більш конкретно. Випадковим чином генерується ключ k довжини l у вигляді бітової послідовності, $k \in B^l$, де $B = \{0,1\}$, а $B^l = B \times B \times ... \times B$ (l раз). Далі ключ підрозділяється на фрагменти $u_1, u_2, ..., u_n$, кожний з яких має довжину m, n – кількість вершин графа. Таким чином, $l = n \cdot m$, а $k = u_1 u_2 ... u_n$. На основі ключа k будується граф, що містить Гамільтонов цикл. На першому етапі задаються n вершин з номерами $1,2,...,n$, а потім вони випадковим чином переставляються, одержуємо номери $i_1, i_2, ..., i_n$. Далі вершини з'єднуються попарно одна з одною дугами циклічно, і кожна дуга одержує позначку $u_i, (i = 1,2,...,n)$. Потім до Гамільтонового циклу додаються випадковим чином додаткові дуги, причому, кількість дуг, що виходять із вершини, не повинна перевищувати 2^m. Ці дуги також позначаються $e_{is}, (i, s = 1,2,...,n)$. Кожна нова дуга одержує мітку, відмінну від тих, котрими вже позначені інші дуги, що виходять із тієї ж вершини. Далі на основі графа (математичного об'єкта O) будується захисний фрагмент у такий спосіб. У фрагментах коду, кожний з яких відноситься до однієї вершини, організовується розгалуження. Причому, у вітці, що відповідає правильному фрагменту ключа (рівному її позначці), виконується перехід на наступну вершину по Гамільтоновому циклу.

к.т.н. Макарчук О.М. (ВІТІ НТУУ „КПІ”)
Ткачик С.В. (ВІТІ НТУУ „КПІ”)

ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

На сьогоднішній день склалася ситуація, коли найбільш поширені методи сигнатурного аналізу для виявлення вторгнень або методи статистичного аналізу для виявлення аномалій не здатні на належному рівні забезпечити інформаційну безпеку.

Основним недоліком існуючих систем захисту від мережевих атак є їх нездатність виявляти нові або невідомі атаки, які характеризуються відсутністю записів у системі про них.

Одним із перспективних напрямів є застосування нейронних мереж, які мають на меті моделювання такі властивості систем як здатність до навчання, самоорганізація та адаптація.

У загальному випадку система виявлення мережевих вторгнень складається з набору нейромережевих детекторів, які перевіряють вхідний і вихідний мережеві трафіки і класифікують їх. Оскільки налічують 22 різновиди мережевих атак, які об'єднані в 4 класи (*DoS – denial of service*, *U2R – user-to-root*, *R2L – remote-to-local* і *Probe*), то в системі застосовуються 22 нейромережевих детектори, навчені на виявлення кожної з 22 різновидів мережевих атак. На нейромережеві детектори по черзі подається 41 параметр мережевого з'єднання і відбувається перевірка на наявність заборонених з'єднань.

На першому етапі з кожного мережевого з'єднання витягується 41 атрибут, які трансформуються в числові значення і подаються послідовно на кожен з 22 нейромережевих детекторів. Активність одного з детекторів вкаже на виявлення аномального з'єднання, тип якого відповідає тій мережевій атаці, на виявлення якої навчався даний детектор.

В якості нейромережевого детектора для виявлення мережевих атак вибрана багатошарова нейронна мережа з одним прихованим шаром, що складається з нейронів Кохонена.

Перший шар нейронних елементів розподіляє вхідні сигнали X – 41 параметр мережевого з'єднання, на нейронні елементи прихованого шару. Кількість нейронних елементів розподільного шару дорівнює кількості атрибутів мережевого трафіку $n = 41$.

Другий шар складається з $m = 41$ нейронів Кохонена, які використовують конкурентний принцип навчання та функціонування відповідно до правила „переможець бере все” *(winner-take all)*. Для визначення нейрона-переможця використовується Евклідова відстань між вхідним і ваговими векторами. Так Евклідова відстань між вхідним і ваговим вектором i-го нейронного елемента визначається наступним чином:

$$D_i = |X - \omega_i| = \sqrt{((X_1 - \omega_{1i})^2 + (X_2 - \omega_{2i})^2 + \ldots + (X_c - \omega_{ci})^2)},$$

де ω_{1i} - ваговий коефіцієнт між c-м нейроном розподільного шару і i-м нейроном шару Кохонена, $X = [X_1, X_2, \ldots, X_n]$ - вхідний образ.

Нейронний елемент-переможець з номером k визначається відповідно до мінімальної Евклідової відстані.

Варто зазначити, що кількість нейронів шару Кохонена m не обов'язково має бути рівною 41. Однак, вплив кількості нейронів прихованого шару не настільки суттєвий, і може змінюватись в межах від 10 до 41.

Третій шар складається з одного лінійного нейронного елемента, який здійснює відображення кластерів, сформованих шаром Кохонена, в два класи, які характеризують нормальне з'єднання або атаку. Активність вихідного нейрона, коли значення його дорівнює одиниці, характеризує атаку. Нуль на виході характеризує нормальне з'єднання.

Запропонований підхід, заснований на застосуванні методу нейронних мереж в якості детекторів мережевих атак, дозволяє підвищити рівень виявлення мережевих вторгнень на комп'ютерні системи. Виявлення деяких типів атак відбувається з максимальною ймовірністю при незначному рівні помилкових виявлень.

Островой М.М. (ВІТІ НТУУ „КПІ”)
к.т.н. Любарський С.В. (ВІТІ НТУУ „КПІ”)

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПОШУКУ ОПТИМАЛЬНОГО РІШЕННЯ НА ОСНОВІ ГЕНЕТИЧНИХ АЛГОРИТМІВ

Аналіз існуючих методів пошуку оптимальних рішень показав що існуючі методи пошуку є не досить ефективними. Пошук оптимальних рішень є одним дуже важливим фактором в різних сферах бізнесу, а у військовій справі у веденні бойових дій. На даний час існує багато способів пошуку оптимальних рішень.

Оптимальне рішення – це рішення, при врахуванні всіх позитивних та негативних чинників, отримується найкращий результат.

Генетичний алгоритм – це проста модель еволюції в природі, реалізована у вигляді комп’ютерної програми. У ньому використовуються як аналог механізму генетичного наслідування, і аналог природного відбору. При цьому зберігається біологічна термінологія в спрощеному вигляді.

Так як ми розглядаємо пошук оптимального рішення на основі генетичних алгоритмів, а це є задачею пошуку, розглянемо задачу пошуку.

Передбачається, що метою завдання пошуку є знаходження об’єкта з деякими властивостями. Як правило, пошук здійснюється серед скінченної (іноді і нескінченної) безлічі об’єктів (потенційних рішень).

Перш ніж побудувати пошуковий алгоритм потрібно визначитися з символьної моделлю задачі, яка включає в себе:

– простір потенційних рішень О;
– простір уявлень S;
– функцію кодування e і декодування e-1;
– функцію мети f;
– функція оцінки уявлень μ.

Постановка завдання Нами буде розглядатися спільне завдання безперервної оптимізації

$\max f(x)$, де $D = \{x = (x_1, x_2,:, x_N) \mid xi$ на $[a_i, b_i]$, i = 1, 2,: $N\}$ (1)
x з D

$f(x)$ – максімізіруемая (цільова) скалярна багатопараметрична функцій, яка може мати кілька глобальних екстремумів, прямокутна область D – область пошуку, D – підмножина R^N.

Передбачається, що про функцію $f(x)$ відомо лише те, що вона визначена в будь-якій точці області D. Ніяка додаткова інформація про характер функції та її властивості (дифференцируемость, ліпшіціруемость, безперервність і т.д.) не враховується в процесі пошуку.

Під рішення задачі (1) будемо розуміти вектор $x = (x1, x2,:, x_N)$.

Оптимальним рішенням завдання (1) будемо вважати вектор x^*, при якому цільова функція $f(x)$ приймає максимальне значення. Виходячи з припущення про можливу многоекстремальності $f(x)$, оптимальне рішення може бути не єдиним. У прийнятих раніше позначеннях під об’єктом будемо розуміти точку x в багатопараметричної просторі $O = D$ в R^N. Роль функції мети гратиме максімізіруемая функція $f(x)$.