ЗМІСТ

(Тези доповідей пленарного засідання)

(Тези доповідей секційного засідання)

Оржешко Д.В. (ВІТІ НТУУ „КПІ")

ВСТУПНЕ СЛОВО

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

Конференція проводиться з метою підбиття підсумків наукової роботи курсантів 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 13.01.2012 р.;

–наказ НІ №94 від 11.08.2011 р. «Про організацію підготовки та проведення науково-технічної діяльності в інституті на 2011 – 2012 навчальний рік»;

–методичних вказівок про організацію роботи ВНТ курсантів;

–положення про воєнно-наукове товариство курсантів (затверджене Вченою радою інституту. Протокол №10 від 27.02.2012 р.).

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

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

–інформаційні технології функціонування комунікаційних систем та мереж;

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

–методологія аналізу, синтезу, 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.

Бажаю вам успіхів під час виступів як на пленарному засіданні так і пі дчас роботи наукових секцій.

Любарський С.В. (ВІТІ НТУУ „КПІ")

ПРО РОБОТУ НАУКОВОГО ГУРТКА КАФЕДРИ №21

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

Метою наукової роботи наукового гуртка кафедри № 21 є підвищення методологічної підготовки, розвиток наукового мислення, набуття навчок дослідницької роботи, творчою 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 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, с його невід'ємним продовженням та повинна відповідати завданням навчального пронесу та основним напрямам науково-дослідної роботи кафедри.

Пріоритетними напрямками сумісної співпраці науково-педагогічних працівників та курсантів є впровадження та застосування сучасних інформаційних технологій в системах 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 нашого факультет досягнули помітних успіхів. Так за кращу наукову працю серед курсантів та студентів ВІТІ НТУУ "КПІ" заохочені наступні члени науковою гуртка кафедри: курсант Пашков В.Ю., курсант Смірнягін А.Є., курсант Дудник В.Ю., курсант Тучак Є.В., курсант Савицький А.Д.

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. Любарський С.В. (ВІТІ НТУУ „КПІ")
Пашков В.Ю. (ВІТІ НТУУ „КПІ")

ОРГАНІЗАЦІЯ ЗАХИЩЕНОГО ОБМІНУ ІНФОРМАЦІЙНИМИ ПОВІДОМЛЕННЯМИ В КЛІЄНТ-СЕРВЕРНИХ АРХІТЕКТУРАХ НА ОСНОВІ WEB-СЕРВІСІВ

Порушення безпеки інформаційної системи корпоративного призначення розглядається як інцидент безпеки інформаційно-аналітичного процесу управління корпоративними мережами через втрату конфіденційності, цілісності, доступності інформаційних ресурсів. Саме тому актуальним є підхід до вирішення проблеми шифрування інформації даних, які передаються по мережі корпоративного призначення, для забезпечення конфіденційності інформації.

Мета дослідження полягає в забезпеченні належного рівня криптозохищеності інформаційних повідомлень, що передаються в корпоративних мережах за протоколом SOAP в клієнт-серверних архітектурах.

Наукова задача полягає в запропонуванні методу шифрування інформаційних повідомлень клієнт-серверних з'єднань на основі WEB-сервісів за рахунок використання існуючих алгоритмів блочного шифрування.

Вирішення даної наукової задачі поділяється на сукупність часткових взаємопов'язаних задач дослідження, а саме:

–аналізі технологічних підходів щодо забезпечення безпеки криптозахисту інформаційних повідомлень, які передаються за протоколом SOAP. Виявлення проблемних питань, обгрунтування напрямку наукових досліджень щодо їх вирішення;

–запропонуванні алгоритму забезпечення конфіденційності інформації в SOAP-повідомленнях для корпоративних мережах на основі симетричного блочного шифрування AES;

–розробці практичної реалізації запропонованого алгоритму шифрування інформаційних повідомлень, які передаються за протоколом SOAP між ASP.NET Web-сервісом та Web-додатком в корпоративних мережах.

Об'єктом дослідження виступає структура інформаційного повідомлення обміну даними за протоколом SOAP в клієнт-серверній архітектурі.

Предметом дослідження виступають алгоритми блочного шифрування на основі операцій заміни байтів, зсуву рядків, перемішування стовпців та складання за раундовим ключем.

к.т.н. Хусаїнов П.В. (ВІТІ НТУУ „КПІ")
Дудник В.Ю. (ВІТІ НТУУ „КПІ")

МЕТОДОЛОГІЯ ВІЗУАЛІЗАЦІЇ ГРАФІВ З ВИКОРИСТАННЯМ ТЕОРІЇ СКЛАДНИХ МЕРЕЖ

Побудова та аналіз потоків даних в комп`ютеризованих інформаційних системах є одним з базових питань розробки програмно-технічних методів їх захисту від силового кібернетичного впливу. Найбільш придатним апаратом для вирішення задач даного класу вважаються методи та алгоритми теорії складних мереж.

Важливим аспектом аналізу нетривіальних структурних властивостей моделі складної мережі є створення сприятливих умов для роботи експерта. Актуальність цього обумовлюється тим, що людина має розвинені інтелектуальні можливості аналізу складних графічних об'єктів, недоступні сучасним технічним засобам. Тому в якості результату розглядається підхід до побудови візуальних моделей комп'ютерних інформаційних систем на основі реєстрації даних мережевого трафіку шляхом формування ділянок насиченості.

Мета дослідження – відображення властивостей графу на основі ділянок насиченості. Наукова задача: розробити процедуру візуалізації властивостей складної мережі на основі формування ділянок інтенсивності.

Часткові задачі дослідження:

1 Провести аналіз методів та алгоритмів побудови (формування) візуальних моделей складних мереж.

2 Розробити процедуру візуалізації властивостей складної мережі на основі формування ділянок інтенсивності.

Об'єкт дослідження – процес аналізу структурних властивостей потоків даних інформаційної системи як візуальних моделей складних мереж.

Предмет дослідження – методи та алгоритми побудови (формування) візуальних моделей складних мереж.

Для відсіювання інформації що не несе корисного змісту використовується відсікання за нижнім пороговим значенням, що обчислюється за формулою

$$n_{\text{пор}} = \frac{\sum_{i=j} n_{i,j}}{q} * \Delta,$$

Де q – кількість напрямків в таблиці, n – кількість пакетів по даному напрямку, а Δ пороговий коефіцієнт, який визначає рівень чутливості візуалізації.

Для підвищення сприймання візуалізованої інформації пропонується використати метод збору ребер у зони насичення шляхом побудови ребер як кривих кусочно-заданих кубічних В-сплайнів. Кубічний В-сплайн – це набір кривих третього порядку в двомірному просторі, для яких виконується умови зшивки перших і других похідних на краях. Для того, щоб управляти ступенем зв'язаності ребер, вводиться параметр β, який приймає значення від 0 до 1:

$$\acute{S}(t) = \beta \cdot S(t) + (1 - \beta)(P_0 + t(P_{N-1} - P_0)),$$

де $S(t)$ — це точки сплайну, $S'(t)$ — це результуюча крива, яка і відображається у вигляді ребра.

к.т.н. Любарський С.В. (ВІТІ НТУУ „КПІ")
Тучак Є.В. (ВІТІ НТУУ „КПІ")

МЕТОДИКА ПРОВЕДЕННЯ МЕРЕЖЕВОЇ РОЗВІДКИ В МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В наш час інформаційна війна є одним із перспективних та основозабезпечуючих напрямків ведення сучасного бою.

Актуальною проблемою інформаційної війни є оперативне отримання інформації за супротивника. Проведення збору інформації про противника відбувається методами мережевої і комп'ютерної розвідки, використовуючи існуючі інформаційні технології.

Мережева розвідка являє собою комплекс заходів щодо отримання і обробки даних про інформаційну систему клієнта, ресурсів ІС, засобів захисту, використовуваних пристроїв і програмного забезпечення і їх вразливостей, а також про межу проникнення.

Мережева розвідка проводиться у формі запитів DNS, ехо-тестування (ping sweep) і сканування портів. Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цього домену привласнені. Ехо-тестування адрес, розкритих за допомогою DNS, дозволяє побачити, які хости реально працюють в даному середовищі. Отримавши список хостів, фахівець з інформаційної безпеки використовує засоби сканування портів, щоб скласти повний список послуг, що надаються цими хостами. І, нарешті, проводиться аналіз характеристик додатків, що працюють на хостах. В результаті здобувається інформація, яку можна використовувати для злому.

Сучасна мережева розвідка в залежності від цілей діяльності, масштабу, і характеру, поставлених для виконання завдань ділиться на:

- стратегічну.
- тактичну (оперативну);

Тактична розвідка забезпечує дії атакуючих. До них відносяться як зловмисники, так і фахівці, які проводять тестування інформаційної системи.

Тактична розвідка виявляє дані про:

- технічне оснащення;
- програмне забезпечення;
- уразливості поштових серверів;
- сервіси і поштових клієнтів;
- межі сегментів мережі;
- канали зв'язку, що використовуються (тип, пропускна здатність);
- державної (географічної, комерційної) приналежності мережі та / або сервера, що полегшує прийняття оптимальних рішень щодо планування та проведення атаки на інформаційні системи.

Ці відомості отримуються за допомогою перехоплення інформації, що передається радіоелектронними засобами.

Далі дії фахівця з інформаційної безпеки залежать від завдання, поставленого перед ним, будь то зміни інформації, підвищення повноважень або утримання системи.

Повністю позбавитися від мережевої розвідки неможливо. Якщо, наприклад, відключити ехо ICMP і ехо-відповідь на периферійних маршрутизаторах, можна позбутися від луна-тестування, але при цьому втрачаються дані, необхідні для діагностики мережевих збоїв. Крім того, сканувати порти можна без попереднього луна-тестування. Це займе більше часу, так як сканувати доведеться і неіснуючі IP-адреси. Системи IDS на рівні мережі і хостів звичайно добре справляються із завданням повідомлення адміністратора про проведення мережевої розвідки, що дозволяє краще підготуватися до майбутньої атаки і оповістити провайдера (ISP), в мережі якого встановлена система. Враховуючи дану інформацію можна зробити висновок, що в обов'язковому порядку завжди має бути присутня технічна захищеність інформаційних ресурсів.

к.т.н. Нестеренко М.М. (ВІТІ НТУУ „КПІ")
Смірнягін А.Є. (ВІТІ НТУУ „КПІ")

МЕТОДИКА РАННЬОГО ВИЯВЛЕННЯ TCP-SYN АТАК

Останнім часом надзвичайно актуальною стала тема захисту від *TCP-SYN* атак, одного з різновидів *DDoS* атак. Це обумовлено стрімко зростаючою популярністю глобальної мережі Інтернет, переведенням багатьох сфер діяльності у інформаційний простір, внаслідок чого винікають нові способи впливу та методи конкурентної боротьби.

Метою даної роботи є вироблення методики раннього виявлення *TCP-SYN* атак на основі математичної моделі, що описує взаємодію клієнта з сервером.

TCP-SYN атаки спрямовані на прикладні сервіси, що використовують протокол транспортного рівня *TCP*. Основна мета атаки – перевищити обмеження на кількість *TCP*-з'єднань, які знаходяться у стані встановлення.

Математичний апарат теорії масового обслуговування дозволяє визначити основні параметри системи, де найбільший інтерес буде представляти середнє число зайнятих приладів:

$$N = \sum_{k=1}^{n} k \cdot p_k = p_0 \sum_{k=1}^{n} \frac{\alpha^k}{(k-1)!} = \alpha(1 - p_n) \qquad \alpha = \lambda / \mu$$

λ - інтенсивність потоку заявок,

$1/\mu$ - математичне очікування часу обслуговування однієї заявки.

p_k - вірогідність знаходження в системі рівно k вимог.

Модель опису роботі сервера в нормальному режимі, що дозволяє враховувати такі параметри, як інтенсивність звернень до сервера і середній час обслуговування заявки:

$$N = \alpha(1 - p_\infty) = \alpha(1 - 0) = \alpha$$

В той же час, дл визначення наявності або відсутності *TCP-SYN* атаки використовується значення функції розподілу:

$$F(n) = \sum_{i=1}^{n} p(i)$$

В результаті проведеної роботи була розроблена методика виявлення *TCP SYN* атаки, що дозволяє виявляти атаку на ранніх стадіях. Відповідно до цього методу, рішення про початок атаки приймається в тому випадку, коли реальна кількість напіввідкритих на сервері з'єднань виходить за межі допустимого інтервалу.

Савицький А.Д. (ВІТІ НТУУ „КПІ")
Поправко Ю.Ю. (ВІТІ НТУУ „КПІ")
к.т.н. Сілко О.В. (ВІТІ НТУУ „КПІ")

ПИТАННЯ ВПРОВАДЖЕННЯ ПРОГРАМНИХ ЗАКЛАДОК В КОМП'ЮТЕРИЗОВАНІ СИСТЕМИ

Сучасні інформаційні технології все глибше проникають в багато сфер управління суспільними процесами. Ці тенденції стають настільки масштабним, що зачіпають життєві інтереси держав, особливо в галузі інформаційної безпеки.

Головною умовою правильного функціонування комп`ютерної системи є забезпечення захисту від втручання в процес обробки інформації тих програм, присутність яких в комп`ютерній системі не обов`язкова. Серед подібних програм, в першу чергу, слід згадати комп'ютерні віруси. Проте існує ще один клас шкідливих програм. Від них, як і від вірусів, слід з особливою ретельністю очищати свої комп`ютерні системи. Ця категорія іменується програмними закладками.

Програмні закладки – навмисно внесені в програмне забезпечення функціональні об`єкти; які за певних умов (вхідних даних) ініціюють виконання не описаних у документації функцій програмного забезпечення, що призводить до порушення конфіденційності, доступності або цілісності оброблюваної інформації.

Аналіз деструктивного впливу програмних закладок дозволяють виділити:

–*програмна закладка першого типу* – вносити довільні спотворення в коди програм, що знаходяться і оперативної пам'яті комп'ютера;

–*програмна закладка другого типу* – переносити фрагменти інформації з одних областей оперативної або зовнішньої пам'яті комп'ютера в інші;

–*програмна закладка третього типу* – спотворювати виведену на зовнішні комп`ютерні пристрої або в канал зв`язку інформацію, отриману в результаті роботи інших програм.

Головне завдання програмної закладки при впровадженні в захищені системи – це створення скритого каналу інформаційного обміну. Існують основні групи деструктивних дій, які можуть здійснюватися програмними закладками:

–копіювання інформації користувача комп`ютерної системи (паролів, криптографічних ключів, кодів доступу, конфіденційних електронних документів);

–зміна алгоритмів функціонування системних, прикладних та службових програм;

–нав`язування певних режимів роботи.

Складність застосування програмної закладки полягає у відмінності єдиних стандартів їх впровадження у програмні продукти. Тому перспективним є розгляд шляхів впровадження програмних закладок в залежності від розроблення вихідного коду, деструктивних дій та заповнення вмісту закладки.

Для проведення дослідження був обраний вірусний продукт „*Pinch*", який вже давно потрапив в бази провідних антивірусних засобів. *Pinch* – це одна з найбільш активно використовуваних троянських програм в мережевому сегменті. В дослідженні деструктивного коду програмної закладки використовувалося наступне спеціальне програмне забезпечення: відлагоджувач *OllyDbg*, редактор коду *WinHex*, утиліта для роботи з *PE*-файлами *LordPE*.

На основі наведених міркувань пропонується сформувати рекомендації щодо методики впровадження програмних закладок, яка забезпечить захист програмної закладки від механізмів *malware*-детента сучасних антивірусних програм.

Усік В.О. (ВІТІ НТУУ «КПІ»)
Муза Р.О. (ВІТІ НТУУ «КПІ»)

ЗАДАЧА АНАЛІЗУ ВІДДАЛЕНИХ АТАК НА КОМП'ЮТЕРИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

В наш час глобальної комп'ютеризації актуальним стало питання забезпечення безпеки роботи інформаційних систем. На сьогодні відома величезна кількість методів таких атак, і їх кількість постійно зростає. Ця загроза в повній мірі стосується як глобальної мережі Інтернет, так і корпоративних мереж, адже вони побудовані за схожими принципами. Для захисту від атак необхідне глибоке розуміння методів, що використовуються атакуючими.

В наш час існує велика кількість методів та засобів комп'ютерних атак, вони важко піддаються класифікації. Існує декілька проектів, які створили власні методи класифікації та аналізу атак на комп'ютеризовані інформаційні системи. До них можна віднести: CAPEC, The WASC Threat Classification, SANS та ін.

CAPEC (Common Attack Pattern Enumeration and Classification) – це суспільний ресурс знань для побудови захищеного програмного забезпечення. Являється загальнодоступною, суспільно створеною системою загальних методів і шаблонів атак з порівняльною схемою та класифікацією. Шаблони атак описані через загальні методи ураження комп'ютерних систем, що формуються з глибокого аналізу реальних прикладів. CAPEC являється зареєстрованою торговою маркою корпорації MITRE та підтримується Національним Дивізіоном Кібернетичної безпеки Міністерства національної безпеки США.

The WASC (Web Application Security Consortium)- це некомерційна міжнародна група експертів, представників організацій, що створюють стандарти безпеки для WWW. Являється open-source проектом.

SANS (SysAdmin, Audit, Network, Security)- один з найбільш великих проектів для навчання та підготовки спеціалістів з інформаційної безпеки. Ця комерційна організація (США) створила власну класифікацію та використовує її в процесі підготовки кадрів.

Нажаль, жодна з існуючих класифікацій не є універсальною, саме тому актуальною задачею являється розробка власної системи класифікації атак на комп'ютеризовані інформаційні системи. Така система дозволить : на основі аналізу існуючих даних, своєчасно визначити, який тип атаки застосовується, та швидко вибрати методи протидії, які необхідно застосувати в даній ситуації, із появою нових методів віддалених атак, класифікувати їх на основі існуючої інформації, проводити підготовку нових спеціалістів, що здатні вести боротьбу у кіберпросторі.

Для реалізації цих задач необхідно створити класифікацію атак, що придатні до використання у збройних силах .

Мельничук І. В.(ВІТІ НТУУ «КПІ»)

ЗАДАЧА РОЗРОБКИ ІЄРАРХІЇ КЛАСІВ АГРЕГАЦІЇ ДАНИХ МЕРЕЖЕВОГО ТРАФІКУ НА МОВІ JAVA

Комп'ютеризована інформаційна система (КІС) — сукупність вузлів, які з'єднані в мережу і можуть обмінюватися інформацією. В останній час складність зв'язків і масштаби таких мереж збільшились, що пов'язано з розвитком обчислювальної техніки. Із збільшенням складності мереж зростає і складність їх дослідження та аналізу. Незмінними залишаються питання захисту комп'ютерних мереж. Існує певна множина практичних задач забезпечення захисту таких систем, які базуються на основі своєчасного виявлення деяких підозрілих ознак в КІС. Одним із шляхів вирішення такої задачі є на дослідження та аналіз деяких властивостей транспортної інфраструктури КІС. З іншого боку, зібрані властивості можна використати і для протилежної цілі — для атаки мережі. Виявивши і припинивши роботу найважливіших вузлів, можна добитися значної деградації рівня інформаційних послуг шляхом впливу на транспортну інфраструктуру мережі.

Зміни у стані моделі будуть свідчити про можливість кібернетичного впливу на КІС. Збирання та порівняння даних з моделі в різні проміжки часу надасть можливість слідкувати за станом мережі і оперативно реагувати на випадки кібернетичного впливу.

Для отримання певних ознак необхідно створення і дослідження певної моделі системи. Найбільш придатним математичним апаратом для для побудови моделі КІС є теорія графів та її сучасний розвиток, відомий як теорія складних мереж. Центральною задачею моделі буде відслідковування інформаційних зв'язків між окремими вузлами та їх зміни з плином часу. Інформаційний зв'язок — це агрегована інформація про інформайні потоки між окремими вузлами КІС.

Вирішення задачі аналізу мережевого трафіку потребує розгляду КІС на різних рівнях. Можна виділити наступні рівні для вирішення задачі:

- на рівні окремого вузла;
- на рівні локальної мережі;
- на рівні вузлів автоматизованої системи.

Необхідно зазначити, що для побудови більш високих рівнів використовується інформація із більш низьких рівнів. В цій інформації буде знаходитися багато непотрібних другорядних деталей, які не будуть нести потрібного навантаження. Необхідно застосування агрегації — відкидання другорядних даних і виокремлення лише потрібних фрагментів. Агрегацією забезпечується виконання наступних задач:

- звільнення ресурсів мережі від передачі непотрібних даних
- полегшення подальшої обробки агрегованої інформації
- можливість ефективного розпаралелювання задачі аналізу мережі. Це надає в перспективі можливість масштабування системи.

Іншим важливим аспектом є візуалізація моделі на всіх вищевказаних рівнях. Для ефективної роботи необхідна візуалізація на всіх рівнях — починаючи від рівня окремого вузла і закінчуючи рівнем автоматизованої системи. Візуалізація дозволить спостерігати систему в цілому, а при потребі – і її складові елементи. Це важливий елемент, роль якого буде зростати із зростанням розміру мережі.

Потрібно зазначити про складність реалізації такої системи у реальному часі. Лише окремі системні інтегратори пропонують комплексні спеціалізовані рішення. Це пов'язано з великими вимогами такої системи до обчислювальних ресурсів і, як наслідок, до великих витрат на таку систему. Менш ресурсоємним і менш вартісним варіантом буде створення системи, яка б аналізувала та візуалізувала дані через дискретні проміжки часу.

Для вирішення задачі пропонується використання мови Java. Це пов'язано з орієнтованістю цієї мови на мережеве програмування і, як наслідок, існування великої кількості бібліотек, які полегшать реалізацію прототипу моделі.

Шпак В.В. (ВІТІ НТУУ «КПІ»)

ЗАДАЧА УПРАВЛІННЯ РОЗПОДІЛЕНИМИ ОБЧИСЛЕННЯМИ ПРИ ОБРОБЦІ ГРАФІВ

В сучасному світі інформаційні системи досить широко використовуються у інфраструктурі різних установ та організацій. Зазвичай вузли (комп'ютери) в таких системах пов'язані між собою локальною мережею, а в банках, державних та військових структурах в якості внутрішньої мережі використовується *Intranet*, так-званий міні-інтернет, який використовує стандарти, технології і програмне забезпечення *Internet*. Мережа підтримує сервіси, наприклад, такі як електронна пошта, веб-сайти, *FTP*-сервери, але в межах організації. Інформаційна система підключається до зовнішніх мереж, у тому числі і до *Internet*, як правило, з використанням засобів захисту від несанкціонованого доступу та проникнення в мережу.

Важливою є задача безпеки мережі, в якій виконуються процеси фіксації та збору інформації, передачі певних повідомлень, збереження інформації та її представлення. Тобто, прослідкувавши навантаження на кожен вузол системи, стан взаємозв'язків між ними та проаналізувавши обробку отриманих результатів, можливо побудувати образ інформаційних потоків даної системи, а отриману інформацію зберегти у вигляді графів. Якщо при періодичному скануванні мережі та порівнянні двох суміжних станів результат не є нормованим значенням, то на підставі цього можна робити висновки, що є негаразди в функціонуванні мережі. Так-як у великих організаціях кількість взаємозв'язків між вузлами може досягати десятків тисяч, то наше порівняння результатів сканування зводиться до порівняння двох графів великої розмірності.

Для обрахунку даних, які потребують потужні обчислювальні ресурси та багато часу, потрібні потужні суперкомп'ютери. Проте таких суперкомп'ютерів одиниці, а наукових проектів, які потребують їхніх обчислювальних здатностей, дуже багато. Альтернативним рішенням обробки таких об'ємів інформації є розподілені обчислення, які є одним із методів розв'язання ресурсомістких обчислювальних завдань з використанням двох і більше комп'ютерів, об'єднаних в мережу. Таким чином, задача управління розподіленими обчисленнями зводиться до розбиття головної задачі на невеликі підзадачі, та одночасного виконання різних частин однієї обчислювальної задачі на різних комп'ютерах. Тому необхідно, щоб завдання, що розв'язується було сегментоване – розділене на підзадачі, що можуть обчислюватися паралельно. В даному випадку, інформація про зв'язки в мережі зберігається у вигляді графів великого розміру, що представлені у вигляді такої структури даних, як матриця суміжностей, яку слід розбити на окремі потоки, що будуть паралельно виконуватись на окремих вузлах мережі. По закінченню обрахунків, усі результати збираються та робиться загальний висновок, про функціонування мережі.

Для розподіленого обчислення даних необхідно поєднувати комп'ютери в кластер, або використовувати спеціалізоване програмне забезпечення. Існує декілька готових рішень для вирішення таких задач, як комерційне (*Solaris Claster* – кластерне програмне забезпечення, яке дозволяє віддаленим комп'ютерам і вузлам працювати разом, при відмові одного з них, інші продовжують виконувати його функції), так і безкоштовне програмне забезпечення (*Linux Virtual Server* – широко розповсюджений засіб управління кластерними системами для *Linux* систем, має гарну масштабуємість, робочі властивості та надійність, *Beowulf* – обчислювальний кластер, який розбиває задачу на гілки, які паралельно виконуються та обмінюються даними по мережі).

Одже, задачу управління розподіленими обчисленнями при обробці графів великого розміру можна вирішити, розбивши головну задачу на окремі інформаційні потоки, які будуть виконуватися на окремих обчислювальних вузлах мережі для більш швидкого отримання результатів, а по закінченню обрахунків із отриманих результатів зробити висновок про стан інформаційної системи в реальний момент часу.