МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
Військовий інститут телекомунікацій та інформатизації

XIV ВОЄННО-НАУКОВА КОНФЕРЕНЦІЯ КУРСАНТІВ (СТУДЕНТІВ)

Факультету інформаційних технологій в системах управління
20 травня 2015 року

(Доповіді та тези доповідей)

Київ – 2015

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 та інших вищих навчальних закладів, в яких розглядаються пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення.

ЗМІСТ

Бойко Є.С. Застосування моделей нейронної мережі Кохонена для виявлення кібернетичної атаки за характерними повторюваними подіями 2

Гусаковський І.П. Використання геоінформаційних систем під час антитерористичної операції 6

Лукашенко Є.О. Модель балансування навантажень на основі методів *Traffic Engineering* 10

Мартиненко А.Г. Розширення можливостей засобів радіозв'язку тактичної ланки управління шляхом впровадження програмно-апаратних рішень 14

Павленко Я.А. Моделі та методи візуального аналізу даних про стан захищенності елементів інформаційної інфраструктури кібернетичного простору 18

Парнюк І.О. Запобігання непродуктивного застосування ПЕОМ на основі інтелектуальних процедур контролю програмного забезпечення 22

Поліщук І.Г. Математичне забезпечення оцінки залежності між часом прийняття рішення та основними ергономічними параметрами інтерфейсу оператора 26

Рубановський П.В. Математичне та прогрмне забезпечення розрахунку артилерійського вогню 30

ДОДАТОК Переможці та призери 2-го етапу конкурсу курсантських (студентських) наукових робіт ВІТІ 2015 року 34

Бойко Є.С.

ЗАСТОСУВАННЯ МОДЕЛЕЙ НЕЙРОННОЇ МЕРЕЖІ КОХОНЕНА ДЛЯ ВИЯВЛЕННЯ КІБЕРНЕТИЧНОЇ АТАКИ ЗА ХАРАКТЕРНИМИ ПОВТОРЮВАНИМИ ПОДІЯМИ

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. Комп'ютерні системи безперервно піддаються різного роду загрозам, наприклад у вигляді вторгнень (атак) і користувач не може бути впевнений у захищеності важливої інформації, оскільки кіберзлочинці продовжують удосконалювати і розвивати методи і засоби організації комп'ютерних атак.

Основним недоліком існуючих *IDS*-систем (*Intrusion Detection System*), заснованих на традиційних методах, є їх нездатність виявляти нові або невідомі атаки, які характеризуються відсутністю записів у системі про них, тому нині є актуальним використання таких нейромережевих алгоритмів, як самоорганізаційні карти Кохонена, що дозволяють підвищити рівень виявлення мережевих вторгнень на комп'ютерні системи.

Система виявлення вторгнень (*IDS*) на сьогоднішній день є невід'ємною частиною системи безпеки будь-якої комп'ютерної системи, підключеної до локальної або глобальної комп'ютерної мережі. *IDS*, як правило, це програма або апаратний засіб, який є «фільтром», тобто знаходиться між комп'ютерною системою та комп'ютерною мережею, і аналізує параметри вхідного і вихідного трафіку з метою виявлення фактів несанкціонованого доступу. *IDS* перехоплює весь мережевий трафік і аналізує вміст кожного пакета на наявність шкідливих компонентів.

Механізми, які застосовуються в сучасних системах виявлення атак *IDS*, засновані на декількох загальних методах, які не є взаємовиключними. У багатьох системах використовуються їх комбінації.

Класифікація *IDS* може бути виконана:

- за способом реагування;
- способу виявлення атаки;
- способу збору інформації про атаку.

Найбільш популярна класифікація *IDS*-систем за способом збору інформації про атаку:

- виявлення атак на рівні мережі (*network-based*);
- виявлення атак на рівні хоста (*host-based*);
- виявлення атак на рівні додатку (*application-based*).

Кожен з цих типів систем виявлення атак (на рівні мережі, на рівні хоста і на рівні додатку) має свої переваги і недоліки. Гібридні *IDS*, що представляють собою комбінацію різних типів систем, як правило, включають в себе можливості декількох категорій.

Типова архітектура системи виявлення атак, як правило, включає в себе наступні компоненти:

- сенсор (засіб збору інформації);
- аналізатор (засіб аналізу інформації);
- засоби реагування;
- засоби управління.

Звичайно, всі ці компоненти можуть функціонувати і на одному комп'ютері і навіть у рамках однієї програми, однак найчастіше вони територіально і функціонально розподілені. Такі компоненти *IDS*-систем, як аналізатори та засоби управління,

небезпечно розміщувати за мережевим екраном у зовнішній мережі, оскільки якщо вони будуть скомпрометовані, то зловмисник може отримати доступ до інформації про структуру внутрішньої мережі, що захищається на основі аналізу бази правил, використовуваної *IDS*-системи.

Задачу розпізнавання атак можна розглядати як задачу розпізнавання образів або задачу класифікації. Для їх вирішення можливе застосування нейронних або імунних мереж. При використанні імунних мереж система імітує механізм негативної селекції, в результаті якої генеруються раніше невідомі сигнатури, порівнювані з нормальним профілем. У свою чергу, для методу нейронних мереж характерно уявлення захищенної системи і взаємодіючих з нею зовнішніх об'єктів у вигляді траєкторій в деякому числовому просторі ознак. В якості методу виявлення зловживань нейронні мережі навчаються на прикладах атак кожного класу і надалі використовуються для розпізнавання приналежності спостережуваної поведінки одного з класів атак.

Всі методи виявлення атак можна розділити на два класи: методи виявлення аномалій і методи виявлення зловживань. Методи першого класу базуються на наявності готового опису нормальної поведінки спостережуваних об'єктів ІС, і будь-яке відхилення від нормальної поведінки вважається аномальним (порушенням). Методи виявлення зловживань засновані на описі відомих порушень або атак: якщо спостерігається поведінка деякого об'єкта ІС співпадає з описом відомої атаки, поведінку об'єкта вважається атакою.

Аналіз публікацій показує, що для більшості методів виявлення аномалій характерна слабка верифікованість і слабка глобальна стійкість (або її відсутність). Основна перевага методів виявлення аномалій полягає в їх адаптивності і здатності виявляти раніше невідомі атаки. Серед глобально стійких і верифікованих методів, можна відзначити метод нейронних мереж, що добре зарекомендували себе у вирішенні численних складних технічних завдань, таких як прогнозування, розпізнавання, адаптація, управління та ін.. Нейромережеві детектори здатні до навчання і класифікації. Навчені на обмеженому обсязі даних вони показують добрі результати виявлення різних типів мережевих атак.

Штучна нейронна мережа (ШНМ) є математичною (а також програмною або апаратною) моделлю, побудованою за принципом організації та функціонування біологічних нейронних мереж. Деякими з особливостей ШНМ є здатність в процесі навчання виявляти складні залежності між вхідною і вихідною інформацією, яка була відсутня в навчальній вибірці, і, здатність коректно класифікувати зашумлені образи. Нейронні мережі мають ряд переваг, які вигідно відрізняють їх від традиційних рішень. Деякі з них: висока ступінь паралелізму обробки інформації, здатність до узагальнення, адаптація до змін навколишнього середовища, розпізнавання зашумлених образів, низький рівень ресурсоємності і т.д.

Виявлення мережевих атак пов'язане з виділенням великої кількості ознак, за якими можна проводити класифікацію. Так, наприклад, в загальнодоступній базі *KDD99*, що містить порядку 5 мільйонів класифікованих за 22 типам примірників атак (класів), використовується 41 ознака. Всі ознаки інформаційно нерівнозначні, причому уточнити їхню справжню значимість можна тільки після проведення додаткових досліджень. Завдання оптимізації кількості ознак є невід'ємною частиною процесу розпізнавання. У реальних умовах система повинна автоматично виділяти ознаки і використовувати їх для вирішення завдання виявлення атаки і визначення її типу. В даний час розробляється велика кількість різних технологій захисту комп'ютерних мереж, заснованих на штучних нейронних мережах і статистичному аналізі.

В теперішній час створення перспективних систем забезпечення інформаційної безпеки ресурсів інформаційних систем асоціюється з використанням інтелектуальних засобів, що функціонують з використанням методів та моделей теорії нейронних мереж. Відповідно до результатів досліджень нейромережеві методи та моделі в основному використовуються для виявлення (розпізнавання) кібератак та вразливостей ресурсів

інформаційних систем. Крім того, ШНМ використовуються для управління параметрами захисту. Перспективність використання нейромережевих методів та моделей підтверджується окремими вдалими застосуваннями ШНМ в системах виявлення кібератак та великою кількістю відповідних теоретико-практичних робіт.

В сучасних *IDS*-системах в основному використовуються класичні типи нейромережевих моделей, які в тій чи іншій мірі адаптовані до умов поставленої задачі. Це дозволяє звузити коло допустимих нейромережевих моделей, що в свою чергу дозволяє підвищити оперативність визначення нейромережевої моделі, оптимальної з точки зору поставленої задачі. Таким чином з'являється можливість підвищення оперативності створення відповідних *IDS*-систем.

Існує велика кількість нейронних мереж, що застосовуються для вирішення тих чи інших складних інженерних завдань.

Серед проаналізованих архітектур нейронних мереж, карти Кохонена мають ряд переваг, що вплинули на вибір саме цієї технології. При формуванні нейронної мережі використовується метод навчання «без вчителя», тобто результат залежить тільки від структури вхідної інформації – властивостей мережевого трафіку. Одночасно, при порівнянні з іншими нейромережевими алгоритмами, в апараті самоорганізаційних карт Кохонена відсутність «вчителя» скорочує час, витрачений на підготовку нейромережі, так як формування вхідних векторів характеристик і їх підстроювання під параметри самонавчання відбуваються паралельно.

Самоорганізаційна карта Кохонена (*self-organizing map – SOM*) – нейронна мережа з некерованим навчанням, що виконує завдання кластеризації. Є методом проектування багатовимірного простору в простір з нижчою розмірністю (найчастіше, двовимірний), застосовується також для вирішення завдань моделювання, прогнозування та інших. Нейронні мережі Кохонена дозволяють в результаті навчання здійснювати топологічно безперервне відображення F-вхідного n-мірного простору в вихідну m-мірний простір. Структура такої нейронної мережі являє собою мережу з прямим розповсюдженням сигналу. В якості методу навчання використовується конкурентну навчання. По мірі надходження вхідних образів на таку мережу за допомогою навчання відбувається розбиття n-мірного вхідного простору на різні області рішень, кожній з яких відповідає окремий нейрон.

Нейромережева модель на основі багатошарової нейронної мережі з одним прихованим шаром нейронів Кохонена містить перший шар нейронних елементів, призначений для розподілу вхідних сигналів на нейрони шару Кохонена. Вхідними сигналами є параметри мережевого з'єднання. Виділяють 41 параметр (атрибут) мережевого з'єднання, які характеризують мережевий трафік і містять інформацію про час з'єднання, тип протоколу, кількість переданих байт, кількість виникнення помилок під час з'єднання і т. д.

Другий шар ШНМ складається з нейронів Кохонена. Шар Кохонена відіграє ключову роль в класифікації даних і здійснює кластеризацію вхідного простору образів, в результаті чого утворюються кластери різних образів, кожному з яких відповідає свій нейронний елемент.

Для навчання шару Кохонена використовується конкурентний метод навчання. Суть даного методу навчання полягає в тому, що в процесі навчання відбувається конкуренція між нейронними елементами, в результаті чого визначається нейронний елемент-переможець, який і характеризує клас даних.

У процесі навчання синаптичні зв'язки для нейрона-переможця посилюються, а для решти нейронів не змінюються. Таким чином, після навчання нейронної мережі, при подачі вхідного образу активність нейрона-переможця приймається рівною одиниці, а решта нейронів «скидається» в нуль. Таке правило навчання відомо під назвою «переможець бере все» (*winner-take-all*).

Так як в шарі Кохонена використовується поділ нейронів, які характеризують або легітимне з'єднання, або мережеву атаку, то коректна класифікація відбувається,

якщо при подачі на вхід мережі параметрів атаки переможцем є один з *f* нейронів шару Кохонена, або, якщо при подачі на вхід мережі параметрів легітимного з'єднання переможцем є один з *l* нейронів шару Кохонена. В інших випадках відбувається некоректна класифікація.

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.

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. Якщо жоден з детекторів не реагує на дане з'єднання, тобто виходи нейронних мереж встановлені в нуль, то дане з'єднання вважається легітимним.

Для тестування нейромережі проведено ряд експериментів, причому в якості вхідних даних використано базу даних *KDD Cup1999 Data*, яка себе зарекомендувала як один з небагатьох загальнодоступних наборів даних для мережевих систем виявлення атак.

Для навчання нейронної мережі сформовано навчальну вибірку, що складається з 80% з'єднань одного з типів атак і 20% нормальних з'єднань, тобто співвідношення аномальних з'єднань до легітимних дорівнює чотири до одного. Таке співвідношення отримано експериментальним шляхом і підтвержено найкращими результатами класифікації мережевого трафіку. Результати експериментів показали, що найкращий відсоток здатності до навчання і виявлення атак відбувається, коли навчання проводиться на 32 з'єднаннях мережевої атаки і 8 з'єднаннях легітимного, нормального трафіку, а відсоток помилкових виявлень, коли легітимне з'єднання приймається за атаку, становить менше 10 %.

В теперішній час створення перспективних систем забезпечення інформаційної безпеки ресурсів інформаційних систем асоціюється з використанням інтелектуальних засобів, що функціонують з використанням методів та моделей теорії нейронних мереж. Перспективність використання нейромережевих методів та моделей підтверджується окремими вдалими застосуваннями ШНМ в системах виявлення кібератак та великою кількістю відповідних теоретико-практичних робіт.

Запропонований підхід, заснований на застосуванні методу нейронних мереж на основі самоорганізаційних карт Кохонена для використання в сучасних *IDS*-системах, дозволяє підвищити рівень виявлення мережевих вторгнень на комп'ютерні системи. Виявлення деяких типів атак відбувається з 100% ймовірністю при незначному рівні помилкових виявлень. Крім цього, запропонований підхід не вимогливий до ресурсів системи і здатний виявляти невідомі типи атак (детектори, яких навчають, на одному типі атак, часто показують хороші результати виявлення інших типів атак, тобто на тих даних, на яких навчання не проводилося).

Рецензент: доцент кафедри бойового застосування математичного та програмного забезпечення АСУ к.т.н., доцент підполковник Хусаінов П.В.

Гусаковський І.П.

ВИКОРИСТАННЯ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ ПІД ЧАС АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ

Згідно з підрахунком, за час АТО Україна втратила 18 літаків і вертольотів, при цьому загинули 89 людей, 11 було поранено, а двоє зникли безвісти. Зокрема, було втрачено 10 вертольотів (по п'ять Мі-8 і Мі-24) і вісім літаків (Ан-30Б, Ан-26, Іл-76, два МіГ-29, два Су-25, Су-24М). Найбільше людей загинули внаслідок збиття військово-транспортного Іл-76 14 червня (49 осіб), і внаслідок аварій п'яти вертольотів Мі-8 – 26 осіб.

Одним з напрямків підвищення ефективності застосування армійської авіації є покращення програмного забезпечення шляхом застосування нових методів вирішення задачі в умовах поганої видимості.

Армійська авіація – рід військ у складі сухопутних військ України або складова частина військово-повітряних сил Збройних сил, призначена для дій безпосередньо в інтересах загальновійськових (танкових, аеромобільних) з'єднань, частин та підрозділів Сухопутних військ та виконує вогневі завдання, завдання бойового та тилового забезпечення. Має у своєму складі авіаційні частини та підрозділи, які мають на озброєнні вертольоти й частково літаки.

Основними вогневими завданнями є:

- нанесення ударів по військам противника;
- знищення повітряних та аеромобільних десантів, передових та інших загонів;
- висадка та підтримка з повітря своїх повітряних та аеромобільних десантів;
- ведення боротьби з вертольотами противника;
- знищення елементів зброї масового ураження та високоточної зброї, танків та іншої броньованої техніки, пунктів управління, вузлів зв'язку та елементів інфраструктури противника.

Армійська авіація – складова Сухопутних військ, що відіграє важливу роль в сучасному бою і виконує завдання в різноманітних умовах загальновійськового бою. До складу армійської авіації Сухопутних військ України входять бойові та транспортно-бойові полки. З'єднання та частини армійської авіації Сухопутних військ України мають на озброєнні вертольоти типу Мі-8, Мі-24 та їх модифікації, які дозволяють виконувати всі завдання за призначенням. Вертолітники, серед яких багато ветеранів Афганістану, Югославії, інших локальних конфліктів, достойно справляються з покладеними на них повсякденними завданнями, гідно представляють нашу країну у миротворчих операціях демонструючи високий професійний вишкіл. На озброєнні армійської авіації вертольоти типу Мі-8, Мі-24, та їх модифікації.

В авіації карти використовують при підготовці до польоту та в процесі польоту. Під час підготовки до польоту карти необхідні:

- прокладання та вивчення маршруту польоту;
- виміру путьових кутів та відстаней між пунктами маршруту;
- визначення географічних координат пунктів;
- нанесення точок розташування радіотехнічних засобів, які забезпечують політ;
- отримання даних про магнітне відхилення району польоту;
- вивчення рельєфу місцевості та визначення висоти гір та окремих точок місцевості.

Під час польоту карти необхідні для:

- ведення візуального та радіолокаційного орієнтування;
- контроль шляху та прокладки ліній положення літака;

– визначення навігаційних елементів польоту.

Без карти не можливо виконати політ. Армійська авіація до початку проведення АТО літала по паперовим картам 1957 року.

Волонтерська група «Повернися живим» передали 15 *GPS*-навігаторів з фізичними кнопками *Garmin Aera* 695, які надають дані про рельєф місцевості, що сильно полегшує польоти на наднизьких висотах. Навігатори передбачається встановити на літаки авіаційних бригад (Су-25, Су-27, МіГ-29). На черзі – гелікоптери, транспортна авіація.

В зоні АТО тип місцевості змішаний, є низини і височини, зона, яка є не дуже легкою та не надто складною для виконання польоту за маршрутом. Для забезпечення польотів військових повітряних суден на малих висотах необхідно видати відповідні оголошення, що стосуються польотів вертольотів на малих висотах, особливо пошукових польотів і польотів з виконанням фігур вищого пілотажу, у межах 3 морських миль від аеродромів не повинно бути небезпечних ліній електропередач, при цьому всі лінії зазначають на картах місцевості.

У зв'язку із зазначеним вище, рішення задачі редагування існуючих ліній електропередач на карті місцевості по картам Укренерго для армійської авіації в умовах АТО є вкрай необхідною.

Враховуючи перераховані вище вимоги, можна визначити базовий набір критеріїв для оцефрування ліній електропредач.

Перший етап. Робота з програмним забезпеченням *SASPlanet*:

- знайти та отримати графічні файли високої роздільної здатності потрібної місцевості;
- відповідно до плану енергосистем України нанести підстанції на карту;
- поєднати нанесені підстанції лініями електропередач;
- підготувати графічний файл для завантаження його в *Google Earth*.

Другий етап. Робота з програмним забезпеченням *Google Earth*:

- експорт фалів з розширенням **.kmz* , які містять лінії передач та мітки підстанцій;
- додавання нових зображень та ліній відповідно до умовних позначень;
- збереження загального зображення регіону з відредагованими лініями електропередач на карті місцевості.

Третій етап. Завантаження карти у *Garmin Aera*.

SASPlanet – геоінформаційна система розроблена групою *SAS*, працює під операційну систему *WindowsXP/2k/Vista/7*, ліцензія *GPLv3* (безкоштовна). Програмне забезпечення дозволяє завантажувати та переглядати карти та супутникові знімки поверхні землі високої роздільної здатності, які надають картографічні *online*-сервіси: *GoogleEarth*, *GoogleMaps*, *Bing Maps*, *DigitalGlobe*, Яндекс.карты, *Yahoo! Maps*, *VirtualEarth*, *Gurtam*, *OpenStreetMap*, *eAtlas*,*iPhonemaps* та інші.

SASPlanet автоматизує процес створення великої деталізованої карти із растрових карт (фотографій поверхні землі), шляхом завантаження їх з різних картографічних систем та нанесення на створену супутникову карту географічної інформації (шляхи, кордони, назви населених пунктів). Географічна інформація в програмі *SASPlanet* отримала назву «шари». Корисним шаром є «*Wikimapia*», який містить пояснення до всіх значимих орієнтирів на місцевості.

Google Earth – геоінформаційна система, розроблена *Google* (написана на мові *C++*),працює під будь якою операційною системою. Програма дозволяє переглядати зображення, які зроблені супутником, карти, *3D*-споруди.

В програмі реалізовані наступні функції *Google Earth*:

- автоматичне завантаження з Інтернет необхідного зображення, збереження їх в пам'яті комп'ютера та на жорсткому диску для подальшого їх використання;

- візуалізація тривимірного зображення земної кулі;
- отримання зображення поверхні з роздільною здатністю 15 м/ піксель, міста з роздільною здатністю від 0,15 до 0,6 м/піксель;
- отримання додаткових даних: назви населених пунктів, водойм, аеропортів, доріг та інше;
- користувач може створювати позначки та накладати їх поверх супутникових знімків;
- наявний шар «*3D* Будівлі» з тривимірними моделями;
- можливість визначення відстаней між об'єктами.

Вдосконалення інструментальних засобів добування видової аерокосмічної інформації веде до необхідності вирішення задачі прогнозування результатів роботи оптико-електронних систем отримання зображень з використанням критерій оцінювання ефективності подальшого дешифрування. Оцінити можливість дешифрування – означає отримати об'єктивні кількісні показники виявлення та розпізнавання об'єктів на аерокосмічних зображеннях, повноти та достовірності одержуваних результатів. Оскільки при плануванні аерокосмічного знімання та розподілі наявних сил і технічних засобів по об'єктах знімання доводиться оперувати імовірностями вирішення поставлених завдань, системи інформаційної підтримки мають виконувати розрахунки імовірностей правильного дешифрування простих об'єктів на одержуваних космічних зображеннях. Отже, в подальшому під оцінкою можливостей дешифрування будемо розуміти кількісну оцінку інтерпретаційних властивостей аерокосмічних знімків – імовірностей правильного виявлення та розпізнавання заданих компактних (простих) об'єктів.

Факти розпізнавання або не розпізнавання об'єкта, зображеного на знімку, є випадковою подією, так як цей процес, навіть при вивченні об'єктів одного й того ж типу, кожного разу відбувається по-своєму. Розпізнавання об'єкта внаслідок своєї випадкової природи характеризується імовірністю. Саме імовірність розпізнавання є кількісним відображенням якості дешифрування. Вона характеризує стійкість процесу розпізнавання при його багаторазовому повторенні.

На теперішній час розроблено багато підходів оцінювання дешифрувальних властивостей аерокосмічних знімків. Частіше за все застосовуються моделі, засновані на різних варіаціях формули Живичина. До найбільш застосовуваних на практиці відносяться роботи, але сама формула та її удосконалення мають свої недоліки.

В роботі запропонована математична модель розпізнавання розмитих зашумлених зображень малорозмірних слабоконтрастних об'єктів у випадку багатоальтернативної задачі. Модель враховує оптичну передавальну функцію іконічної системи та відношення сигнал-шум в інтерпретаційному тракті.

В той самий час виникає задача, як об'єднати отримані результати імовірності правильного виявлення об'єкта для різних зображень з різних джерел (датчиків) різної фізичної природи. Для цього використовують процес так званого «злиття даних» (*data fusion*) – процес комбінування даних з різних джерел таким чином, що результат забезпечує більш високу інформативність, ніж та, що може бути отримана аналізом кожного окремого джерела. Одним з найбільш коротких, але змістовних визначень процесу злиття даних є наступний: «Клас методів і засобів, що використовують дані декількох сенсорів різної природи для підвищення якості інформації, що міститься в цих даних».

До першого і головного, при здійсненні злиття даних, компонента належать джерела даних: оптико-електронні, інфрачервоні та радіолокаційні знімальні системи, бортові спектрометри, радіометри, лідари та інша апаратура, яка може бути застосована для дистанційного знімання. Другий компонент – допоміжна інформація. Вона є досить різноманітною: тактико-технічні характеристики знімальної апаратури, дані її калібровки, польотні умови виконання зйомки, службові дані і т.п. Третій компонент –

база знань, яка є основним постачальником апріорної інформації. Апріорна інформація використовується при управлінні процесом злиття даних, для розуміння фізичних, просторово-часових та інших обмежень на умови протікання процесів тощо. Зокрема, апріорну інформацію тематично-просторового характеру може надавати залучена до бази знань спеціалізована геоінформаційна система.

Очевидно, що мова йде про злиття даних з джерел, які відносяться до однієї предметної області, тобто дистанційних зображень одних і тих же об'єктів. Однак, при злитті даних виникають проблеми, до однієї з яких можна віднести ідентифікацію об'єкта (*entity identification problem*). Суть цієї проблеми полягає в необхідності установлення однозначної відповідності між вхідними зображеннями, що надаються з різних джерел, але відносяться до одного об'єкта. У багатьох випадках проблема ідентифікації об'єкта є основною проблемою при злитті даних з різних джерел. Тому необхідно яким-небудь чином вирішувати проблему однозначної відповідності і тим самим отримувати дані про конкретний екземпляр об'єкта з різних джерел.

Інша проблема при злитті даних – це проблема різної фізичної природи локальних джерел. Ця проблема полягає в тому, що одні і ті ж об'єкти в різних зображеннях можуть реєструватися з різними наборами розпізнавальних ознак, що визначається особливостями знімання у різних спектральних діапазонах.

Усі вище перелічені проблеми є складовими загальної проблеми, яка називається проблемою неконгруентності даних. Тому не менш важливий вибір конкретного методу злиття даних. Від нього залежить тип попередньої обробки даних.

Алгоритми злиття даних різних дистанційних датчиків можуть бути умовно розбиті на три групи в залежності від інформаційного рівня, на якому відбувається основний блок обробки: рівень елементів зображення (піксельний рівень), рівень об'єктів, рівень рішень.

Злиття зображень на піксельному рівні має на увазі по-елементне додавання вимірюваних фізичних параметрів. Таким чином, в кожен елемент нового ("злитого") зображення закладається інформація з усіх вхідних сенсорів. Саме тому тут потрібне дуже точне суміщення всіх зображень (геокодування), оскільки помилки поєднання приведуть до спотворень розподілу інформації, і результат спільної обробки буде погіршений.

Злиття на рівні об'єктів вимагає попереднього виділення цих об'єктів на всіх вхідних зображеннях (процедура класифікації). Залежно від типів вирішуваних завдань такими об'єктами можуть бути лінійні структури, межі, замкнуті криві, області визначеної геометричної форми, розміру, типу відбиття/розсіяння, текстури і так далі. Потім обробці піддаються саме ці області (об'єкти одного класу) за допомогою різних методів і алгоритмів.

Окреме місце займає мережевий підхід, сутність якого у тому, що дані, які формуються при зніманні, подаються до мережі, де вони обробляються за законами, обумовленими структурою мережі і характеристиками її елементів. Якщо елементи однотипні, а зв'язки між ними (принаймні на початку функціонування мережі) випадкові, то таку мережу класифікують як нейронну.

Якщо структура мережі детермінована, а структурні елементи розподіляються за своїм функціональним призначенням, і хоча б деякі з них здатні здійснювати змістовну обробку даних, то таку мережу класифікують як семантичну.

Злиття даних на рівні рішень використовується для різних знімальних систем або для різночасових знімків. Результатом злиття є відновлення спільної імовірності (імовірностей) гіпотез про наявність відповідних об'єктів з урахуванням результатів обробки різних зображень. Для відновлення спільної імовірності звичайно використовуються методи теорії статистичного навчання.

Рецензент: професор кафедри бойового застосування математичного та програмного забезпечення АСУ к.т.н., доцент пр.ЗСУ Горбенко В.І.

Лукашенко Є.О.

МОДЕЛЬ БАЛАНСУВАННЯ НАВАНТАЖЕНЬ НА ОСНОВІ МЕТОДІВ *TRAFFIC ENGINEERING*

Ефективність функціонування телекомунікаційних мереж визначається рішенням задач маршрутизації. У більшості випадків маршрутизація передбачає два етапи виконання дій: підготовчий і власне сам процес маршрутизації. У сучасних *IP*–мережах для вирішення завдань маршрутизації використовуються децентралізовані підходи управління, які схожі між собою, але при цьому призводять до нерівномірного завантаження мережі.

Перспективним напрямком розвитку є оптимальна маршрутизація, використання якої на практиці передбачає реалізацію централізованого підходу до управління мережею. Таке управління хоч і теоретично дає кращі результати, але на практиці має низку труднощів. Основними недоліками є велика розмірність моделі мережі і повільна збіжність, оскільки управління залежить від глобальних параметрів. При наявності недоліків децентралізованого та централізованого управління, виникає потреба в об'єднанні їх позитивних особливостей.

Задача оптимального використання обмежених мережевих ресурсів частково вирішується за допомогою інтелектуальної маршрутизації на основі методів передбачення та завчасного перенаправлення інформаційних потоків на мало завантажені маршрути із компенсацією ресурсів для дотримання вимог параметрів якості сервісу. За таким сценарієм, мережа повинна мати інформацію про можливі піки завантаженості та здійснювати моніторинг за інтенсивністю потоків, для їх уникнення. Головна проблема такого підходу полягає у складності забезпечення чіткої «картини» повного завантаження мережі, не застосовуючи централізовані системи маршрутизації, або завантаження мережі надлишковою службовою інформацією. Водночас, розглядати ресурси окремих елементів мережі, якими є маршрутизатори з приналежними до них лініями зв'язку є недоцільно. Доцільно розглядати мережу на деякому проміжному рівні, який представляє собою набір маршрутів з максимально можливим рангом, для знаходження всіх можливих «перехресних» вузлів, щоб виявити вузькі місця та здійснити завантаження невикористаних ресурсів. Існуючі протоколи маршрутизації, на старті своєї роботи, здійснюють побудову таблиці маршрутизації за алгоритмами, що враховують наявні загальні ресурси мережі, та в процесі подальшого функціонування не враховують поточний стан завантаження робочих маршрутів. Це призводить до використання найкоротших або найбільш ресурсомістких маршрутів із їх повним завантаженням, і простою решти довгих або низько швидкісних маршрутів.

Для визначення найкоротших або найбільш ресурсомістких маршрутів використовується низка протоколів маршрутизації.

В інтерпретації телекомунікаційних мереж, запасами є ресурси мережі під якими розуміють наступні параметри *Quality of Service (QoS)*:

- пропускна здатність;
- втрати пакетів;
- затримка пакетів;
- джитер.

Вичерпання одного із даних ресурсів приводить до припинення обслуговування нових абонентів та зростання потоку від абонентів, що вже обслуговуються. Загальний запас є функцією від вище перелічених параметрів *QoS*.

Кожен параметр *QoS* має межі свого запасу, а при їх вичерпанні поповнення даного запасу здійснюється за рахунок запасів решти параметрів QoS. Для прикладу, неможливість передачі заданого об'єму трафіку за певний час по каналу зв'язку призводить до накопичення пакетів в буфері тим самим збільшуючи затримку передачі,

тобто вичерпання запасу пропускної здатності компенсується запасом затримки, а в умовах вичерпання і запасу затримки використовується запас втрат пакетів, за рахунок переповнення буферів.

Таким чином, запас ресурсів визначається не лише фізичними параметрами каналів та швидкістю обробки пакетів, а і інтенсивністю потоків, параметрами розподілу потоків, надійністю обладнання тощо. Найкритичнішим запасом є пропускна здатність, що залежить від наявної інфраструктури фізичних каналів мережі. Мережа не в змозі передати більший об'єм інформації, ніж це передбачено об'ємом фізичного каналу. У випадку недостатньої кількості запасу пропускної здатності пакети починають нагромаджуватись в буферах мережевих пристроїв тим самим впливаючи на решту параметрів *QoS*. Запас пропускної здатності визначається при проектуванні і будівництві мережі і є незмінним параметром, допоки не буде здійснена модернізація або нарощування фізичної ємності. Даний запас розподіляється між обслуговуваними пакетами та, в залежності від необхідного ресурсу для кожного пакету може забезпечити передачу певної кількості пакетів (оскільки протокол *IP* передбачає змінну довжину пакету та його фрагментування).

Окрім протоколів маршрутизації, на сьогоднішній день існує безліч технологій та механізмів, які в своїй роботі використовують вищезгадані протоколи маршрутизації та методів забезпечення якості обслуговування, тим самим забезпечуючи маршрутизацію та виконання показників *QoS*.

Для забезпечення виконання показників *QoS* в *IP*–мережах використовуються наступні методи:

- резервування ресурсів;
- пріоритезація трафіку;
- динамічна перемаршрутизація.

Отже, сучасні протоколи маршрутизації неадаптивні до перезавантажень мережі і не забезпечують заданих параметрів *QoS*. Існуючі на сьогоднішній день моделі забебезпечення якості обслуговування проявляють найбільший ефект на різних ділянках мережі. Однією із можливостей реалізації *Traffic Engineering* є технологія *Multiprotocol Label Switching (MPLS)*.

Найбільш ефективними, але і, мабуть, найскладнішими, є способи динамічної (адаптивної) маршрутизації. При динамічній маршрутизації вміст таблиць маршрутів змінюється залежно від стану і завантаження каналів передачі даних і вузлів комутації. Для адаптації до зміни навантаження кожному вузлу комутації надається певна інформація про стан мережі передачі даних і, насамперед, про її топологію, інтенсивність потоків даних і затримки (черги) у вузлах комутації. Ця інформація відстежується (збирається) спеціальними керуючими пакетами, якими обмінюються вузли комутації. Якість маршрутизації значною мірою залежить від оперативності відновлення керуючої інформації. Загалом, найбільш оптимальна маршрутизація досягається за наявності інформації про миттєвий стан мережі та її завантаження. Проте це найчастіше призводить до значного збільшення потоку керуючих пакетів у мережі передачі даних і до зниження її ефективності.

Динамічна маршрутизація є досить складним процесом, під час якого виконуються такі дії:

- формування маршрутів, яке здійснюється за допомогою алгоритмів маршрутизації шляхом упорядкування у кожному вузлі комутації таблиць маршрутів пакетів;
- реалізація маршрутів, тобто керування пакетами під час проходження їх підмережею зв'язку до місця призначення за допомогою спеціальних протоколів мережевого рівня;
- контроль стану мережі, у тому числі аналіз топології мережі, структури потоків і затримок у вузлах комутації;

- передача інформації про стан мережі, яку використовують для коригування таблиць маршрутів;
- коригування маршрутів.

Залежно від обраної стратегії коригування маршрутів розрізняють централізовану, розподілену, локальну і гібридну маршрутизації.

Найефективнішим методом маршрутизації можна вважати гібридну маршрутизацію, яка поєднує позитивні властивості локальної і централізованої маршрутизацій. Прикладом є «дельта–маршрутизація», за якої менеджер з деяким запізненням стежить за глобальною ситуацією у мережі, тоді як вузлам надана певна свобода дій з тим, щоб вони могли швидко реагувати на локальні коливання навантаження мережі та зміни стану її окремих компонентів.

Різноманітність у способах маршрутизації пояснюється відсутністю універсального способу, оптимального для різних прикладних програм і характеристик мережі (рівня потоку даних, надійності передачі, часу встановлення наскрізного (через мережу) з'єднання, швидкості передачі блоків даних тощо).

Технологія *MPLS* була розроблена для організації єдиного протоколу передачі даних як для додатків з комутацією каналів, так і додатків з комутацією пакетів (маються на увазі програми з дейтаграмному передачею пакетів). *MPLS* може бути використаний для передачі різного виду трафіку, включаючи *IP*-пакети, осередки *ATM*, фрейми *SONET / SDH*, і кадри *Ethernet*. Для вирішення ідентичних завдань раніше були розроблені такі технології як Frame *Relay* і *ATM*. Багато інженерів вважали, що технологія *ATM* буде замінена іншими протоколами з меншими накладними витратами на передачу даних і при цьому забезпечують передачу пакетів даних змінної довжини з встановленням з'єднання між вузлами мережі. Технологія *MPLS* розроблялася з урахуванням сильних і слабких сторін *ATM*. В даний час устаткування з підтримкою MPLS замінять на ринку обладнання з підтримкою згаданих вище технологій. Цілком можливо, що в майбутньому *MPLS* повністю витіснить дані технології. Зокрема *MPLS* обходиться без комутації осередків і набору сигнальних протоколів, характерних для банкоматів. При розробці *MPLS* прийшло розуміння того, що в рівні ядра сучасної мережі немає необхідності в осередках *ATM* маленького фіксованого розміру, так як сучасні оптичні мережі володіють такою великою швидкістю передачі даних (на 2011 р. Пропускна спроможність магістралей більшості провайдерів становить 40 Гбіт/с або 100 Гбіт/с), що навіть пакет даних максимальної довжини в 1500 байт відчуває незначну затримку в чергах буферів обладнання комутації (необхідність скорочення таких затримок, наприклад для забезпечення заданої якості голосового трафіку, вплинула на вибір осередків малого розміру, характерною для *ATM*). У той же час *MPLS* спробував зберегти механізми оптимізації та управління трафіком і управління окремо від переданого потоку даних, які зробили технології *Frame Relay* і *ATM* привабливими для впровадження у великих мережах передачі даних. Незважаючи на те, що перехід на *MPLS* дає переваги управління потоками даних (поліпшення надійності і підвищення продуктивності мережі), існує проблема втрати контролю потоків даних, що проходять через мережу *MPLS*, з боку звичайних *IP*–додатків.

Технологія *MPLS* основана на обробці заголовка *MPLS*, який додається до кожного пакету даних. Заголовок *MPLS* може складатися з однієї або кількох «міток». Кілька записів (міток) в заголовку *MPLS* називаються стеком міток. Кожен запис в стеку міток складається з наступних чотирьох полів:

- значення мітки. Займає 20 біт;
- поле класу трафіку, необхідного для реалізації механізмів *QoS* і явного повідомлення про перевантаження. Займає 3 біти;
- флаг дна стеку. Якщо флаг встановлений, то це означає, що поточна мітка остання в стеці. Займає 1 біт;
- поле *TTL(Time To Live)*. Займає 8 біт.

Протокол *RSVP–TE* представляє собою розширення стандартного протоколу резервування мережевих ресурсів *RSVP*, яке підтримує конкретну реалізацію *LSP* з резервуванням мережевих ресурсів чи без нього. У разі резервування мережевих ресурсів при прокладанні шляху *LSP* в кожному сигнальному повідомленні вказується не тільки необхідна адресна інформація, але і резервована пропускна здатність, що вираховується даним мережевим пристроєм із загальної пропускної здатності відповідного інтерфейсу. Протокол *RSVP–TE* підтримує безперебійну (*smooth*) ремаршрутизацію, пріоритетне переривання обслуговування і виявлення «петель».

Першою з двох функцій, покладених на *RSVP* технологією *MPLS*, є розподіл міток (замість протоколу *LDP*). Друга, традиційна для *RSVP* роль полягає у підтримці *QoS* в мережі *MPLS*. Незалежно від використовуваного протоколу розподілу міток, маршрутизатори *LSR* повинні узгодити між собою параметри *QoS* для кожного *FEC*. Мітки дозволяють визначити величезне число класів *QoS*, але реально в типових мультисервісних мережах, навіть при дуже великій кількості класів *FEC*, будуть існувати, як правило, всього кілька класів *QoS*.

Переваги роботи протоколу розподілу міток *RSVP-TE*:

- резервування ресурсів мережевого обладнання для забезпечення необхідних параметрів *QoS*;
- контроль, оновлення (резервування) встановленого з'єднання;
- розподіл навантаження при врахуванні коефіцієнту завантаження елементів мережі.

Недолік роботи протоколу розподілу міток *RSVP-TE* – неоптимальна завантаженість елементів мережі в залежності від кількості та величини навантажень інформаційних потоків.

Слід відмітити, що *Traffic Engineering* працює тільки з протоколами *Link State Routing Protocols (IS–IS, OSPF)* і не працює з протоколами *Distance Vector Routing Protocols (RIP, EIGRP)*. Для вирішення завдання *TE* в протоколи *OSPF* і *IS–IS* включені нові типи оголошень для розповсюдження по мережі інформації про номінальну і незарезервовану (доступну для потоків *TE*) пропускну спроможність кожного зв'язку. У технології *TE* інформація про знайдений раціональний шлях використовується повністю – тобто запам'ятовується не тільки перший транзитний вузол, як в основному режимі маршрутизації *IP*, а всі проміжні вузли шляху разом з початковим і кінцевим, тобто маршрутизація проводиться від джерела.

Тому достатньо, щоб пошуком шляхів займалися тільки прикордонні мережі *LSR*, а внутрішні – лише поставляли їм інформацію про поточний стан мережі, яка необхідна для ухвалення рішень.

В даній роботі була проведена оцінка ефективності застосування механізмів *Traffic Engineering* для вирішення задач управління телекомунікаційними мережами в умовах перевантажень. Це пояснюється тим, що сучасні мережеві протоколи не дозволяють повністю і якісно керувати перерозподілом навантаження.

В результаті аналізу було запропоновано адаптивну модель управління потоками даних у мережі, яка необхідна для уникнення високого завантаження окремих ліній, у той час як інші залишаються менш завантаженими. Дана модель є комплексною, а саме враховує коефіцієнт завантаження всіх ліній, допустимих метрик маршрутів та інші параметри мережі, тобто враховує динаміку мережі. Що в свою чергу, збільшує об'єм необхідної службової інформації та ускладнює процес передачі інформації.

Запропоновані підходи дозволять удосконалити і розширити можливості мережевих протоколів щодо управління потоками мережевим трафіком.

Рецензент: доцент кафедри бойового застосування математичного та програмного забезпечення АСУ к.т.н., доцент підполковник Нестеренко М. М.

Мартиненко А.Г.

РОЗШИРЕННЯ МОЖЛИВОСТЕЙ ЗАСОБІВ РАДІОЗВ'ЯЗКУ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ШЛЯХОМ ВПРОВАДЖЕННЯ ПРОГРАМНО-АПАРАТНИХ РІШЕНЬ

Зв'язок є невід'ємним елементом для побудови системи управління. Під час участі в антитерористичній операції, боєздатність збройних сил, мобільність та ефективність на пряму залежать від чіткої організації зв'язку. Скритність є однією з основних вимог до зв'язку, що забезпечує безпеку наших підрозділів. Безпека полягає у недопущенні виявлення місця знаходжень підрозділів та недопущенні витоку інформації про заплановані дії. Зрозуміло, що противник намагатиметься будь-що перехопити інформацію, що зможе забезпечити йому перемогу або не допустити власних втрат. Бойові дії, що проводяться в антитерористичній операції, проводяться підрозділами тактичного рівня. Оскільки саме на ці підрозділи покладається основне завдання, виникає необхідність забезпечення скритності зв'язку саме для їх взаємодії.

Останні публічні виступи Президента України – Верховного Головнокомандувача Збройних Сил України дають підставу передбачати застосування цифрових методів передачі інформації на всіх ієрархічних рівнях системи зв'язку військового призначення, з урахуванням тенденцій розвитку збройної боротьби, яка зазнала значних змін щодо реалізації. Переоснащення військ інноваційною технікою військового зв'язку – одне з найважливіших завдань. Таким чином постає завдання модернізації засобів зв'язку тактичної ланки управління та захисту інформації в їх каналах.

Система зв'язку ЗСУ представлена як комплекс, що складається з різних видів радіо-, проводового, гідроакустичного та фельд'єгерсько-поштового, сигнального зв'язку для забезпечення управління в усіх ланках управління та взаємодії між ними. Застосування різних видів зв'язку у різних ланах управління характеризується зручністю застосування кінцевих засобів цих видів для виконання різних завдань. Основними видами радіозв'язку є радіо-, радіорелейний, тропосферний, супутниковий, транкінговий зв'язок. Якщо розглядати систему зв'язку тактичної ланки управління, то згідно керівних документів основою її побудови є радіозв'язок та проводовий зв'язок. Але з досвіду участі тактичних підрозділів у антитерористичній операції для побудови системи зв'язку також застосовується радіорелейний та транкінговий зв'язок.

Виходячи з принципів побудови системи зв'язку та особливостей застосування засобів зв'язку, предметом подальшого розгляду є радіозв'язок, як основний вид для побудови системи зв'язку тактичної ланки управління.

На даний час для забезпечення радіозв'язку використовуються як техніка, що була виготовлена у радянському союзі так і сучасні засоби. Але сучасними засобами забезпечені лише бойові підрозділи, що на даний момент приймають участь в АТО. В якості техніки, що прийнята на озброєння в ЗСУ в загальному, використовуються зразки техніки, виготовлені в радянському союзі. Ця техніка має високу якість, завдяки чому працює у складних умовах і забезпечує виконання завдань у тактичній ланці управління.

Але, не зважаючи на це, ця техніка є застарілою і має ряд недоліків, що становлять загрозу при організації управління в тактичній ланці управління.

Основні недоліки техніки старого парку:

- відсутня частотна адаптація. В наслідок цього, ця техніка стає вразливою при застосуванні противником засобів радіоелектронної боротьби;
- показники маси і габаритів. Громіздкість техніки і її маса спричиняють незручність при застосуванні техніки особовим складом;

– відсутність засобів криптографічного захисту. Вся інформація, що передається по радіоканалу є незахищеною, а отже може без усіляких перешкод бути перехоплена противником.

Оскільки переважну кількість засобів радіозв'язку складає техніка старого парку, використання якої спричиняє ряд проблем, необхідно шукати можливості для їх вирішення.

Не дивлячись на велику кількість видів зв'язку, радіозв'язок є основою для побудови системи зв'язку тактичної ланки управління в ЗСУ. І хоча радіозв'язок і є основою, для його застосування використовуються застарілі засоби, що мають значні проблеми. Основними проблемами пов'язаними з застосування засобів радіозв'язку старого парку є відсутність можливості частотної адаптації для протидії засобам РЕБ противника, показники маси та габаритів, відсутність засобів криптографічного захисту. Вирішення цих проблем може бути повне та часткове. Повне вирішення полягає у повному переоснащенні підрозділів новими засобами радіозв'язку. Враховуючи обмеженість у часі та коштах через ситуацію на сході країни, даний підхід є неможливим. Виходячи з цього, існує можливість лише частково вирішити проблеми на основі старої техніки. Оскільки вирішення проблеми частотної адаптаціє є неможливим, через великий час переналаштування між частотами і малий діапазон робочих частот, можливою для вирішення є лише проблема криптографічного захисту. Враховуючи всі обставини для вирішення даної проблеми пропонується програмний підхід. Він полягає у створенні програмного засобу для шифрування.

Програмна реалізація криптографічного шифрування передбачає застосування ЕОМ для модернізації аналогових засобів радіозв'язку старого парку. Враховуючи специфіку застосування засобів радіозв'язку, для виконання шифрування пропонується використовувати міні-ЕОМ.

Радіостанція виступає в якості каналу передачі даних. Оскільки радіостанція сприймає лише аналоговий сигнал, а для виконання операцій шифрування нам необхідна інформація у цифровому вигляді, проміжним елементом між радіостанцією та міні-ЕОМ, що вирішить дану проблему, буде аналогово-цифровий та цифрово-аналоговий перетворювач. Міні-ЕОМ буде виконувати функції шифрування та управління всією системою передачі, прийняття даних, зміни конфігурацій. Взаємодія з користувачем буде здійснювати за допомогою гарнітури під'єднаної до міні-ЕОМ.

Для програмної реалізації системи криптографічного захисту необхідно обрати ЕОМ, яка зможе виконувати поставлене завдання і за своїми показниками маси та габаритів не буде створювати додаткових незручностей при застосуванні особовим складом засобів радіозв'язку. Серед усіх класів ЕОМ найзручнішими для вирішення нашої задачі будуть представники класу міні-ЕОМ, які мають достатньо малі розміри. Необхідно лише обрати такий міні-ЕОМ обчислювальні можливості якого зможуть забезпечити виконання задачі. Ринок міні-ЕОМ представляють наступні зразки: *Raspberry Pi*, *Intel Galileo*, *Intel Edison*, *Hackberry*.

Представники сімейства *Intel* мають практично ідентичні характеристики і відрізняються лише процесором *Intel Quark*. За результатами тестів, не зважаючи на різницю у ціні процесор *Intel Quark* не є продуктивнішим за *ARM 11*, встановленим на *Raspberry Pi*, хоча і є більш коштовним.

Порівнявши основних представників ринку міні-ЕОМ, для вирішення задачі було обрано *Raspberry Pi*. Даний пристрій має достатні показники продуктивності для виконання завдання та має оптимальну ціну порівняно з іншими представниками свого класу за співвідношенням «продуктивність – ціна».

Окрім ЕОМ необхідно обрати операційну систему та мову програмування для розробки програмного модуля.

Даний апаратний засіб підтримує 7 схвалених спілкою розробників операційних систем. Переважна частина серед них розроблена на базі ядра *Linux*. Всі вони є відкритими і доступні для завантаження з офіційного сайту *Raspberry Pi*. Це такі

дистрибутиви як: *Raspbian*, *Snappy Ubuntu*, *OPENELEC*, *RASPBMC*, *Pidora*, *Arch Linux* та *Risc OS*, що не є дистрибутивом *Linux*.

Raspbian – операційна система, розроблена на базі операційної системи *Debian*. Ідея полягає у забезпеченні роботи більш ніж 10000 пакетів *Debian*, скомпільованих спеціально для *Raspberry Pi*. Такий підхід дозволяє забезпечити швидкодію необхідну для використання можливостей *Raspberry Pi* у повному обсязі.

Snappy Ubuntu – дистрибутив операційної системи *Ubuntu*. Дана операційна система розроблялася спеціально для апаратних платформ, що забезпечують роботу систем типу «розумний дім».

Для виконання задачі було обрано операційну систему *Raspbian*. Цей дистрибутив оптимізований спеціально під апаратну архітектуру *Raspberry Pi* і для даного пристрою має найбільшу швидкодію.

Для швидкої і якісної розробки програмного додатку необхідно використовувати мови програмування високого рівня. В наш час найбільш продуктивними та широкого вживаними мовами програмування є *C++*, *C#*, *Java*. Дані мови програмування є об'єктно-орієнтовані, що дозволяє розробникові будувати свій програмний додаток абстрагуючи предмети реального світу. Такий підхід дозволяє швидко побудувати зрозумілу та гнучку архітектуру з можливістю її зміни в подальшому.

Виходячи з обраної операційною системою для вирішення нашої задачі маємо можливість використовувати такі мови високого рівня як *Java* та *C++*.

Мова програмування *Java* – сучасна мова програмування заснована лише на об'єктно орієнтованому підході. *Java* є *C*-подібною мовою, але має значну кількість переваг порівняно зі своїм пращуром. Серед цих переваг: механізм обробки виключень, механізм автоматичної збірки сміття, чітка типізація, кросплатформеність. Завдяки наявності власної віртуальної машини код написаний на *Java* може бути запущений на будь-якій операційній системі. Крім того, віртуальна машина в рази зменшує ризик завдання шкоди своїм додатком власне операційній системі. А тому, застосування даної мови є більш безпечним.

Виходячи з огляду доступних операційних систем, серед існуючих дистрибутивів для роботи с *Raspberry Pi* обрано операційну систему на базі ядра *Linux* – *Raspbian*,яка розроблена і оптимізована спеціально для даного пристрою. Даний дистрибутив включає в себе підтримку віртуальної машини *Java*. Виходячи з цього та проаналізувавши доступні сучасні мови програмування, вирішення задачі буде здійснюватися саме за допомогою цієї мови програмування, оскільки вона є найбільш гнучкою та безпечною для застосування.

Більшість режимів роботи розробленого програмного додатку працюють із застосування потоків виконання, а отже він є багатопотоковим. При реалізації багатопотоковості та взаємодії між потоками виникали проблеми з створенням надмірної кількості потоків, що викликало помилку роботи віртуальної машини *Java*. Вирішення цієї проблеми було здійснено за допомогою застосування патерну проектування *Singleton* – одинак. Сутність цього патерну полягає у тому, що архітектура класу дозволяє створити лише один його об'єкт.

Також, оскільки більшість режимів є дуже схожими, було застосовано патерн проектування *Factory* (фабрика). Цей патерн дозволяє групувати в собі схожі за функціями класи для створення однотипних об'єктів від них. Реалізація фабрики можлива з застосуванням єдиного для усіх однотипних класів інтерфейсу.

Сутність роботи основних режимів роботи полягає в зчитуванні голосу, його шифруванні та відправці на визначені адреси. Виходячи з цього було вирішено ряд таких питань: запис звуку за допомогою *Java*, реалізація шифрування, розбиття потоку звуку на блоки для подальшого шифрування, визначення характеристик аудіо формату для забезпечення передачі голосового потоку у визначеному каналі, реалізація алгоритму Діффі-Хеллмана, обрахунок та збір пакетів при віддаленому оновлені конфігурацій, відтворення звуку.

Робота з аудіо у *Java* здійснюється в основному за допомогою *Java Sound API*. Робота *Java Sound API* заснована на концепції ліній та мікшерів. Мікшер представляє аудіо пристрій, який містить декілька ліній. Він не створений безпосередньо для змішування аудіо сигналів. За своєю структурою мікшер має декілька вхідних ліній (ресурсних) і одну результуючу (цільову). Об'єкти порти представляють собою конкретні об'єкти аудіо системи і можуть бути як і вхідними лініями для мікшера так і об'єктом результуючої. Лінія представляє собою звуковий потік. Аудіо потік, що проходить через цю лінію може бути одно- або багатоканальною(стерео звук, як приклад). Лінія(канал) може мати контролери(підсилити, відбити, захопити).

Для реалізації прийому і передачі голосу застосовується протокол *UDP* (*User Datagram Protocol*). Цей протокол не потребує підтвердження про доставку, а отже відправляє дані більш швидко ніж протокл, що потребує підтвердження про доставку (*TCP*). Оскільки при передачі голосового потоку відправляється велика кількість пакетів, втрата пакету не грає ролі і є майже непомітною. Отримавши встановленим буфером порції байт з цільового каналу, вміст буферу шифрується (якщо це захищений режим), формується пакет і відправляється на визначену адресу. Прийом відбувається за оберненою схемою. Пакет приймається, дешифрується та відправляється до ресурсного каналу (*SourceDataLine*).

Для вирішення задачі криптографічного захисту використовується симетричний алгоритм шифрування *DES*. Отримавши блок з цільового каналу вміст буферу шифрується 64-бітним ключем, після чого формується в пакет для відправлення. Дешифрування відбувається за зворотною схемою: вміст прийнятого пакету дешифрується.

Алгоритм Діффі-Хеллмана реалізується виконанням послідовності операцій:

1) генерація правила для обрахунку та публічного ключа стороною ініціатором;
2) обмін правилом;
3) генерація приватних ключів на обох сторонах;
4) виконання операцій за правилом над публічним ключем, застосовуючи приватний;
5) обмін результатами;
6) виконання операцій за правилом над отриманими результатами з застосуванням свого приватного ключа.

У результаті виконання останньої дії обидва користувачі мають однаковий ключ.

Розробка будь-якого програмного продукту передбачає поєднання багатьох процесів для забезпечення результату. Процеси безпосередньо пов'язані один з одним, оскільки результат виконання одного є основою для наступного. В основному процес розробки передбачає п'ять основних етапів: аналіз вимог, проектування, розробку, тестування, супровід. При розробці програмного модулю криптографічного захисту радіоканалу дотримувалась чітка послідовність процесів. На основі аналізу системи зв'язку тактичної ланки управління та завдань, що висуваються до даної системи, було сформовано вимоги, які визначили особливості проектування та розробки. Результати процесу проектування представлені діаграмами варіантів використання та діаграмою класів. Після розробки програмного продукту було проведено тестування на відповідність поставленим вимогам та можливості продукту. Тестування проводилось із застосуванням програмного продукту *WANem*, що забезпечує можливість симуляції каналів різної пропускної спроможності та втрату пакетів у каналів. Розроблений модуль при тестуванні показав спроможність виконувати завдання в повному обсязі.

Рецензент: викладач кафедри бойового застосування математичного та програмного забезпечення АСУ майор Шкіцькій В.В.

Павленко Я.А.

МОДЕЛІ ТА МЕТОДИ ВІЗУАЛЬНОГО АНАЛІЗУ ДАНИХ ПРО СТАН ЗАХИЩЕНОСТІ ЕЛЕМЕНТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ КІБЕРНЕТИЧНОГО ПРОСТОРУ

Створення високоефективних і багатофункціональних інформаційних систем (ІС) дозволяє на сьогоднішній день реалізувати їх в різних сферах життя сучасного суспільства. ІС дозволяють автоматизувати та підвищити ефективність обробки інформації шляхом застосування відповідного програмного і апаратного забезпечення. Проте використання ІС одночасно загострює і проблеми захисту ресурсів цих систем від загроз інформаційної безпеки. Однією з таких найбільш критичних загроз є можливість реалізації порушником інформаційних атак, спрямованих, наприклад, на порушення працездатності ІС або отримання несанкціонованого доступу до інформації, що зберігається в ІС, що є актуальним питанням, особливо коли автоматизація процесів управління військами визнається одним з пріоритетних напрямків розвитку ЗС України. Для протидії інформаційним атакам в даний час все частіше застосовуються спеціальні системи захисту – системи виявлення вторгнень.

В даний час інтенсивна поява і розростання інформаційного простору призводить до необхідності не тільки несанкціоновано поділити цей простір, а й контролювати й управляти процесами, які протікають в ньому. Для цього використовується, так звана, інформаційна зброя, яка представляє собою засоби знищення, перекручення або розкрадання інформації; обмеження санкціонованого допуску користувачів. Обороноздатність від такої атакуючої інформаційної зброї як комп'ютерні віруси, логічні бомби, засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікації інформації в каналах державного та військового управління, безпосередньо залежить від правильності і надійності систем мережевого захисту інформації, у тому числі засобів виявлення і запобігання мережевих атак.

Використання інформаційних мереж має ряд очевидних переваг, першочерговою з яких для ЗС України є підвищення оперативності прийняття та доведення рішень у процесі управління військами (силами). Але поруч з перевагами використання інформаційних мереж, існують і суттєві недоліки, основним з яких є підвищені вимоги до забезпечення безпеки функціонування та відмовостійкості таких мереж. Звісно, в сучасних операційних системах та іншому програмному забезпеченні використовуються технології, що забезпечують безпеку системи та попереджують про її можливий вихід із ладу. Але, як свідчить світовий досвід, цього не достатньо для забезпечення оперативного реагування на комп'ютерні атаки. Перегляд докладного звіту подій в системі виявлення вторгнень вручну через консоль це трудомісткий рутинний процес, що уповільнює аналіз даних та реагування на події в системі виявлення вторгнень. У зв'язку з цим розробка графічних інтерфейсів розподілених систем виявлення комп'ютерних атак із використанням методів візуалізації даних, набуває все більшого та перспективного розмаху у інформаційних технологіях.

Системи виявлення комп'ютерних вторгнень (*IDS – Intrusion Detection Systems*) – один з найважливіших елементів систем інформаційної безпеки інформаційної мережі органу військового управління (ОВУ), враховуючи, як зростає в останні роки число проблем, пов'язаних з комп'ютерною безпекою. Хоча технологія *IDS* не забезпечує повний захист інформації, проте вона грає досить помітну роль в цій галузі. Так як число і частота атак весь час збільшуються, стає дуже важливим ідентифікувати атаки на ранньому етапі їх розвитку і своєчасно зреагувати на них. У критичних випадках втручання в атаку має бути реалізовано набагато швидше, ніж зможе зреагувати людина.

Для забезпечення високої якості аналізу даних моніторингу об'єктів мережі адміністратором безпеки (далі користувачем) та візуалізації даних аналізу потрібен відповідний графічний інтерфейс, у складі якого має функціонувати підсистема управління компонентами системи виявлення вторгнень. Зазначений графічний інтерфейс має надавати користувачеві можливість зміни політики безпеки для різних компонентів системи виявлення атак (наприклад, модулів стеження) та отримання інформації від цих компонентів (наприклад, відомості про зареєстровану атаку).

Для ефективної діяльності персоналу потрібна безперервна робота системи виявлення вторгнень. У зв'язку з цим накопичується дуже великий файл з інформацією про діяльність системи. З досвіду можна сказати, що об'єм інформації, який потрібно обробити адміністратору, значно перевищує оптимальний об'єм, який він в змозі обробити. З цього випливає, що час реакції оператора системи на певну проблему в мережі не дає змогу оперативно реагувати на події, що відбуваються в мережі. Тобто потрібно автоматизувати рутинні операції обробки великої кількості подій щодо реагування на невідомі досі події.

Під візуалізацією даних розуміємо спосіб представлення багатовимірного розподілу даних на N-вимірній площині, при якому якісно відображені основні закономірності властиві вихідному розподілу – його кластерна структура, топологічні особливості простору, внутрішні залежності між ознаками, інформація про розташування даних у вихідному просторі.

До способів візуального або графічного представлення даних відносять графіки, діаграми, таблиці, звіти, списки, структурні схеми, карти і т.д.

Візуалізація традиційно розглядалася як допоміжний засіб при аналізі даних, проте зараз все більше досліджень говорить про її самостійну роль.

Багато сучасних засобів аналізу даних дозволяють будувати сотні типів різних графіків і діаграм. Тому вибір методу візуалізації, якщо він самостійно здійснюється користувачем, не такий простий і легкий, як може здатися на перший погляд. Одну і ту ж інформацію можна представити за допомогою різних засобів, для того щоб засіб візуалізації мав змогу виконувати своє основне призначення – представляти інформацію в простому і доступному для людського сприйняття вигляді – необхідно дотримуватися законів відповідності обраного рішення змістом відображуваної інформації та її функціональним призначенням. Іншими словами, потрібно зробити так, щоб при погляді на візуальне подання інформації можна було відразу виявити закономірності у вихідних даних та приймати на їх основі рішення.

Паралельні координати є одним з найбільш відомих методів візуалізації, і одними з найбільш поширених предметів наукових робіт у візуалізації. Вони є дуже потужним інструментом для розуміння багатовимірних числових наборів даних.

Цей метод представлення багатовимірних даних був винайдений Альфредом Інселбергом (*Alfred Inselberg*) в 1985 році.

У паралельних координатах змінні кодуються по горизонталі, вертикальна лінія визначає значення змінної. Цей метод може обробляти кілька факторів для великого числа об'єктів на одному екрані, так що задовольняє критерію різноманітності даних. Всі фактори даних для аналізу розміщені на одній осі, а відповідні значення об'єкта даних у відносній шкалі розміщені на іншій. Кожен об'єкт даних представлений низкою пов'язаних траверс ліній, показуючи своє місце в контексті інших об'єктів.

Оскільки метод заснований на відносних величинах, це вимагає обчислення мінімального і максимального значень для кожного фактора. У той час як значення змінюються між мінімальним і максимальним значеннями кожного фактора, немає ніякої потреби в перефарбовуванні всіх зображень, але для випадку, коли значення перевищує ліміт, ми повинні перефарбувати зображення, щоб показати адекватну візуалізацію. Такий підхід може бути використаний для візуалізації динамічних даних.

Основною перевагою методу паралельних координат є те, що чинник упорядкування даних не впливає на загальне сприйняття діаграм, а також метод дозволяє аналізувати як весь набір даних об'єктів відразу, так і окремі об'єкти даних.

Основними недоліками є:

- обмеження числа факторів, що показуються відразу;
- візуалізація динамічних даних закінчується зміною представлення даних.

Одним з важливих аспектів візуалізації інформації – є масштабованість. Паралельні координати забезпечують більшу масштабованість для багатовимірної розмірності. Вони дозволяють гіперрозмірним зразкам бути проаналізованими та призводять до більш швидкого розуміння даних. У цього методу немає теоретичної межі в числі параметрів, які можуть бути візуалізованими. Тому, можливо збільшити масштаб додатку, з приростом представляючи нові параметри візуалізації в міру необхідності. Крім того, це не становить зміщення ні для якої певної розмірності, при показі видних тенденцій, кореляцій і розбіжностей від необроблених даних. Ці переваги дозволяють отримати критичне розуміння потоків у трафіку під час тесту і встановити надійні інтуїтивні гіпотези. Навіть якщо невідома атака відбувається, певний зразок зображення може бути отриманий, і атака може бути виявлена вчасно.

Багато технологій виявлення вторгнень мають деякі слабкі місця. Звичайні системи виявлення вторгнень, які засновані на відомих сигнатурах атак, не можуть виявляти невідомі атаки. Крім того, системи виявлення вторгнень на основі аномалій механізмів виявлення часто генерують великий ряд помилкових тривог, які значно завантажують адміністраторів безпеки. Крім того, традиційні системи моніторингу, такі як *IDS* і міжмережеві екрани забезпечують елементарний рівень відображення результатів візуально. Один з перспективних підходів є візуалізація – оброблення складних ситуацій, використовуючи інтуїтивний метод.

Візуальні зображення можуть бути отримані з вихідних даних з використанням графічних комп'ютерних технологій та алгоритмів. Ефективна зв'язка людського розуму з сучасним комп'ютером представляє ключову технологію для добування нових знань. Візуальне представлення набирає все більш і більш важливого значення в області виявлення вторгнень.

Приведемо простий спосіб для візуалізації Інтернет-атаки на паралельних координатах. Особливістю методу паралельних координат є властивість представлення більш ніж трьох полів у двовимірному просторі. Для того щоб візуалізувати найвідоміші атаки, такі як інтернет-хробаки, відібрано чотири важливих поля, доступних для кожного потоку. У результаті, можна розробити дев'ять графічних підписів для виявлення нападу, у тому числі інтернет-хробаків, *DDoS* атак і мережевого сканування.

Ефективність пропонованого підходу візуалізації має місце на реальному мережевому трафіку з метою виявлення прихованого нападу та з використанням потоків. Потік є одним із мережевих з'єднань і може складатися з мільйонів пакетів.

Мережеві потоки, використовуючи ретельно підібрані значення утворюють унікальний графічний образ для кожного вторгнення.

Існують три основні переваги при застосуванні візуалізації даних щодо проблеми виявлення вторгнень. По-перше, візуалізація атаки здійснюється на основі неоднорідних даних. Мережевий трафік має складну структуру, що потребує співвіднесення кількох змінних, таких як адреса джерела, адреса призначення, номер порта і довжина пакету та прапор *TCP*. Проте візуалізація атаки дозволяє представити ситуацію в інтуїтивно зрозумілій формі. По-друге, візуалізація атаки не вимагає розуміння складних математичних або статистичних алгоритмів. Візуальні образи дають загальні уявлення на основі яких виконується оцінка про вторгнення. По-третє, візуалізація атаки дозволяє отримати цінну інформацію з аналізованих даних і вивести нові гіпотези.

З метою розробки візуального механізму найпопулярніших інтернет-атак, таких як *DDoS* атаки, атаки хробака, або мережеві сканування, їх характеристики повинні бути розглянуті в умові візуалізації. Ці атаки мають одну спільну особливість, яка називається «один-до-багатьох» між атакуючими і жертвою, у той час як стандартні потоки інформації мають відношення один-до-одного. Це сприятливий момент для візуалізації атаки. Атака *DoS* являється атакою на комп'ютерну систему або мережу, що призводить до відмови в обслуговуванні, як правило, до втрати зв'язку та послуг мережі, споживаючи пропускну здатність цільової мережі або перевантаження обчислювальних ресурсів цільової системи. У розподіленої атаки *DoS*, атакуючою стороною часто виступає особливий вузол з широкосмуговим підключенням до Інтернету, що було скомпрометовано вірусами або троянськими програмами, дозволяючи злочинцю дистанційно керувати комп'ютерами, часто через мережу бот мережу.

Використання методу паралельних координат дозволяє представити атаки на площині, що має ряд переваг:

1. Немає відхилення у бік будь-якої конкретної розмірності.
2. Відсутні обмеження по числу параметрів.
3. Візуалізація кореляцій і відхилень від вихідних даних.

Паралельні координати можуть бути використані для опису атаки в графічному зображенні. Координати представляють чотири різних параметри. Перший являє собою адресу джерела кожного потоку, другий - адресу призначення, третій - порт призначення і четвертий представляє середню довжину пакету кожного потоку. Ці чотири значення, наведені в кожному потоці, дозволяють відобразити надходження пакетів за певний час у вигляді зв'язної лінії з паралельними координатами. Таким чином, одна лінія представляє одне з'єднання.

Аналіз результатів досліджень та публікацій, а також досвіду експлуатації СВА, показав, що сучасні СВА з відкритим кодом, наприклад, *NetSTAT, OSSEC, Bro, Snort, Prelude* збирають значну кількість інформації, але жодна з них, не покриває всі рівні спостереження за ІС, та не є адаптивною для виявлення атак невідомих класів. Дослідження показують, що у теперішній час, однією з найбільш ефективних систем виявлення вторгнень є СВА *Prelude*, завдяки своїм широким можливостям щодо виявлення та реагування на кібернетичні атаки. СВА *Prelude* дозволяє забезпечити аналіз як даних з локальних системних джерел, так і мережевих даних, має додаткові механізми, що забезпечують безпеку її компонентів, а також має найменше недоліків як в архітектурі, так і в реалізації, основними з яких є відсутність адаптивності до невідомих атак і неможливість аналізувати поведінку розподіленої ІС на всіх рівнях одночасно.

Таким чином, один з напрямків удосконалення СВА *Prelude*, є розробка моделей та методик візуалізації даних АБ та спеціального програмного забезпечення, яке підвищує ефективність його роботи під час виявлення кібернетичних атак на ІС ОВУ, яка підлягає захисту, під час її функціонування.

В рамках роботи було спроектовано та розроблено СППР, яка у режимі реального часу здатна відслідковувати зміни, що викликають потік інформації до сховища даних, їх аналіз та виведення на екран попередження про спробу чи реалізацію комп'ютерного вторгнення. СППР на основі сигнатур СВВ *Prelude* має функціональні можливості відображення атак та суб'єктів атаки за останні 24 години, за розподілом часу, а також графічно представляти виявлення підозрілої активності. Все це дає змогу адміністратору безпеки в режимі реального часу відслідковувати зміни, що відбуваються в мережі та приймати невідкладні рішення щодо подальших дій.

Рецензент: начальник кафедри бойового застосування математичного та програмного забезпечення АСУ д.т.н., доцент полковник Субач І. Ю.

Парнюк І.О.

ЗАПОБІГАННЯ НЕПРОДУКТИВНОГО ЗАСТОСУВАННЯ ПЕОМ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ ПРОЦЕДУР КОНТРОЛЮ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

На сьогоднішній день автоматизація здійснення певних дій займає вагоме місце в житті суспільства, особливо якщо ці дії однотипного характеру. Дана тема являється актуальною, оскільки аналогів автоматизованого програмного контролю за роботою ПЕОМ не існує на даний момент. Можливість керувати роботою процесів віддалено надає змогу контролювати процес роботи ПЕОМ, що робить можливим звершувати небажані або небезпечні процеси, які можуть якимось чином принести шкоду даним, програмному забезпеченню, апаратній складовій контрольованого вузла.

Контроль за використанням ПЗ – це процес забезпечення досягнення об'єктом, який здійснює контроль, своїх цілей.

Контроль – одна з основних функцій системи управління. Контроль здійснюється на основі спостереження за поведінкою керованої системи з метою забезпечення оптимального її функціювання (вимірювання досягнутих результатів і співвіднесення їх із очікуваними результатами). На основі даних контролю здійснюється адаптація системи, тобто, прийняття оптимальних управлінських рішень.

Функція контролю – це така характеристика управління, яка дозволяє виявити проблеми і скорегувати діяльність ПЗ до того, як ці проблеми переростуть в кризу. Контроль базується на трьох основних елементах:

- встановлення контрольованих стандартів діяльності;
- вимір і аналіз результатів діяльності, інформація про які отримана за допомогою контролю;
- коректування технологічних, господарських та інших процесів у відповідності зі зробленими висновками і прийнятими рішеннями.

Без надійної системи контролю жодна організація не може успішно функціонувати. Виділяють наступні завдання систем контролю:

- по-перше, контроль дозволяє виявити у зовнішній або внутрішньому середовищі організації фактори, які можуть зробити істотний вплив на її функціонування і розвиток, і своєчасно на них відреагувати.
- по-друге, контроль допомагає розкрити неминучі в діяльності будь-якої організації порушення, вади, помилки і оперативно вжити заходів щодо їх усунення.
- по-третє, результати контролю служать основою для оцінки роботи організації та її персоналу за певний період, ефективності та надійності системи управління нею.

Таким чином, можливо виділити основні причини необхідності контролю роботи ПЗ, яке встановлено на ПЕОМ:

- невизначеність – зміна законів, технологій, умов конкуренції приводять до необхідності до постійного коригування планів через систему зворотного зв'язку, яку забезпечує контроль.
- попередження кризових ситуацій – одне з головних призначень контролю - виявити проблеми і скоригувати діяльність організації до того, як ці проблеми переростуть в кризу.
- підтримання успіху – в будь-якій організації важливо визначити, які напрямки діяльності найбільш ефективно сприяють досягненню цілей і підтримувати саме ці сфери діяльності.

Модель контролю ПЗ не змінюється на етапах життєдіяльності процесу контролю та містить чотири етапи.

На першому етапі відбувається визначення параметрів функціонування і розвитку програм, які необхідно згодом контролювати, і джерел інформації про них.

На другому етапі створюється модель системи управління програми, у якій відбиваються потоки ресурсів, інформації, точки утворення проміжних і кінцевих результатів, а також найбільш підходящі моменти для здійснення контрольних дій – так звані «точки контролю».

Третій етап полягає в отриманні інформації про реально досягнуті результати і зіставленні її з відповідними нормативами, що дозволяє визначити, чи є відхилення від стандартів, чи знаходяться вони в допустимих межах і чи не час здійснювати коригувальні дії.

Четвертий етап процесу контролю полягає в коригуванні діяльності програми, модифікації цілей, перегляд планів, перерозподілі завдань, вдосконаленні технологій виробництва і управління .

Системи контролю програмного забезпечення можуть бути різними як за принципом дії так і за призначенням. В основному системи контролю можна класифікувати за такими основними ознаками, як:

- за способом доступу;
- за типом впливу на вузол;
- за типом ресурсів, що контролюються;
- за принципом роботи;
- за періодом контролю;
- за способом сповіщення адміністратора.

Для локального контролю вузлів, використовують антивірусну програму (антивірус) – програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом .

Для контролю доступу до системи, яка знаходиться в мережі, використовують системи виявлення атак (вторгнень) – програмні або апаратні засоби, призначені для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет (відповідний англійський термін – *Intrusion Detection System (IDS))*. Системи виявлення вторгнень забезпечують додатковий рівень захисту комп'ютерних систем разом з системою запобігання вторгненням (*IPS* –англ. *Intrusion Prevention System*) .

Системи IPS класифікують наступним чином:

- мережеві *IPS (Network – based Intrusion Prevention, NIPS)* – відстежують трафік в комп'ютерній мережі і блокують підозрілі потоки даних;
- *IPS* для бездротових мереж *(Wireless Intrusion Prevention Systems, WIPS)* – перевіряє активність в бездротових мережах. Зокрема, виявляє невірно сконфігуровані точки бездротового доступу до мережі, атаки людина посередині, спуфинг *MAC*-адрес;
- поведінковий аналіз мережі *(Network Behavior Analysis, NBA)* – аналізує мережевий трафік, ідентифікує нетипові потоки, наприклад *DoS* і *DDoS* атаки;
- система попередження вторгнень для окремих комп'ютерів *(Host – based Intrusion Prevention, HIPS)* – резидентні програми, які виявляють підозрілу активність на комп'ютері.

Часто системи виявлення атак працюють разом із брандмауером, який використовується як інструмент для захисту. Система виявлення атак керує фаєрволом (брандмауером), виконуючи різноманітні блокування на встановлені проміжки часу, створюючи і видаляючи правила роботи брандмауера. Брандмауер – програмне або програмно-апаратне рішення, яке налаштоване, щоб допускати, відмовляти, шифрувати, пропускати через проксі весь комп'ютерний трафік між областями різної безпеки згідно з набором правил та інших критеріїв вузла інформаційної системи .

Віддалене адміністрування необхідне для зручності контролювання вузла або при неможливості локального контролю. Існує декілька програмних засобів, які дають можливість віддаленого контролю.

Система навчання являється складним ієрархічним об'єктом, який містить в собі множини різних об'єктів та суб'єктів різного призначення. Данні множини організують підсистеми. В останні роки ПЕОМ стала не від'ємною складової системи навчання, їх множина об'єднана метою підготовки фахівця складає підсистему інформаційного забезпечення навчального процесу.

Віддалений контроль дозволяє адмініструвати ПЕОМ практично із будь-якого місця за допомогою дротового або бездротового з'єднання. Система віддаленого контролю може функціонувати тільки при наявності розгорнутої інформаційної мережі, тому можливо абстрагуватись від фізичного, канального і мережевого рівнів моделі *OSI*.

Система контролю буде розрізняти небажані та шкідливі процеси, які можуть порушити нормальну роботу вузла, який контролюється. Це одне із завдань, яку повинно вирішуватись без втручання користувача і прийняття рішення у разі переключення на автономний режим роботи. Цю задачу вирішує система штучного інтелекту – це штучних системи, створених людиною на базі ЕОМ, що імітують розв'язування людиною складаних творчих завдань.

Розрізняють три види інтелектуальних АС:

- інтелектуальні інформаційно-пошукові системи (системи типу «запитання–відповідь»), які в процесі діалогу забезпечують взаємодію кінцевих користувачів – які не є програмістами і базами даних та знань з професійними мовами користувачів, близьких до природних;
- розрахунково-логічні системи, які дають змогу кінцевим користувачам, що не є програмістами та спеціалістами в галузі прикладної математики, розв'язувати в режимі діалогу з ЕОМ свої задачі з використанням складаних методів і відповідних прикладних програм;
- експертні системи, які дають змогу провадити ефективну комп'ютеризацію областей, у яких знання можуть бути подані в експертній описовій формі, але використання математичних моделей утруднене або неможливе.

Інтелектуальною системою для застосування вирішено обрати експертну систему, так як вона має наступні переваги:

- переважає можливості людини при вирішенні надзвичайно громіздких проблем;
- не має упереджених думок, тоді як експерт може користуватися побічними знаннями і легко піддається впливу зовнішніх факторів;
- не робить поспішних висновків, нехтуючи певними етапами знайдення рішення;
- забезпечує діалоговий режим роботи;
- дозволяє роботу з інформацією, що містить символьні змінні;
- забезпечує коректну роботу з інформацією, яка містить помилки, за рахунок використання ймовірнісних методів досліджень;
- дозволяє проводити одночасну обробку альтернативних версій;
- за вимогою пояснює хід кроків реалізації програми;
- забезпечує можливість обґрунтування рішення та відтворення шляху його прийняття.

Експертні системи досить давно використовуються у діагностиці, зокрема у медичній та автомобільній. Також ЕС використовують в прогнозуванні, плануванні, контролі, управлінні та навчанні. Процес створення експертних систем значно змінився за останні роки. Завдяки появі спеціальних інструментальних засобів побудови

експертних систем значно скоротились терміни та зменшилась трудомісткість їх розробки.

Головна відмінність ІС і ЕС від інших програмних засобів - це наявність бази знань (БЗ), у якій знання зберігаються у формі, зрозумілій фахівцям предметної області і можуть бути змінені і доповнені також у зрозумілій формі. Це і є мови представлення знань – МПЗ.

Для вирішення завдань, поставлених перед розроблюваною системою, будуть використовуватися індуктивні типи логічного виведення, евристичні типи логічного виведення, судження по замовчуванню та судження за аналогією.

Подання інформації про поводження експертної системи в процесі формування ланцюжка логічного виведення при пошуку рішення є важливим.

Види пояснень виділяють такі:

- каузальні пояснення;
- пояснення через закон;
- функціональні пояснення.

Методи формування пояснень – призначені для пояснення вихідних даних у світлі закладених в експертну систему знань і одержання відповідей на питання про те, як і чому система прийшла до деякого висновку, чому вона розмірковувала саме так: чому рекомендація системи є правильною і т.п.

Методи формування пояснень – призначені для пояснення вихідних даних у світлі закладених в експертну систему знань і одержання відповідей на питання про те, як і чому система прийшла до деякого висновку, чому вона розмірковувала саме так: чому рекомендація системи є правильною і т. п. Виділяють такі методи формування пояснень:

- метод фіксації ситуацій;
- метод трасування.

На основі проведених аналізів, було обрано метод трасування, який використовує при породженні пояснень слід (трасу) судження, проведеного експертною системою. Метод широко поширився при розробці блоків пояснення в системах, заснованих на поданні евристичного знання у формі продукцій.

Для оцінки отриманих результатів, буде приведено порівняльну характеристику відомого програмного продукту *Radmin,* який може використовувати в якості аналогу для розробленого програмного продукту.

Проблема програмного продукту *Radmin* саме у тому, що він не має можливості автоматизованого контролю. Адміністрування у даному в випадку здійснюється виключно за участі адміністратора. При умові, що контроль буде здійснюватися кожні 5 хвилин, і при контролюванні мережі, яка містить у собі 1 комп'ютерний клас з 10 ПЕОМ, адміністратор буде витрачати для циклу контролю близько 2-2,5 хвилини. Для такої кількості вузлів час являється припустимим. Але якщо їх кількість зросте до 20, то адміністратор буде вимушений виконувати процедуру контроль у безперервному порядку. З подальшим збільшенням кількості ПЕОМ своєчасний контроль стане неможливим за умови використання програмного продукту *Radmin.*

Для розробленого програмного модуля час, який витрачається для аналізу складає приблизно 30 мілісекунд. Даний процес виконується виключно на кожному вузлові, що контролюється, тому час аналізу не залежить від їх кількості.

Рецензент: викладач кафедри бойового застосування математичного та програмного забезпечення АСУ майор Шкіцькій В.В.

Поліщук І.Г.

МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОЦІНКИ ЗАЛЕЖНОСТІ МІЖ ЧАСОМ ПРИЙНЯТТЯ РІШЕННЯ ТА ОСНОВНИМИ ЕРГОНОМІЧНИМИ ПАРАМЕТРАМИ ІНТЕРФЕЙСУ ОПЕРАТОРА

Прогрес науки і техніки обумовив поширення складних технічних систем. Головна роль людини в таких системах, складність аналізу інформації і реалізації функцій управління стали основою для комплексу досліджень різноманітних сторін проблеми поєднання технічних засобів та операторів. Актуальність тематики постійно зростає, оскільки теорія і практика показують, що неможливо повністю автоматизувати складні процеси управління та обробки інформації. Одним із головних напрямків досліджень є розробка рекомендацій щодо врахування психофізіологічних можливостей і здібностей людини при взаємодії з технічною системою. Особливо важливим даний напрямок при оперативному прийнятті рішень, де функції оператора зводяться до прийому і аналізу інформації, прийнятті рішень в режимі реального часу.

Сучасні технології проектування автоматизованих систем надають потужні інструменти їх реалізації. Однак можуть виникати ситуації, коли технічно ідеально спроектована система не виправдовує очікувань і дуже часто це відбувається через недостатнє врахування людського фактору в процесі проектування.

Невід'ємною частиною будь-якого програмного продукту, який призначений для використання в режимі реального часу, є інтерфейс оператора. Він об'єднує в собі всі елементи і компоненти програми, які здатні впливати на взаємодію оператора з програмним забезпеченням. Інтерфейс за допомогою інструментальних засобів «збирається» з готових елементів – «кубиків». Однак з одних і тих же кубиків можна «побудувати» інтерфейси різної якості та з різними ергономічними властивостями.

На даний час інтерфейси більшості інструментальних систем, з якими доводиться мати справу розробникам програмного забезпечення, відносяться до класу так званих офісних інтерфейсів, які беруть свій початок від офісних систем. Інтерфейси же програм автоматизованих систем наукових досліджень і автоматизованих систем управління технологічним процесом, відносяться до класу інформаційно-керуючих, ергономіка яких кардинально відрізняється.

В цілому правильна розробка інтерфейсу оператора дозволяють забезпечити:

- високу продуктивність роботи оператора, тому що оператор отримає і буде використовувати засоби, що легко сприймаються при вирішення професійних завдань з мінімальним ризиком зустріти труднощі або перешкоди;
- малий час навчання - оператору буде достатньо вивчити одну систему і отримані знання та навички стануть базовими при використанні інших систем;
- скорочення часу розробки - не буде необхідності проектувати кожну компоненту окремо, оскільки з'являться попередньо розроблені відповідно до нормативів універсальні програмні компоненти.

Використання цих компонент в поєднанні з керівництвами по людино-комп'ютерним інтерфейсам, формам, що деталізуються, застосування цих компонент на рівні конкретних типів додатків, дозволить мінімізувати відмінності інтерфейсів і буде сприяти скороченню часу розробки.

Проектування інтерфейсу становить самостійну проблему, яка найчастіше перевершує по складності проблему розробки кодів програми, і вимагає, як і процес проектування будь-якої складної системи, відповідних методів, засобів. Тому розробники програмного забезпечення відокремлюють, принаймні концептуально, функціональне призначення програмних продуктів від проблем, пов'язаних з

організацією взаємодії оператора з цими продуктами. Такий поділ є необхідною умовою створення інтерфейсів, що забезпечуватимуть ефективну роботу оператора.

Елементи інтерфейсу оператора технічної системи:

- засоби відображення інформації, пристрої та технології введення даних;
- відображувана інформація, формати і коди;
- командні режими, мова оператор-інтерфейс;
- сценарії діалогу і самі діалоги;
- зворотний зв'язок з оператором;
- підтримка прийняття рішень у конкретній предметній області;
- порядок використання програми і документація на неї.

Основними принципами проектування інтерфейсу є мінімізація зусиль оператора при виконанні роботи:

- скорочення тривалості операцій читання, редагування і пошуку інформації;
- зменшення часу навігації і вибору команди;
- підвищення загальної продуктивності оператора, що полягає в обсязі оброблених даних за певний період часу;
- збільшення тривалості стійкої роботи оператора.

Проблеми, що виникають на етапі розробки прототипу інтерфейсу оператора та варіанти їх вирішення:

1. Врахування особливостей пристроїв введення/виводу інформації, що використовуються оператором.
2. Специфіка інтерактивних елементів, пов'язана з вибором платформи, стандартних бібліотек.
3. Вибір технології та методів ведення діалогу програми з оператором.
4. Розміщення інформації та керуючих елементів у полі екрана, у вікні. При композиції екрану необхідно враховувати обмежені розміри простору екрану, в зв'язку з чим виникає задача оптимального розташування максимально можливого обсягу інформації.
5. Формування зворотного зв'язку між оператором і додатком.
6. Проектування панелей меню та інструментів і вибір пунктів в них.
7. Розробка засобів орієнтації та навігації.
8. Створення форм для введення даних.

З точки зору експлуатаційних характеристик прикладних програм значення для оператора інтерфейсу як засобу комунікації важко переоцінити. Характеристики інтерфейсу майже повністю визначаються тривалістю часу, необхідного для навчання оператора роботі з системою, таким чином, з'являється і соціальний аспект. Послідовно розроблений і логічний інтерфейс спрощує освоєння та використання системи, зменшує частоту помилок оператора і, завдяки цьому, збільшує ефективність її використання.

Ефективність інтерфейсу полягає у швидкому розвитку у операторів простої концептуальної моделі взаємодії, що досягається через узгодженість. Концепція узгодженості полягає в тому, що при роботі з комп'ютером у оператора формується система очікування однакових реакцій на однакові дії. Іншою складовою інтерфейсу є властивість його конкретності та наочності. Воно забезпечується застосуванням в панелях різних кольорів та інших виразних засобів. Ідеї та концепції потім знаходять фізичне відображення на екрані, з яким безпосередньо взаємодіє оператор.

Ініціатором діалогового процесу є людина, яка вибирає мету і в якійсь мірі може впливати на способи її досягнення за допомогою запитів. Система забезпечує адекватну реакцію на запити оператора технічної системи. Діалог є автоматизованим методом вирішення слабоформалізованих завдань. При цьому розподіл функцій між людиною і комп'ютером наступний: людина ставить завдання, а система надає засоби для

вирішення під задач. Потім виконує об'єднання результатів, а прийняття проектних рішень залишається за людиною.

Створення якісного інтерфейсу, який можна назвати точкою зв'язку між людиною і комп'ютером, є кінцева мета вивчення людино-комп'ютерного взаємодії.

В операторів технічних систем зорова система виступає як пороговий засіб, оскільки виявлення сигналу, що відображається на екрані, стає можливим при перевищенні певних світлових характеристик чутливості ока оператора. Його залежність від умов роботи вивчені не достатньо. Встановлено, що величина абсолютного часового порогу коливається в межах тисячних і сотих секунди і залежить від інтенсивності світлового спалаху: чим він більше, тим менший часовий поріг, і навпаки.

Однакову інформацію можна представити у різному вигляді. Необхідною умовою є відповідність вимогам адекватності інформаційної моделі. Але в різних випадках на аналіз інформації оператор технічної системи може витрачати різний час. Тому інформаційна модель повинна адекватно відповідати не лише дійсності, але враховувати можливості людини по оперативній обробці інформації.

В оператора на основі аналізу отримуваної інформації виникає власне представлення про стан об'єктів, яке прийнято називати концептуальною моделлю. Для її формування оператору необхідний певний час. Чим ближча інформаційна модель до концептуальної, тим вища пропускна спроможність оператора технічної системи.

Інформаційна модель може містити дані з різними пріоритетами. В залежності від цього розрізняють детальні та інтегральні інформаційні моделі. Детальні моделі містять точні дані про об'єкти та їх параметри, за якими оператор може приймати рішення відносно кожного об'єкта. Інтегральні моделі необхідні на вищих рівнях, там, де приймаються важливі рішення. Вони дозволяють дати лише якісну оцінку ситуації. В залежності від задач, які вирішує оператор, необхідно використовувати детальні, інтегральні моделі або їх поєднання. В окремих випадках це сприяє підвищенню пропускної спроможності оператора.

Загального вирішення проблеми, щодо визначення кількості необхідної інформації, яку одночасно можна представити оператору технічної системи, поки що немає. В даний час досліджуються лише окремі процеси прийому і обробки інформації. При цьому складність обрахунку максимальної кількості інформації, що передається людині в різних видах діяльності, додає складності при розрахунках часу її передачі. Дана проблема вирішувалась дослідниками по різному. В одних випадках в якості міри часу брали інтервал між моментом появи сигналу і початком певної реакції у відповідь (латентний період реакції), в других – мінімальний час експозиції сигналу, необхідний для того, щоб отримати адекватну відповідь, в третіх випадках – середній час на передачу одного сигналу.

Якщо оператор повинен здійснювати перебір всіх елементів інформаційної моделі або пошук необхідних йому елементів, то оцінити затрати часу на інформаційний пошук можливо, знайшовши добуток математичного сподівання числа кроків в пошуку на середню довжину кроку. При незмінно високих затратах часу необхідно відшукувати нові способи кодування.

Важкість оцінки пропускної спроможності полягає також в її залежності від характеру задачі, яка вирішується оператором, і ступені його участі в роботі конкретної системи. Тому неможливо говорити про певну «загальну» пропускну спроможність.

Різноманітні проведені досліди отримали суперечливі дані про пропускну здатність зорової системи людини – від 50 до 600 млн. двійкових одиниць в секунду. Дані результати отримані на різних моделях і в різних умовах, тобто фактично вони характеризували лише певне миттєве значення пропускної спроможності. Необхідно також вивчити зміну пропускної здатності зорової системи в ході діяльності.

Вимірювання пропускної спроможності в більшості випадків обмежувалось мовною реакцією, що використовувалась в якості індикатора впізнання. Операції

передачі збільшують час пропускної спроможності. Будь-яке ускладнення моторної відповіді на вхідну інформацію призводить до зменшення пропускної спроможності. Як наслідок, для підвищення пропускної спроможності людини необхідно максимально спростити моторну реакцію.

Якщо швидкість надходження вхідної інформації переважає можливості людини, він допускає різного роду помилки:

- пропускання і спотворення сигналів (помилка розпізнання, неадекватна реакція);
- затримка в передачі певних сигналів;
- фільтрація потоку інформації (вибір сигналів певної категорії);
- пропускання деяких ознак сигналів, що призводить до втрати частини інформації;
- відмова від вирішення задачі, призупинення діяльності.

Дослідження показали, що основним видом помилок при перевантаженні – втрати інформації в результаті пропуску частини вхідних сигналів. Якщо потік інформації стає занадто великим і продовжує зростати тривалий час, наступає зрив діяльності людини. В подібних випадках необхідно змінити умови роботи оператора.

Слід зазначити, що необхідно враховувати монотонність і невелику кількість зовнішніх впливів, які також призводять до збільшення помилкових дій, зниження емоційного тонусу, появи сонливості тощо. Тому при створенні пристроїв відображення інформації важливо орієнтуватись не лише на оптимальну пропускну спроможність але і на мінімальну, що забезпечуватиме підтримку активної діяльності оператора.

При дослідженні теоретичних питань пов'язаних з проведенням експериментів, важливу роль відіграє дослідження помилок і невизначеностей. Результати всіх експериментів містять помилки, які можуть бути суттєвими. Жоден експеримент неможливо спланувати без ретельного вивчення даного важливого фактора. Якщо невизначеності ігноруються чи оцінюються недбало, це може призвести до втрат часу і роботи. Технічні прорахунки можуть призвести до різного роду небезпечних відмов і неполадок.

В теоретичних роботах по математичній статистиці вивчається велика кількість різних розподілів. На даному етапі розглянемо нормальну криву помилок, яка називається *розподілом Гаусса*. Формула для даного розподілу виводиться на основі двох допущень:

1. Остаточна помилка будь-якого вимірювання являє собою результат великої кількості дуже малих помилок, розподілених випадково.
2. Додатні і від'ємні відхилення відносно істинного значення рівно ймовірні.

Статистична обробка результатів вимірювань основана на теоремі Чебишева і Бернуллі. Відповідно до *теореми Чебишева* середнє арифметичне з виміряних результатів експериментальних досліджень при необмеженому збільшенні числа вимірювань співпадає по імовірності із математичним сподіванням. Відповідно до *теореми Бернуллі* частота подій при необмеженій кількості вимірювань приходить до імовірності даної події.

На практиці можемо отримати кінцеве значення невеликої кількості вимірювань. Тому за їхніми результатами можливо лише приблизно робити висновки про дійсні значення імовірнісних характеристик.

Рецензент: доцент кафедри бойового застосування математичного та програмного забезпечення АСУ к.т.н., доцент підполковник Хусаінов П.В.

Рубановський П.В.

МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ РОЗРАХУНКУ АРТИЛЕРІЙСЬКОГО ВОГНЮ

Проблема автоматизації розрахунку артилерійського вогню пов'язана із використанням застарілих засобів розрахунку артилерійського вогню під час проведенням Антитерористичної операції на сході України. Наземна артилерія є важливою ланкою під час проведення Антитерористичної операції на сході України, так, як ураження цілі найбільше припадає на артилерію. Проте, на даний час розрахунок артилерійського вогню роблять вручну, що займає досить довгий час. Тому, проблема автоматизації артилерійського вогню залишається відкритою.

Актуальним підходом до вирішення даної проблеми є розробка та застосування програмного забезпечення автоматизації розрахунку артилерійського вогню, яке дозволить зменшити час розрахунку артилерійського вогню та збільшити точність ураження цілі.

Значення артилерії як головної вогневої сили Сухопутних військ було завжди високим і залишається таким сьогодні. У ході проведення Антитерористичної операції на сході України на частку артилерії припадало до 70% усіх завдань з вогневого ураження противника.

Наземна артилерія в залежності від обставин та характеру цілей (об'єктів) виконує завдання з ураження наземних елементів систем високоточної зброї, артилерії, танків, БМП (БТР), протитанкових та інших вогневих засобів, живої сили, вертольотів на посадкових майданчиках, пунктів управління, засобів ППО, радіоелектронних засобів противника; руйнування фортифікаційних споруд; дистанційного мінування місцевості.

Крім того, артилерія може виконувати завдання світлового забезпечення бойових дій військ вночі, задимлення місцевості, цілевказівки і доставки в розташування противника агітаційного матеріалу.

Збереженню ролі артилерії сприяють якісні зміни, що відбуваються в її озброєнні. Це насамперед розроблення і прийняття на озброєння артилерійських боєприпасів підвищеної потужності, високоточних боєприпасів та боєприпасів для дистанційного мінування місцевості, модернізація та удосконалення всіх видів артилерії, засобів автоматизованого управління вогнем та засобів артилерійської розвідки.

Артилерія володіє великою потужністю, точністю вогню і дальністю стрільби, має великі можливості для широкого маневру та зосередження вогню в короткий термін і на велику глибину. Артилерія може уражати різноманітні цілі, які розташовані відкрито та приховано, рухомі й нерухомі, спостережні, наземні та надводні.

До позитивних якостей артилерії належить також практична незалежність від ступеня ППО противника і метеорологічних умов. Досвід АТО свідчить, що за складних метеорологічних умов і відсутності застосування авіації у вогневому ураженні противника, на артилерію покладається до 90 % усіх вогневих завдань.

Вищезазначені якості дозволяють зробити висновок, що сучасна артилерія є найбільш дієвим та ефективним засобом ураження противника і вогневої підтримки загальновійськових підрозділів і частин у сучасному бою. В обороні артилерія наносить рішуче ураження противнику на підступах до оборони, перед переднім краєм і вглибині оборони наших військ. У наступі артилерія своїм вогнем знищує вогневі засоби і живу силу противника, руйнує його оборонні споруди, які перешкоджають успішному просуванню наших механізованих і танкових військ.

Під час проведення АТО на сході України використовують таку наземну артилерію:

– самохідна гаубиця 2С19 «МСТА-С» призначена для знищення тактичних ракетних засобів та далекобійної артилерії противника, знищення живої сили, вогневих засобів та бойової техніки на марші, в місцях зосередження та в опорних пунктах, ураження органів управління та тилу противника;
– самохідна гаубиця 2С3 «Акація» призначена для знищення бронетанкової техніки, артилерії і мінометів, а також живої сили противника, руйнування його польових споруд і загороджень, боротьби з танками та іншими броньованими засобами;
– самохідна гаубиця 2С1 «Гвоздика» призначена для знищення і придушення живої сили противника, руйнування польових споруд і загороджень, а також боротьби з танками та іншими броньованими засобами;
– гаубиця Д-30 призначена для знищення і пригнічення живої сили противника, відкритої та яка знаходиться в укриттях польового типу; знищення і пригнічення вогневих засобів піхоти противника, руйнування дзотів та інших споруд польового типу, пророблення проходів у мінних полях та дротяних загородженнях, боротьби з артилерією, механізованими засобами і танками противника.

Стрільба наземної артилерії ведеться для поразки живої сили, вогневих засобів, танків, надводних цілей, руйнування оборонних споруд, дистанційного мінування, світлового забезпечення, задимлення (засліплення)противника, а також поширення агітаційних матеріалів.

Підготовка стрільби включає: розвідку і визначення координат цілей, організацію зв'язку, топогеодезичну прив'язку, метеорологічну, технічну, балістичну підготовку стрільби і визначення установок для стрільби. Стрільба ведеться із закритих вогневих позицій або прямим наведенням. Снаряд, заряд, детонатор, вид траєкторії снаряду вибирають виходячи з характеру цілі, дальності, завдання і умов стрільби на ураження.

При повній підготовці, використанні даних пристрілювальних гармат і перенесенні вогню відкривають раптовий вогонь на ураження цілі (без пристрілки). При скороченій підготовці, як правило, потрібна пристрілка. Стрільба на поразку цілі ведеться гарматою, взводом, батареєю, дивізіоном або декількома дивізіонами. Обстріл цілі ведеться одиночними пострілами, методичним вогнем, швидким вогнем, залпами, на одній або декількох установках прицілу і кутоміра, при зосередженому веєрі або по ширині цілі.

На сьогоднішній день досвід застосування артилерії у зоні проведення Антитерористичної операції на Сході України показав, що для розрахунку артилерійського вогню необхідно вирішувати ряд розрахункових задач, які обчислюються вручну і займають досить довгий час, тоді коли як він є чи не найважливішим показником.

Для вирішення даної проблеми, доцільно розробити комплекс програмного забезпечення по автоматизації розрахунків артилерійського вогню.

До основних даних таблиць для ударної стрільби належать установки прицілу, горизонтальні дальності польоту X, висоти траєкторії Y, час польоту до точки падіння T, остаточна швидкість в точці падіння Vc і кут падіння θo. Усі ці елементи зазначаються залежно від дальності польоту X, що задається через постійний табличний інтервал (через 200 м).

Розрахунок етапів артилерійського вогню складається з наступних етапів:
– розрахунок основних табличних даних;
– розрахунок поправочних граф і допоміжних даних;
– обчислення характеристики розсіювання;
– обчислення поправок кута прицілювання на кут місця цілі.

Розрахунок основних табличних даних проводиться в два етапи.

Перший етап. Спочатку обчислюють основні табличні елементи для кутів кидання, кратних 5°, і граничного для даної системи, а також для кутів кидання 1, 2, 3 і 4°. Ці розрахунки проводяться за балістичною збіркою. Для цього з графіка $c = f(\theta o)$, отриманого в процесі узгодження, знімають значення балістичного коефіцієнта для названих значень кутів кидання. Входять у балістичну збірку за величинами трьох параметрів: кута кидання, за відповідним цьому куту значенням балістичного коефіцієнта і табличною початковою швидкістю. Потім лінійною інтерполяцією за величиною балістичного коефіцієнта і початкової швидкості визначають необхідні елементи траєкторій.

Другий етап. Розраховані значення табличних елементів поширюються (інтерполюється) через табличний інтервал дальності. Це поширення (інтерполяція) проводиться, як правило, графічним, а іноді аналітичним методом. Аналітичний метод базується на застосуванні інтерполяційних формул.

Окрім розрахунку основних табличних елементів проводиться розрахунок поправочних граф і допоміжних даних.

Дані поправочних граф розраховують для кутів кидання, кратних 5°, оскільки для цих кутів складені таблиці поправочних коефіцієнтів. Крім того, розраховують поправки для кутів кидання 1 і 3° (за поправочними формулами).

Для названих кутів кидання з графіка $c = f(\theta o)$ знімають значення балістичного коефіцієнта. Маючи вхідні параметри θo, c і $Vo_{табл}$, за таблицями інтерполяцією визначають значення поправочних коефіцієнтів

$$Q_{\frac{бс}{c}}, Q_r, Q_{v_0}, Q_{w_x}, Q_{w_z}.$$

Розсіювання точок падіння снарядів характеризується серединними відхиленнями *Вд*, *Вб* і *Вв* по дальності, по напрямку і по висоті. Під час проведення ударних стрільб визначаються серединні відхилення *Вд* і *Вб*, а за наслідками стрільб по щитах – серединні відхилення *Вб* і *Вв*.

Як показує досвід, величини серединних відхилень у ході повторних стрільб змінюються у значних межах. Серединні відхилення самих характеристик *Вд* і *Вб* становлять близько 20% від їх середніх значень. Тому не уявляється можливим обчислювати табличні значення характеристик розсіювання *Вд*, *Вб*, *Вв* безпосередньо за наслідками стрільб, оскільки, з одного боку, важко побудувати усереднені плавні криві залежності *Вд* і *Вб* від кутів кидання і дальності, а з іншого – за умови невеликого числа табличних стрільб величини серединних відхилень можуть бути визначені недостатньо точно. На цій підставі табличні значення характеристик розсіювання *Вд*, *Вб* і *Вв* обчислюють, виходячи з урахування розсіювання основних балістичних чинників, що визначають розсіювання траєкторій.

Коли ціль розташована на горизонті гармати (точки вильоту), кут піднесення φ_0 дорівнює табличному куту прицілювання a_0. Якщо ж ціль розміщена вище або нижче за горизонт гармати, то кут піднесення дорівнює сумі кута прицілювання a_ε і кута місця цілі ε.

$$\varphi = a_\varepsilon + \varepsilon.$$

Але кут прицілювання a_ε відрізняється від табличного кута прицілювання a_0, хоча горизонтальна дальність до цілі залишається однаковою. Відмінність кутів прицілювання у зазначених випадках пояснюється відмінністю форми траєкторій, що відповідають різним кутам підвищення. Різниця кутів прицілювання під час стрільби на однакову дальність, коли кут місця цілі відмінний від нуля і дорівнює нулю, називається поправкою кута прицілювання на кут місця цілі

$$\Delta a_\varepsilon = a_\varepsilon - a_0.$$

Ці поправки обчислюються для заданої горизонтальної дальності. Таблиці поправок кута прицілювання на кут місця цілі складаються для кутів прицілювання

через 20 тисячних і для кутів місця цілі від 0 до ±130 тисячних через 10 тисячних. Значення поправок у таблицях даються в тисячних. Ці таблиці можуть бути окремими для кожного заряду або загальними для групи зарядів і снарядів, близьких один до одного за формою, якщо таке узагальнення не приводить до відхилень у дальності, що перевищують 50 м. Опорні значення поправок розраховуються для кутів прицілювання α_0= 100, 200, 300, 400, 440, 480, 520, 560, 600 тисячних і далі через 20 тисячних до 900 тисячних, а далі через 40 тисячних і для кутів місця цілі ε = 10, 40, 70, 100 і 130 тисячних. Для обчислення поправок кута прицілювання на кут місця цілі застосовуються два методи: точний і наближений. Точний метод застосовується, коли кути місця цілі більше 8– 10°, а наближений – коли кути місця не перевищують 8 –10°.

Для розробки програмного забезпечення було обрано операційну систему *Android*, яка є для мобільних телефонів та планшетних комп'ютерів. *Android* є з відкритим вихідним кодом, та найбільш популярний у використані.

Інструментами для створення програмного продукту на базі операційної системи *Android* було обрано:

1. *AndroidStudio* – інтегроване середовище розробки для платформи *Android*.
2. *AndroidSDK* (*SoftwareDevelopmentKit*) – набір із засобів розробки, утиліт, який дозволяє створювати прикладні програми для платформи *Android*.
3. Комп'ютерний планшет – для тестування та використання програмного продукту.

За своєю структурою програмне забезпечення розрахунку артилерійського вогню складається з трьох складових. Кожен із блоків має своє чітко визначене призначення, але полягає в реалізації певної функції.

Перелік складових:

1. Взаємодія з користувачем – модуль, який відповідає за введення користувачем вхідних даних.
2. Розрахунок – модуль, який розраховує вихідні дані для артилерійського вогню.
3. Результат обчислення – модуль, який виводить результат артилерійського вогню для подальшого його використання.

Проведений аналіз застосування артилерії у зоні проведення Антитерористичної операції на сході України дозволив зробити наступні висновки:

по-перше, на сьогоднішній час актуальним питанням у Сухопутних військах Збройних Сил України є автоматизація розрахунку артилерійського вогню, яка повинна забезпечити перевагу українських військових у артилерійських дуелях в швидкості вогневої відповіді та точності ураження по цілі.

По-друге, проведений аналіз етапів методики розрахунку артилерійського вогню, надав можливість визначити основні напрямки автоматизації: розрахунок основних значень, розрахунок поправочних граф і допоміжних даних, обчислення характеристик розсіювання, поправок кута прицілювання на кут місця цілі.

По-третє, для розробки програмного забезпечення автоматизації розрахунку артилерійського вогню було обрано інтегроване середовище розробки *AndroidStudio*для професійної розробки програмного забезпечення. Був створений алгоритм програмного забезпечення функціонування мобільного пристрою; також представлена функціональна залежність між модулями та ієрархія об'єктів додатку. Наведений порядок встановлення програмного продукту на мобільний пристрій, а також приклади користування мобільним додатком та рекомендації щодо налаштування пристрою на робочий режим функціонування.

Рецензент: заступник начальника кафедри бойового застосування математичного та програмного забезпечення АСУ к.т.н., доцент підполковник Сілко О.В.

ДОДАТОК

ПЕРЕМОЖЦІ ТА ПРИЗЕРИ 2-ГО ЕТАПУ КОНКУРСУ КУРСАНТСЬКИХ (СТУДЕНТСЬКИХ) НАУКОВИХ РОБІТ ВІТІ 2015 РОКУ

ДИПЛОМ

І СТУПЕНЯ

НАГОРОДЖУЄТЬСЯ

ЗА КРАЩУ НАУКОВУ РОБОТУ СЕРЕД КУРСАНТІВ ВІЙСЬКОВОГО ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

(за напрямком „Телекомунікації")

Лукашенко Євгеній Олегович

Начальник інституту генерал-майор А.І. МІНОЧКІН

30 червня 2015 року

ДИПЛОМ

І СТУПЕНЯ

НАГОРОДЖУЄТЬСЯ

ЗА КРАЩУ НАУКОВУ РОБОТУ СЕРЕД КУРСАНТІВ ВІЙСЬКОВОГО ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

(за напрямком „Інформаційні системи")

Павленко Ярослав Аркадійович

Начальник інституту генерал-майор А.І. МІНОЧКІН

30 червня 2015 року

ДИПЛОМ

І СТУПЕНЯ

НАГОРОДЖУЄТЬСЯ

ЗА КРАЩУ НАУКОВУ РОБОТУ СЕРЕД КУРСАНТІВ ВІЙСЬКОВОГО ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

(за напрямком „Інформаційні технології")

Поліщук Ірина Григорівна

Начальник інституту генерал-майор А.І. МІНОЧКІН

30 червня 2015 року

ДИПЛОМ

І СТУПЕНЯ

НАГОРОДЖУЄТЬСЯ

ЗА КРАЩУ НАУКОВУ РОБОТУ СЕРЕД КУРСАНТІВ ВІЙСЬКОВОГО ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

(за напрямком „Військові науки")

Рубановський Павло Валентинович

Начальник інституту генерал-майор А.І. МІНОЧКІН

30 червня 2015 року

ДИПЛОМ

II СТУПЕНЯ

НАГОРОДЖУЄТЬСЯ

ЗА КРАЩУ НАУКОВУ РОБОТУ СЕРЕД КУРСАНТІВ ВІЙСЬКОВОГО ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

Бойко
Єлизавета Сергіївна

Начальник інституту
генерал-майор А.І. МІНОЧКІН

30 червня 2015 року

ДИПЛОМ

II СТУПЕНЯ

НАГОРОДЖУЄТЬСЯ

ЗА КРАЩУ НАУКОВУ РОБОТУ СЕРЕД КУРСАНТІВ ВІЙСЬКОВОГО ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

Гусаковський
Іван Петрович

Начальник інституту
генерал-майор А.І. МІНОЧКІН

30 червня 2015 року

ДИПЛОМ

II СТУПЕНЯ

НАГОРОДЖУЄТЬСЯ

ЗА КРАЩУ НАУКОВУ РОБОТУ СЕРЕД КУРСАНТІВ ВІЙСЬКОВОГО ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

Мартиненко
Артем Геворкович

Начальник інституту
генерал-майор А.І. МІНОЧКІН

30 червня 2015 року

ДИПЛОМ

II СТУПЕНЯ

НАГОРОДЖУЄТЬСЯ

Парнюк
Ігор Олександрович

Начальник інституту
генерал-майор А.І. МІНОЧКІН

30 червня 2015 року