НПК МНІС ІП–2019

ЗБІРНИК НАУКОВИХ ПРАЦЬ МОЛОДИХ НАУКОВЦІВ І СТУДЕНТІВ

ЧАСТИНА 2

ПРИСВЯЧУЄТЬСЯ 30-РІЧЧЮ КАФЕДРИ КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ ХМЕЛЬНИЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ

КбКСМ ХНУ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Хмельницький національний університет

Військовий інститут Київського національного університету ім.Тараса Шевченка

ПВНЗ “Університет економіки і підприємництва”

Вінницький національний технічний університет

Тернопільський національний економічний університет

Інтелектуальний потенціал - 2019

збірник наукових праць молодих науковців і студентів

Присвячується 30-річчю кафедри кібербезпеки та комп’ютерних систем і мереж Хмельницького національного університету

сформовано за матеріалами
Всеукраїнської науково-практичної конференції
молодих науковців і студентів «Інтелектуальний потенціал – 2019»

20-22 листопада 2019р.

Частина 2
Комп’ютерна інженерія та системне програмування

Хмельницький
2019

ББК 74.480.278
С.88

«Інтелектуальний потенціал – 2019» - збірник наукових праць молодих науковців і студентів з нагоди 30-річчя кафедри кібербезпеки та комп'ютерних систем і мереж ХНУ/Колектив авторів – Хмельницький: ПВНЗ УЕП, 2019. – Ч.2: Комп'ютерна інженерія та системне програмування. – 88 с.

ЗМІСТ

Робот-садівник

Авчієв А. О.
Науковий керівник – к. т. н. доц. Меркулова К. В.
Донецький Національний Університет ім. Василя Стуса

Мета роботи – огляд проблеми бур'янів, пошук технічних та програмних засобів для створення робота-садівника, який в майбутньому зможе розпізнавати та знищувати непотрібні рослини на прибудинковій земельній ділянці. В даній роботі виконується огляд засобів для створення модулю, який відповідатиме за роботу з вхідним зображенням та контурами, ознайомлення з можливостями цих засобів та отримання досвіду загалом.

Завдання дослідження: проаналізувати поточний стан ринку на наявність близьких аналогів, обрати засоби реалізації які дозволять досягти мети, ознайомитись з ними.

В грудні 2018 року у Європі було проведено опитування кількох десятків садівників (маються на увазі люди, яких наймають для догляду за прибудинковою територією) з метою визначення існуючих засобів, за допомогою яких вони борються з бур'янами. Відповіддю було загалом лише два варіанти: за допомогою хімічних речовин, або ніяк.

Також важливим фактором є введення заборон на використання деяких хімічних речовин у Франції (зазвичай незабаром такі ж рішення з невеликою затримкою приймають в Європі), набір обертів теми екології в світі та збільшення кількості досліджень, які обов'язково призведуть до нових обмежень.

При дослідженні виявлено, що всі близькі аналоги розроблюваного робота або орієнтовані на агрономічну промисловість, або мають суттєві недоліки, поки що не випускаються і непридатні для використання на приватних ділянках.

Серед апаратної частини обрано моноплатний комп'ютер Raspberry Pi Model 3b+ (рис. 1, далі RP), та камери для нього Raspberry Pi Camera.

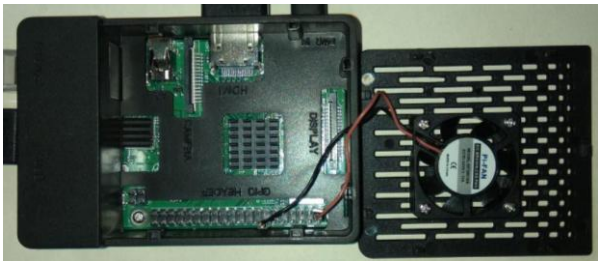

Рисунок 1 – Raspberry Pi 3b+, яка використовувалась для досліджень

З програмної частини обрано мову Python 3 та бібліотеку з реалізаціями функцій комп'ютерного бачення OpenCV (далі OCV) версії 3 та 4 (розробка на OCV 3 на ОС Windows, тестування на OCV 4 на комп'ютері RP, ОС Raspbian).

При ознайомленні та тестуванні можливостей обраних засобів було написано додаток у вигляді бібліотеки (розширюваного модулю, який може запускатись окремо як виконуваний скрипт python, або підключатись як бібліотека для надання доступу до реалізованих у ньому засобів), містить такі функції:

1) Захоплення об'єкту з використанням кольорових масок (в результаті обробки зображення такою маскою залишається лише колір, який був у діапазоні цієї маски, це дозволяє легко виділяти об'єкти, колір яких статично відрізняється від кольору навколишнього середовища)

2) Тестування засобів OCV для отримання контурів зображення (з використанням користувацьких налаштувань)

3) Користувацький інструмент для налаштування бібліотеки.

Бібліотека використовується в одному з чотирьох режимів:

1) Режим налаштування (додатково обирається джерело зображення – камера в режимі реального часу з оновленням результату, або завантаження зображення з файлу). Дозволяє змінювати, бачити результат в реальному часі і зберігати налаштування фільтрів кольору.

2) Режим пошуку центру прямокутної фігури. Виконано в якості ознайомлення з методами отримання контуру за допомогою фільтрації кольору та роботи з отриманими контурами.

3) Режим показу контурів зображення з камери у режимі реального часу. В цьому режимі користувач бачить зображення з камери, та результат обробки цього зображення в режимі реального часу.

4) Режим обробки зображення, отриманого з файлу.

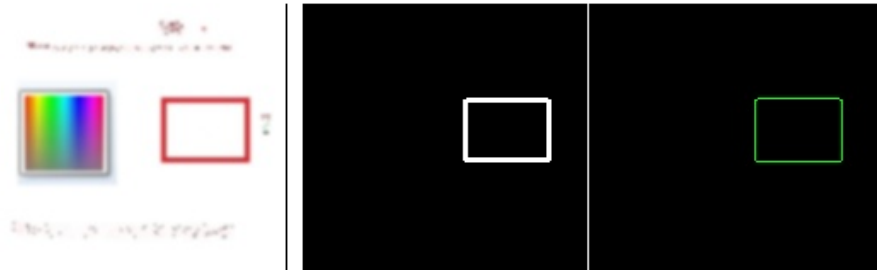

Рисунок 2 – Проміжні дані при обробці зображення з файлу, зліва направо: 1) вхідне зображення після згладжування; 2) результат роботи масок кольорів; 3) знайдений контур.

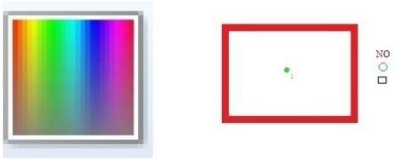

Рисунок 3 – Знайдений центр прямокутника, помічений зеленою крапкою.

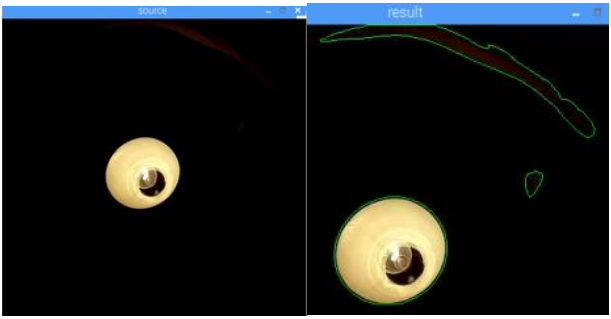

Рисунок 4 – Пошук контурів на зображенні з камери в реальному часі

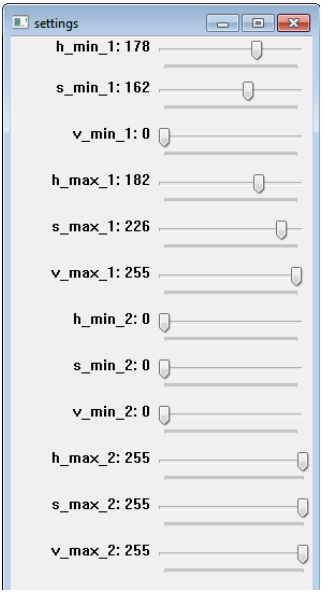

Рисунок 5 – Створений інструмент для налаштування масок кольорів

Висновки: бібліотека OCV може використовуватись для попередньої обробки зображення з камери перед використанням нейронних мереж у майбутньому для класифікації рослин, оскільки лише за допомогою знайдених контурів ця задача не вирішуватиметься достатньо точно. При розробці потрібно враховувати, що тип світла (сонячне, штучне) та його інтенсивність сильно впливають на якість зображення та кольоропередачу, а внаслідок і на результати роботи алгоритмів.

Перелік послань

1. Документація мови Python. URL: https://docs.python.org/3/ (Дата звернення: 01.02.2019)

2. Документація бібліотеки OpenCV. URL: https://docs.opencv.org/ (Дата звернення: 01.02.2019)

Аналіз вимог до програмного забезпечення комп'ютерних систем

Боднар М. А.
Науковий керівник – д.т.н.,проф. Говорущенко Т. О.
Хмельницький національний університет

Вступ. Практично усі сфери людської діяльності на сьогодні пов'язані з комп'ютерними системами, основою яких є програмне забезпечення (ПЗ). Ключовим фактором забезпечення ефективного застосування ПЗ та однією із основних вимог користувачів і зацікавлених осіб до сучасного ПЗ є досягнення високих значень показників його якості. Згідно зі стандартами ISO 25010 [1], ISO 25030 [2], SWEBOK [3], якість ПЗ розглядається як його здатність задовольнити заявлені і передбачувані потреби при його використанні за певних умов. Одним з основних чинників, що впливають на якість ПЗ, є якість та достатність інформації нормативної документації (в першу чергу, специфікації вимог до ПЗ), оскільки сформовані вимоги до ПЗ можуть не відображати повною мірою потреби замовників. Враховуючи вищевикладене, метою даного дослідження є дослідження сучасних проблем аналізу вимог до ПЗ.

Аналіз специфікації вимог до ПЗ. Сьогодні оцінювання атрибутів для нефункційних характеристик ПЗ відбувається лише на етапі оцінювання ПЗ для готового програмного коду [4]. Але всі необхідні атрибути та показники закладено вже у специфікації вимог до ПЗ [4], тобто на основі специфікації вимог до ПЗ можна оцінити достатність інформації щодо майбутнього забезпечення нефункційних характеристик ПЗ. Якщо деякі атрибути відсутні, то у специфікації вимог недостатньо інформації для тієї чи іншої нефункційної характеристики. Для усунення недостатності інформації до розробників вхідної інформації необхідно сформувати повторний запит щодо вимог, які регламентують таку нефункційну характеристику, на основі якого

вони повинні внести необхідні доповнення у вхідну інформацію при формуванні вимог до ПЗ.

Одним з підходів виявлення факту недостатності інформації у специфікації вимог до ПЗ є оцінювання достатності інформації щодо якості у специфікаціях вимог до ПЗ на основі порівняльного аналізу онтологій [5]. В рамках такого підходу розроблено теоретичні та прикладні засади інформаційної технології оцінювання достатності інформації щодо якості у специфікаціях вимог до ПЗ, зокрема, розроблено систему оцінювання достатності інформації щодо якості у специфікаціях вимог до ПЗ на основі порівняльного аналізу онтологій.

Дана система працює наступним чином: 1) генерує та наповнює шаблони онтологій для визначення якості конкретного ПЗ (за стандартом ISO 25010 [1]); 2) порівнює онтології для визначення якості конкретного ПЗ з відповідними базовими онтологіями предметної галузі «Інженерія програмного забезпечення» (частина «Якість ПЗ»); 3) на основі порівняння онтологій, враховуючи критерій достатності інформації щодо якості у специфікаціях вимог до ПЗ, робить висновок про достатність або недостатність інформації щодо якості у специфікації вимог до конкретного ПЗ; 4) якщо інформації щодо якості у специфікації достатньо, то продовжується робота над проектом за цією специфікацією; 5) якщо інформації щодо якості у специфікації недостатньо, то формується запит на додавання інформації щодо вимог, які регламентують характеристики якості, у вхідну інформацію при формуванні вимог до ПЗ. Цей запит містить перелік атрибутів, для зазначення яких у специфікації вимог не вистачає інформації у бізнес-вимогах, а також рекомендовану пріоритетність доповнення цих атрибутів у специфікацію (в залежності від важливості та вагомості того чи іншого атрибута). На наступному кроці здійснюється ітерація доповнення специфікації інформацією щодо якості ПЗ.

Схема процесу оцінювання достатності інформації щодо якості у специфікаціях вимог до ПЗ представлена на рис. 1 [5].

За аналогією, на основі порівняльного аналізу онтологій, можна оцінювати достатність інформації щодо решти нефункційних характеристик у специфікаціях вимог до ПЗ, але для цього потрібно розробити частини базової онтології предметної галузі «Інженерія програмного забезпечення» для нефункційних характеристик, використовуючи відповідні стандарти, що регламентують атрибути, на основі яких відбувається визначення та оцінювання тієї чи іншої нефункційної характеристики, на що й будуть спрямовані подальші зусилля авторів.

Висновки. Чинники якості сучасних програмних систем є менш залежними від написання програмного коду, але суттєво залежать від формування та формулювання вимог і проектування архітектури.

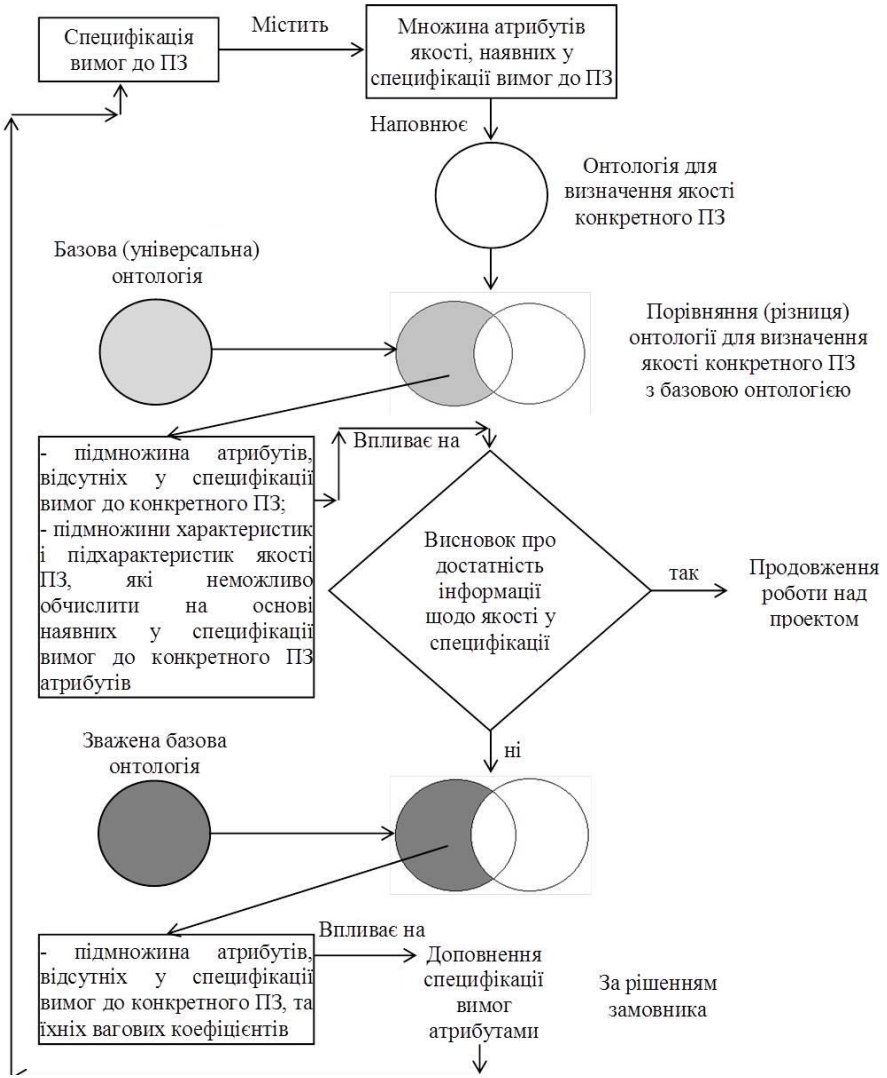

Рисунок 1 – Схема процесу оцінювання достатності інформації щодо якості у специфікаціях вимог до ПЗ

Аналіз специфікацій вимог до ПЗ показав можливість оцінювання інформації у специфікаціях вимог до ПЗ на предмет її достатності. В разі встановлення факту недостатності інформації у специфікаціях вимог до ПЗ, до розробників вхідної інформації надходить повторний запит на додавання

інформації щодо вимог, які регламентують нефункційні характеристики. Запит містить перелік атрибутів, для зазначення яких у специфікації вимог не вистачає інформації у бізнес-вимогах, а також рекомендовану пріоритетність доповнення цих атрибутів у специфікацію (в залежності від важливості та вагомості того чи іншого атрибута). На наступному кроці здійснюється ітерація доповнення специфікації інформацією (атрибутами).

Дослідження процесу оцінювання достатності інформації у специфікації вимог до ПЗ показало необхідність розроблення частин базової онтології предметної галузі «Інженерія програмного забезпечення» для нефункційних характеристик на основі відповідних стандартів, на що й будуть спрямовані подальші зусилля авторів.

Перелік посилань

1. Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models: ISO/IEC 25010:2011. – [Introduced 01.03.2011]. – Geneva (Switzerland): ISO, 2011. – 34 p. – (International standard).

2. Software engineering. Software product Quality Requirements and Evaluation (SQuaRE). Quality requirements: ISO/IEC 25030:2007. – [Introduced 01.06.2007]. – Geneva (Switzerland): ISO, 2007. – 36 p. – (International standard).

3. Software Engineering. Guide to the software engineering body of knowledge (SWEBOK): ISO/IEC TR 19759:2015. – [Introduced 01.10.2015]. – Geneva (Switzerland): ISO, 2015. – 336 p. – (International standard).

4. Маевский Д. Где и когда формируется качество программного обеспечения? / Д. Маевский, Ю. Козина // Электротехнические и компьютерные системы. – 2015. – № 18. – С. 55-59.

5. Говорущенко Т. О. Методологія оцінювання достатності інформації для визначення якості програмного забезпечення: монографія / Т. О. Говорущенко. – Хмельницький: Хмельницький національний університет, 2017. – 310 с.

Методи за засоби ідентифікації бот-мереж, що використовують технологію “динамічної перереєстрації доменів”

Бурдаш Є. С.
Науковий керівник- к.т.н., доцент Лисенко С. М.
Хмельницький Національний Університет

Кіберзлочинність - одна із найбільш активних небезпек із якою зустрічаються інтернет користувачі. Все частіше кіберзлочинці розробляють нові та покращують наявні методи для швидкого заробітку.

Одним із таких методів який з’явився не так давно є метод динамічної перереєстрації доменів (Fast flux). Fast flux мережі [1] складаються із взламаних комп'ютерних систем з публічними записами DNS, які постійно змінюються через певний інтервал часу. Часто цей інтервал часу може становити кожні 2-5 хвилин. Саме висока частота зміни архітектури робить процес виявлення та слідкування за цим методом кіберзлочинності тривалим там трудомістким.

Технологія Fast flux не є небезпечною як така, оскільки не використовує будь-які уразливості DNS. Але кіберзлочинці знайшли застосування для цієї технологої. Вони почали використовувати її у парі із ботнетом, що дозволяє приховувати сліди і долати фільтри провайдерів, які блокують доступ по IP-адресам. Fast flux це метод який злочинець може використовувати задля запобігання ідентифікації IP-адреси власного комп’ютера. Проте, злочинці виявили, що вони можуть приховувати ключові сервера, використовуючи 1/62 часу життя (TTL) запису DNS ресурсу пов'язаного CIP-адресою і міняти їх надзвичайно швидко.

При аналізі відомих для нас підходів виявлення бот-мереж було виявлено низький рівень ідентифікації невідомих ботів бот-мереж. Виходячи із того факту, що основна частина бот-мереж у процесі їх функціонування використовує систему доменних імен, то задача яка представляє в собі розробку програмного забезпечення по виявленню бот-мереж в корпоративних системах є актуальною [3]. Тому пропонується технологія по виявленню бот-мереж в корпоративних мережах на основі аналізу DNS трафіку, що дозволить значно підвищити виявлення бот-мереж.

Організаційно ботнет поділений на дві підмережі, які використовуються по різному: одна - це проксування командного трафіку, друга - для розміщення шкідливих бінарних файлів, фішингових сайтів та площадок, які продають викрадені кредитні картки та ідентифікаторами.

Мережі послуг fast flux використовуються для досягнення двох цілей: для розміщення перенаправляючих веб-сайтів. Боти в даній мережі послуг зазвичай не розміщують клієнтських даних fast flux, а виконують перенаправлення на веб-сервер, з якого клієнт fast flux виконує несанкціоновані або протизаконні дії. Якщо для хостингу fast flux використовується тільки ця мережа, то використовується термін застосовується термін single flux; для розміщення серверів імен. Боти в даній мережі послуг запускають напрямляючі сервери для клієнта fast flux. Ці сервери імен переадресовують DNS-запити на приховані сервери, на яких розміщені зони, що містять записи DNS для набору перенапрявляючих веб-сайтів. Приховані сервери не пересилають запити назад через направляючий сервер імен, а відправляють відповідь безпосередньо хост. Коли для посилення ефекту атаки разом з мережею single flux використовується друга мережа, для опису даної діяльності застосовується термін double flux.

Вхідними даними системи аналізу корпоративних бот-мереж є DNS трафік, який збирається із мережі за допомогою мережевих давачів, які у свою чергу підключені до портів керованих комутаторів.

Даний метод виявлення бот-мереж у корпоративних бот-мережах ґрунтується на властивості групової активності ботів DNS трафіку. Метод враховує певні особливості поведінки груп [4], які вже є інфікованими та є характерними для багатьох видів бот-мереж: групи ігнорують TTL-період DNS, здійснюють DNS-запити використовуючи нелокальні DNS-сервери.

Ідея методу заключається в наступних кроках:

– збір вхідного DNS-трафіка;

– визначення усіх наявних параметрів на ознак у сформованому трафіку;

– виявлення груп,які ігнорують TTL - період;

співставлення кількох груп ознак та їх аналіз за допомогою штучного інтелекту на машинного навчання.

Для того щоб визначити результати використовуються наступні ознаки:

– n_{ns} - кількість NS-записів у DNS-відповіді;

– s_{ns} - середня дистанція між IP-адресами для множини NS-записів щодо доменного імені;

– v_{retry} - значення поля retry, отримане у DNS-відповіді на SOA-запит;

– n_{asn} - кількість різних номерів автономних систем (ASN), до яких належать IP-адреси, пов’язані з серверами імен;

– n_{asa} - кількість різних номерів автономних систем, до яких належать IP- адреси, пов’язані з доменним іменем.

На основі цих ознак та певних правил визначається наявність технологій ухилення DNS.

На рисунку 1 зображена схема аналізу DNS -трафіка бот-мережі та етапи обробки отриманих даних.

Кіберполіції постійно доводиться витрачати багато часу на аналіз тривалості життя кожного з'єднання, встановленого з ботнетом. Також вони повинні отримувати інформацію від різних інтернет-провайдерів, які не завжди бажають співпрацювати, та аналізувати незліченну кількість журналів реєстру домену, щоб знайти та відфільтрувати будь-яку шкідливу діяльність, яка могла б дати їм вагомий слід у пошуку їхніх центрів управління ботнету.

Представлений вище метод ідентифікації бот-мереж, в основі якого лежить сканування DNS - трафіку, вибірка та співставлення ознак в отриманому трафіку надає можливість ідентифікувати бот-мережі, як відомі так і не відомі, та початковій стадії інфікування мережі. Описаний метод також дозволяє визначати технології ухилення від виявлення на основі DNS, що надає можливість виявляти існуючі та нові бот-мережі.

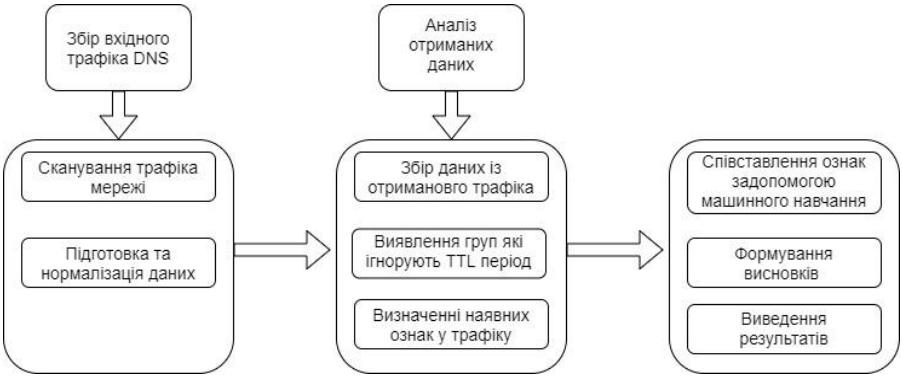

Рисунок 1. Схема аналізу DNS трафіка

Перелік посилань

1. Alieyan K, ALmomani A, Manasrah A, Kadhum MM (2015) A survey of botnet detection based on DNS. Neural Comput Appl 1–18. doi: 10.1007/s00521-015-2128-0

2. Caglayan A, Toothaker M, Drapeau D, Burke D, Eaton G (2012) Behavioral analysis of botnets for threat intelligence. IseB 10(4):491–519 CrossRef Google Scholar

3. McAfee. (2015) McAfee labs threats report. Accessed 18 May 2015. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf

4. E. Soltanaghaei and M. Kharrazi (2015) Detection of fast- ux botnets through DNS trac analysis http://www.cs.virginia.edu/~es3ce/ Elahe%20Soltan_files/papers/fastflux.pdf

Дослідження пожежонебезпечності лісових територій на основі використання капсульних та згорткових нейронних мереж

Главчева Д. М., Яловега В. А.
Науковий керівник – к.т.н., доц. Подорожняк А. О.
Національний технічний університет «Харківський політехнічний інститут»

Штучні нейронні мережі моделюють роботу людського мозку та використовуються для вирішення найрізноманітніших задач, що вимагають складних аналітичних обчислень.

У дослідженні нейронні мережі глибокого навчання використовуються для вирішення науково-прикладної задачі визначення пожежонебезпечних лісових територій на прикладі пожежі «Camp Fire», що сталася в штаті Каліфорнія (США) в листопаді 2018 року. Проблема лісових пожеж є актуальною. Аналізуючи статистику США [1], можна спостерігати, що порівняно з 1980-тими роками, станом на кінець 2017 року площа території, на якій відбувалися пожежі збільшилася майже вдвічі.

Дистанційне зондування Землі є методом вимірювання характеристик об'єктів на земній поверхні [2]. Одними з актуальних даних дистанційного зондування Землі у якості мультиспектральних зображень є дані з супутника Landsat 8. Зображення Landsat 8 використовуються у дослідженні для розрахунку спектральних індексів. Такі індекси допомагають визначати пожежонебезпечні лісові території шляхом розрахунків кількості засушливої рослинності, вмісту вологи та карбону (у вигляді лігніна та целюлози) в рослинах. Для аналізу мультиспектральних зображень та формування єдиного індексного зображення (у трьох кольорових каналах) для території пожежі «Camp Fire» було використано спектральні індекси NDVI, NDWI та PSRI [3-4].

Згорткова нейронна мережа (Convolutional neural network, ConvNet) була запропонована Яном Лекуном у 1988 році [5]. Структура ConvNet не включає в себе зворотні зв'язки, є односпрямованою та багатошаровою. Загальна ідея згорткових нейронних мереж полягає в чергуванні згорткових шарів і шарів підвибірки [6]. Для навчання такої нейронної мережі найчастіше використовують метод зворотного поширення помилки.

Капсульні нейронні мережі були представлені Джеффрі Хінтоном у [7]. Капсульна нейронна мережа (Capsule neural network, CapsNet) – штучна нейронна мережа, яка створена для покращення моделювання ієрархічних зв'язків між об'єктами різних рівнів [8-9]. CapsNet працює з цілими наборами нейронів (векторами). Роутинг між капсулами відбувається за допомогою алгоритму динамічної маршрутизації.

Вхідне зображення для нейронних мереж мало розмір (32×32) пікселів та три кольорові канали. Навчалися обидві нейромережі по 50 епох. Графіки залежності точності класифікації від кількості епох для навчальної та затверджувальної вибірок зображенні на рис. 1 та рис. 2.

ConvNet та CapsNet показали майже однакові результати на тестовому наборі даних. Точність класифікації для згорткової нейронної мережі склала 94.27%, а для капсульної – 94.89%. Аналіз отриманих залежностей (рис. 1–2) показав, що найбільша точність для згорткової нейронної мережі на навчальних даних склала – 99.92% на 39 епосі, найменша – 94.53% на першій епосі, а для капсульної мережі найбільша точність склала 95.17% на 50 епосі, найменша – 94.53% на першій епосі.

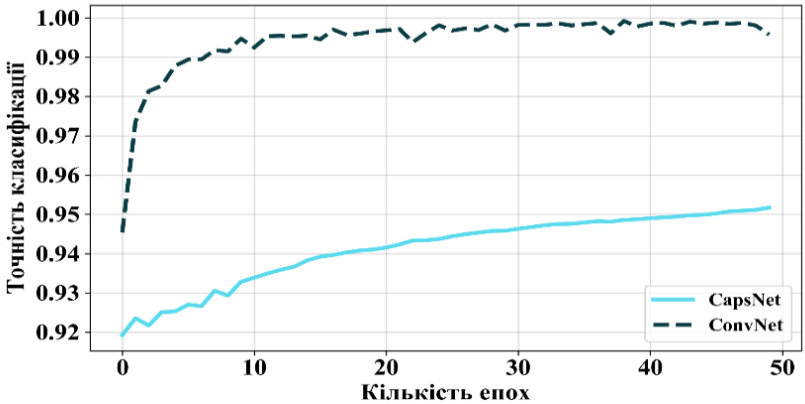

Рисунок 1 – Графік залежності точності класифікації на навчальній вибірці від кількості епох навчання для капсульної та згорткової нейронних мереж

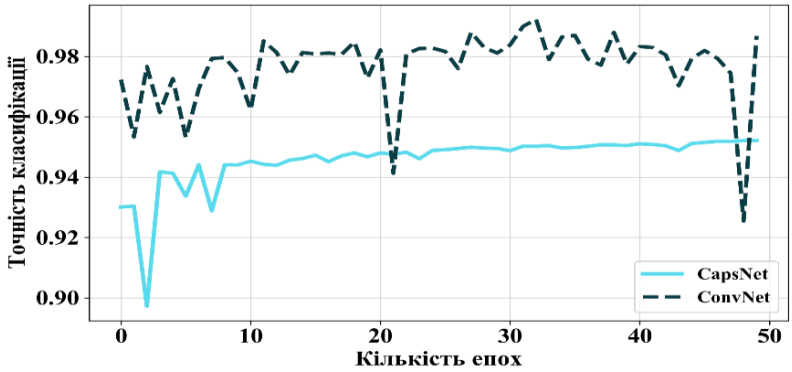

Рисунок 2 – Графік залежності точності класифікації на затверджувальній вибірці від кількості епох навчання для капсульної та згорткової нейронних мереж

На затверджувальному наборі даних найбільша точність для ConvNet становила 99.23% на 33 епосі, а найменша – 92.55% на 49 епосі. Для CapsNet ці показники склали відповідно 95.12% на 49 епосі та 89.72% на третій епосі. Точність класифікації на затверджувальній вибірці (рис. 2) у CNN вища ніж у CapsNet у середньому на 4%, проте видно великі стрибки на деяких епохах, що не характерно для капсульної мережі. Ми припускаємо, що такі результати можуть свідчити про те, що капсульні нейронні мережі навчаються узагальнювати отриману інформацію, більш стійкі до проблеми

перенавчання та мають тенденцію до плавного росту точності класифікації, що може бути зумовлено їх архітектурою.

Виявлено, що при використанні відносно нескладної архітектури, розглянуті нейронні мережі здатні впоратися з поставленою задачею. Встановлено, що капсульні нейронні мережі демонструють менше значення помилки (приблизно на 12%) на затверджувальній вибірці, ніж згорткові нейронні мережі. Отримані результати можна використовувати для визначення пожежонебезпечних лісових територій.

Перелік посилань

1. Hoover K. Wildfire Statistics / K. Hoover // Congressional Research Service [Electronic resource]. – 2018. – [Cited 2018, 15 December]. – Available from: https://fas.org/sgp/crs/misc/IF10244.pdf.

2. Шовенгердт Р.А. Дистанционное зондирование. Модели и методы обработки изображений. Часть 1 / Р.А. Шовенгердт // – М.: Техносфера, 2010. – 560 с.

3. McFeeters S. K. Remote Sensing The use of the Normalized Difference Water Index (NDWI) in the delineation of open water features / S. K. McFeeters // International Journal of Remote Sensing. – V. 17. – No 7. – 1996. – P. 1425-1432.

4. Merzlyak M. N. et al. Non-destructive Optical Detection of Pigment Changes During Leaf Senescence and Fruit Ripening. / M. N. Merzlyak, A. A. Gitelson et al. // Physiologia Plantarum. – 1999. – P. 135-141.

5. LeCun Y. et al. Backpropagation applied to handwritten zip code recognition / Y. LeCun, B. Boser, G. Hinton // Neural computation. – 1989. – V. 1. – No. 4. – P. 541-551.

6. Podorozhniak A. Neural network approach for multispectral image processing / A. Podorozhniak, N. Lubchenko, O. Balenko, D. Zhuikov // Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET-2018), 14th International Conference on: IEEE, pp. 978-981, http://dx.doi.org/10.1109/TCSET.2018.8336357.

7. Sabour S., Frosst N., Hinton G. E. Dynamic routing between capsules / S. Sabour, N. Frosst, G. E. Hinton // Advances in Neural Information Processing Systems. – 2017. – P. 3856-3866.

8. Главчева Д. М. Капсульні нейронні мережі / Д. М. Главчева, В. А. Яловега // Системи управління навігації та зв'язку. – Полтавський національний технічний університет імені Юрія Кондратюка. – №. 5 (51). – 2018. – С.132-135, https://doi.org/10.26906/SUNZ.2018.5.132.

9. Hlavcheva D. CapsNet versus ConvNet / D. Hlavcheva, V. Yaloveha // Інформатика, управління та штучний інтелект: Тези доп. V міжнародної науково-технічної конференції студентів, магістрів та аспірантів (20-22 листопада 2018 року, м. Харків). – Харків, НТУ «ХПІ», 2017. – С. 22-23.

Аналіз методів виявлення шкідливого програмного забезпечення та захисту web-систем

Денисюк Д.О.
Науковий керівник – к.т.н., доцент Бобровнікова К.Ю.
Хмельницький національний університет

Стрімкий розвиток Інтернет-простору сприяє поширенню зловмисних технологій, спрямованих на отримання конфіденційної інформації користувача без його відома. Тим часом кіберзлочинці постійно вдосконалюють методи отримання доступу до web-систем та персональних даних.

Одна з найбільших вірусних кібератак на території України, відбулася 27 червня 2017 року [1]. Зокрема, негативних наслідків цієї атаки зазнали інфраструктури інформаційних систем "Укренерго", "Київенерго", "Епіцентру", "Київстару", "Vodafone", "Lifecell", телеканалу ATR, "Укрзалізниці", Київського метрополітену, "Ощадбанку", "Нової пошти", аеропорту "Бориспіль", мережі заправок WOG, "Укргазвидобування" та ін.

Статистичні дані щодо web-загроз по Україні на кінець 2019 року наведено в таблиці 1 [2].

Таблиця 1 – Статистика web-загроз по Україні

Назва загрози	Відсоток інфікування від загальної кількості виявленого шкідливого програмного забезпечення (ШПЗ)
Trojan.Script.Generic	54.33%
Trojan.Script.Miner.gen	8.99%
Trojan.Multi.Preqw.gen	7.7%
Backdoor.HTTP.TeviRat.gen	6.64%
Trojan-Clicker.HTML.Iframe.dg	5.25%
Trojan.BAT.Miner.gen	4.39%
Trojan-Downloader.JS.Inor.a	1.18%
Trojan-PSW.Win32.Predator.nt	1.03%
Trojan.Win32.Generic	0.63%
DangerousObject.Multi.Generic	0.54%

На сьогоднішній день відомо багато різноманітних підходів виявлення шкідливого програмного забезпечення у web-системах. Основними з них є наступні.

Методи контролю цілісності [2] ґрунтуються на створенні контрольної точки для програмного забезпечення та подальшому контролюванні змін стану програмного забезпечення. Для здійснення контролю достатньо

запам’ятати характеристики, що підлягають змінам, та порівнювати їх з початковими значеннями.

Методи резидентного сторожа [2] спрямовані на виявлення підозрілих дій користувача. До підозрілих дій можна віднести запис даних на диск за абсолютним шляхом, форматування диску, зміну завантажувального сектору тощо. При виявлені таких дій програма захисту відправляє запит користувачеві для отримання підтвердження або скасування підозрілої дії.

Методи евристичного аналізу [3] ґрунтуються на емпіричних припущеннях (наборах евристик, підтверджених дослідним шляхом) про характерні ознаки ШПЗ та призначені для виявлення ще не відомих вірусів та загроз. Кожна ознака додатково може характеризуватись певною вагою, що визначає важливість або достовірність цієї ознаки. Евристичні методи засновані на перевірці гіпотез в умовах невизначеності, тому основним і важливим їх недоліком є схильність до помилок як першого роду (не виявлення загроз), так і другого роду (хибних спрацювань).

Метод сканування, описаний в [8], є найбільш простим підходом. Він заснований на послідовному скануванні пам’яті комп’ютера та завантажувальних секторів і порівняні зі зразками не зараженого програмного забезпечення.

Одним з поширених методів захисту є використання протоколу HTTP [4]. Цей протокол може бути використаний лише за умови отримання SSL сертифікату у спеціалізованих центрах сертифікації. Але протокол HTTPS також має низку наведених нижче вразливостей, що використовуються кіберзлочинцями.

SWEET32 [5] – спосіб атаки шифрованого web-з'єднання шляхом створення великої кількості web-трафіку. SWEET32 – це класична атака, заснована на колізіях та припущенні, що алгоритм шифрування припуститься помилки, і таким чином кіберзлочинці одержать інформацію про шифрування.

DROWN, Decrypting RSA using Obsolete and Weakened eNcryption [4] – атака, що дозволяє дешифрувати TLS-трафік клієнта, якщо на серверній стороні не відключена підтримка протоколу SSLv2 у всіх серверах, що оперують одним і тим самим приватним ключем.

ROBOT, Return Of Bleichenbacher's Oracle Threat [5] – атака є незначною модифікацією першої практичної атаки на RSA, запропонованої Daniel Bleichenbacher в 1998 році. Було виявлено, що навіть через 19 років багато з HTTPS-хостів ще й досі вразливі до варіацій цієї атаки. Суть атаки полягає в тому, що атакуючий на підставі різних відповідей від сервера може відокремити коректні і некоректні блоки додаткового заповнення (padding oracle) в режимі PKCS # 1 v1.5. Відмінність нового методу від оригінальної атаки Блейхенбахера полягає в використанні додаткових сигналів для поділу типів помилок, таких як таймаут, скидання з’єднання і дублікати TLS-

повідомлень. Маніпулюючи інформацією про коректність блоків додаткового заповнення, атакуючий може шляхом перебору визначити відповідний шифротекст.

Іншим підходом є використання програм-ревізорів (CRC-сканерів) [6]. Принцип роботи цих методів побудований на підрахунку CRC-сум (кодів циклічного контролю) для присутніх на диску файлів. Обчислені CRC-суми зберігаються в базі даних антивірусу. При подальшому запуску CRC-сканери звіряють дані, що містяться в базі даних, з реально підрахованими значеннями. Наприклад, якщо інформація про CRC-суми для фото, записані в базі даних, не збігається з реальними значеннями, то CRC-сканер сигналізує про те, що файл був змінений або заражений вірусом. Прикладом CRC-сканера є програма ADinf і ревізор AVP Inspector.

В [7] представлено метод, що використовує мутаційне тестування. Запропонований підхід має на меті покращити набір тестів для тестування web-ресурсів на наявність ШПЗ шляхом створення множини альтернативних несправностей. Основним недоліком підходу є надлишковість, оскільки створюється велика кількість семантично еквівалентних зразків. Іншим важливим недоліком підходу є те, що автоматизація цього процесу не можлива без участі спостерігача.

Таким чином, набуває актуальності питання розроблення нових методів виявлення ШПЗ у web-системах та їх захисту від ШПЗ, які б усували недоліки відомих підходів.

Перелік посилань

1. ТСН. М.Е. DOC підтвердила розповсюдження вірусу PETYA.A через їхнє ПЗ: ймовірна нова кібератака [Електронний ресурс]. – Режим доступу: https://tsn.ua/ukrayina/m-e-doc-pidtverdila-rozpovsyudzhennya- virusu-petya-a-cherez-yihnye-po-ymovirna-nova-kiberataka-956212.html.

2. LeBlanc J., Messerschmidt T. Identity and Data Security for Web Development: Best Practices. - O'Reilly Media, 2016.- 204 p.

3. ROJAS, José Miguel, et al. Code Defenders. Software Engineering und Software Management 2018, 2018.

4. Kaspersky Lab. ИНТЕРАКТИВНАЯ КАРТА КИБЕРУГРОЗ [Електронний ресурс]. – Режим доступу: https://cybermap.kaspersky.com/ ru/stats/#country=27&type=wav&period=w.

5. SINGH, Ajay; LOAR, Ramesh. Web Security and Enhancement Using SSL: A Review. 2018.

6. Karthikeyan Bhargavan and Gaëtan Leurent. 2016. On the practical (in-) security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN. In Proceedings of ACM SIGSAC Conference on Computer and Communications Security.

7. Aviram, N., Schinzel, S., Somorovsky, J., Heninger, N., Dankel, M.,

Steube, J.,Valenta, L., Adrian, D., Halderman, J.A., Dukhovni, V., K¨asper, E., Cohney, S., Engels, S., Paar, C., Shavitt, Y.: DROWN: Breaking TLS Using SSLv2. In: Proceedings of USENIX Security Symposium. pp. 689–706 (2016)

8. JAGER, Tibor; KAKVI, Saqib A.; MAY, Alexander. On the security of the PKCS# 1 v1. 5 signature scheme. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018. p. 1195-1208.

Мікропроцесорна система контролю параметрів системи очищення питної води

Димид Р. В.
Науковий керівник - к.т.н., Пташник В. В.
Львівський національний аграрний університет

Актуальність проблеми очищення питної води завжди знаходиться на високому рівні. З кожним роком якість води погіршується, а найбільш гостро проблема постає перед промислово розвиненими країнами, адже санітарний стан водних джерел різних районів значною мірою залежить від ступеня концентрації у них промисловості, її характеру, а також обжитості водойми. Навіть якщо говорити про воду яка поступає до населення через мережу централізованого водопостачання часто спостерігається значне відхилення її параметрів від санітарних норм та правил.

Внаслідок термодинамічних обмежень очисні системи не здатні повернути воду у вихідний стан. В таких умовах забезпечення населення якісною питною водою є високовартісним, ресурсо- та енергоємним процесом, який вимагає залучення сучасних технологічних рішень. Тому, навіть у регіонах з достатніми запасами прісної води її вартість невпинно зростає.

В Україні якість води, що транспортується системами централізованого водопостачання визначається кількома чинниками: первинними джерелами водозабору, матеріально-технічними оснащенням систем очищення та кондиціонування води, станом мереж водогону. І саме останній чинник унеможливлює отримання чистої питної води без застосування технологій її доочищення безпосередньо перед використанням.

Сьогодні найпопулярнішою технологією побутового очищення питної води є вугільна фільтрація у багатоступеневих або кувшинних фільтрах. Однак їх ресурс та ефективність процесу очищення істотно залежать від якості вхідної води та умов експлуатації фільтру. У багатьох випадках основною причиною передчасного виходу фільтруючих елементів з ладу є

високий рівень їх мікробіологічного забруднення, що робить подальше використання не просто шкідливим, але й небезпечним.

З метою проведення контролю ефективності очищення води та забруднення фільтруючих елементів доцільно обладнати їх недорогими та простими у обслуговуванні сенсорами, з'єднаними з мікропроцесорною системою контролю, обладнаною відповідними засобами індикації.

Враховуючи вартість сучасних систем фільтрації необхідно розробити систему контролю, вартість якої не перевищуватиме 10–15 % від загальної вартості. У таких умовах для побудови подібної системи доцільно використати апаратну платформу Arduino та універсальні датчики параметрів води.

Одним з ефективних методів дослідження активованих вуглецевих матеріалів – основних наповнювачів фільтруючих елементів – є імпедансна спектроскопія. З літературних джерел відомо, що зі збільшенням забруднення фільтруючого елементу відбувається зменшення дійсної частини опору у діапазоні 0,01-0,1 Гц, що робить цей параметр достатньо зручним для контролю забруднення. Вимірювальні електроди по типу конденсаторної комірки доцільно вмонтувати безпосередньо у вугільний наповнювач фільтруючого елементу. Міжелектродну відстань варто обрати для кожного типу фільтрів індивідуально.

Відомо, що стандартні засоби апаратної платформи Arduino підтримують роботу зі змінним струмом частотою 3 Гц, однак використання додаткових схемотехнічних рішень дозволить зменшити апаратну похибку вимірювання частотної залежності опору за рахунок генерування стабільного синусоїдального сигналу заданої частоти. Генерацію опорного сигналу та вимірювання напруги змінного струму можна реалізувати за допомогою мікросхеми AD9850, яка може працювати на частоті до 40 Гц.

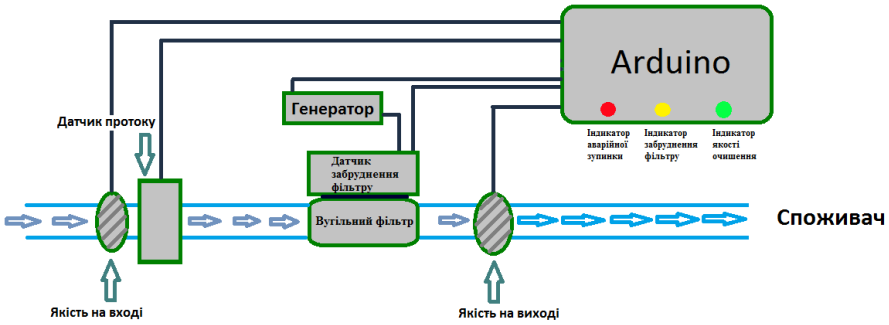

Рисунок 1 – Узагальнена схема мікропроцесорної системи контролю параметрів системи очищення питної води

Після заміни фільтруючого елементу мікропроцесор запам'ятовує початкове значення опору та регулярно відслідковує його зміну. Однак для визначення гранично допустимого рівня зміни опору необхідно провести ряд додаткових статистичних досліджень.

Для контролю якості очищення доцільно використати такі інтегральні показники води як електропровідність та водневий показник. Контроль електропровідності можна реалізувати шляхом вимірювання опору води на частоті 1 кГц, а для оперативного та неперервного вимірювання водневого показника можна використати pH-транзистори. Використання однотипних датчиків до та після фільтруючого елементу дозволить використати порівняльний підхід та нівелювати вплив неконтрольованих домішок. Для відображення режимів роботи фільтру можна використати звичайний LCD-дисплей, або обладнати систему світлодіодною та звуковою індикацією.

Розробка лабораторного стенду для дослідження завадостійких біноміальних кодів

Єрмаков М.С.
Науковий керівник – д.т.н., професор Борисенко О.А.
Сумський державний університет

Широке застосування лічильників робить актуальним задачу підвищення їх швидкодії, перешкодостійкості. Останнє досягається введенням в лічильник заборонених комбінацій за допомогою використанням завадостійких систем числення [1]. Наприклад із 16 станів чотирьохрозрядного двійкового лічильника перші десять вибираються дозволеними, а шість що залишилися – забороненими. Тоді перехід лічильника в один із заборонених станів буде розцінюватися як помилка лічби. Лічильники, які використовують заборонені стани, вирішують доволі складну задачу і вимагають розробки додатково до них контролюючого пристрою, за правильністю роботи якого також потрібно слідкувати. Виникає так звана проблема "охоронці охоронців". Сам лічильник набуває неоднорідну структуру, яку складно спроектувати і налаштувати.

Подолати вказані противоріччя можливо шляхом створення перешкодостійких систем числення. Розроблені на їх основі лічильники перешкодостійкі і мають однорідну структуру, тому що вони не містять спеціального контролюючого пристрою.

До цього класу перешкодостійких систем числення належать і біноміальні системи числення за допомогою яких будуються біноміальні лічильники. Крім того, зменшуються апаратурні витрати у дешифраторів, які розпізнають їх стани. У ряді випадків це може привести до того, що кількість

апаратурних витрат у пристрою з біноміальними лічильниками в цілому зменшиться в порівнянні з пристроєм, який містить двійкові лічильники з дешифраторами. Крім цього, ці лічильники дозволяють змінювати коефіцієнт перерахунку адаптуючись до інтенсивності і характеру перешкод. Пропонується відповідний стенд, який дозволяє досліджувати завадостійкість біноміальних лічильників в реальних умовах. Цей стенд дозволяє змінювати коефіцієнт перерахунку і тим самим змінювати завадостійкість. Це дозволяє адаптувати дослідження до різного рівня завад.

Перелік посилань

1. Борисенко А. А., Ермаков М.С. и другие "Формирование помехоустойчивых перестановочных кодов на основе факториальных чисел" (III Міжнародна конференція "Комп'ютерна алгебра і інформаційні технології" CAIT-Odessa-2018-С. 129-132)

Експертна система оцінки стану електродвигунів на основі зовнішніх діагностичних показників

Карабаш Є.О.
Науковий керівник – старш. викл. Чорна О.А.
Кременчуцький національний університет імені Михайла Остроградського

Актуальність: на сьогоднішній день не існує універсальних, простих і дешевих засобів та методів діагностики електричних двигунів, які б не вимагали зупинки технологічного процесу. Існуючі системи вимагають використання складного вартісного обладнання, яке обслуговується висококваліфікованими спеціалістами. Дуже важливим є встановлення ознак дефектів, що тільки починають розвиватися. Своєчасне їх виявлення можливе лише в разі неперервного контролю режиму роботи двигуна. Зовнішні ознаки режиму роботи: шум, вібрація, перегрів тощо і є такими показниками, які просто спостерігати і при їх зміні зробити відповідні висновки про зміну стану двигуна [1]. Така робота може бути легко виконана обслуговуючим персоналом, який проводить щоденний огляд обладнання при наявності відповідного програмного забезпечення на основі штучного інтелекту. Тому актуальною задачею є розробка системи діагностики електричних двигунів за зовнішніми ознаками режиму їх роботи.

Метою роботи є побудова експертної системи визначення несправностей електричних машин на основі аналізу зовнішніх ознак, що характеризують режим роботи.

Основний алгоритм розробленої системи базується на використанні ймовірнісного аналізу. Головне вікно системи показане на рис.1.

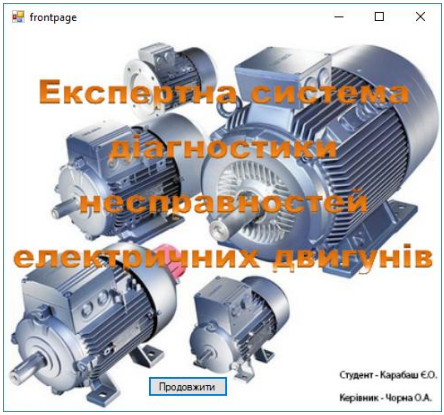

Рисунок 1 – Вікно-заставка експертної системи

Після виконання входу до бази даних пропонується або редагування бази даних, що притаманно оператору програми або безпосередній пошук пошкодження. При виконанні редагування бази даних не виконується ймовірнісного перерозподілу, а лише додаються, змінюються або видаляються записи безпосередньо з базі даних. Блок пошуку несправності має чотири поля: елемент двигуна, який аналізується на несправність та відповідно характеристика елемента, що демонструє несправність, характеристика, що непритаманна правильній роботі двигуна та її відхилення відповідно. Після того як буде змінено один з чотирьох полів програма відшукає всі релевантні записи та відсортує їх за відсотковим показником (рис.2).

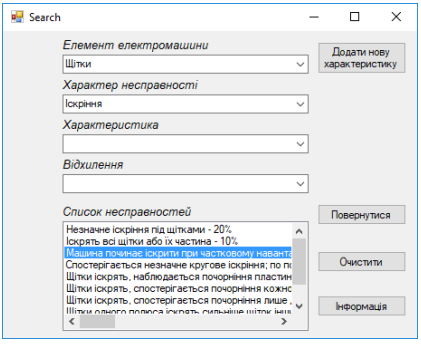

Рисунок 2 – Вікно пошуку та виводу несправностей

Експертна система призначена для фахівців, які займаються ремонтом та обслуговуванням електричних двигунів. Основне призначення ПП – видача рекомендацій обслуговуючому персоналу в разі виявлення відхилень в роботі електричних двигунів.

Таким чином розроблена інформаційна технологія оцінки стану електродвигунів на основі зовнішніх діагностичних показників. Система дозволяє проводити попередню діагностику двигуна з видачою рекомендацій про можливість і доцільність його подальшої експлуатації.

Запропоновані алгоритми і на їх основі розроблене програмне забезпечення добору діагностичних параметрів, що ґрунтується на критерії максимальної індивідуальності. Добір діагностичних параметрів, що дозволяють вирішити задачу розпізнавання, здійснюється методом послідовних доповнень.

Перелік посилань

1. Гемке Р.Г. Неисправности электрических машин / Р.Г. Гемке. Под ред. Р.Б. Уманцева. 9-е изд., перераб. и доп. – Л.:Энергоатомиздат, Ленингр. отд-ние, 1989. – 336с.

2. Муромцев Д.И. Введение в технологию экспертных систем. СПб: СПб ГУ ИТМО, 2005. – 390с

Аналіз задач розпізнавання образів

Кирилюк О.О.
Науковий керівник – к.т.н., проф. Савенко О.С.
Хмельницький національний університет

На сьогодні нові інформаційні технології тісно вплітаються у повсякденне життя кожної людини. Завдяки інноваційним розробкам в цій галузі, кожного дня покращується стан сфери діяльності суспільства: з'являються нові професії, що пов'язані з ними, винаходять пристрої для впровадження цих ідей. Питання розпізнавання структурних об'єктів в системах комп'ютерного зору наразі стоїть дуже гостро. Ця технологія має величезне практичне значення. Вона покликана допомогти людині у різний спосіб: відстеження появи машин на стоянці, забезпечення захисту від несанкціонованого проникнення на певні захищені об'єкти, розпізнавання автомобільних знаків, написів, тексту, облич людей, тощо.

Існує безліч таких завдань, в яких потрібно прийняти деяке рішення в залежності від присутності на зображенні об'єкту та класифікувати його. Таке просте завдання для людини – вирізняти об'єкти, що її оточують, з якою вона справляється щодня, є неймовірно складною для обчислювальної

техніки. Саме тому, розпізнавання (або часто вживається інший термін – «класифікація») об'єктів є однією з найфундаментальніших проблем теорії інтелектуальних систем.

Можна сказати, що розпізнавання образу можна визначити, як віднесення вихідних даних до певного класу за допомогою виділення істотних ознак та властивостей, що характеризують ці дані, із загальної маси несуттєвих деталей.

Частіше всього вихідним матеріалом служить отримане з камери зображення. Задачу можна сформувати як отримання векторів ознак для кожного класу на цьому зображенні. Процес можна розглядати як процес кодування, сутність якого можна описати присвоєнням значення кожній ознаці з простору ознак для кожного класу.

Саме структурний (синтаксичний) підхід використовується до задач розпізнавання образів, в яких важлива інформація про структуру конкретного об'єкта. Ця процедура розпізнавання потребує не тільки те, щоб вона могла визначити клас цього об'єкта, а і встановити таку інформацію про нього, яка не дозволяє віднести його до інших класів. З математичного погляду таке розпізнавання образів є далеким від узагальнення ідеї екстраполяції функції [1]. Для опису текстур широко застосовуються ознаки Тамура, які були виділені в результаті психологічних експериментів [2]. Саме структурне розпізнавання часто реалізується за допомогою алгоритмів зіставлення графів.

До прикладу візьмемо розпізнавання автомобільних знаків на фотознімку. Структура алгоритму буде такою:

Попередній пошук номеру – виявлення області в якій знаходиться номер.

Нормалізація номеру – визначення точних меж номеру, нормалізація контрасту.

Розпізнавання тексту – читання всього що ми знайшли у нормованому зображенні.

Це базова структура. Звичайно, в ситуації, коли номер лінійно розташований і добре освітлений, а у Вас в розпорядженні є чудовий алгоритм розпізнавання тексту, то перші два пункти відпадуть. В деяких видах алгоритму можуть об'єднуватись пошук номеру та його нормалізація.

Зупинимося детальніше на алгоритмі попереднього пошуку. Припустімо, що у нас ідеальний знімок з достатнім освітленням. Структурний підхід для даної проблематики можна виразити за допомогою графу (рис.1).

Цей підхід виділяє морфологічні особливості та їх взаємозв'язки в межах кожної фігури. В даному випадку, ми використали сегменти фігури як елементарну морфологію. Стабільнішим можна назвати підхід, де від рамки аналізується лише її окрема частина. Для будь-яких двох прямих, що

розташовані недалеко один від одного, з деяким зміщенням по осі X та Y, з правильним відношенням відстані між ними до їх довжини, розглядається гіпотеза того, що номер знаходиться між ними. Цей підхід схожий на спрощений метод HOG(англ. Histogram of Oriented Gradients).

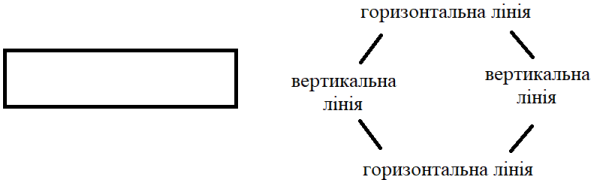

Рисунок 1 – Структурний підхід для розпізнавання образу.

Існує дуже багато можливих методів аналізу зображення, які з різною точністю допомагають досягти бажаного результату. Всі ці методи базуються на якихось певних принципах, в яких є свої недоліки. Саме тому актуальним є пошук підходів для розв'язування даних задач та механізмів їх коригування, які б забезпечили прийнятний рівень розв'язку.

Перелік посилань

1. Стокман Дж. Компьютерное зрение = Computer Vision / Джордж Стокман, Линда Шапиро. – М.: Бином. Лаборатория знаний, 2006. – 752 с.

2. CBIR: Texture Features [Електронний ресурс]. – The University of Auckland. New Zealand. Режим доступу до ресурсу: http://www.cs.auckland.ac.nz/compsci708s1c/lectures/Glect-html/topic4c708FSC.htm

Розподілені системи виявлення зловмисного програмного забезпечення

Комар А., Стецюк М.В., Паюк В.П.
Науковий керівник – к.т.н., доц. Медзатий Д.М.
Хмельницький національний університет

Невпинне щоденне збільшення та використання зловмисного програмного забезпечення (ЗПЗ) створює проблеми користувачам комп'ютерних систем (КС). Отримання фінансової вигоди або іншої переваги вмотивовують розробників зловмисного програмного забезпечення до його збільшення та розповсюдження [1, 2]. Ними до його створення залучаються сучасні технології розробки програмних засобів, в тому числі і розподілених.

Ефективне застосування методів та засобів виявлення ЗПЗ потребує розробки системи, яка б включала в себе достатню кількість реалізованих ефективних методів у вигляді відповідних підсистем, мала можливість до нарощування та враховувала б майбутні тенденції розвитку як антивірусних засобів, так і ЗПЗ. Оскільки, сучасне ЗПЗ переважно є керованим розподіленим програмним забезпеченням зловмисника, то перспективним напрямом досліджень на противагу є розроблення теорії і практики створення розподілених систем виявлення [3]. Важливими задачами при цьому є розробка методу виявлення бот-мереж із застосуванням розподілених систем та методу взаємодії їх компонентів в локальних мережах, особливістю якого була б можливість такої організації системи, що надавала б узгоджену підтримку методам виявлення безпосередньо мережного ЗПЗ.

Відомі методи (метод сигнатурного аналізу, метод контрольних сум, метод евристичного аналізу та інші) виявлення ЗПЗ переважно орієнтовані на застосування в кінцевих КС. Для антивірусних засобів мережного типу розроблено методи, застосування яких є можливим переважно на сервері або в корпоративних чи локальних мережах. Більшість з цих методів розроблено з використанням технологій та компонентів штучного інтелекту. Як правило, сучасні системи виявлення ЗПЗ містять набори багатьох методів та їх комбінацій, на що впливає зростання різновидів ЗПЗ. Розглянемо детальніше відомі системи та методи для виявлення ЗПЗ.

Новими сферами застосування ЗПЗ для отримання вигод і переваг, враховуючи попередню фінансову, стали військова і політична. Військові доктрини багатьох країн світу включають розвиток військових кіберпідрозділів, які розвивають і використовують ЗПЗ для нанесення матеріальної шкоди інфраструктурі інших країн. Застосування руйнуючих технологій ЗПЗ дозволяє здійснювати віддалені атаки, не потребуючи перебування поряд з об’єктом атаки [3]. Особливої уваги заслуговує захист від таких атак підприємств і організацій реального сектору економіки, атаки на які протягом останніх років суттєво зросли і завдають їм значних збитків. Проведення успішних атак в різних секторах країни може паралізувати на тривалий час її основну інфраструктуру та фінансовий сектор. Крім того, поява нових фінансових інструментів, зокрема альтернативних валют, мотивує зловмисників до подальшого технологічного розвитку ЗПЗ для отримання вигоди. При цьому вони починають залучати обчислювальні потужності не тільки власні, а і інших користувачів, комп’ютерні системи яких приєднані до глобальної мережі. Тому, проблема виявлення ЗПЗ для організацій та підприємств залишається актуальною.

Файлове зловмисне програмне забезпечення, яке характеризується тим, що його поширення першочергово має відбуватись в окремій комп’ютерній системі. Файлове ЗПЗ, що міститься у файлах виконуваних

програм, після запуску виконуваних програм отримує можливість для пошуку програмних файлів для подальшого свого поширення, для виконання деструктивних дій та отримання контролю над КС з метою приховування своєї присутності. Переміщення файлового ЗПЗ в інші КС мережі може бути здійснено переважно користувачами через порушення політик безпеки. Наявність однакового за функціоналом файлового ЗПЗ в різних КС локальної мережі організації чи підприємства потребує для його виявлення наявності таких методів його виявлення, які б дозволяли враховувати результати моніторингу і сканування різних КС локальної мережі і приймати рішення про наявність ЗПЗ. Тому, перспективною задачею є розробка методів виявлення файлового ЗПЗ з врахуванням особливостей їх використання саме в розподілених системах.

Для підтримки цілісності розподілених систем потрібно буде розробити метод взаємодії компонентів. Напрямками подальших досліджень є розробка нових методів виявлення ЗПЗ. Розроблені методи повинні орієнтуватись на особливості архітектури розподіленої системи та використовувати цю перевагу над іншими хостовими методами.

Перелік посилань

1. Security Response Publications. (2019). Monthly Threat Report. Retrieved from https://www.symantec. com/security_response/publications/ monthlythreatreport.jsp.

2. McAfee Labs. (2019). McAfee Labs Threat Report. December 2017. Retrieved from https://www.mcafee.com /us/resources/reports/rp-quarterly-threats-dec-2017.pdf.

3. Markowsky, G., Savenko, O., Sachenko, A. (2019). Distributed Malware Detection System Based on Decentralized Architecture in Local Area Networks. Advances in Intelligent Systems and Computing III, 871, 582–598. DOI: 10.1007/978-3-030-01069-0_42.

Метод та засоби ідентифікації бот-мереж, що використовують технологію «потік доменів»

Комаров В.І.
Науковий керівник – к.т.н., доц. Лисенко С.М.
Хмельницький національний університет

Сучасні IT-системи зазвичай покладаються на систему доменних імен (DNS) для перекладу важких для запам’ятовування IP-адрес на легкі для розуміння людиною слова. Також вона виступає в якості системи каталогів, яка використовує ієрархічну схему іменування для ефективного

відображення імен за адресами[1]. Однак кіберзлочинці часто зловживають доменними іменами, оскільки DNS трафік, як правило, нефільтрований або дозволений через брандмауер, тим самим забезпечується стійкий і безперешкодний канал зв'язку.

Сучасні бот-мережі, такі як Zeus (Zbot, PRG, Wsnpoem, Gorhax, Kneber)[2], Torpig[1], Kraken[3], Conficker (DownUp, DownAndUp, DownAdUp, Kido)[2, 3], зазвичай використовують технологію, яку називають «потік доменів», або алгоритм генерації домену (DGA)[4], щоб генерувати велику кількість псевдовипадкових доменних імен[1], аби динамічно керувати операторами бот-мереж та їх ботами. «Потік доменів» – це техніка для збереження шкідливої бот-мережі в роботі шляхом постійної зміни доменного імені Command and Control (C&C) сервера. Доменні імена змінюються з часом на основі певного алгоритму, який відомий лише власнику бот-мережі, що ускладнює виявлення шкідливого трафіку, серверів команд та управління[1]. Такі бот-мережі стають однією з найсерйозніших загроз безпеки інтернету.

Однак бот-мережі з технологією «потік доменів» мають деякі унікальні характеристики, які ми можемо використовувати для їх виявлення. Зазвичай вони генерують велику кількість запитів DNS, зареєстрованих на одну і ту ж IP-адресу, і вони часто генерують багато збоїв у DNS-трафіку[5]. Невдалі
DNS-запити можуть вказувати на наявність ботів на клієнтах, тоді як успішні запити, які відбуваються в часі поруч з невдалими, ймовірно пов’язані з неінфікованими клієнтами. Також доменні імена в запитах DNS генеруються випадковим чином або алгоритмічно, і їх буквено-цифровий розподіл значно відрізняється від сформованих людиною[5].

При аналізі відомих для нас підходів виявлення бот-мереж з технологією «потік доменів» прослідковувався незначний рівень ідентифікації ботів бот-мереж, а також значна кількість помилкових спрацювань. Тому ми зосереджуємось на виявленні бот-мереж з технологією «потік доменів» в мережі на основі ознак DNS трафіку. Цей метод фіксує весь DNS-трафік із шлюзу відстежувальної мережі або окремого її вузла, а потім витягує і опрацьовує ключові ознаки для ефективного виявлення бот-мереж та шкідливого трафіку.

У технології «потік доменів» інфікований хост використовує алгоритм генерації домену (DGA) для запиту на існування серії доменних імен, які, як очікується, будуть C&C-серверами, тоді як власник повинен зареєструвати лише одне таке доменне ім’я[5]. Ця методика призводить до багатьох збоїв у запитах DNS, оскільки не всі ці доменні імена зареєстровані[6]. Серед ознак, які формує наш метод виявлення є збої у запитах DNS, що виникають у результаті використання технології «потік доменів». Ми оброблятимемо мережевий трафік та аналізуватимемо всі збої і буде запропонований поріг

відмов DNS-запиту з тієї ж IP-адреси за допомогою аналізу ознак та їх значень, що дозволить виявити бот-мережу «потік доменів» та ідентифікувати заражений хост.

В якості додаткового методу виявлення бот-мережі з технологією «потік доменів» будемо також використовувати частотний лексичний аналіз доменних імен [2, 7], адже частота вживання літер та цифр в сформованих людиною доменах буде істотно відрізнятись від генерованих алгоритмом генерації домену бот-мережі[3] (генератором псевдовипадкових доменних імен [4]).

Для того щоб виявити діяльність бот-мережі, яка використовує технологію «потік доменів» використовуються наступні ознаки:

1. N_{dom} – кількість доменних імен, які спільно використовують IP-адресу.
2. S – бінарна ознака успішності DNS-запиту (якщо S = false – невдалий DNS-запит, а якщо S = true – вдалий DNS-запит).
3. T_{mod} – TTL-період, мода (значення, яке найчастіше зустрічається).
4. T_{med} – TTL-період, медіана (середнє значення з усієї вибірки, яке розділяє її на дві рівні частини).
5. T_{aver} – TTL-період, середнє арифметичне значення.
6. L_{dom} – довжина доменного імені.
7. W_{dom} – зважена оцінка частотного лексичного аналізу доменних імен, визначається за формулою:

$$W_{dom} = \frac{\sum_{i=0}^{n} X_i}{n}, \quad (1)$$

де n – кількість літер в доменному імені, а X_i – частота використання i-тої літери.

На основі цих ознак та певних правил відбувається виявлення бот-мереж з технологією «потік доменів» (рис. 1).

Ідея методу виявлення бот-мережі з технологією «потік доменів» наступна:

1. Збір вхідного DNS-трафіка.
2. Визначення усіх наявних параметрів та ознак у зібраному трафіку.
3. Виявлення запитів, в яких доменні імена за методом статистичного аналізу найімовірніше сформовані алгоритмічно.
4. Виявлення груп, в яких DNS-запит є невдалим.
5. Виявлення, обробка та обрахунок ознак запитів, які ігнорують TTL-період.
6. Співставлення кількох груп ознак та їх аналіз за допомогою штучного інтелекту на машинного навчання.

Сучасні бот-мережі з технологією «потік доменів» використовують дедалі складніші методи генерації доменів та генерують щодня десятки тисяч псевдовипадкових доменних імен[5]. Вони все частіше змінюють свої

характеристики та поведінку, тому потрібний комплексний підхід для виявлення бот-мереж з технологією «потік доменів». В основі представленого вище методу лежить поєднання: вибірки та співставлення ознак отриманого трафіку, опрацювання збоїв у DNS-запитах та використання частотного лексичного аналізу доменних імен. Все це дозволить комплексно опрацювати отриманий DNS-трафік та ідентифікувати бот-мережі з технологією «потік доменів».

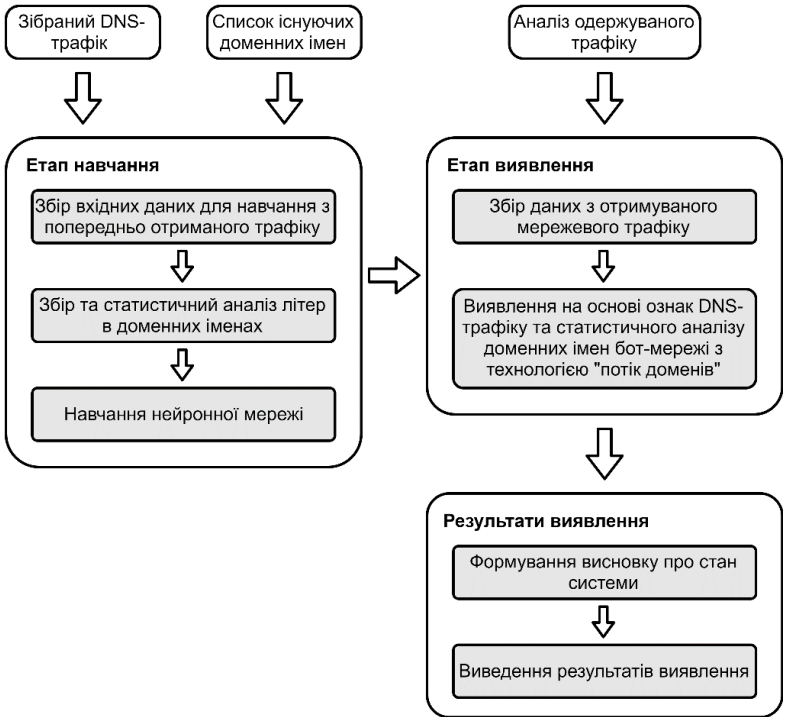

Рисунок 1 Процес виявлення бот-мережі з технологією «потік доменів»

Перелік посилань

1. R. Dodopoulos, “DNS-based Detection of Malicious Activity”, Master’s thesis, Eindhoven University of Technology, 2015.

2. Truong, D. - T., and Cheng, G. (2016) Detecting domain- flux botnet based on DNS traffic features in managed network. Security Comm. Networks, 9: 2338– 2347. doi: 10.1002/sec.1495.

3. R. Kokkelkoren, “Catching flux-networks in the open”, thesis, , University of Twente, 2019.

4. U. Sternfeld, (2016). Dissecting domain generation algorithm: eight real world DGA Variants. Available: http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-Dissecting-DGAs-Eight-Real-World-DGA-Variants.pdf.

5. Agyepong, Enoch & Buchanan, William & Jones, Kevin. (2018). Detection of Algorithmically Generated Malicious Domain Using Frequency Analysis. International Journal of Computer Science and Information Technology. 10. 91-111. 10.5121/ijcsit.2018.10306.

6. P. Arntz, (2016, June 27). Explained: Domain Generating Algorithm. Available: https://blog.malwarebytes.com/security-world/2016/12/explained-domain-generating-algorithm/.

7. Agyepong, Enoch & Buchanan, William & Jones, Kevin. (2018). Detection of Algorithmically Generated Malicious Domain Using Frequency Analysis. International Journal of Computer Science and Information Technology. 10. 91-111. 10.5121/ijcsit.2018.10306.

Планування мережі доступу NGN для нових груп користувачів

Котюк Д.Ю.
Науковий керівник – к.т.н.доц. Чорненький В.І.
Хмельницький національний університет

В даний час все частіше зустрічаються публікації, присвячені корінного перетворення ТМЗК і переходу до мережі наступного покоління (NGN). Вона позиціонується як універсальна мережа, здатна задовольнити практично будь-які потреби користувачів із заданою якістю обслуговування. При цьому передбачається простота введення нових послуг.

Зазвичай розглядається два основних варіанти переходу до NGN - починаючи з транспортної мережі і з мережі доступу. У даній роботі розглядається другий варіант переходу до мереж наступного покоління.

Сьогодні вже все рідше висловлюються думки про те, що NGN радикально знизить витрати на побудову мережі, так само як і про те, що NGN мало не в рази скорочує вимоги до смуги пропускання. Дана робота покликана оцінити необхідні ресурси мережі доступу, виявити недоліки і переваги NGN.

Для побудови мережі, що задовольняє концепції GII, в функціональній моделі NGN ITU виділяє три категорії об'єктів: функції, сервіси, ресурси. Сервіси реалізуються різними функціями за допомогою доступних ресурсів. Один і той же сервіс може реалізовуватися різним набором функцій і навпаки,

одна функція може використовуватися для реалізації різних сервісів. Їх взаємозв'язок показана на рис. 1.

Архітектура мережі зв'язку, побудованої відповідно до концепції NGN, представлена на рис. 2.

Основу мережі NGN складає універсальна транспортна мережа, яка реалізує функції транспортного рівня і рівня управління комутацією і передачею. До складу транспортної мережі NGN можуть входити: транзитні вузли, що виконують функції перенесення і комутації; кінцеві (граничні) вузли, що забезпечують доступ абонентів до мультисервісної мережі; контролери сигналізації, які виконують функції обробки інформації сигналізації, управління викликами і з'єднаннями; шлюзи, що дозволяють здійснити підключення традиційних мереж зв'язку (ТМЗК, МПД, МРЗ).

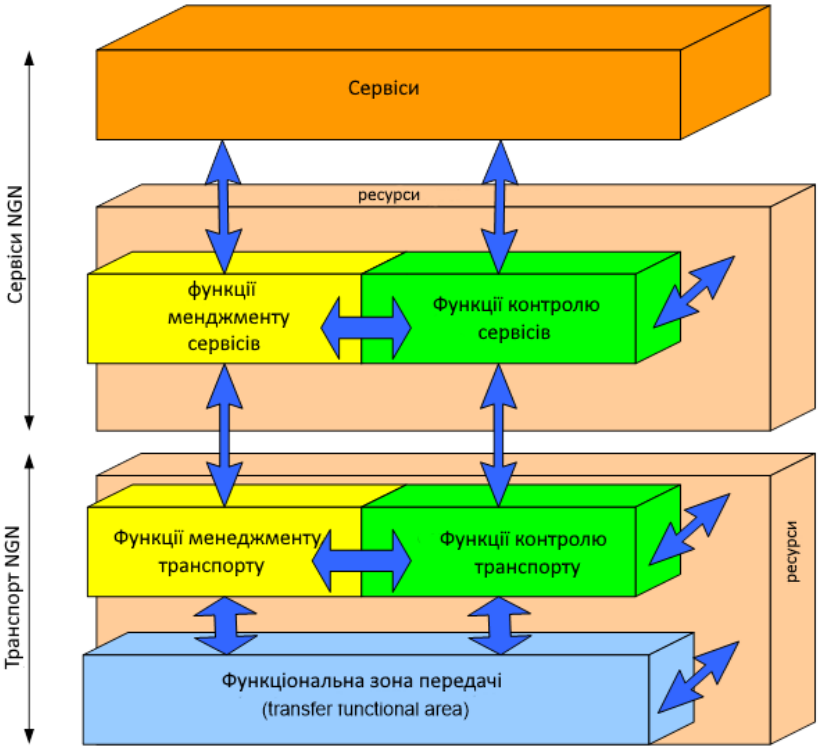

Рисунок1- Узагальнена функціональна модель NGN

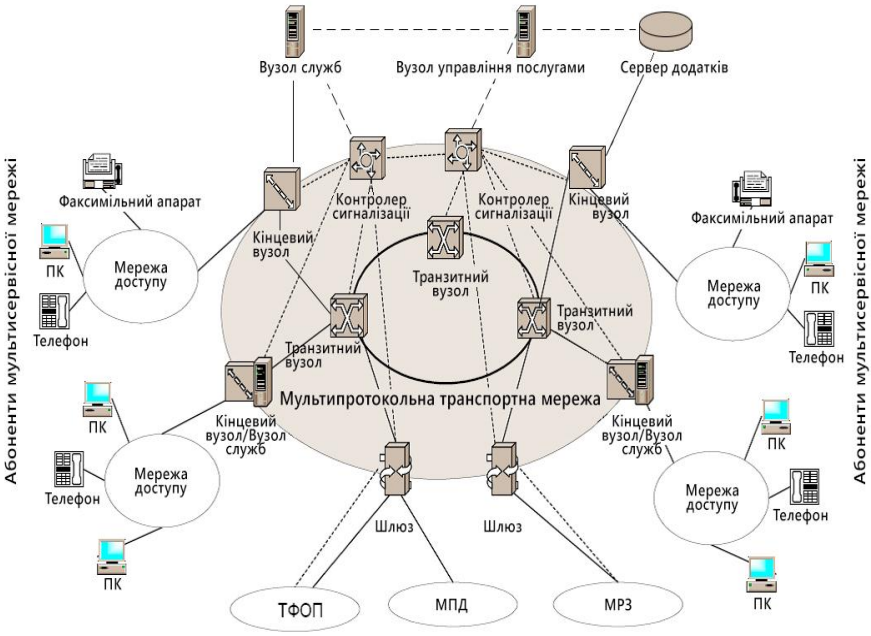

Рисунок 2- Мережа, побудована відповідно до концепції NGN

Перелік посилань

1. Пінчук А.В. Соколов Н.А. Модернізація МТС без вузлів. - Вісник зв'язку, 2005, №12.

2. Пінчук А.В. Соколов Н.А. Модернізація МТС з вузлами вхідного повідомлення. - Вісник зв'язку, 2006, №1.

3. РТМ «Модернізація мереж доступу». - НТЦ Протей, 2005.

Аналіз проблем багатофункціональних кооперативних робототехнічних систем

Красовський М.В.
Науковий керівник – д.т.н.проф. Говорущенко Т. О.
Хмельницький національний університет

Вступ. Сьогоднішнє покоління роботів – це «інтелектуальні» роботи, обладнані системами управління з елементами штучного інтелекту, які є повністю автономними і не потребують втручання оператора [1]. Кооперативна робототехніка – це нова галузь промислової робототехніки, яка

дає можливість спільного виробництва. Кооперативне виробництво значною мірою залежить від наявності кооперативного (колективного, коллаборативного робота (кобота). Кобот – це варіант промислового робота, оснащеного системою сенсорів та комп'ютерного зору, що дозволяє з високим ступенем ймовірності попереджати зіткнення пристрою з людиною та перешкодами, включаючи ситуацію збою вбудованого програмного забезпечення [2]. Основна задача коботів – допомогти розв'язати складні задачі, які неможливо автоматизувати. Очікується, що ринок коботів досягне 12303 млн. дол. США до 2025 р. з 710 млн. дол. США у 2018 р., тобто на 50,31% протягом 2018-2025 років [3]. Враховуючи актуальність використання кооперативної робототехніки, інтенсивний розвиток ринку коботів, метою даного дослідження є аналіз сучасних проблем багатофункціональних кооперативних робототехнічних систем.

Аналіз відомих методів та рішень в галузі багатофункціональних кооперативних робототехнічних систем. У кооперативній робототехніці як людина, так і робот виконують завдання над тим самим продуктом у спільній робочій області, але не одночасно. Коботи – універсальні і можуть виконувати різні задачі. Їх можна швидко переналагодити на розв'язання різноманітних задач. Вони не вимагають особливих увимог до умов експлуатації – вони можуть встановлюватись як на повітряних суднах, так і в звичайних квартирах. Роботи взаємодіють один з одним і безпечно працюють поруч з людьми та навчаються у них. Об'єднання працівника та коботу в одній виробничій комірці може забезпечити простий і дешевий спосіб гнучкого налаштування виробництва, а також спосіб адаптації до виробничих потреб у реальному часі без зупинки та змін виробничих операцій [1].

В роботі [4] доведено факт, що наразі збільшився науковий інтерес до систем, що складаються з декількох автономних мобільних роботів, які демонструють кооперативну поведінку, але при цьому теоретична підтримка такої кооперації певної кількості робототехнічних засобів все ще перебуває у стадії формування.

Наявність декількох робототехнічних систем, здатних спільно працювати під контролем одного оператора, може спростити виконання складних завдань, які були би складними для однієї роботизованої системи. Система управління в реальному часі Sandia SMART (послідовна модульна архітектура для робототехніки та телеоперації) дозволила розробити такі системи. Системи здатні підтримувати знання про своє положення і положення інших систем, розташування об'єкта і спільну роботу для виконання складних завдань, покладених на них одним оператором [5].

Автори [6] показують, що запропоновано багато підходів до розробки командно-кооопераційної співпраці між людьми та машинами, включаючи розподіл функцій, наглядний контроль, адаптивну автоматизацію, динамічний розподіл завдань, регульовану автономію, взаємодію з

ініціативами, але всі ці підходи спираються на концепцію автономії як еталон для продуктивності машин і критерій прийняття рішень про розподіл завдань між людиною та машиною. Автори [6] доводять, що концепція рівнів автономії (рис. 1) є неповною і недостатньою для моделювання складних людино-машинних команд, в основному тому, що вона недостатньо враховує взаємозалежність їх членів. У статті введено поняття коактивного дизайну, запропоновано підхід до людино-машинної взаємодії, який приймає взаємозалежність як центральний принцип організації між людьми та агентами, які працюють разом як команда.

Level	Description
High	10. The computer decides everything, acts autonomously, ignoring the human.
	9. The computer informs the human only if it, the computer, decides to.
	8. The computer informs the human only if asked, or
	7. The computer executes automatically, then necessarily informs the human, and
	6. The computer allows the human a restricted time to veto before automatic execution, or
	5. The computer executes that suggestion if the human approves, or
	4. The computer suggests one alternative
	3. The computer narrows the selection down to a few, or
	2. The computer offers a complete set of decision/action alternatives, or
Low	1. The computer offers no assistance; the human must take all decisions and actions.

Рисунок 1 – Схема процесу оцінювання достатності інформації щодо якості у специфікаціях вимог до ПЗ [6]

Проведений аналіз відомих методів та рішень в галузі кооперативної робототехніки свідчить про те, що було досягнуто значного прогресу в кооперативній робототехніці, але наразі все ж залишається ряд невирішених питань, зокрема: 1) як кооперативна робототехнічна система може обробляти більш складні завдання, які можуть вирішувати люди? – проста схема дворівневого планування завдань більше не підходить; важливою є багатошарова схема, що включає аналіз завдань, узгодження завдань, виконання завдань і нагляд за завданнями; 2) як забезпечити надійність руху фізичної кооперативної робототехнічної системи у реальному світі? – невирішеними залишаються проблеми зіткнення, перевантаження та заїзду в тупик; 3) як більш раціонально спланувати та проаналізувати інформацію, отриману кожним окремим роботом (а потім зробити їх рішення більш ефективними)? – існує вимога обміну інформацією, оскільки робот в команді може тільки сприймати місцеву інформацію; ефективне злиття даних може

допомогти створити ефективний план, а потім провести координацію між роботами; 4) як організувати легке втручання людини до кооперативної робототехнічної системи відповідно до потреб? – наразі багато завдань все ще надто складні для роботів, і координація між людьми і роботами повинна бути вивчена, оскільки в сучасних умовах взаємодія людини з машиною є повсюдною.

Висновки. Проведений аналіз відомих методів та рішень в галузі кооперативної робототехніки, а також методів формалізації задач, на вирішення яких орієнтовано розроблювані коботи, свідчить про те, що при чималій кількості ефективних рішень наразі в галузі залишається ряд невирішених питань, зокрема, проблема раціонального планування та підвищення якості аналізу інформації, якою обмінюються люди та коботи в спільному середовищі, підвищення ефективності їх рішень. Всі зазначені невирішені проблеми є важко формалізованими та потребують використання компонентів штучного інтелекту для їх вирішення.

Перелік посилань

1.Sadik, A. R. An Ontology-Based Approach to Enable Knowledge Representation and Reasoning in Worker-Cobot Agile Manufacturing / A. R. Sadik, B. Urban // Future Internet. – 2017. – Vol. 9. – Issue 4. – Article number 90.

2.Инновации в робототехнике и безопасность [Електронний ресурс]. – Режим доступу: https://controlengrussia.com/innovatsii/innovatsii -v-robototehnike-i-bezopasnost/.

3.Collaborative robot market projected to grow at a CAGR of 50.31% from 2018 to 2025 [Electronic resource]. – Access mode: https://www.reportsnreports.com/reports/650005-collaborative-robots-market-by-payload-up-to-5-kg-up-to-10-kg-above-10-kg-application-industry-and-geography-global-forecast-to-2022.html.

4.Uny Cao, Y. Cooperative Mobile Robotics: Antecedents and Directions / Y. Uny Cao, A. S. Fukunaga, A. Kahng // Autonomous Robots. – 1997. – Vol. 4. – Issue 1. – Pp. 7-27.

5.Multi-Robot Cooperative Behavior [Electronic resource]. – Access mode: https://www.sandia.gov/research/robotics/advanced_controls/multi_robot_cooperative_behavior.html.

6.Johnson, M. Beyond Cooperative Robotics: The Central Role of Interdependence in Coactive Design / M. Johnson, J. M. Bradshaw, P. J. Feltovich, R. R. Hoffman, C. Jonker, B. Riemsdijk, M. Sierhuis // Intelligent Systems. – 2011. – Vol. 26. – Issue 3. – Pp. 81-88.

Аналіз проблем верифікації врахування інформації предметної галузі в процесі розроблення програмного забезпечення комп'ютерних систем

Лопатто І. Ю.
Науковий керівник – д.т.н.проф. Говорущенко Т. О.
Хмельницький національний університет

Вступ. Успішність програмних проектів і досі залежить від знань та досвіду розробників. На сьогодні в світі витрачається більше 250 млрд. USD щорічно на розроблення приблизно 175 тис. програмних проектів [1]. При цьому значна кількість (до 70%) програмних проектів є проблемними (проекти, які мали перевищення термінів, перевитрати або не мали необхідних можливостей та функцій) або провальними (проекти, які були скасовані до завершення, або були доставлені, але ніколи не використовуються) [1].

Успішність реалізації програмного проекту часто є низькою через те, що недостатньо уваги приділяється питанню відношення до інформації предметної галузі на різних етапах життєвого циклу програмного забезпечення (ПЗ), її достатності, достовірності, уточнення. Деяка інформація аналізується занадто прискіпливо, а деяка – взагалі не враховується. Часто відкидається інформація предметної галузі з малою ймовірністю, а інколи й імовірність її взагалі не оцінюється. Нова інформація може надходити на різних етапах життєвого циклу – як на етапах формування та формулювання вимог і проектування архітектури, так і на етапах реалізації та експлуатації, але нею часто нехтують. Таке нехтування інформацією предметної галузі на всіх етапах життєвого циклу є одним з критичних факторів при розробленні програмного забезпечення [2, 3].

Розроблення ПЗ комп'ютерних систем вимагає врахування інформації предметної галузі на усіх етапах його проектування та розробки з метою підвищення його надійності, функціональної безпеки, живучості та гарантоздатності. Відтак, верифікація врахування інформації предметної галузі в процесі розроблення ПЗ є важливою та актуальною задачею.

Аналіз проблем верифікації врахування інформації предметної галузі в процесі розроблення програмного забезпечення комп'ютерних систем. В процесі роботи над програмним проектом важливо оцінити частку інформаційної невизначеності проекту. Причиною виникнення інформаційної невизначеності проекту є низький рівень документування знань, особливо на системному рівні (рис. 1 [4]).

На рис. 2 зображено ситуацію, що характеризується передчасністю проектних рішень та їх документації до розуміння проектування. Показану область називають «розривом у знаннях» (knowledge gap), наявність якого є практичним результатом і першопричиною багатьох інженерних невдач [5].

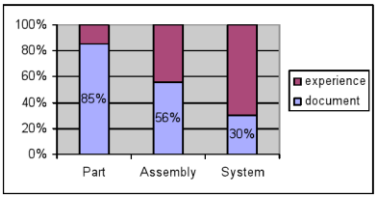

Рисунок 1 – Документування знань на системному рівні [4]

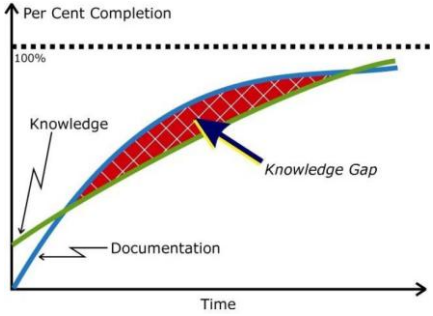

Рисунок 2 – Розрив у знаннях (Knowledge Gap) [5]

Факт часткового неврахування інформації предметної галузі на різних етапах життєвого циклу ПЗ свідчить про те, що розмір розриву у знаннях не є сталим для програмного проекту – в процесі життєвого циклу він може збільшуватись і зменшуватись, оскільки з'являється нова інформація, яку потрібно враховувати.

Для інженерії ПЗ представлена на рис. 2 точка зору на розрив у знаннях не зовсім відповідає реальності. Часткове врахування інформації предметної галузі протягом життєвого циклу і вплив її вже на готовий продукт призводять до збільшення розміру розриву у знаннях в процесі життєвого циклу, що може стати причиною збоїв та інших проблем з ПЗ. Для безпечного функціювання ПЗ розмір розриву у знаннях бажано зменшувати за рахунок більш повного врахування (зменшення втрат) інформації предметної галузі протягом життєвого циклу програмного проекту [6].

Враховуючи вищесказане, всі наявні знання та інформацію про програмну систему представимо у вигляді діаграми, в якій є сектор, що відображає об'єм недостатньої (невідомої) інформації (розрив у знаннях) – рис. 3.

Даний сектор складає неврахована інформація предметної галузі (в тому числі інформація, відсутня у специфікації вимог до ПЗ). Розміри сектору з невідомою інформацією не визначені, оскільки незрозуміло, яка і скільки інформації залишається невідомою. Сектор з невідомою інформацією слід звужувати – за рахунок більш повного врахування інформації предметної галузі, починаючи з ранніх етапів життєвого циклу. Чим меншим буде розмір

сектору невідомої інформації, тим якіснішою буде програмна система, тим безпечніше вона працюватиме та тим успішнішою буде її реалізація. Отже, актуальним є підхід до зменшення частки невідомої інформації про програмну систему.

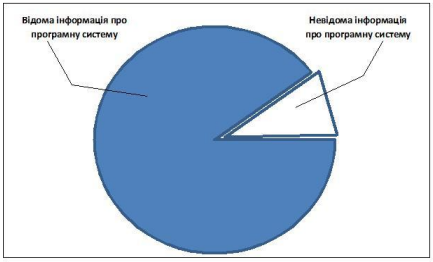

Рисунок 3 – Поле знань про ПЗ із сектором невідомої інформації

Висновки. При розробленні програмних проектів існує розрив у знаннях про характеристики майбутнього ПЗ. Цей розрив з'являється через відсутність знань про те, яка інформація з'явиться в процесі взаємодії «підсистем – інтерфейсів – даних – зовнішніх впливів» і якими характеристиками ПЗ вона проявиться, а також через часткове врахування інформації предметної галузі протягом життєвого циклу ПЗ. Розмір розриву у знаннях не є сталим для програмного проекту. Імовірність того, що в процесі життєвого циклу проекту розрив у знаннях зникне, є низькою, а при появі нової інформації предметної галузі може відбутись збільшення розміру розриву у знаннях. Для успішної реалізації та подальшого безпечного функціонування ПЗ, розмір розриву у знаннях бажано зменшувати, враховуючи якнайбільше інформації предметної галузі протягом життєвого циклу ПЗ. Тому потрібні принципово нові підходи, пов'язані із врахуванням інформації предметної галузі в процесі розроблення програмного забезпечення комп'ютерних систем.

Перелік посилань

1.Hastie, S. Standish Group 2015 Chaos Report – Q&A with Jennifer Lynch [Electronic resource] / S. Hastie, S. Wojewoda. – Access mode: http://www.infoq.com/articles/standish-chaos-2015.

2. Munch, J. Perspectives on the future of software engineering / J. Munch, K. Schmid. – Berlin: Springer-Verlag Berlin Heidelberg, 2013. – 365 p.

3. Diaz, V. G. Handbook of research on innovations in systems and software engineering / V. G. Diaz, J. M. Lovelle, B. C. Garcia-Bustelo. – Hershey (USA): IGI Global, 2015. – 745 p.

4. Maier, R. Knowledge management systems. Information and

communication technologies for knowledge management / R. Maier. – Berlin: Springer Science & Business Media, 2013. – 635 p.

5. Patterson, Jr. F. G. Life cycles for system acquisition / Jr. F. G. Patterson // Encyclopedia of Life Support Systems, Systems Engineering and Management for Sustainable Development. – Paris, 2004. – Pp. 82–110.

6. Pomorova, O. The way to detection of software emergent properties / O. Pomorova, T. Hovorushchenko // The 8-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems, September 24-26, 2015: Proceedings. – Vol. 2. – Warsaw, 2015. – Pp. 779–784.

Використання операційної системи «Linux»

Молочко В. С, Прибіш В. В.
Науковий керівник – к. ф.-м. н., доц., Частоколенко І. П.,
викладач Марченко А.П.
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля
Національного університету цивільного захисту України

З метою легалізації та уніфікації комп'ютерних програм, які використовуються у ДСНС України, та відповідно до постанови Кабінету Міністрів України від 10 вересня 2003 р. № 1433 «Про затвердження Порядку виконання комп'ютерних програм в органах виконавчої влади» потрібно використовувати тільки ліцензійні примірники комп'ютерних програм. Як відомо в ДСНС України, зазвичай, використовуються не ліцензійне ПЗ, яке потрібно замінити на ВПЗ, яке має ліцензію. Насамперед потрібно замінити ОС, найкраще для цього «підходить» «Linux». Більшість дистрибутивів Linux поширюються абсолютно безкоштовно. Це означає, що ДСНС України не повинна платити за сам факт використання операційної системи, за призначені для користувача ліцензії та інші відрахування, які притаманні комерційним системам. Безкоштовність і, як наслідок, економія коштів - одна з основних причин впровадження Linux у ДСНС України.

Метою роботи є дослідження особливостей умов впровадження ОС Linux у ДСНС України, дослідження готовності звичайних користувачів, науково-педагогічних працівників, курсантів та студентів, надання знань про операційну систему Linux, її устрій, безпеку, в порівнянні з Windows, низькі системні вимоги, принцип роботи, недоліки та переваги, легалізація та уніфікації комп'ютерних програм, які використовуються у ДСНС України та ЧІПБ відповідно до діючого законодавства Кабінету Міністрів України, а також огляд подібного безкоштовного програмного забезпечення для отримання оптимального результату та висновку.

У відповідності з метою дослідження у роботі ставляться такі завдання: використання ОС Linux в навчальному процесі ЧІПБ імені Героїв Чорнобиля та інших ВНЗ України та органах і підрозділах ДСНС України, переваги використання операційної системи Linux, проблеми впровадження ОС Linux в навчальний процес та органи і підрозділи ДСНС України, економія коштів, що є одною з основних причин впровадження Linux у ДСНС України.

Об'єкт дослідження – дослідження особливостей умов впровадження ОС Linux, дослідження готовності користувачів для організації електронного документообігу у ДСНС України та Черкаському інституті пожежної безпеки ім. Героїв Чорнобиля НУЦЗ України.

Предмет дослідження – особливості впровадження нових інформаційних технологій, які вільно-розповсюджуються, що можуть використовуватись в підрозділах ДСНС України.

У процесі дослідження використовувався такий метод: програмно–апаратний метод дослідження з використання операційної системи «Linux» в органах та підрозділах, як альтернатива платній операційній системі «Windows».

Наукове значення дослідження полягає в тому, що: обгрунтовано дидактичні умови ефективного використання теоретичних та практичних основ з використання операційної системи «Linux» в органах та підрозділах, як альтернатива платній операційній системі «Windows».

Практичне значення результатів. Розроблені теоретичні та практичні рекомендації, які можуть бути надані для використання служб і відділів науково–педагогічними працівниками та співробітниками ДСНС України для перспективи та практичного використання операційної системи «Linux» в органах та підрозділах, як альтернатива платній операційній системі «Windows» та з метою підвищення захисту документообігу, а також зберігання службової інформації.

Перелік посилань

1. Постанова Кабінету Міністрів України від 10 вересня 2003 р. № 1433 «Про затвердження Порядку виконання комп'ютерних програм в органах виконавчої влади».
2. https://uk.wikipedia.org/wiki/Linux.
3. https://uk.wikipedia.org/wiki/Дистрибутив_Лінукс.
4. http://linux2u.ru/vnedrenie-linux-v-organizacijah.html.
5. http://works.doklad.ru/view/PNWsJdsbJOQ.html.
6. Наказ ДСНС України № 476 від 18.08.2014 «Про використання комп'ютерних програм у ДСНС України».

Навчальний лабораторний стенд на мікроконтролері архітектури ARM

Наумчук М.М.
Науковий керівник – к.т.н., доц. Тиртишніков О.І.
Полтавський національний технічний університет
імені Юрія Кондратюка

Сфера застосування мікроконтролерів (МК) постійно розширюється. Одночасно розширюються функціональні можливості МК, розробляються нові їх архітектури та вдосконалюються існуючі. Відповідно, вивчення найбільш розповсюджених архітектур МК, методів та засобів їх програмування є невід'ємною частиною підготовки фахівця спеціальності «Комп'ютерна інженерія».

Однією з найбільш популярних архітектур МК є архітектура ARM – 32-бітна RISC-архітектура процесорів [1, 2], яку розробила компанія ARM Limited. Вона є фактично домінуючою в галузі створення різноманітних портативних пристроїв, що обумовлено широким впровадженням в ARM МК енергозберігаючих технологій.

Метою дослідження є обґрунтування структури, розробка та реалізація прототипу навчального лабораторного стенда (НЛС) на основі ARM-МК сімейства STM32F7.

Був проведений аналіз архітектурних особливостей та функціональних можливостей сучасних ARM-МК архітектури та обґрунтований вибір конкретного МК, спроектований та реалізований НЛС, який структурно складається з двох модулів – системної плати та процесорного модуля. Загальний вигляд НЛС із встановленим процесорним модулем показаний на рис. 1.

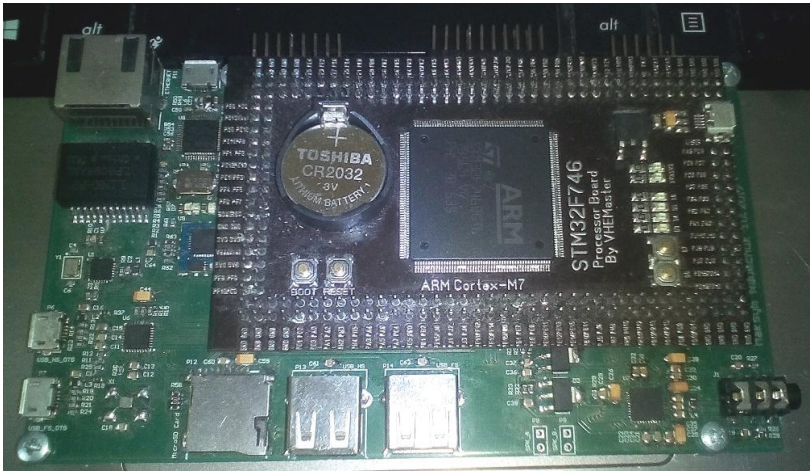

Рисунок 1 – Загальний вигляд НЛС

Основні можливості стенда:

- має 168 портів загального призначення, за допомогою яких МК може керувати будь-якими зовнішніми пристроями;
- високошвидкісне ARM-ядро центрального процесора;
- швидке перепрограмування та налагодження коду завдяки вбудованому програматору;
- обробка великих масивів даних завдяки великому обсягу убудованої пам'яті (256 Мбайт);
- можливість використання багатозадачної операційної системи;
- підтримка WiFi, Ethernet; створення портативної WiFi точки доступу;
- можливість виведення зображення на LCD дисплей, наприклад, від ноутбуку;
- можливість підключення MicroSD карти пам'яті;
- робота з USB периферією (миші, клавіатури, флеш-накопичувачі, звукові адаптери);
- декодування аудіо у форматі WAV, MP3, вихід у високоякісний аудіо ЦАП;
- декодування потокового інтернет-радіо;
- підключення будь-яких додаткових модулів;
- веб, FTP сервер.

Напрямками подальших досліджень можуть бути:

- створення лабораторного практикуму з вивчення архітектури сучасних ARM МК, методів та засобів їх програмування в курсах відповідних навчальних дисциплін;
- розширення та вдосконалення функціональності прототипу НЛС.

Перелік посилань

1. Reduced Instruction Set Computing – Вікіпедія [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Reduced_Instruction_Set_ Computing.

2. Архітектура ARM – Вікіпедія [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/ARM.

3. STM32F7 series of very high-performance MCUs with ARM® Cortex®-M7 core – STMicroelectronics [Електронний ресурс] – Режим доступу: http://www.st.com/en/microcontrollers/stm32f7-series.html.

4. High-performance and DSP with FPU, ARM Cortex-M7 MCU with 1 Mbyte Flash, 216 MHz CPU, Art Accelerator, L1 cache, SDRAM, TFT. [Електронний ресурс] – Режим доступу: https://www.st.com/en/ microcontrollers/stm32f746ng.html.

Аналіз потенційних вразливостей в IoT системах

Нічепорук Ю.О., Фегир О.В.
Науковий керівник – к.т.н. Нічепорук А.О.
Хмельницький національний університет

Зростаюча популярність IoT (або “інтернет речей”) надає широкі можливості для покращення, планування та автоматизації нашого життя. IoT дозволяє поєднувати в мережу та керувати множиною пристроїв, які забезпечують збір, аналіз та передачу даних. Сфера застосування IoT з кожним роком продовжує розширюватися, охоплюючи нові сфери життя, починаючи від розумних будинків, міст та закінчуючи сферою охорони здоров’я.

Проте разом із очевидними перевагами та зручностями, що несе із собою використання IoT, концепція “інтернет речей” залишає для зловмисників ряд потенційних “вузьких”місць у безпеці таких систем. Персональні дані, зібрані IoT-пристроями, завжди мають цінність для хакерів і викрадачів конфеденційної інформації. Крім того, кібератака на IoT-рішення потенційно здатна завдати шкоди фізичним сервісам та фізичній інфраструктурі. Наприклад, хакери успішно атакували автомобіль Jeep Cherokee в той час, коли він рухався по шосе під керуванням водія. Тому своєчасне виявлення та вирішення таких вразливостей є пріоритетними напрямками у розвитку всієї IoT індустрії.

Будь-який пристрій, що підключений до мережі може бути потенційно вразливим [1-3]. Зловмисник може здійснити атаку на будь-яку ланку інформаційної системи IoT, зокрема на фізичні пристрої (збір конфіденційної інформації, атака по захопленню вузлів), мережеві сервіси (DoS, jummong-атаки), хмарні сервіси (SQL ін’єкції, SYN-флуд), веб додатки (віруси, програми-вимагачі, bluesnarfing-атаки) та вразливості, які притаманні виключно IoT-системам. Класифікацію атак на IoT системи наведено на рис.1.

Рисунок 1 – Можливі види атак на IoT системи

Незважаючи на те, що IoT-пристрої наслідують концепцію клієнт-серверної архітектури, яка лежить в основі локальних мереж, існує ряд вразливостей, які притаманні виключно IoT-системам. В основі таких вразливостей лежить основоположні принципи IoT-систем: взаємозалежність, взаємопов'язаність та постійна комунікація IoT-пристроїв. Розглянемо їх детальніше.

Загрози, спричинені взаємозалежним середовищем IoT.

Зі швидким зростанням кількості об'єктів, що імплементуються у IoT систему, комунікація між ними стала все більш автоматизованою і такою, що проявляє тенденцію до зменшення людського втручання. IoT-пристрої більше не просто взаємодіють один з одним, як звичайні пристрої в мережі. В даний час багато пристроїв IoT розроблені з позиції бачення розумного міста, таким чином, що багато з цих пристроїв контролюються іншими пристроями або залежать від внутрішнього стану інших пристроїв або навколишнього середовища.

Наприклад, якщо GPS-датчик знає про дорожню ситуацію на шляху від дому користувача до роботи і відомий стан здоров'я користувача (наприклад астма), то GPS повинен вибрати маршрут, що найбільш підходить для його стану здоров'я (менше кількість транспорту та забруднення атмосферного повітря) на основі даних про стан здоров'я та датчиків руху і забруднення повітря. Ще одним прикладом, що ілюструє вразливість IoT через взаємозалежність середовища є ситуація, при якій здійснюється відкриття вікна, у випадку якщо температура в приміщенні підвищена та охолоджувач повітря вимкнений. Такі взаємозалежні процеси поширені в додатках, які використовують пристрої IoT для досягнення повністю автоматизованого процесу. У цьому середовищі цільовий пристрій IoT може бути недоступним для зловмисника, проте зловмисник може змінити режим роботи іншого пристрою або його параметр через навколишнє середовище, що має пряму взаємозалежність для активації загрози.

Тому атака на одне місце, наприклад зниження температури або маніпулювання даними про забруднення може спричинити серйозні наслідки для інших датчиків, операції яких залежать від інформації цих датчиків. У такому взаємозалежному середовищі зловмисник може вибрати найслабші ланки в системі для порушення роботи всієї системи.

Загрози, спричинені взаємопов'язаним середовищем IoT.

На сучасному етапі розвитку технологій до IoT систем можуть підключатися мільйони пристроїв. За допомогою цих сильно пов'язаних пристроїв інфікована інтернет річ може стати руйнівним інструментом атаки, яка може інфікувати множину речей у великому масштабі, тим здійснюючи вплив на всю систему (наприклад розумне місто).

Дослідження [2] показують, що пристрої IoT, навіть із захищеними стандартними криптографічними методами, можуть використовуватись

зловмисниками для створення нової категорії ризиків для безпеки, яка може бути розповсюджена від одного пристрою IoT до всіх фізично підключених пристроїв через IoT з'єднання.

Отже, зловмисник може запускати швидкі та руйнівні атаки, якими може бути нелегко керувати. Для ілюстрації впливу такого сценарію було проведено експериментальне дослідження у якому, було змодельовано поширення інфекції за допомогою розумних ламп Philips Hue, які можуть бути однією із складових розумного міста.

Зловмисне програмне забезпечення розповсюджувалося шляхом переміщення безпосередньо від однієї лампи до сусідньої лампи через бездротове підключення ZigBee. Дослідники [2] виявили, що глобальний ключ AES-CCM можна використовувати для шифрування та аутентифікації нової мікропрограми, не знаючи при цьому реальних оновлень смарт-ламп. Ця ситуація показує, наскільки вразливими є такі пристрої, навіть якщо вони використовують надійні криптографічні методи безпеки. Такі атаки можуть розпочатися в одній точці, і можуть закінчитися зараженням усієї системи міста, тим самим дозволяючи зловмисникам керувати вогнями міста або використовувати лампи IoT в атаках DDoS [2]. Таким чином можна констатувати, що взаємопов'язане середовище відкриває широкі можливості для швидкого поширення загроз в IoT системах.

Загрози, спричинені відстеження характеру зміни мережевого трафіку

Аналіз метаданих трафіку, що надсилається з IoT-пристроїв, може надати інформації про звички і стиль життя власника. Згідно з дослідженням [3], зловмисник, що використовує перехоплення мережевого трафіку, може використовувати методи пасивного мережевого моніторингу для збору метаданих, якими обмінюються IoT-пристрої з серверами дистанційного керування.

Навіть якщо трафік від IoT-пристроїв зашифрований, або передається через VPN-тунель, у зловмисника є можливість ідентифікувати власника пристрою шляхом використання DNS запитів та MAC-адреси пристроїв.

Іншим способом ідентифікації є визначення інтенсивності мережевого трафіку, тобто періодичність повторюваних запитів до серверів дистанційного керування і перші шість цифр MAC-адреси, які є унікальним ідентифікатором. Для реалізації такого сценарію зловмиснику необхідно мати доступ до локальної мережі жертви, оскільки MAC-адреси недоступні для трафіку на рівні Інтернет-провайдера.

З метою моделювання сценарію отримання метаданих з мережевого трафіку, авторами було розглянуто чотири популярні пристрої розумного будинку, зокрема будильник та контролер сну Hello Sense, камера відеонагляду, розетка Belkin WeMo та колонка Amazon Echo.

В результаті дослідження було встановлено, що зловмисник має можливість визначити час, коли власник пристрою знаходився вдома, що проявляється у сплесках активності від таких пристроїв як Amazon Echo і Wi-

Fi-розеток. Крім того, дослідники також змогли визначити, коли власник спав. В цей час спостерігалася підвищена активність з боку Sense Sleep Monitor. Пристрій ставав активнішим, коли йому доводилося збирати і відправляти дані про активність користувача під час сну. За активністю камер відеоспостереження Nest можна визначити, коли власник залишає будинок. Камери активувалися тільки коли людина виходила з будинку і вмикала систему відеоспостереження, що проявлялось у відправленні з певним інтервалом знімків з камер на віддалений. Проведений аналіз показав, що успішність подібних атак пояснюється принципом роботи IoT-пристроїв та необхідністю постійного інтернет-підключення.

Підсумовуючи можна відзначити, що розробники IoT систем дуже часто відносять на другий план питання безпеки IoT-пристроїв, надаючи тим самим зловмисникам широкий спектр можливих атак на ту чи іншу інфраструктуру мережі. Враховуючи, що IoT системи наслідують концепцію клієнт-серверної архітектури, яка лежить в основі локальних мереж, багато вразливостей є спільними як для локальних мереж так і для IoT систем. Проте існує ряд вразливостей, які притаманні виключно IoT-системам: взаємозалежність, взаємопов'язаність та постійна комунікація IoT-пристроїв. Тому розробка нових підходів для підвищення ефективності захищеності IoT-систем є важливим перспективним напрямком.

Перелік посилань

1. Al-Garadi M. A. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security / M.A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, M. Guizani. – arXiv:1807.11023, 2018.

2. Ronen E. IoT Goes Nuclear: Creating a ZigBee Chain Reaction / E. Ronen, A, Shamir, A.-O. Weingarten, C. O'Flynn // 2017 IEEE Symposium on Security and Privacy (SP), May 22-26, 2017: Proceedings. – San Jose, CA, (USA), 2017. – Pp. 195-212.

3. Apthorpe N. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic / N. Apthorpe, D. Reisman, N. Feamster. – arXiv:1705.06805, 2017.

Дослідження рівня унікальності текстового контенту та розробка програмного застосування для перевірки рівня унікальності текстового контенту

Овчинніков В.М.
Науковий керівник – к.ф.-м.н., доц. Розум М.В.
Одеський національний морський університет

В науково-дослідній роботі об'єктом дослідження є унікальність інформації, предметом дослідження – проведення розгляду та аналізу

перевірки текстової інформації на унікальність з метою запобігання плагіату текстового контенту. Відкритий доступ до літератури чи текстового контенту в мережі Інтернет, а також застосовування принципу Copy&Paste призвели до появи робіт, що дублюють одна одну. Вважаю, що оскільки виконана робота зі створеним додатком допоможе виявити таке дублювання, то вона є актуальною.

Мета роботи - розробити програмне застосування для оцінки рівня унікальності текстового контенту для забезпечення функцій швидкої та якісної перевірки унікальності заданого тексту.

Унікальність тексту - показник відсутності дублів тексту в Інтернеті [1]. Унікальність є одним з базових критеріїв, за якими пошукові системи оцінюють якість текстового контенту. За публікацію неунікального контенту, на сайт, скоріше за все, будуть накладені санкції пошукових систем. До того ж, неунікальна інформація навряд чи представляє цінність і користь для відвідувачів сайту. Плагіат — привласнення авторства на чужий твір або на чуже відкриття, винахід чи раціоналізаторську пропозицію, а також використання у своїх працях чужого твору без посилання на автора [2]. Методи виявлення плагіату характеризуються по типу оцінки подібності (рис. 1).

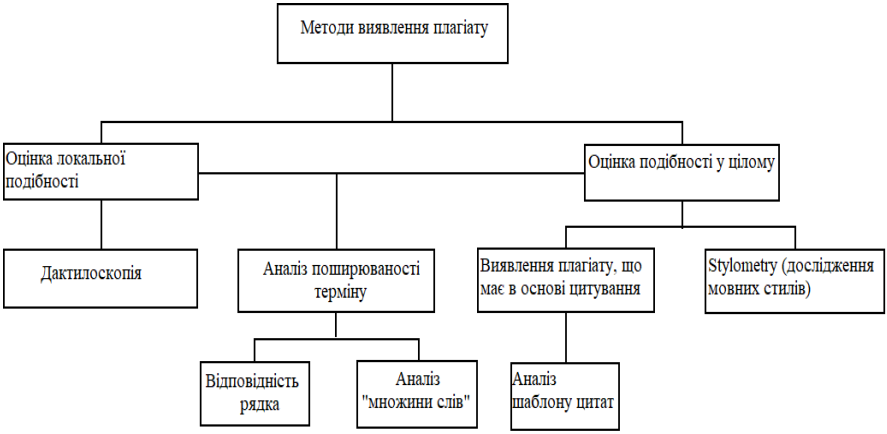

Рисунок 1 – Схема класифікації методів комп’ютерного виявлення плагіату

Існує два способи перевірки тексту на унікальність:

1. Онлайн сервіси. Більшість з них працює безкоштовно або умовно безкоштовно: без оплати є можливість перевірити на унікальність обмежене число текстів на добу та/або статті обмеженого об’єму, наприклад від п’яти до десяти тисяч символів.

2. Програми-антіплагіатори. Такі програми встановлюються на персональний комп'ютер та працюють як і інше програмне забезпечення. Кожна програма використовує свій алгоритм перевірки тексту. Для перевірки обов'язково потребується доступ до Інтернету.

Розглянемо декілька комп'ютерних програмних продуктів для статистичної обробки даних: Antiplagiarism.NET, Advego Plagiatus, Антиплагиат.ру та запишемо результати у таблицю 1.

Таблиця 1 - Аналіз програм для статистичної обробки даних

Критерій	Antiplagiarism.NET	Advego Plagiatus	Антиплагиат.ру
Тип поширення	Freemium	Shareware	Freemium
Тип програми	Програмне застосування	Веб сервіс та програмне застосування	Веб сервіс
Необхідність вводити капчу	+	При використанні програмного застосування	-
Додаткові можливості	Перевірка на рерайт, перевірка унікальності малюнків, порівняння текстів, SEO-перевірка тексту	Перевірка на рерайт, SEO-перевірка тексту	Глибока перевірка на рерайт
Доступні платформи	Windows	Windows, Linux, MacOS та Веб версія	Веб версія
Ціна	20$	Безкоштовна	Від 2$ в день до 2740$ в місяць
Швидкість перевірки	Повільна	Середня	Середня
Точність результатів	Середня	Середня	Середня

За результатами проведеного аналізу якості програм перевірки рівня унікальності тексту, найбільш якісною є програма Advego Plagiatus за показниками: тип поширення, тип програми, доступні платформи. Проте і це програмне застосування має ряд недоліків, таких як середня швидкість перевірки тексту та недостатня точність результатів.

Програмне застосування, розроблене нами, має більшу точність результатів і тому є актуальним для застосування у прикладній діяльності

вищих учбових закладів та наукових журналів з метою пошуку плагіату та перевірки на плагіат кваліфікаційних робіт студентів та науковців.

Перед використанням розробленого програмного застосування, на комп'ютер потрібно встановити Java Runtime Environment. Далі треба запустити на виконання виконуваний файл TextUniqueness.jar. Відкриється головне вікно програмного застосування, яке містить дві вкладки – головну та вкладку з налаштуваннями.

На головній вкладці можливі наступні дії:

1) маємо змогу ввести текст, який треба перевірити на унікальність;

2) за допомогою спеціальної кнопки "Вибрати файл" вибрати файл або групу файлів (.doc, .docx, .txt, .pdf), які містять текст для перевірки рівня унікальності текстового контенту:

3) за допомогою кнопки "Збереження результатів у файл", результат перевірки буде збережений у файл (директорія для збереження визначається у налаштуваннях програми, якщо перевіряється декілька файлів, для кожного з них результат буде збережений у окремий файл виду "UniqOutput + ім'я перевіреного файлу".

4) для очистки поля з результатами натиснути кнопку "Скидання".

На вкладці "Налаштування" маємо змогу вибрати максимальну кількість слів у одному пошуковому запиті за допомогою Google Search API, а також вказати директорію для збереження файлів-звітів (за замовчуванням файли-звіти зберігаються у системній папці Документи даного користувача). Також маємо змогу скинути усі налаштування на налаштування за замовчуванням.

Після успішної перевірки рівня унікальності введеного тексту чи файлу, у програмі з'явиться нова вкладка, яка буде містити кругову діаграму унікальності текстового контенту. В цій діаграмі будуть вказані сайти та відсоток запозичень контенту початкового тексту з даних сайтів. Також на діаграмі буде показаний відсоток унікального тексту (якщо текст має хоча б 1% унікальності).

Перелік посилань

1. Что такое уникальность текста? [Електронний ресурс]. – Режим доступу: https://wiki.rookee.ru/unikalnost/. – Дата доступу: 16.11.2018.

2. Великий тлумачний словник сучасної української мови [уклад. В.Т.Бусел]. — К.: Ірпінь: ВТФ «Перун», 2005. – 1728 с.

Інтелектуальна автоматизована система контролю знань на основі формування семантичної мережі

Омельчук Р.
Науковий керівник – к.т.н., доц. Медзатий Д.М.
Хмельницький національний університет

Вміння кваліфіковано проводити тести є одним із важливих показників обізнаності викладачів. Контроль за рівнем знань і вмінь як один із дієвих і практично необхідних засобів перевірки знань і практичних навичок студентів: особистість, діяльність, увага, відчуття, сприймання, пам'ять, мислення, уява, почуття, темперамент, характер. Тестування проводиться з використанням автоматизованих систем, які є основною формою опанування конкретних експериментальних методик. При виконанні деяких тестів студенти можуть працювати групами по три особи. Це дозволяє кожному побувати в ролі експериментатора, протоколіста, досліджуваного. Застосовуються зазвичай методики, які не потребують складної спеціальної апаратури. І водночас це мають бути валідні, класичні тести, випробувані у світовій науці, які широко впроваджуються впрофесійний відбір і розстановку кадрів, для контролю, для оптимізації навчання, прогнозування поведінки.

Питання теорії і методології педагогічного контролю на основі тестової технології розглядали такі науковці, як: В.С. Аванесов, В.П. Безпалько, Н.В. Козленкова, А.І. Майоров, О.А. Рикова, Л.О. Федотова та інші. Практиків тести приваблюють можливістю масового, точного і об'єктивного оцінювання знань студентів. На думку багатьох викладачів, тестування є ефективним засобом контролю, що дає змогу якнайшвидше сформувати уявлення про знання студентів. Тестування як термін у вузькому значенні означає використання і проведення тесту, а в широкому – сукупність етапів, планування, складання і випробування тестів, обробки та інтерпретації результатів проведення тесту. Основним поняттям тестування є поняття тесту.

У теорії контролю знань визначені наступні дидактичні принципи: дієвість, систематичність, індивідуальність, диференціювання, об'єктивність і єдність вимог. До основних принципів тестування належать: об'єктивність вимірювання; систематичність контролю; відкритість; незалежність від суб'єктивних оцінок викладача, стандартизація процедури оцінювання; наявність різних рівнів тестування в залежності від мети навчання (інтелектуальний розвиток, розвиток соціального інтелекту, підготовка до професійної діяльності, формування світогляду тощо);валідність і надійність завдань, якими контролюють; застосування сучасних технологій створення й обробки для досягнення точності оцінювання; організація вивчення й обліку зворотного впливу нових форм контролю на процес навчання; об'єктивне оцінювання ступеня досягнення студентів навчальних стандартів.

Узагальнюючими критеріями сучасного тестового контролю є: науковість методу, тобто спирання на теорію педагогічних вимірювань,

теоретичний аналіз можливостей, емпірична перевірка якості, обов'язкова перевірка отриманих даних статистичними методами за критеріями надійності і валідності; технологічність – можливість застосування автоматизованих методів перевірки і опрацювання результатів; ефективність, тобто перевірка знань швидше у порівнянні з традиційними методами, з меншими витратами. Тому підрахунок балів і виведення оцінки повинні проводитися по можливості в короткий термін, бажано, підрахування балів на ЕОМ; студент повинен знати, що після кожного екзамену тест переглядається.Перш, ніж складати тести викладач повинен проаналізувати матеріал і виділити ті блоки, які будуть перевірятися методом тестового контролю. Саме викладач формує еталонні вимоги до теоретичних знань і практичних навичок до кожного блоку навчального матеріалу. Еталонні вимоги формуються на основі вимог навчальних програм і входять до навчального-методичного комплексу дисципліни. Вони доводяться до відома студентів, які мають можливість ознайомитися з ними в кабінетах, читальному залі. Еталонні вимоги викладач подає в формі рівневих тестів з урахуванням підготовки студентів. За допомогою тестів робиться спроба визначити підготовку студента до діяльності на тому чи іншому рівні. Розробка тестів повинна відповідати наступним головним вимогам: адекватність (валідність); визначеність (загальне розуміння); простота; однозначність; надійність.Адекватність поділяється на функціональну і змістовну. Функціональна адекватність – точна відповідність завдань еталонним вимогам знань.

Надійність вимагає перевірки забезпечення послідовних результатів тестування методами статистичного аналізу. Отже, тестова система оцінювання знань відповідає таким вимогам: відображає глибину засвоєння навчального матеріалу; забезпечує об'єктивність та індивідуальний підхід в оцінюванні рівня сформованості знань і якості навчання кожного студента як особистості; стимулює студентів до активної самостійної роботи в оволодінні професійно значущими знаннями.

Для вирішення цих завдань необхідним є розробка автоматизованої системи контролюзнань на основі семантичних мереж.

Перелік посилань

1. Аванесов В.С. Методологическое и теоретическоеобоснование тестового педагогического контроля. Диссертация на соискание ученой степени доктора педагогических наук. С-Пб.: Госуниверситет. С-Пб. 1994. С 205-214.

2. Аванесов В.С. Научные проблемы тестового контроля знаний. М.: Исслед. центр, 1994. -48с.

3. Агапов В.Ю., Мишакова Л.М.Алгоритмы целеполагания в современных педагогических технологиях. –Рязань, 1994. -33с.

4. Гулюкина Н.А., Клишина С.В. Педагогический тест: этапы и особенности конструирования и использования. Пособие для преподавателей. Новосибирск: Изд-во НГТУ, 2001. –132с.

Метод та засоби ідентифікації шпигунського програмного забезпечення

Омельяненко В.Ю.
Науковий керівник - к.т.н., доц. Лисенко С.М.
Хмельницький національний університет

Деякі програми включають у себе шпигунське програмне забезпечення, рекламне програмне забезпечення, трояни. Вони можуть загрожувати конфіденційності, цілісності та доступності системи та можуть отримувати конфіденційну інформацію без інформування користувача.

Шпигунський програмний продукт (Spyware) – це програмний продукт особливого виду, що встановляється без відому користувача і використовується без належного сповіщення користувача, метою якого є збір даних про систему та її власника та передача цих данних власнику продукту.[3]

Шпигунські програмні продукти поділяються на декілька основних видів:

1.Моніторингові програмні продукти (англ. Tracking Software).[2]

2.Призначені для контролю натискань клавіш на клавіатурі комп'ютера (англ. Keyloggers)[2].

3.Призначені для контролю скриншотів екрану монітора комп'ютера (англ. Screen Scraper).

Шпигунське програмне забезпечення відрізняється від звичайних вірусів, тому їх не вдається виявити за допомогою звичайного антивірусного програмного забезпечення. Традиційно для виявлення шпигунських програм було представлено два підходи: виявлення на основі сигнатур та виявлення на основі евристичного аналізу[5]. Цей підхід добре працює проти відомих шпигунських програм, але не є успішним у виявленні нових шпигунських програм. Навіть якщо у користувачів встановлено антивірусне програмне забезпечення, воно може не бути корисним проти шпигунських програм, поки воно не буде розроблене саме для цієї загрози. Існує три основні види виявлення ГПЗ: Статичгий аналіз, динамічний та гібридний.[4]

Статичний аналіз - це процес аналізу виконуваного коду без виконання вихідного файлу. Він просто дивиться на вихідний код і розкриває інформацію про нього. У статичному аналізі для виявлення шкідливого коду застосовують розподіл частоти операційного коду, підпис рядків, байт-послідовність, графік потоку управління, n-грам тощо. Мова статистичного рівня та операційна система потрібно знати при статистичному аналізі.

У динамічному аналізі дуже важливо виконати файл. Після виконання шкідливого коду він відстежує його (зловмисне) поведінку і бачить, наскільки це впливає на хост-машину. Отже, його ще називають поведінковим аналізом. Виявити невідомі шкідливі програми в динамічному аналізі легко. Пісочниця, симулятор, віртуальна машина тощо використовуються для аналізу зараженого коду.

Гібридний аналіз включає як статичний, так і динамічний аналіз. Він бере частину підпису зі статичного аналізу, а потім поєднує в собі поведінкову частину динамічного аналізу. Тож гібридний аналіз є більш ефективним, ніж інші два аналізи. Але він повинен підтримувати обмеження як статичного, так і динамічного аналізу.

Виходячи з того факту, що існуючі способи виявлення не здатні виявляти нове шпигунське програмне забезпечення, пропонується метод по виявленню ШПЗ, в основі якого лежить принцип Data mining[1], котрий дозволить виявляти нове ШПЗ, за динамічними класифікаторами. Data mining - це процес аналізу електронно збережених даних шляхом автоматичного пошуку шаблонів.

У цьому методі бінарні функції витягуються з виконуваних файлів, створюється набори файлів з доброякісних та заражених. Потім метод зменшення функцій використовується для отримання підмножини даних, яка надалі використовується як навчальний набір для автоматичного генерування класифікаторів за допомогою нейромережі. Доступно багато методів класифікації даних, але запропонована система використовує алгоритм дерева рішень для прийняття рішень, пов'язаних з тестуванням файлу EXE. Потім для сканованого файлу теж виділяються ознаки, проходять оптимізацію, і також передається до нейромережі, де за допомогою дерева рішень вона видає результат. Дерево рішень дає результат на основі навчального набору даних про те, що файл сканування є шпигунським або ні.

Алгоритми машинного навчання зазвичай використовуються для виявлення нових закономірностей або співвідношень у даних, які надалі використовуються для розробки моделі, тобто класифікатора або функції регресії. Алгоритми навчання широко використовуються для різних проблем з обробкою даних для виявлення шаблонів та пошуку кореляцій між екземплярами даних та атрибутами.

Ідея методу полягає в наступних кроках:

1. Збір даних(файли заражені ШПЗ та незаражені).
2. Генерація послідовностей байтів для цих файлів.
3. Витягування ознак.
4. Генерація Attribute Relation File Format (ARFF)[2] для файлів ознак.
5. ARFF генерація сканованого файлу.
6. Передача даних в нейромережу.

Представлений вище метод ідентифікації бот-мереж, в основі якого лежить сканування Data mining та обробка видобутих даних нейромережею дозволить здобути такі переваги над існуючими методами. Швидкість виявлення цим методом буде більшою, ніж методом заснованим на сигнатурах. Це зменшить кількість хибних негативних спрацювань, збільшить виявлення відомих, а також невідомих шпигунських програм. Значно підвищить точність та адаптивність керування мережевою безпекою.

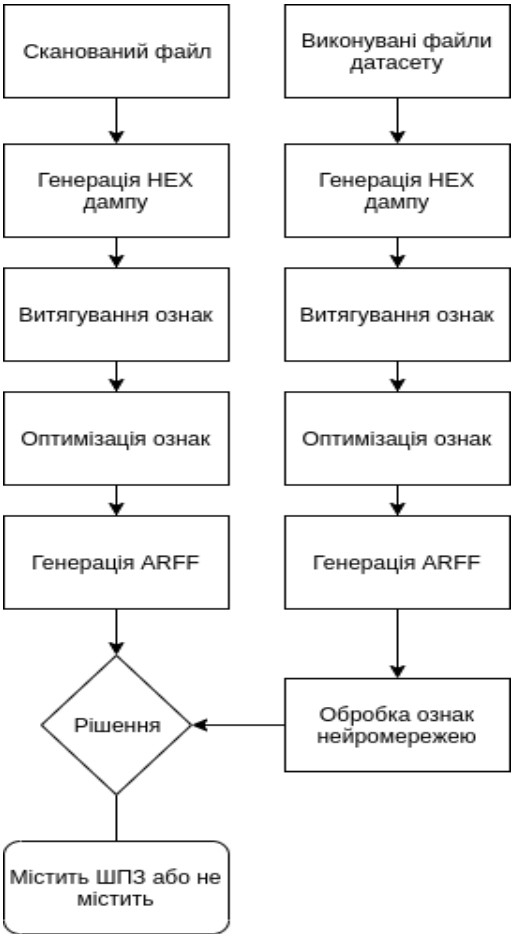

Рисунок 1 Схема сканування файлу на наявність ШПЗ

Перелік посилань

1. Salma Elmalaki, Bo-Jhang Ho, Moustafa Alzantot, Yasser Shoukry, Mani Srivastava SpyCon: Adaptation Based Spyware in Human-in-the-Loop IoT(2019) https://www.ieee-security.org/TC/SPW2019/SafeThings/papers/SpyConAdaptationBasedSpywareinHumanintheLoopIoT.pdf.

2.Leena T. Patil , Shamal S. Pawar,Shrutika N. Lad,Nilambari Joshi (April 2014),Implementation of Spyware Detection Using Data Mining With Decision Tree Algorithm https://www.diva-

portal.org/smash/get/diva2:835504/FULLTEXT01.pdf.

3.V Lakhno, D Kasatkin, V Kozlovsky, A model and algorithm for detecting spyware in medical information systems(2019) https://www.researchgate.net/profile/Dmitro_Kasatkin/publication/332112238_Article_ID_IJMET_10_01_029_Medical_Information_Systems/links/5ca1e54145851506d738c69b/Article-ID-IJMET-10-01-029-Medical-Information-Systems.pdf

4.Ishita Basu , Nidhi Sinha , Diksha Bhagat , Saptarsi Goswami, Malware Detection Based on Source Data using Data Mining: A Survey(2019) https://www.researchgate.net/profile/Saptarsi_Goswami/publication/297640864_Malware_Detection_Based_on_Source_Data_using_Data_Mining_A_Survey/links/57260d1108aef9c00b88f348.pdf

5.Allan Ninyesiga,Behavioral malware detection by data mining(2016)https://utamu.ac.ug/docs/research/studentresearch/masters/proposals/NINYESIGA%20ALLAN%20PROPOSAL-BEHAVIORAL%20MALWARE%20DETECTION%20BY%20DATA%20MINING.pdf

Інтелектуальна система для визначення достатності метричної інформації у вимогах до програмного забезпечення

Павлова О.О.
Науковий керівник – д.т.н.проф. Говорущенко Т. О.
Хмельницький національний університет

Вступ. Враховуючи той факт, що у сучасному світі розробка програмного забезпечення (ПЗ) перетворилася в одну із найдорожчих індустрій, і будь-які вузькі місця в технологічному процесі його створення можуть привести до небажаних результатів, однією із основних вимог користувачів до сучасного ПЗ є його висока якість та низька складність. На сьогодні існує ряд моделей, що дають змогу розраховувати якість та складність ПЗ, однак багатозначність трактування цих характеристик ускладнює такі розрахунки. Більшість моделей базуються на використанні різних метрик ПЗ. Згідно зі стандартом ISO 24765 [1], метрика ПЗ – це міра, яка надає числове значення деякої властивості ПЗ як зважене середнє арифметичне з урахуванням значень показників, що оцінюють цю метрику, та коефіцієнтів їхньої вагомості.

Сучасна програмна індустрія накопичила велику кількість метрик, які оцінюють окремі виробничі та експлуатаційні властивості ПЗ, але сучасне ПЗ не є ідеальним з точки зору його якості [2], а в галузі оцінювання та прогнозування характеристик ПЗ на основі аналізу метрик залишається ряд невирішених питань [3]. Складність обґрунтування вибору та інтерпретації метрик в процедурах прийняття виробничих рішень та ігнорування етапів життєвого циклу ПЗ не

дозволяють повноцінно використовувати метрики для оцінювання та прогнозування характеристик ПЗ на ранніх етапах життєвого циклу ПЗ. Тоді актуальною задачею наразі є обчислення значень метрик для оцінювання та прогнозування якості та складності ПЗ на ранніх етапах життєвого циклу ПЗ.

У [3] запропоновано нейромережний метод для оцінювання та прогнозування якості та складності ПЗ. Авторами [3] обрано 24 метрики якості та складності ПЗ, які можуть бути розраховані вже на етапі проектування (з точними або прогнозованими значеннями). Значення таких метрик аналізуються штучною нейронною мережею, яка на основі цього аналізу видає оцінки складності та якості програмного проекту, а також прогнозовані оцінки складності та якості розроблюваного ПЗ. Отримані оцінки опрацьовуються згідно розроблених продукційних правил (сформованих на основі порогових значень, отриманих емпірично) та в результаті користувачу видаються висновки щодо рівня складності та якості програмного проекту, а також висновки-прогноз щодо рівня складності та якості розроблюваного ПЗ. Розроблений метод орієнтований не на програмний код, а на специфікацію вимог до ПЗ, але базується на аналізі готових значень 24-х метрик складності та якості (як залежать від 72 показників, в тому числі від 42 різних показників) і не враховує можливості чи неможливості розрахунку таких метрик за інформацією, наявною у специфікації вимог до ПЗ.

При цьому актуальною є задача оцінювання достатності метричної інформації на ранніх етапах життєвого циклу ПЗ, зокрема, у вимогах до ПЗ (як можливості отримання показників для обчислення значень метрик). Тоді метою даного дослідження є розроблення інтелектуальної системи для визначення достатності метричної інформації у вимогах до ПЗ, яка на основі опрацювання природомовних вимог забезпечить висновки про достатність метричної інформації (показників для обчислення обраних метрик) у вимогах.

Інтелектуальна система для визначення достатності метричної інформації у вимогах до ПЗ. Інтелектуальна система для визначення достатності метричної інформації у вимогах до ПЗ розробляється як агентно-орієнтована система, яка складається з двох інтелектуальних агентів (рис. 1) – агента для парсингу специфікації вимог до ПЗ на предмет пошуку метричної інформації (показників для обчислення метрик) та агента для оцінювання достатності метричної інформації у специфікаціях.

Обидва інтелектуальні агенти побудовані на основі онтологічного підходу. В якості відомих знань інтелектуальні агенти використовують базову онтологію предметної галузі «Інженерія програмного забезпечення» (частина «Якість та складність ПЗ. Метричний аналіз»), розроблену у [4].

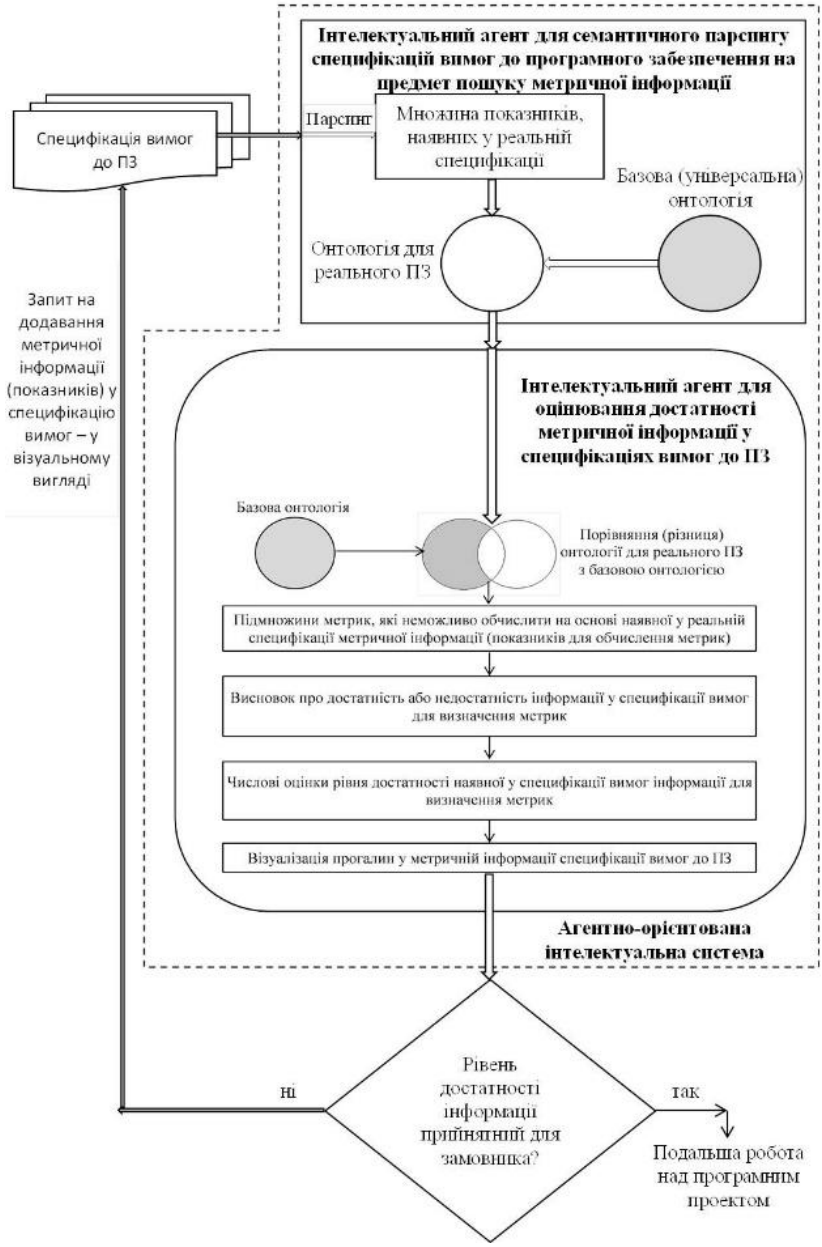

Рисунок 1 – Інтелектуальна система для визначення достатності метричної інформації у вимогах до ПЗ

Отже, запропонована інтелектуальна система для визначення достатності метричної інформації у вимогах до ПЗ виконує парсинг (семантичний аналіз) природомовної специфікації вимог до ПЗ на предмет пошуку показників, необхідних для обчислення метрик складності та якості ПЗ на ранніх етапах життєвого циклу, а також формує висновок про достатність або недостатність метричної інформації у специфікації вимог до ПЗ, обчислює числову оцінку рівня достатності метричної інформації, а також візуалізовано надає відсутні показники з розподілом за метриками, для яких вони використовуються.

Висновки. У статті розроблено інтелектуальна система для визначення достатності метричної інформації у вимогах до ПЗ, яка на основі опрацювання природомовних вимог надає: висновок про достатність метричної інформації (показників для обчислення метрик) у вимогах, числову оцінку рівня достатності метричної інформації у специфікації вимог до ПЗ, візуалізацію відсутніх показників для обчислення метрик, приріст достатності інформації до 100% – за необхідності (для систем критичного застосування) або за вимогою замовника.

Розроблена інтелектуальна система для визначення достатності метричної інформації у вимогах до ПЗ може використовуватись в процесі розроблення ПЗ для державних установ, військових формувань та правоохоронних органів, комерційних організацій (як для організацій, які займаються розробленням ПЗ, так і для організацій, які є замовниками ПЗ).

Перелік посилань

1. Systems and software engineering. Vocabulary: ISO/IEC/IEEE 24765:2010. – [Introduced 15.12.2010]. – Geneva (Switzerland): ISO, 2010. – 410 p. – (International standard).

2. Pomorova O. The way to detection of software emergent properties / O. Pomorova, T. Hovorushchenko // The 8-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems, September 24-26, 2015: Proceedings. – Vol. 2. – Warsaw, 2015. – Pp. 779–784.

3. Pomorova O. Research of Artificial Neural Network's Component of Software Quality Evaluation and Prediction Method / O. Pomorova, T. Hovorushchenko // The 6-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems, September 20-23, 2011: Proceedings. – Vol. 2. – Prague, 2011. – Pp. 959–962.

4. Hovorushchenko T. Models and methods of evaluation of information sufficiency for determining the software complexity and quality based on the metric analysis results / T. Hovoruschenko // Central European Researchers Journal. – 2016. – № 2. – С. 42-53.

Адаптивне управління ресурсами в гетерогенних мережах

Поплавський С.Ю.
Науковий керівник – к.т.н., доц. Хмельницький Ю.В.
Хмельницький національний університет

При адаптивному управлінні ресурсами в гетерогенних мережах для вибору мережі доступу в гетерогенному середовищі на основі застосування теорії нечітких множин розглянемо різнотипність інформаційних потоків та критерії ініціації міжсистемного переходу чи хендовера. Рисунок 1демонструє найпоширеніші типи мережного потоку та певних однотипних критеріїв для реалізації хендовера, що застосовуються у якості вхідних даних для алгоритмів горизонтально - вертикального хендовера

Рисунок 1 - Різнотипність мережного потоку та критерії щодо ініціації переходу

Для випадку обслуговування користувачів є можливість призначення пріоритетності критеріїв при прийнятті рішення щодо ініціації процедури міжсистемного хендовера. Запропонований підхід має можливість гнучкого пріоритету, тому для певних категорій кінцевих абонентів зазначена вище пріоритетність критеріїв може зазнати зміни в процесі динамічної роботи [1]. Одним із запропонованих у роботі варіантів розв'язку даної задачі є метод адаптивного вибору мережі доступу в гетерогенному середовищі на основі застосування теорії нечітких множин. Даний метод включає в себе три основні компоненти збір даних, нормалізація даних і прийняття рішення про переключення. Для того щоб виконати інтелектуальні рішення передачі

обслуговування в гетерогенному середовищі запропоновано поділити всі параметричні критерії на дві групи: якісно-залежні та такі, що залежать безпосередньо від властивостей інтерфейсу мережної системи рис.2.

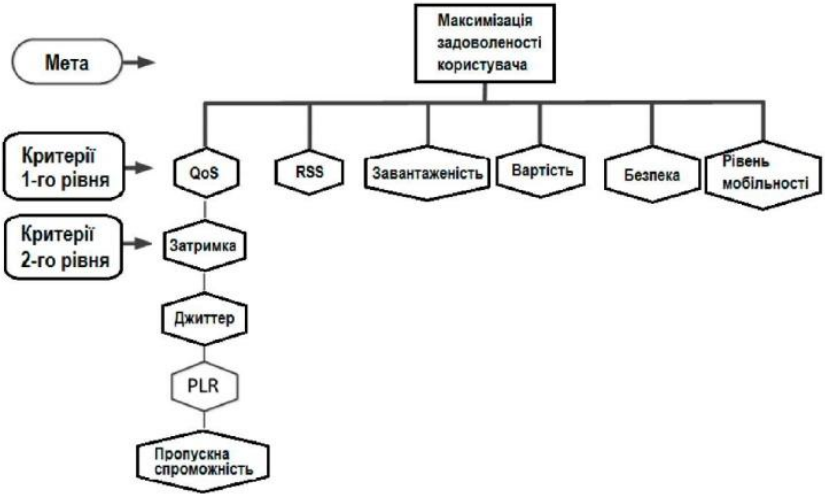

Рисунок 2 - Множина критеріїв для прийняття рішення щодо ініціалізації процесу вертикального переходу

По скільки гетерогенна мережа забезпечує функціонування різних технологій доступу із різними структурно - функціональними характеристиками. В загальному ці параметри неможливо порівнювати напряму. Таким чином, з метою їх нормалізації в діапазоні [0, 1] використовуються підходи нечіткої логіки. Удосконалений метод вибору мережі доступу в гетерогенному середовищі на основі застосування теорії нечітких множин, дає змогу централізовано прийняти обґрунтоване рішення щодо проведення процедури горизонтально-вертикального переходу, базуючись на групі якісно-залежних критеріїв та таких, що залежать безпосередньо від властивостей інтерфейсу мережної системи, яке передбачає можливість адаптування правил прийняття рішень, залежно від різних умов. Розвиток технологій виготовлення пристроїв дав можливість створення таких пристроїв, які можуть паралельно спілкуватися з декількома безпровідними системами обслуговування. Інтеграція та конвергенція мереж на основі IP протоколу дозволили реалізувати комунікацію між системами доступу різних технологій. Основною проблемою при наявності декількох систем доступу та можливості їх одночасного використання для обслуговування користувача є відсутність оптимальних алгоритмів здійснення переключення між ними, тобто здійснення вертикального переходу.

Для вирішення задачі ініціації та здійснення переходу пропонується централізований метод керування процесом переходу на основі хмарних технологій з використанням міжсистемних інтерфейсів до засобів управління системами доступу на основі технології ВЕБ - сервісів. Для здійснення переходу пропонується використовувати принципи паралельних обчислень на основі кластеру серверів. Такий кластер може встановити кожний оператор для себе, інтегрувавши його у власну інфраструктуру. Як варіант оператор може використати сервісні моделі систем та розробивши власне програмне забезпечення використовувати обчислювальні потужності як сервіс у провайдерів для розгортання власного програмного забезпечення. Це дозолить йому значно знизити капітальні витрати. Такий підхід продиктований тим, що для прийняття рішення про здійснення переходу та вибору конкретної системи доступу, як кандидата для переключення, необхідно, використовуючи математичні методи прогнозування та вибору, провести великий обсяг обчислень, що може зайняти велику кількість часу.

В умовах мобільності абонентів, час є критичним фактором, оскільки при великих швидкостях пересування та передавання мультимедійного потоку реального часу, тривале обчислення критеріїв здійснення переходу може призвести до банального розриву сесії та складностей у подальшому її відновленні. Використання можливостей хмарних технологій дасть змогу провести ці обчислення в лічені секунди та забезпечити оптимальний вибір системи доступу для переключення [2]. Для того, щоб швидко розв'язати завдання вибору мережі доступу у гетерогенній мережній платформі, в цьому розділі роботи запропоновано централізовану реалізацію процесу управління переходом на основі хмарних технологій із використанням методів нечіткої логіки. Оптимізація ресурсів, що представляє собою їх перерозподіл, згідно інтересів кінцевих користувачів спрямована на пошук екстремального значення у процесі вивчення поведінки безпровідної системи доступу (максимум з точки зору результатів, мінімум - витрат), яка оцінюється, як кращий варіант з множини можливих. В процесі оптимізації з'ясовується, який стан логістичної системи буде найкращим з точки зору пропонованих до неї вимог. Для цього розроблено програмне забезпечення на серверному кластері, що керує процесами ресурсної оптимізації (вертикального переходу), які представлено на рис. 3 [2].

Використовуючи можливості та засоби хмарних сервісних платформ, подібні розрахунки оптимального вибору мережної системи забезпечується в межах кількох секунд. Механізми рішення передачі обслуговування або управління перемикання між каналами можуть бути централізованими або приймати сам пристрій або в мережевому об'єкті. Ці випадки називаються передачею обслуговування контролю і передача обслуговування контрольованою мережею.

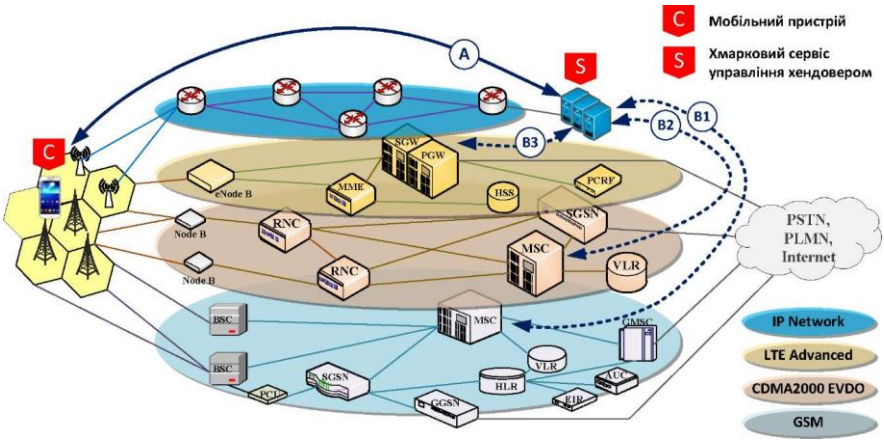

Рисунок 3 - Структурна схема гетерогенної мережі з централізованим управлінням ресурсів

Це вигідно, коли рішення передачі обслуговування приймається мережею, по скільки:

- мережа може пере направити пристрій на іншу мережу, що має достатню ємність для обробки своїх поточних комунікацій;
- мережа може також координувати мобільність всіх пристроїв таким чином, що загальний інформаційний потік рівномірно розподілявся по всім ресурсам, перенавантаження були зведено до мінімуму, і загальна пропускна здатність досягало максимального рівня.

Недоліком такого підходу є те, що для мережі може не вистачати деяких параметрів, які впливають на рішення передачі, такі як вимоги абонентів, точний тип послуги, кількість активних пристроїв, і деяких політик оператора, що мають відношення до рухливості між мобільним системами. Розумна інтеграція Wi-Fi як частини операторської мережі забезпечує значні переваги з точки зору підвищення можливостей і покриття, особливо там, де люди збираються найчастіше - транспортні вузли, торгові центри, міські центри тощо. Інтелектуальна інтеграція передбачає вибір мережі і ідентифікацію оператора, якому належить Wi-Fi автоматично та безпечно, забезпечуючи при цьому надійну і високу якість послуг. Інтегровані Wi-Fi мережі забезпечать операторам більше контролю та видимості при використанні Wi-Fi, а також можливість забезпечення дотримання загальної політики. Оператори звертаються до інтеграції Wi-Fi в якості альтернативної технології доступу, щоб додати ємність і для надання послуг доданої вартості.

Аналіз збережених даних дозволяє дізнатись операторам про параметри що впливають на якість обслуговування у різних пристроях,

сервісах та мережевих ресурсах. Після чого використання глобальної оптимізації гетерогенної мережі дає змогу виявити причину проблем і вибрати найкращі відповідно дії. Загалом, метою оптимізації мережі є максимізація якості обслуговування для користувачів з належним розподілом ресурсів, при мінімізації витрат на інфраструктуру за допомогою аналізу даних. Тим не менше, великі схеми інформаційних даних також становлять серйозні проблеми. Перш за все, як зібрати зібрані великі дані не тільки від користувачів, а і від операторів. Таким чином, багато проблем, необхідно належним чином вирішити для того, щоб максимально збільшити продуктивність всієї гетерогенної мережі і тим самим забезпечити безвідмовне надання послуг користувача.

На відміну від традиційних методів навчання, при розгляді неструктурованої навчальної архітектури, глибоке навчання виникає за допомогою контрольованих та неконтрольованих методів автоматичного вивчення ієрархічних представлення в глибоких архітектура для класифікації. У зв'язку з недавнім зростанням даних в гетерогенних мережах, величезні зусилля були зосереджені на ефективних і масштабованих паралельних алгоритмах для підготовки глибоких моделей. Необхідно використовувати глибоку довірчу мережу з глибокою архітектурою, щоб захоплювати представлення функцій не тільки міток, але й не замічених даних. У гетерогенної мережі глибокої довіри використовується попередня підготовка для безконтрольного навчання, а також налаштовуються стратегії нагляду за навчанням, що в кінцевому підсумку призведе до створення моделі навчання. Зокрема, це включає в себе неконтрольоване навчання для отримання розподілених даних без допомоги мічених даних, а також контролюється тонке налаштування, для покращення, як недавно доданих класифікації рівнів так і попередньо підготовлених рівнів.

Для прийняття оптимального за критеріями рішення щодо процедури ресурсного перерозподілу під час обслуговування користувачів мережних платформ гетерогенного доступу автоматизовано централізований метод управління переходом. Уточнений підхід дає змогу уникати двозначності у трактуванні нечітко заданих, двозначних та суб'єктивних суджень у процесі багато критерій оптимізації. Для дослідження процесів функціонування реальних гетерогенних мережних систем в умовах високої мобільності користувачів розроблено імітаційну модель, яка реалізує запропоновану в роботі метод прийняття рішення щодо вертикального переходу. Це дає змогу налаштовувати велику кількість параметрів моделювання, використовуючи допоміжні математичні моделі, зокрема для опису та прогнозування процесів руху (мобільності) користувачів, а також поширення радіохвиль до їх термінального обладнання. Як показано, вибір оптимального мережного вузла доступу на основі вирішення багато критерій завдання прийняття рішення щодо переходу є нетривіальним, по скільки на результати цього

розв'язання впливають одночасно кілька динамічно-змінних та взаємопов'язаних факторів, тому їх агрегація згідно із запропонованими у роботі підходами є необхідною.

Таки чином за допомогою імітаційної моделі проведено дослідження не тільки процесів балансування навантаження між станціями різних типів, але і підвищено якість обслуговування клієнтів операторами гетерогенних мереж.

Перелік посилань

1. Масюк А. Р. Алгоритм інтелектуального вертикального хендоверу в гетерогенній мобільній мережі на основі хмарних обчислень / А. Р. Масюк, І.Б. Стрихалюк, М. В. Брич, І. О. Кагало, Г. В. Бешлей // Вісник Національного університету «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації. — Львів: Видавництво Львівської політехніки, 2017. — № 874. — С. 110-121.

2. Бешлей М.І. Підвищення ефективності роботи гетерогенних мереж методом динамічного перерозподілу ресурсів між різними безпроводовими тех-нологіями / Бешлей М.І., Селюченко М.О., Гуськов П.О., Масюк А.Р. // Міжнародна науково-технічна конференція «Сучасні інформаційно-телекомунікаційні технології»: матеріали науково-технічної конференції (17-20 листопада 2015 р. м.Київ), Т.2 - К: ДУТ. - 2015. - С. 49-50.

Розробка структурної схеми маршрутизатора

Смаглюк Н.
Науковий керівник – к.т.н., доц. Медзатий Д.М.
Хмельницький національний університет

Темою даної дипломної роботи є розробка структурної схеми маршрутизатора, що реалізує логічний спосіб формування плану розподілу інформації. Робота включає в себе загальний опис широкосмугових мереж інтегрального обслуговування; класифікацію алгоритмів маршрутизації. Розроблено структурну схему маршрутизатора, що реалізує аналізований метод маршрутизації. Наведено математичну модель для даного методу.

Динаміка сучасного економічного і соціального розвитку країни в значній мірі визначається розвитком інфраструктур, найважливішим елементом якої є зв'язок. Мережі зв'язку повинні забезпечувати передачу і розподіл всіляких інформаційних потоків, необхідних для задоволення потреб населення, ефективного функціонування виробничих процесів ділового та промислового сектора, проведення державних і політичних заходів. Сучасний етап розвитку мереж зв'язку характеризується стрімким збільшенням обсягів переданої інформації.

В даний час суспільство поступово вступає в еру інформаційної економіки, тому традиційна класифікація основних видів виробництва "товари і послуги", трансформується в "товари, послуги та інформація". Успіхи в створенні та впровадженні сучасних мережевих технологій створили передумови для широкомасштабної реалізації нових мережевих рішень.

Бурхливе зростання користувачів телекомунікаційних мереж призвів до серйозного попиту на послуги передачі даних і їх якість. Між компаніями, що надають різні мережеві послуги, виникла жорстка конкуренція, в результаті якої намітилася тенденція об'єднання різних інформаційних структур в єдину технологію здатну підтримувати передачу даних будь-якого типу. Впровадження широкосмугових мереж інтегрального обслуговування (Ш-ЦМІО) з використання технології АТМ (Asynchronous Transfer Mode) дозволяє вирішити це завдання.

Схема адресації в широкосмугових мережах з використанням технології АТМ має ряд особливостей: схема адресації в АТМ не залежить від будь-яких протоколів верхніх рівнів і прийнятих в них схем адресації. Тобто не існує зв'язку між адресою IP і адресою АТМ. Проте, існує необхідність дозволу адрес IP в адреси АТМ і узгодження роботи протоколів верхніх рівнів в мережі АТМ. Формат адрес в приватних мережах і мережах загального користування розрізняються. Це дозволяє телекомунікаційним компаніям гнучко реалізовувати внутрішню адресацію і маршрутизацію. Адресація АТМ ієрархічна. Розмір адреси обраний з великим запасом (20 байт).

В даний час використовується чотири різних формати адрес. Три типи адрес для приватних мереж: DCC AESA, ICD AESA і E.164 AESA. Для АТМ мереж загального користування надається вибір між форматом адреси E.164 (E.164 і E.164 AESA) і трьома типу адрес AESA представленими вище. Адреси AESA представляються в шістнадцятковій формі, довжиною 20 байт. Адреса має ієрархічну структуру і ділиться на два сегменти: IDP (Initial Domain Part) і DSP (Domain Specific Part), кожен з яких складається з декількох полів.

Для сучасного суспільства характерний швидке зростання обсягу інформації, що передається. У зв'язку з цим виникає проблема знаходження оптимального маршруту для передачі даних, тобто проблема маршрутизації. Управління процесами маршрутизації є найважливішою функцією мережевого рівня еталонної моделі взаємодії відкритих систем (ЕМ ВОС). У загальному випадку, маршрут - це список вузлів комутації від вузла-джерела до вузла-одержувача. Маршрутизація - це набір процедур, що дозволяють визначити оптимальний маршрут по заданих параметрах на мережі зв'язку між парою вузлів комутації. Тоді можна сказати, що маршрутизатор - це пристрій третього рівня еталонної моделі ЕМВОС, що використовує одну і

більше метрик для визначення оптимального маршруту передачі трафіку на основі інформації мережевого рівня [1]. У загальному випадку маршрутизація складається з трьох етапів: формування і корекція плану розподілу інформації (ПРИ), тобто таблиць маршрутизації для кожного вузла комутації; формування таблиць комутації, що забезпечують оптимальні для кожної служби маршрути доставки повідомлень користувачів; передача інформації користувача. Сукупність таблиць маршрутизації на мережі називається планом розподілу інформації. Сучасні мережі дуже критичні до всяких видів затримок і вимагають застосування нових маршрутізатіров з дуже високою продуктивністю. Одним із способів підвищення продуктивності маршрутизаторів є використання високошвидкісних апаратних маршрутизаторів. Одним з обмежень використання апаратних маршрутизаторів є неповна підтримка протоколів мережевого рівня [1]. Функції маршрутизатора можуть бути розбиті на три групи відповідно до рівнів еталонної моделі OSI: рівень інтерфейсів, рівень мережевого протоколу і рівень протоколу маршрутизації [1].

Розроблена структурна схема маршрутизатора для широкосмугової мережі інтегрального обслуговування, що реалізує логічний метод формування плану розподілу інформації. В роботі здійснено опис і розробку маршрутизатора, що реалізує логічний метод маршрутизації. Розроблено математичну модель для опису логічного методу маршрутизації.

Перелік посилань

1. Каракулова Е.Г., Котельникова А.В., Силаева М.А. Структурные схемы маршрутизаторов Ш-ЦСИО с АТМ // Материалы международной научно-практической конференции “Информатика и проблемы телекоммуникаций”. - Новосибирск, 2001.-15с.

Система підтримки обчислень у децентралізованих мережах

Тимошенко В.С., Рудьковський О.Р.
Науковий керівник – к.т.н., доц., Киричек Г.Г.
Запорізький національний технічний університет

На даний час майже всі додатки працюють як клієнт-серверні сервіси, що дозволяють обмінюватись повідомленнями, передавати файли, отримувати новини та публікувати їх. Вони взаємодіють з користувачами і з іншими сервісами, що часто використовують зловмисники при викраденні публічної інформації, даних банківських карток та ін приватних даних, тому захист даних є одним з пріоритетних питань кампаній [1].

Усе біль популярними стають децентралізовані мережі, які підтримують виконання власних додатків. Найбільш популярними є Manet, ZigBee, Ethereum, EOS. Manet та ZigBee є фізичними децентралізованими

мережами, а Ethereum та EOS – оверлейні мережі з підтримкою роботи децентралізованих додатків. Для того, щоб децентралізовані додатки могли замінити централізовані, мережа не повинна їх обмежувати, або обмежувати значно менше. Ethereum та EOS не здатні вносити записи до баз даних, робити запити до сторонніх ресурсів або обладнання. Це є суттєвим недоліком існуючих мереж, що робить їх непридатними для повноцінного використання [2,3].

Основною задачею роботи є розробка системи підтримки обчислень у децентралізованих мережах, яка підтримує: децентралізований обмін даними; зберігання інформації та запуск сервісів у децентралізованій мережі. За результатами попереднього аналізу та проведених досліджень виявлена необхідність у децентралізованій мережі, яка здатна підтримувати роботу сервісних додатків [4]. В результаті першого етапу її реалізації розроблено та наведено модель децентралізованої системи, загальними елементами якої є фізичні елементи мережі та логічні зв'язки між ними (рис. 1).

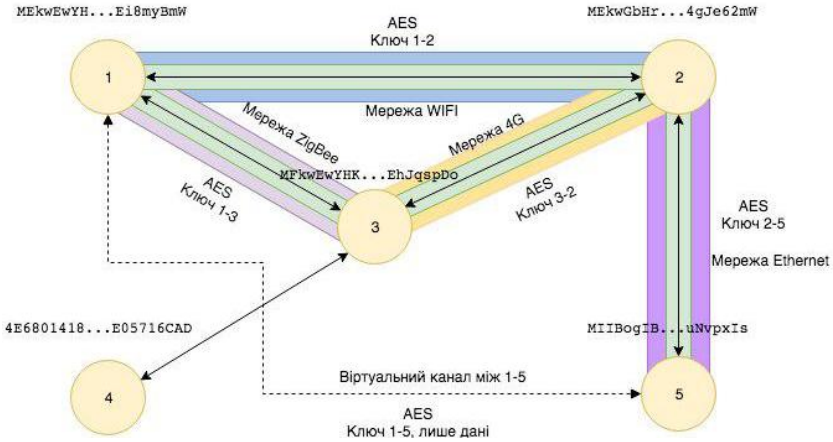

Рисунок 1 – Модель системи

Протокол описує оверлейну децентралізовану мережу, яка здатна передавати, зберігати та обробляти дані користувачів. Передача виконується децентралізовано без прямого встановлення зв'язку між клієнтами. Дані зберігаються розподіллено та публічно.

Обробка даних виконується за рахунок підтримки роботи сервісних додатків у рамках мережі. Протокол описує взаємодію різних окремих модулів мережі. Кожен модуль відповідає за певні функції в рамках мережі. Такий підхід дозволяє швидко змінювати складові частини додатка, які реалізує клієнт мережі, не впливаючи на роботу інших модулів. Усього

протокол описує дев’ять модулів: мережі; повідомлень; хешування; шифрування; команд; пам’яті; маршрутизації; серіалізації; додатків та розширень (рис.2) [4].

Додаток, що реалізує протокол, може використовувати не всі модулі, а лише необхідні для його роботи. Кожен модуль виконує одну дію і це зменшує кількість помилок та допомагає тестувати окремі частини мережі. Далі детально розглянемо усі модулі.

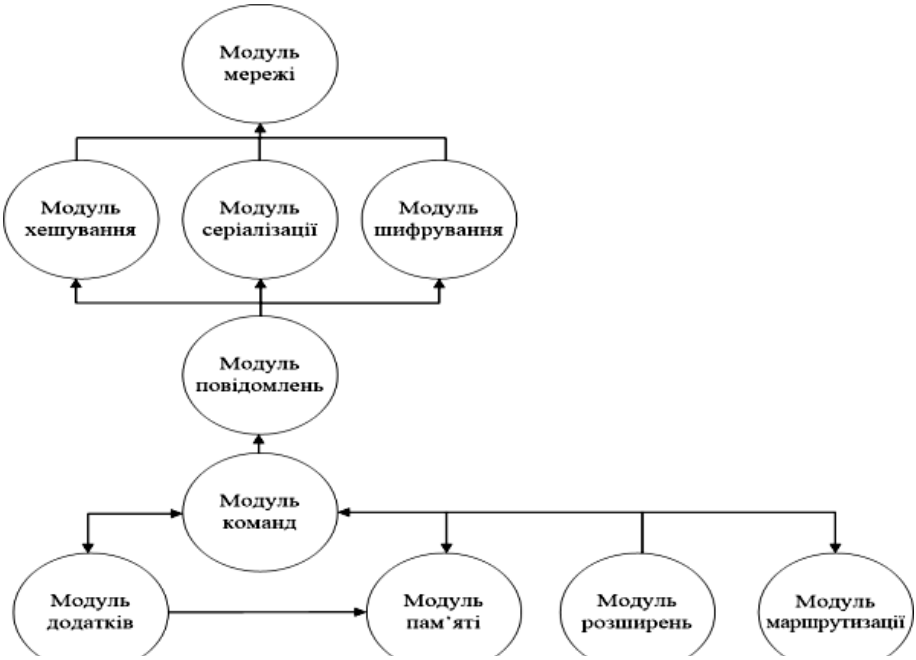

Рисунок 2 – Взаємозв’язок модулів протоколу

Додатково протокол описує структуру пакетів у рамках мережі, алгоритми та формат адрес і даних, що передаються. Додаткове ПЗ, необхідне для роботи мережі, обирається програмістом, який інтегрує мережу у свій додаток. Протокол описує взаємодію двох типів пристроїв у мережі: кінцеві та транзитні. Транзитним – є будь-який вузол, що не є відправником або отримувачем повідомлення. Один фізичний пристрій може одночасно бути як транзитним вузлом, так і кінцевим, оскільки кожен додаток, що використовує мережу є незалежною одиницею та має власну адресу.

В роботі за основу взято цибулеву маршрутизацію. Після отримання списку вузлів, які треба додати до ланцюга, вони шифруються. Адреса приймача є останньою у ланцюзі. Сегменти ланцюга шифруються починаючи з кінця попереднім сегментом, тобто для кожного сегмента використовується окремий ключ. Чим ближче сегмент до кінця, тим більше разів його зашифровано, таким чином кількість шифрувань можна вирахувати за формулою: $N_e = i - 1$, де N_e – кількість шифрувань; i – номер поточного сегмента ланцюга.

Сервісні додатки та данні виконуються на транзитних вузлах. Транзитні вузли передають дані та не мають доступу до вмісту даних. Будь-який транзитний вузол може отримати будь-яку інформацію, що зберігається у мережі. Не всі рівні моделі використовуються під час роботи протоколу. Деякі додатки можуть обмежуватись певним необхідним рівнем, наприклад транзитні вузли можуть реалізовувати рівні до модуля повідомлень включно, оскільки інші рівні в їх випадку не використовуються. Додатково кожен з модулів є незалежним і може використовуватись з будь-якого іншого модуля, наприклад модуль команд може шифрувати та дешифрувати дані напряму без звертання до модуля повідомлень [4,5].

В роботі реалізовано систему, здатну виконувати оригінальний код але децентралізовано і в рамках системи, яка дозволяє використовувати практично будь-яку мову програмування, позбавлена недоліків інших технологій за рахунок виконання програм в спеціальному ізольованому середовищі але не у віртуальній машині. Це може бути корисним у багатьох сферах: у інтернеті речей для розширення функціоналу пристроїв без зайвих витрат; банківській та юридичній сферах при проведенні операцій третьою, незалежною стороною або проведення трудомістких обчислень без необхідності створення власного кластеру пристроїв.

Перелік посилань

1. Ахметов Б.С., Корченко А.Г., Сиденко В.П. Прикладная криптология: методы шифрования. Алматы: КазНИТУ им. К.И. Сатпаева, 2015. 496 с.

2. Eastlake D., Hansen T. US Secure Hash Algorithms. 2006. URL: https://tools.ietf.org/html/rfc4634 (дата звернення: 10.10.18).

3. Rivest R., Shamir A., Ademan L. Cryptographic communications system and method. URL: https://patentimages.storage.googleapis.com/49/43/9c/b155bf231090f6/US4405829.pdf (дата звернення: 10.10.18).

4. Киричек Г.Г. Децентралізована система підтримки обчислень / Г.Г. Киричек, О.Р. Рудьковський, В.С. Тимошенко // Вчені записки ТНУ ім. В.І. Вернадського. Серія: Технічні науки. - 2018. - Том 29 (68) № 6 - С. 161-166.

5. Хайнеман Д., Поллис Г., Селков С. Алгоритмы. Справочник с примерами на C, C++, Java и Python. 2017. М: Альфа-книга. 434 с.

Система ємнісного сенсорного керування на основі Arduino

Фалько І. М., Цапко А. Е.
Науковий керівник – к.т.н., доц. Славко О. Г.
Кременчуцький національний університет імені Михайла Остроградського

«Інтернет речей» (Internet of Things, IoT) – концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу й обмін даними між фізичним світом і комп'ютерними системами за допомогою використання стандартних протоколів зв'язку [1]. Окрім датчиків мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. За рахунок використання інтелектуальних інтерфейсів в IoT-пристроях можна виключити необхідність участі людини та розширити діапазон використання. Однак на сьогодні вартість обладнання для IoT є високою.

Тому актуальним завданням є застування нових підходів і технологій для розширення можливостей реалізації та зменшення загальної вартості пристроїв для «Інтернету речей». Зокрема, в роботі запропоновано використання сенсорних датчиків в системах для IoT на основі програмно-апаратних засобів Arduino.

Метою роботи є здешевлення технології ємкісного сенсорного керування в IoT шляхом використання нестандартизованих електропровідників.

Як відомо, Arduino – апаратна обчислювальна платформа для конструювання, основними компонентами якої є плата мікроконтролера з елементами вводу/виводу та середовище розробки Processing/Wiring на мові програмування, що є спрощеною підмножиною C/C++ [2].

В роботі проведено аналіз існуючих підходів і можливостей використання апаратно-програмних засобів Arduino в контексті IoT та запропоновано використання нестандартизованих електропровідників для сенсорного керування на основі платформи Arduino.

Найпростіша форма конденсатора може бути виконана з двома провідниками, розділеними ізолятором. У ємнісних сенсорних датчиках електрод являє собою одну з пластин конденсатора. Друга пластина представлена двома об'єктами: одне середовище електрода – датчик, який утворює паразитний конденсатор, а інший – представляє собою провідний об'єкт, такий, як людський палець, який утворює сенсорний конденсатор. Електрод датчика підключений до вимірювальної схеми, а ємність вимірюється періодично. Вихідна ємність збільшується, якщо провідний об'єкт торкається або наближається до електрода датчика. Вимірювальна схема виявить зміну ємності та перетворить її в тригерний сигнал [3].

Основні проблеми та обмеження в сенсорних системах створюють кондуктивні та випромінюючі перешкоди, які можуть викликати помилкові спрацьовування ємнісних сенсорів. Кондуктивні завади виникають в системах, які отримують зовнішнє живлення по дротах – це прилади з живленням від напруги, від USB та ін., в яких немає можливості забезпечити поділ «землі» пов'язаних пристроїв. Випромінювані перешкоди діють на всі прилади, в не залежності від типу живлення.

Ємнісний сенсор підключається до входу мікроконтролера. Таким чином, електронні прилади, що випромінюють електромагнітні поля близько пристроїв з ємнісними сенсорами (стільникові телефони, лінії зв'язку, драйвера електролюмінесцентних ламп і т.п.), будуть впливати на ємнісні сенсори. Крім того, коли користувач торкається ємнісного сенсора, він стає частиною системи. Якщо користувач і система мають різні потенціали землі, то вплив перешкоди буде рівнозначно інжектуванням змінної напруги в сенсор. Інжектована перешкода призведе до зміни аналогового сигналу на вході детектора (для методу детектування на основі вимірювання напруги) або зміни частоти (для частотного методу детектування). При частотному методі вимірювання ємності випробовування перешкод буде залежати від частоти перешкоди. З цієї причини при експлуатації в умовах сильних кондуктивних або випромінюваних перешкод кращими є методи, засновані на вимірі напруги. Для методів детектування на основі вимірювання тиску в залежності від взаємного співвідношення сигналу перешкоди і моменту вимірювання можна отримати різний рівень виміряного сигналу.

Простим способом стабілізації читання сенсора є встановлення послідовного резистора між сенсором і портом мікроконтролера. Зазвичай застосовується резистор 1кОм, але значення можна вибирати в діапазоні 100 Ом – 10 кОм. Резистор разом з ємністю утворює фільтр нижніх частот і зменшує вплив високочастотних промислових перешкод [4].

Для створення тестового сенсорного датчику було обрано нестандартні підходи до його реалізації. На звичайному аркуші паперу було намальовано простим олівцем коло, що було підключено до контролера. Завдяки електропровідності графіту [5] реалізується ємкісний сенсорний датчик. Датчик можна реалізувати за допомогою будь-якого іншого електропровідного матеріалу і легко підключити до різних мікроконтролерів.

В роботі розроблено концепцію побудови системи ємнісного сенсорного керування на основі платформи Arduino. Розробка тестового модулю з ємкісним сенсорним датчиком відбувалася на макетній платі за схемою, наведеною в [6].

Узагальнений алгоритм роботи ємкісного сенсорного датчику:

1. Перевірка умови «Є живлення?» – перевірка, якщо є живлення, то контролер працю за алгоритмом, якщо ні, то завершення роботи алгоритму.

2. Ініціалізація – ініціалізація бібліотек, констант, змінних.

3. Опитування порту – перевірка напруги на вході порту.

4. Перевірка умови «Більше порогу шумів» – при збільшенні порогу шумів запускається процедура запуску вихідних портів.

В роботі розроблено функції та модулі програмного забезпечення для запропонованої системи ємнісного сенсорного керування на основі Arduino.

Модель програмного коду складається з декількох шарів, зокрема, ініціалізація параметрів апаратної платформи, Serial-порту, прослуховування та зчитування вхідних портів, автокалібрування сенсору, запуск процедури активації вихідних портів.

Для тестування ємкісної сенсорної системи проводились експериментальні дослідження, що можна поділити за наступними критеріями: 1) чутливість при використанні резисторів з різним значенням опору; 2) чутливість при зменшенні поверхні для натискання; 3) чутливість при різному ступені твердості олівця.

В роботі підготовлено та проведено експериментальні дослідження спроектованої системи. Аналіз отриманих результатів функціонування системи ємнісного сенсорного керування на основі платформи Arduino показав, що розроблена система відрізняється від аналогів своєю простотою та доступністю. Експерименти були проведенні при використанні звичайних олівців різної твердості та аркуша А4. На основі результатів можна вважати, що як ємкісний сенсорний датчик можуть виступати й інші нестандартизовані електропровідники, що дозволить створювати на їх основі різні підсистеми для пристроїв IoT.

В роботі вперше запропоновано використання нестандартизованих електропровідників для ємкісного сенсорного керування в задачах IoT, а також розроблено прототип системи ємкісного сенсорного керування на основі Arduino. Розроблена система ємкісного сенсорного керування, на відміну від існуючих, дає можливість використовувати в якості сенсорного датчика нестандартизовані електропровідники. Використання запропонованих підходів і впровадження їх у системи розумного будинку дає змогу здешевити технологію ємкісного сенсорного керування.

Перелік посилань

1. Інтернет речей [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Інтернет_речей.

2. Arduino [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Arduino.

3. Сенсорні сенсори [Електронний ресурс]. – Режим доступу: https://www.electronicshub.org/touch-sensors/.

4. Технология mTouch(tm). Создание емкостных клавиатур, сенсоров и экранов. [Електронний ресурс]. – Режим доступу: http://pickit2.ru/doku.php/all_articles:mtouch.

5. Електричний Опір [Електронний ресурс]. – Режим доступу: http://klasnaocinka.com.ua/uk/article/elektrichnii-opirtsikl-lektsii-dlya-9-klasu-v-mezh.html/.

6. Capacitive Sensing Library [Електронний ресурс]. – Режим доступу: https://playground.arduino.cc/Main/CapacitiveSensor?from=Main.CapSense.

Особливості методів управління контентом Веб - сайту

Ціліцінський А.В.
Науковий керівник – к.т.н.,доц. Хмельницький Ю.В.
Хмельницький національний університет

Керування Веб - контентом – це галузь, що набула великої актуальності із розвитком інформаційних мереж. Потреба в інтенсивній підтримці Веб - сайтів і великих порталів вимагає засобів автоматизації процесу організації і управління їх інформаційним наповненням. Тут на допомогу стали системи керування контентом - СМ8-системи. Це забезпечення, що автоматизує процеси створення і підтримки Веб - сайтів. Як галузь розробки інформаційного забезпечення, проектування і реалізація ця система спирається на досягнення в сфері методології моделювання і розробки інформаційних систем та забезпечення якості їх роботи [1]. Із розвитком Веб - технологій та спеціального інструментарію для обслуговування Веб - сайтів широкого розповсюдження набув клас масштабних Інтернет - ресурсів, які називають Веб -порталами. Веб - портал - це Веб - сайт, що надає велику кількість послуг та надає доступ до великої кількості інформаційних ресурсів широкій аудиторії користувачів. До Веб - порталів відносяться корпоративні, державні, портали новин, розважальні тощо. Активний розвиток Інтернету і явище «інформаційного вибуху» зумовили велику актуальність ресурсів навчального призначення - інформаційно-навчальних порталів. Під інформаційно-навчальним порталом слід розуміти Веб - портал, метою якого є надання доступу до різної інформації, затребуваної користувачем. Для побудови таких порталів застосовуються як системи загального призначення, так і спеціальні системи, серед яких системи керування навчальним контентом, системи дистанційного навчання, системи керування навчанням тощо

При проектуванні інформаційно-навчальних порталів слід враховувати багатий досвід в області розробки інтелектуальних навчаючих систем і адаптивних медіа-систем. Деякі технології, що застосовуються в навчальних Веб - системах, беруть також свій початок в таких технологіях як машинне навчання, інформаційний пошук та в інших галузях штучного інтелекту. Адаптивні та інтелектуальні системи навчання широко розглянуті в роботах[1]. Аналіз цих робіт дозволив зробити огляд ключових технологій і методів, що застосовуються в таких системах. Адаптивні медіа-системи - це усі медіа-системи, які зберігають опис особливостей користувача в моделі

користувача і застосовують цю модель для адаптації до користувача різних візуальних аспектів системи. Іншими словами така система повинна задовольняти трьом критеріям: вона має бути гіпертекстовою чи медійною, вона повинна мати модель користувача і вона повинна адаптувати свій медіа - простір, використовуючи цю модель. Інтелектуальні навчаючі системи - це комп'ютерні навчальні системи, що містять моделі освітнього контенту, які визначають, чому потрібно навчати, викладацькі стратегії, які визначають, як потрібно навчати. Такі системи роблять висновки щодо ступеня оволодіння студентами тих чи інших тем або завдань з метою динамічної адаптації контенту або стилю викладання. Моделі контенту - бази знань, експертні системи чи симуляції надають цим системам виразності, завдяки чому студенти «вчаться, діючи» в реалістичному і смисловому контексті. На рис.1 представлені методи і технології, що використовуються в адаптивних медіа-системах і інтелектуальних навчаючих системах, та можуть бути застосовані для потреб інформаційно-навчальних Веб - систем, що служать для побудови інформаційно-навчальних порталів.

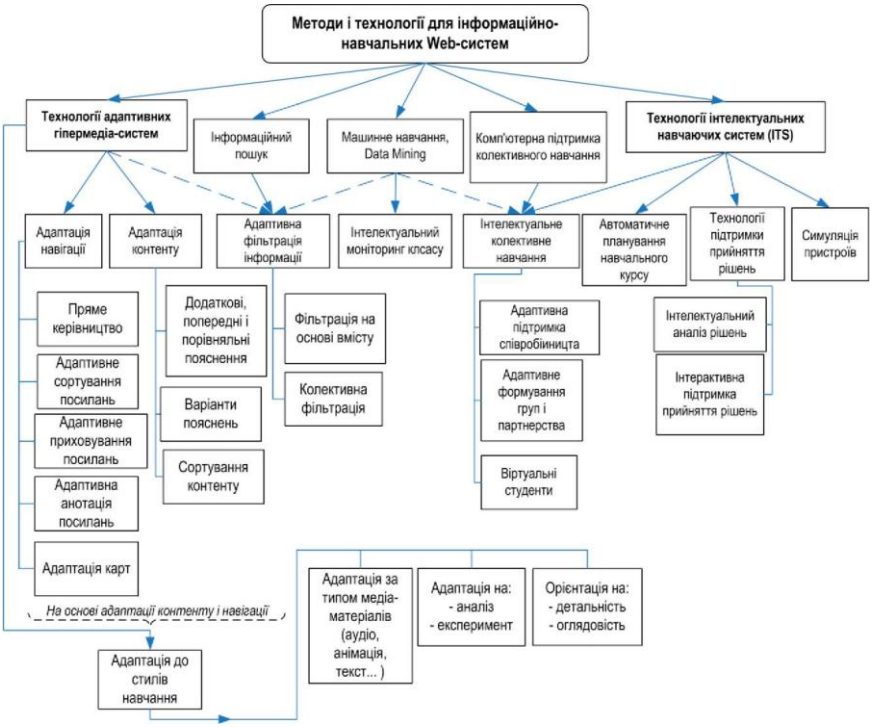

Рисунок 1 - Методи і технології для інформаційно-навчальних Веб - систем

До сучасних методів адаптивних медіа-систем відносяться адаптація

контенту та адаптація навігації - дві найпоширеніші технології, що застосовуються системами адаптивного тексту та адаптивного медіа. Метою технології адаптивного контенту є пристосування вмісту кожного вузла чи сторінки до цілей студента - користувача, знань і іншої інформації, що зберігається в моделі студента. У системі адаптивного подання контенту сторінки - не статичні, а такі, що адаптивне генеруються для кожного користувача. Метою технології адаптивної навігації є допомога студенту зорієнтуватися і переміщуватися у просторі за допомогою зміни вигляду видимих посилань. Система адаптивного медіа може адаптивне сортувати, анотувати чи частково сховати посилання поточної сторінки для того, щоб спростити вибір, куди пересуватися далі. Підтримка адаптивної навігації розділяє ту саму мету, що й автоматичне планування курсу навчання - допомогти студенту знайти оптимальний шлях через навчальний матеріал. Підтримка адаптивної навігації менше керуюча і більше «партнерська», ніж традиційне автоматичне планування: вона провадить студента, залишаючи йому можливість самостійно обрати наступний елемент знань для вивчення, наступне завдання для розв'язання. У контексті, де медіа є базовою організаційною парадигмою, підтримка адаптивної навігації є природною і ефективною.

Ще одна технологія, це адаптивна фільтрація інформації - класична технологія з області інформаційного пошуку. Її мета - знайти декілька елементів, що відповідають інтересам користувача, у великому об'ємі документів. В Інтернеті ця технологія була використана як у пошукових цілях, так і в цілях перегляду інформації. Вона застосовується для пристосування результатів Веб - пошуку із використанням фільтрації і впорядкування та для вироблення рекомендацій щодо найбільш відповідних документів серед отриманого набору із використанням генерації посилань. Хоча механізми, що використовуються у системах фільтрації інформації, дуже відрізняються від механізмів адаптивного медіа, на рівні інтерфейсу користувача в контексті системи фільтрації найчастіше використовують техніку адаптивної навігації. Існує два принципово різних типи механізмів фільтрації інформації, які можуть розглядатися, як дві різні технології фільтрації - фільтрація на основі вмісту і колективна фільтрація. Перша спирається на вміст документа, тоді як остання абсолютно його ігнорує, намагаючись замість цього підібрати коло користувачів, які будуть зацікавлені в однакових документах. Сучасна технологія фільтрації інформації широко використовує технології машинного навчання, особливо це стосується фільтрації на основі вмісту. Маючи велику розповсюдженість в галузі інформаційних систем, автоматизовані фільтри інформації проте не використовувалися в навчальному контексті у минулому. Об'єм навчального вмісту був порівняно невеликим, і потреба спрямовувати користувача до найбільш підходящого матеріалу з легкістю підтримувалася адаптивним плануванням і адаптивними медіа-технологіями. Однак Інтернет із його великою кількістю відкритих освітніх ресурсів зробив такої фільтрації технологію дуже привабливою для освітян.

До інформаційно-навчальних технологій також відносяться методи

інтелектуальних навчаючих систем, один із них - інтелектуальний аналіз рішень має справу із студентськими розв'язками навчальних задач, які можуть змінюватись від простих запитань до комплексних програмних завдань. На відміну від не інтелектуальних контролюючих інструментів, які здатні вказати лише на вірність або хибність розв'язку, інтелектуальні аналізатори можуть сказати, що саме невірно або що розв'язано не повністю, і які пропущені чи невірні знання можуть відповідати за помилку. Інтелектуальні аналізатори здатні забезпечити користувача студента потужною технікою зворотного зв'язку опрацювання помилок і оновленням моделі студента. Через низьку активність і здатність до використання інтерфейсів Веб - форм ця технологія була реалізована в WWW одною з перших. Метою інтерактивної підтримки прийняття рішень є забезпечення користувача студента інтелектуальною допомогою на кожному етапі вирішення проблеми - від надання підказки до повного виконання наступного етапу замість студента. Технологія інтерактивної підтримки прийняття рішень не на стільки популярна у Веб - системах, як в окремих інтелектуальних навчальних комплексах. Зумовлено це в основному складністю реалізації. Як було показано першими системами, чиста реалізація на стороні сервера не в змозі активно слідкувати за діями студента і може забезпечувати допомогу лише по запиту. Чиста реалізація на стороні клієнта має обмеження по складності. Необхідна функціональність і рівень складності для реалізації інтерактивної підтримки прийняття рішень потребує клієнт-серверної реалізації, але такі системи складніші в реалізації. Слід зазначити, що Веб - технологія асинхронного обміну даними, а також концепція розвинених Інтернет – відносин представляють відповідну технічну платформу для реалізації алгоритмів інтерактивної підтримки прийняття рішень на основі WWW.

Розглянемо методи інтелектуального колективного навчання [2] до яких відносять інтелектуальне колективне навчання – це група технологій, розроблена на перехресті двох областей, що на початку були далеко одна від одної: комп'ютерна підтримка колективного навчання та інтелектуальні навчаючі системи. Сучасний напрямок роботи по використанню штучного інтелекту для підтримки колективного навчання призводить до збільшення рівня взаємодії цих двох областей. Ранні роботи в області інтелектуального колективного навчання виконувались в Інтернет контексті. Сьогодні ж Інтернет та дистанційна освіта забезпечили як платформу, так і зростаючий попит на технології такого типу. В Інтернет - освіті потреба в інструментах підтримки колективного навчання є критичною, тому що користувачі студенти рідко особисто зустрічаються один з одним. Інтелектуальні технології можуть корінним чином розширити можливості простих інструментів підтримки колективної роботи, що надаються різними системами керування курсами. На даний момент можемо зазначити як мінімум три окремі технології у групі інтелектуального колективного навчання: адаптивне формування груп і партнерства, адаптивна підтримка співробітництва та віртуальні студенти.

Сучасні технології адаптивного формування груп і партнерства намагаються використовувати знання про спів працюючих членів групи для формування підходящої групи для різних типів колективних завдань. Це можна застосувати, наприклад, для задач по формуванню груп для спільного розв'язання задач та пошуку найбільш компетентного члена групи для відповіді на питання. Технології для адаптивної підтримки співробітництва намагаються забезпечити інтерактивну підтримку колективного процесу так само, як системи інтерактивної підтримки прийняття рішень допомагають окремому студенту у розв'язанні проблеми. Використовуючи деякі знання про хороші і погані зразки співробітництва, системи підтримки співробітництва можуть тренувати або консультувати членів колективу. Технологія віртуальних студентів порівняно стара. Замість підтримуючого навчання або співробітництва з позиції старшого над студентами, викладача або консультанта ця технологія намагається ввести різні типи рівноправних віртуальних партнерів у навчальне середовище. У контексті Інтернет -освіти, коли користувачі студенти часто спілкуються через низько пропускні канали, віртуальний студент стає дуже привабливим уособленням для реалізації різних стратегій підтримки. Перспективною є інтеграція цього методу з напрямками агентів та інтелектуальної підтримки співробітництва. Інтелектуальний моніторинг класів - технологія, дуже актуальна для дистанційної освіти. У контексті Інтернет - освіти «віддалений викладач» не може бачити вирази нерозуміння або загубленості на обличчях студентів. З таким браком зворотного зв'язку стає дуже важко визначити проблемних студентів, що потребують додаткової уваги, яскравих студентів, яким слід кинути виклик. Так само важким є і визначення частин навчального матеріалу, які є занадто легкими, занадто складними, або незрозумілими. Системи освіти на основі WWW можуть відслідковувати кожну дію студента, проте викладачу майже неможливо самостійно зробити необхідні висновки на основі великого об'єму даних, які збираються системою. Системи інтелектуального моніторингу класу намагаються використовувати штучний інтелект, щоб допомогти викладачу в даній ситуації. Цей напрямок роботи зосереджений на підтримці викладача та спирається на такі технології штучного інтелекту як інтелектуальний аналіз даних та машинне навчання. Можливим є також інтеграція інтелектуального моніторингу класу із адаптивною підтримкою співробітництва з метою інформування викладача про хід колективної студентської роботи і про потребу його особистого втручання для підтримки процесу.

На основі даних отриманих у результаті проведених досліджень, уточнено реалізацію комплексу управління і оптимізація ефективності передачі системи управління контентом Веб – сайтів. Теоретичний аналіз системи управління контентом виявляється досить складним технічним завданням, що обумовлено ускладненням системи рівнянь із порівнянням з аналогічною системою в одно користувацькому випадку. Із огляду, що рішення оптимізаційної задачі залежить не тільки від передавальних коефіцієнтів, але і від їх співвідношення для різних типів користувачів Веб - сайтів.

Перелік посилань
1. Берко А.Ю. Застосування маркетингових методів для аналізу життєвого циклу комерційного web-контенту / А. Ю. Берко, В. А. Висоцька // Вісн. Нац. ун-ту «Львівська політехніка» «Комп'ютерні науки та інформаційні технології». – Львів, 2011. – № 699. – С. 3–12.
2. Балашов О.Ф. Система управління наповненням контентом сайту / О.Ф. Балашов // Міжнародна науково-практична конференція молодих вчених, аспірантів та студентів «Актуальні проблеми науки та освіти молоді: теорія, практика, сучасні рішення», 21-22 квітня 2011р.: тези допов. Том І. – Х. : ХНЕУ, 2011. – С. 14 – 15.

Впровадження термінальних рішень у навчальний процес вищих навчальних закладів системи цивільного захисту

Чмир П.О.
Науковий керівник – к.т.н., Бурак Н.Є.
Львівський державний університет безпеки життєдіяльності

Інформатизація суспільства потребує відповідних фахівців, підготовлених за новітніми технологіями у результаті вдосконалення системи вищої освіти.

Застосування сучасних інформаційних технологій у вищій освіті вносить у розвиток студента ґрунтовні зміни, які стосуються як пізнавальних, так і емоційно-мотиваційних процесів, маю значний вплив на характер людини, під час цього спостерігається підсилення пізнавальної мотивації студентів у процесі роботи із засобами обчислювальної техніки.

Сьогодні у значної кількісті навчальних закладів, підприємств та організацій, зокрема державних, виникають проблеми із використанням застарілих апаратних засобів персональних комп'ютерів [1], наслідком чого є не спроможність інтеграції у свою повсякденну діяльність сучасного програмного забезпечення, зупинка у підвищенні кваліфікаційних вмінь та навичок персоналу, а також відсутність змоги повноцінно проводити заняття із застосуванням сучасного програмного забезпечення.

Одним із перспективних шляхів вирішення таких проблем є переведення існуючих засобів обчислювальної техніки у режим клієнт – серверного способу організації внутрішньої мережі на основі термінального доступу або встановлення фізичних компонентів таких як «тонкі клієнти». [2] Даний метод дозволяє здійснити оновлення можливостей мережі та обладнання шляхом створення потужного серверного комп'ютера та дає змогу зекономити фінансові ресурси закладу.

Використання термінальних клієнтів взамін звичайних персональних комп'ютерів є достатньо ефективним методом оновлення матеріально-технічної інфраструктури навчального закладу, який має значні переваги, зокрема:

- економія коштів на придбання нового потужного обладнання

шляхом використання техніки із мінімальними вимогами;

- ідентичність – усі клієнти термінального доступу доповнюється ідентичним програмним забезпеченням, що оптимізує налаштування;

- простота реалізації завдань – відсутня потреба виконувати налаштування кожного робочого місця окремо, оскільки усе здійснюється централізовано;

- оперативність роботи системного адміністратора – максимально спрощуються усі процеси адміністрування системи;

- швидкість оновлення прикладного програмного забезпечення шляхом переходу на нові версії лише сервера;

- масштабованість – збільшення кількості робочих станцій такої системи зводиться лише до копіювання попередньо сформованого та записаного образу системи одного клієнта на нову робочу машину;

- захист інформації – усі дані обробляються і зберігаються на сервері, на якому регулярно і централізовано створюються резервні копії даних, що дає змогу якісно захистити інформацію від несанкціонованого доступу.

Такі технології ефективно використовувати при організації навчальних занять у комп'ютерних лабораторіях де є постійна зміна користувачів - у вищих навчальних закладів, зокрема і системи цивільного захисту. Даний вид під'єднання дасть змогу оперативно організувати робоче місце кожного студента та забезпечити йому доступ до необхідного програмного забезпечення під час навчання. На рисунку 1 подано загальну схему побудови запропонованої термінальної мережі комп'ютерної лабораторії.

Передбачено використання 1-го потужного та швидкого сервера, 2-ох робочих місць викладачів та 30-ти місць студентів.

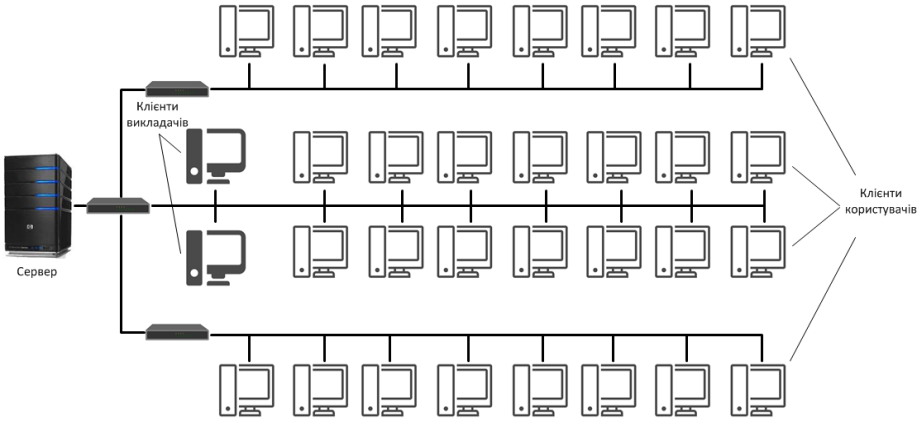

Рисунок 1 - Загальна схема організації термінальної комп'ютерної лабораторії

Таким чином, використання застарілих ПК при інтеграції

термінального рішення в комп'ютерній лабораторії – це найрозумніший і найпростіший шлях оптимізації витрат на придбання як апаратного, так і програмного забезпечення для ефективного оновлення ресурсів комп'ютерної лабораторії відповідно до вимог сьогодення.

Перелік посилань

1. Осадчий В.В. Сучасні реалії і тенденції розвитку інформаційно-комунікаційних технологій в освіті / В. В. Осадчий, К. П. Осадча // Інформаційні технології і засоби навчання. - 2015. - Т. 48, вип. 4. - С. 47-57.

2. Лисенко В.П. Термінальні рішення для навчальних закладів / В.П. Лисенко, О.О. Опришко, Ю.В. Решетняк // Аграр. наука і освіта. – 2005. – Т.6, № 5/6. – С. 130 – 133.

Оптимізація алгоритму функціонування людино-машинної системи в умовах дефіциту часового ресурсу

Щербань Т.В.
Науковий керівник – професор Лавров Є.А.
Сумський державний університет, Суми, Україна

Існуючі алгоритми оптимізації орієнтовані на обмеження середнього часу виконання, а тому не забезпечують необхідну своєчасність при випадковому характері витрат часового ресурсу. Існує різноманітність варіантів взаємодії людини з технікою і, відповідно, безліч факторів, що впливають на якість алгоритму функціонування. Сучасні автоматизовані системи вимагають особливої уваги до питань ергономічного якості. До цього часу не реалізовані алгоритми оптимізації, які сприймають час як ймовірнісну величину, що в свою чергу підвищить ефективність.
Можна сформулювати математичну модель в загальному вигляді:

$$\begin{cases} B(\mathrm{X}) \to max \\ P\{T(\mathrm{X}) \le T_0\} \ge \theta_0 \\ X \in X' \\ U(\mathrm{X}) \le U_0 \end{cases}$$

, де $B(\mathrm{X}) \to max$, тобто максимізація ймовірності безпомилкового виконання, X – спосіб виконання операції, заміна обмеження на математичне сподівання на ймовірність своєчасного виконання: $P\{T(\mathrm{X}) \le T_0\} \ge \theta_0$, $T(\mathrm{X})$ – випадкова величина часу виконання, θ_0 - мінімальна ймовірність своєчасного виконання, U(X) – витрати ресурсів при даному способі виконання. U_0 – задана кількість ресурсів. X' – ОДР задачі оптимізації.

Оптимізація алгоритму функціонування може проводитися на основі двох типів моделей: граф робіт та граф подій. Приклад переходу від графа робіт до графа подій показаний на рис.1

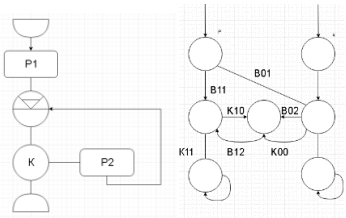

Рисунок 1 – Перехід від графу робіт(зліва) до графу подій(справа)

Дослідження показали, що при даних умовах вже не можна розглядати час як постійну величину, і тому вони дають помилковий результат. Був запропонований та реалізований алгоритм оптимізації з урахуванням ймовірнісного характеру часу.

Було проведено серію комп'ютерних експериментів, метою яких була перевірка роботи алгоритму при різних вхідних даних, велику увагу яких мала дисперсія. В результаті було доведено оптимальність та ефективність роботи алгоритму оптимізації. Розроблений продукт дозволяє вирішити задачу будь-якої складності гарантуючи своєчасність.

Евристичні механізми виявлення зловмисних програм

Щука Р.В.
Науковий керівник – к.т.н., доц. Лисенко С.М.
Хмельницький національний університет

Одним з важливих прикладних завдань, яке виникає при використанні автоматизованих систем, є забезпечення захисту інформації. Його вирішення уможливлює існуюче різноманіття підходів до виявлення шкідливого програмного забезпечення (ШПЗ). В даній статті описано новітні методики евристичних методів боротьби зі шкідливими програмами.

В даній статті обґрунтовано можливість побудови евристичного аналізатора зловмисних програм на базі нейронних мереж та дерев прийняття рішень в процесі виконання статичного аналізу виконуваних файлів (САВФ). Також зроблено спробу описати функціональну модель системи виявлення зловмисних програм за допомогою згаданого САВФ.

Забезпечення захисту інформації посідає важливе місце серед пріоритетів, що викликає до життя використання автоматизованих комп'ютерних систем. Подібне положення справ зумовлюється об'єктивним існуванням загроз, що їх створює шкідливе програмне забезпечення. Останнє здатне змінювати або видаляти дані з пристроїв, викрадати конфіденційну інформацію, вносити зміни до роботи операційної системи. Дане дослідження обґрунтовує можливість використання статичного аналізу виконуваних файлів для вирішення задачі евристичного виявлення ШПЗ за

допомогою нейронних мереж та дерев рішень.

Сьогодні існують різні методи виявлення зловмисних програм. Найбільш досліджені серед них прийнято об'єднувати утри класи:

1. сигнатурні — виявляють зловмисний код на основі послідовності байтів, що його точно характеризує;
2. евристичні — сегрегують шкідливий код на основі непрямих атрибутів, які характеризують його як шкідливий;
3. поведінкові — полягають в спостереженні за роботою програм та подальшому прийнятті рішення щодо їх шкідливості чи безпечності.

Вищезгаданим методам притаманні суттєві недоліки, що роблять сумнівним їх використання для дієвої боротьби з ШПЗ. Тобто відомі сигнатурні, евристичні і поведінкові методи характеризуються обмеженими можливостями щодо виявлення модифікованих і нових вірусів, та на додаток вимагають залучення до процесу прийняття рішень стосовно класифікації підозрілих файлів кваліфікованих фахівців.

Результати тестів, проведених McAfee Global Threat Intelligence [2], показують, що загальна кількість шкідливих програм за останні два роки виросла майже вдвічі. Проте, відоме антивірусне програмне забезпечення не може гарантувати 100% захист від ШПЗ.

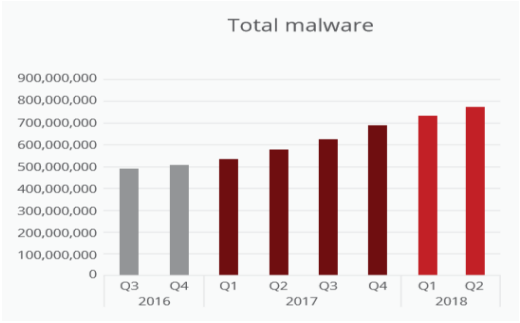

Рисунок 1 – Загальна кількість ШПЗ [2]

Дослідження предметної галузі показали, що підвищення ефективності евристичного аналізу виконуваних файлів можливо досягти шляхом залучення техніки виявлення ШПЗ на основі нейронних мереж. У цьому випадку використання математичного апарату нейронних мереж разом із синтезованим простором функцій спроможне дозволити вирішувати три такі наступні завдання:

1. генерування класів в процесі навчання (незаражені файли та зловмисне програмне забезпечення);
2. розробку процедури сегрегації ШПЗ за допомогою використання функціонального вектора на основі статичного аналізу виконуваних файлів (САВФ);
3. класифікацію виконуваних файлів без апріорних даних про їх

зараження шкідливим кодом.

Розв'язання задачі розробки нейронної мережі для виявлення шкідливих програм на основі САВФ доцільно здійснювати у два етапи:

1. навчання нейронної мережі, яка визначає шкідливі програми та незаражені класи файлів (навчальна підсистема);

2. обчислення вихідних значень нейронної мережі на основі послідовності функцій, виділених з аналізованих файлів, та прийняття рішень щодо файлів, які належать до певного класу (класифікаційна підсистема).

Цікавим з точки зору альтернативного підходу до виявлення ШПЗ виявляється застосування композиції дерев рішень. Як правило, така композиція розглядається як комбінація N алгоритмів $d_1(x),\ldots, dN(x)$. Суть ідеї полягає у вивченні алгоритмів та усередненні отриманих відповідей:

$$a(x) = \frac{1}{N}\sum_{i=1}^{N} d_n(x) \qquad (1)$$

Дана формула безпосередньо відповідає на проблему регресії. У випадку бінарної класифікації $d_1(x),\ldots, dN(x)$ вартообчислювати сигнумотриманої формули:

$$a(x) = sign\frac{1}{N}\sum_{i=1}^{N} d_n(x) \qquad (2)$$

Для побудови композиції дерев рішень спочатку необхідно згенерувати випадкові підмножини з навчального набору та вивчити роботу N алгоритмів на цих підмножинах. Для генерації наборів підмножин можна використовувати різні методики, наприклад bootstrap[5].

Таким чином, перспектива комбінування евристичних механізмів виявлення шкідливого програмного забезпечення потенційно може підвищити точність виявлення вірусів. Перспективи такого підходу були запропоновані [5] та ін. Ця обставина спонукає вдосконалювати існуючі методи виявлення шляхом комбінації наявних та створення нових методик на базі удосконалених евристичних стратегій із залученням елементів штучного інтелекту, зокрема - нейромереж.

Перелік посилань

1. Kozachok, A. V. Mathematical model of destructive software recognition tools based on hidden Markov models [Text] / A. V. Kozachok // "Vestnik SibGUTI". – 2012. – Vol. 3. – P. 29–39. – (in Russian).

2. Christiaan Beek, Carlos Castillo, "McAfee Labs Threats Report", September 2018.

3. Muazzam Siddiqui, Morgan C. Wang, Joohan Lee, "A Survey of Data Mining Techniques for Malware Detection using File Features"

4. Shi, T. Unsupervised learning with random forest predictors [Text] / Tao Shi, Steve Horvath // Journal of Computational and Graphical Statistics. – 2006. – Vol. 15, no. 1. —P. 118–138.

5. Kozachok A.V Heuristic Malware Detection Mechanism Based on Executable Files Static Analysis - 3rd International conference "Information Technology and Nanotechnology 2017".

Наукове видання

«Інтелектуальний потенціал – 2019» - збірник наукових праць молодих науковців і студентів з нагоди 30-річчя кафедри кібербезпеки та комп'ютерних систем і мереж ХНУ/Колектив авторів – Хмельницький: ПВНЗ УЕП, 2019. – Ч.2: Комп'ютерна інженерія та системне програмування. – 88 с.

Відповідальність за зміст текстів і якість редагування матеріалів покладена на авторів і наукових керівників.

Комп'ютерна верстка: Чешун В.М.
Дизайн: Муляр І.В.

Здано до складання 11.11.19. Підписано до друку 14.11.19. Формат 60x84/16. Папір друкарський. Тираж 50 прим. Умовних друкованих аркушів – 6,38.

Редакційний відділ ПВНЗ УЕП 29016, м. Хмельницький, вул. Львівське шосе, 51/2.

ББК 74.480.278
С.88