МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ

XV МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

КОМП'ЮТЕРНІ СИСТЕМИ
ТА МЕРЕЖНІ ТЕХНОЛОГІЇ

25-26 квітня 2024 року

Київ 2024

УДК 004.7(043.2)

Збірник тез доповідей XV Міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2024), м. Київ, 25–26 квітня 2024 р., Національний авіаційний університет. – К.: НАУ, 2024. – 179 с.

В процесі доповідей здійснено обмін новими ідеями, отриманими теоретичними і практичними результатами наукових досліджень в області інформаційних технологій. Обговорено сучасний стан ІТ галузі в Україні та світі, перспективні напрямки розвитку інформаційних технологій. Для науковців, викладачів, аспірантів, студентів, співробітників наукових установ та ІТ компаній. Матеріали подані мовою оригіналу (українська, англійська). Редакційна колегія зберегла авторський текст без істотних змін, звертаючись до коректування в окремих випадках.

Відповідальність за достовірність матеріалів несуть автори.

Рекомендовано до видання вченою радою Факультету комп'ютерних наук та технологійї Національного авіаційного університету (протокол № 4 від 15 квітня 2024 р.).

Редакція не обов'язково поділяє думку автора. Відповідальність за достовірність фактів, цитат власних імен та іншої інформації несуть автори.

ЗМІСТ

І.В.Апаренков, А.В.Хилевич
ЗАСОБИ МОДЕЛЮВАННЯ КІБЕРАТАК У СУЧАСНОМУ КІБЕРПРОСТОРІ 10

А.С.Биков
ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ У ВИЯВЛЕННІ ТА ПРОТИДІЇ КІБЕРАТАКАМ 12

А.І.Вавіленкова
ФУНКЦІЇ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕННЯМ 14

В.С.Васильєва
ІННОВАНЦІЙНІ ПІХОДИ ДО НАПИСАННЯ КОДІВ ПРОГРАМ У БОРОТЬБІ ПІД ЧАС КІБЕРВІЙНИ 16

О.О.Волобуєв
СПОСІБ КОРЕКТНОЇ ПЕРЕДАЧІ ДОКУМЕНТІВ ПІД ЧАС ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ МІЖ СИСТЕМАМИ 18

В.І.Воронцов
ОСОБЛИВОСТІ СТАНДАРТУ МОВИ ОПИСУ АПАРАТУРИ VERILOG ПРИ ПРОЕКТУВАННІ RISC ІНСТРУКЦІЙ 20

В.П.Гамаюн
ТЕХНОЛОГІЯ ОБРОБКИ ВЕЛИКИХ МАСИВІВ ДАНИХ 23

В.В.Гамоля, В.А.Мельник, А.О.Мельник
ПРОБЛЕМНІ ПИТАННЯ РОЗПОДІЛУ ОБЧИСЛЮВАЛЬНОГО НАВАНТАЖЕННЯ В ГЕТЕРОГЕННИХ КОМП'ЮТЕРНИХ СИСТЕМАХ 26

І.Г.Гіваргізов, М.О.Ковальчук
КОНЦЕПЦІЇ ПОБУДОВИ ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ LLM У БАНКІВСЬКОМУ СЕРЕДОВИЩІ 28

С.Я.Гільгурт, І.А.Жуков
ПІДХІД ДО РЕАЛІЗАЦІЇ АДАПТИВНИХ МОЖЛИВОСТЕЙ РЕКОНФІГУРОВНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ СИГНАТУРНОГО ТИПУ 31

Є.А.Гупало
НЕЙРОННІ МЕРЕЖІ У ЗАХИСТІ ІНФОРМАЦІЇ 35

А.Д.Данилов
ОГЛЯД СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ДАНИХ 37

К.Дахал, О.П. Мартинова, А.А.Крайносвіт
СУЧАСНІ ПІДХОДИ ДО УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЇ: ТЕХНОЛОГІЯ SIEM 39

Ю.Є.Добришин
КЛАСИФІКАЦІЯ ТА ОПИС ІНФОРМАЦІЇ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ЩОДО ВИЯВЛЕННЯ, ПОПЕРЕДЖЕННЯ КІБЕРАТАК 41

Б.І.Долінце
ОСОБЛИВОСТІ ОБРОБКИ ІНФОРМАЦІЇ В БАГАТО-СУПУТНИКОВИХ СИСТЕМАХ ПОЗИЦІОНУВАННЯ З ВИКОРИСТАННЯМ LEO-СУПУТНИКІВ 43

В.А.Дорогань
ВИЯВЛЕННЯ ТА ЗАХИСТ ВІД SQL-ІН'ЄКЦІЙ У ВЕБ-ДОДАТКАХ 45

В.І.Дрововозов, С.В.Водоп'янов, О.В.Андреєв, А.Б.Коцюр
ЕВОЛЮЦІЯ КЛЮЧОВИХ ПАРАМЕТРІВ КОМП'ЮТЕРНИХ МЕРЕЖ ПРИ ПЕРЕХОДІ ДО БЕЗПРОВОДОВИХ РЕЖИМІВ РОБОТИ 47

О.В.Дубчак, Н.К.Гулак
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ УБЕЗПЕЧЕННЯ КОМУНІКАЦІЙНИХ МЕРЕЖ 53

О.В.Дубчак, Є.С.Тимофіїв
АНАЛІЗ ЗАСОБІВ ЗАХИСТУ WI-FI РОУТЕРІВ 55

О.В.Дубчак, О.О.Левченко
ПРОБЛЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ КОРИСТУВАЧА ВЕББРАУЗЕРІВ 57

Т.С.Дьячук
АВТОМАТИЗОВАНА ПЕРЕВІРКА ЗАВДАНЬ ПРИ НАВЧАННІ ПРОГРАМУВАННЮ 59

В.В.Дяк
ЩОДО ПИТАННЯ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ В УКРАЇНІ 61

М.С.Жижкін, М.В.Куклінський
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА НАДІЙНОСТІ ОБМІНУ ДАНИМИ 64

А.В.Закружний
ПРОГРАМНІ СЕРВІСИ МОНІТОРИНГУ ТРАФІКУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ 66

А.Л.Зірка, М.В.Зірка, Н.П.Кадет
ТЕОРЕТИЧНІ ОСНОВИ СТРУКТУРНОГО СИНТЕЗУ ЛІНІЙНИХ ТА НЕЛІНІЙНИХ МАТЕМАТИЧНИХ МОДЕЛЕЙ АЕРОДИНАМІКИ В ЗАДАЧАХ ОЦІНКИ АЕРОДИНАМІЧНИХ ХАРАКТЕРИСТИК БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ 68

О.М.Зудов, В.В.Горіна, Н.О.Рибасова
ПРОТОКОЛИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ КРИПТОГРАФІЧНОЇ СХЕМИ "СЛІПОГО ПІДПИСУ" І БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ 71

А.В.Ільєнко, С.С.Ільєнко, О.Л.Яковенко
ПІДХІД ЩОДО ПЕРЕВІРКИ ЦИФРОВИХ СЕРТИФІКАТІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ BLOCKCHAIN 74

Є.Є.Карпов, О.В.Вовна
ПІДВИЩЕННЯ БЕЗПЕКИ ТА НАДІЙНОСТІ КОМП'ЮТЕРНО-ІНТЕГРОВАНОЇ СИСТЕМИ МОНІТОРИНГУ В МЕЖАХ АЕРОПОРТУ НА БАЗІ РАДІОМЕРЕЖІ LORAWAN 76

А.С.Климова
БАГАТОКРИТЕРІАЛЬНИЙ ПАРАМЕТРИЧНИЙ СИНТЕЗ АВІАЦІЙНО-КОСМІЧНИХ СИСТЕМ 79

А.М.Козуб, Д.П.Кучеров, О.М.Пошивайло
РЕКОМЕНДАЦІЙНА СИСТЕМА ДЛЯ ЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ ПОВІТРЯНОГО ТРАНСПОРТУ В СКЛАДНИХ УМОВАХ ПОЛЬОТУ 83

В.В.Константиненко, Є.В.Куляк
TRELLO ПРОГРАМА ДЛЯ ІТ-ПРОЄКТУВАННЯ ТА УПРАВЛІННЯ 85

В.А.Копитов
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ В СУЧАСНІЙ УКРАЇНСЬКІЙ ЕНЕРГЕТИЦІ З УРАХУВАННЯМ НАСЛІДКІВ ВІЙСЬКОВОЇ АГРЕСІЇ 87

Р.І.Кормиш, Р.С.Савіцький
АНАЛІЗ ПРОЦЕСІВ АВТОМАТИЗАЦІЇ МЕНЕДЖМЕНТУ БУДІВЕЛЬНИХ ПРОЕКТІВ 89

С.В.Костюков, О.П.Мартинова, О.О.Кучмій
КОНТЕЙНЕРИЗАЦІЯ ТА ЇЇ ВПЛИВ НА ПРОЦЕС РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ 91

М.М.Котенко, Т.А.Вакалюк
МЕТОДИКИ ВИМІРЮВАННЯ ТА АНАЛІЗУ ВЗАЄМОДІЇ МІКРОСЕРВІСНИХ КОМПОНЕНТІВ 93

Є.В.Красовська, О.Д.Красовський
ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ 3D МОДЕЛЮВАННЯ 95

С.О.Кудренко, А.Л.Столяр
ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМІ ДИСТАНЦІЙНОГО СПІЛКУВАННЯ 97

Ю.О.Кулаков, Д.В.Коренко
МЕТОД БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В МЕРЕЖАХ SDN З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ 101

Ю.О.Кулаков, О.В.Череватенко
ДИНАМІЧНА РЕКОНФІГУРАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЇ SDN 104

Ю.В.Лукаш
МЕТОД АВТОМАТИЗОВАНОГО СТВОРЕННЯ ДАТАСЕТУ ДЛЯ НЕЙРОМЕРЕЖІ РОЗПІЗНАВАННЯ ОБРАЗІВ 106

А.А.Малахова, А.Д.Данилов
ЮРИДИЧНІ ТА ЕТИЧНІ АСПЕКТИ ЗБОРУ МЕРЕЖЕВИХ АРТЕФАКТІВ: БАЛАНС МІЖ БЕЗПЕКОЮ ТА КОНФІДЕНЦІЙНІСТЮ 108

А.О.Мельник, Ю.В.Морозов, Б.І.Гаваньо, П.А.Гупало
СПОСІБ АНОНІМІЗАЦІЇ ДАНИХ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ 110

П.І.Мельниченко
АНАЛІЗ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ БЕЗПЕЧНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ 112

Н.А.Москвичова, Н.О.Шибаєва
ІНТЕГРОВАНА ЕЛЕКТРОННА ПЛАТФОРМА ДЛЯ ОПТИМІЗАЦІЇ ПРОЕКТУВАННЯ ТА УПРАВЛІННЯ КОМП'ЮТЕРНИМИ СИСТЕМАМИ В УМОВАХ ЗМІНИ ПАРАДИГМИ НАВЧАННЯ ... 116

М.О.Московко, О.П.Мартинова
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SDN В ПОЛЬОВИХ УМОВАХ... 118

В.В.Нікітін, М.М.Козуля
ZKSNARKS ТЕХНОЛОГІЯ ДЛЯ СЕРТИФІКАЦІЇ ЦИФРОВОГО КОНТЕНТУ 120

М.К.Печурін, Л.П.Кондратова, С.М.Печурін
МОВА ВЗАЄМОДІЇ ДЛЯ НАДЛЕГКИХ БПЛА 122

П.А.Поліщук
СТРАТЕГІЯ РОЗРОБКИ ВЕБ-ЗАСТОСУНКІВ..... 124

О.І.Полотай, А.П.Тераз, Б.В.Шаповалов
СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ 126

Д.О.Пономаренко, П.І.Іванчук
СУЧАСНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ: КОМПЛЕКСНИЙ ПІДХІД ДО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ 128

І.Г.Прокопенко, А.С.Савченко, К.І.Прокопенко, А.Ю.Дмитрук
ПОРІВНЯННЯ ЕФЕКТИВНОСТІ НЕЙРОМЕРЕЖЕВОГО ТА СТАТИСТИЧНОГО ПІДХОДІВ ДО ЗАДАЧІ ВИЯВЛЕННЯ СИГНАЛІВ 130

В.А.Пургін, О.П.Мартинова
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ LANGCHAIN З ВЕКТОРНОЮ БАЗОЮ ДАНИХ PINECONE ДЛЯ ГЕНЕРАЦІЇ ВІДПОВІДІ ШТУЧНИМ ІНТЕЛЕКТОМ ДЛЯ КОРИСТУВАЧА 133

О.В.Русанова, О.В.Корочкін, О.П.Шевело
ПРОБЛЕМА АВТОМАТИЗАЦІЇ ПЛАНУВАННЯ РОБІТ У ІТ БІЗНЕС ПРОЄКТАХ 136

А.С.Савченко, О.В.Толстікова, С.В.Водоп'янов
СИСТЕМНИЙ ПІДХІД ДО РОЗВ'ЯЗАННЯ КОНФЛІКТІВ МІЖ КЛЮЧОВИМИ ПАРАМЕТРАМИ БЕЗПРОВОДОВИХ МЕРЕЖ 138

Д.О.Сак
АНАЛІЗ МІЖНАРОДНИХ ДОКУМЕНТІВ З УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ..... 144

В.С.Сахно, О.П.Мартинова
ПРОБЛЕМАТИКА ПОЛЬОТНОГО КОНТРОЛЮ В СУЧАСНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ..... 146

С.М.Сидоренко
ДЕЗІНФОРМАЦІЯ ЯК СИНДРОМ ВИНИКНЕННЯ КІБЕРЗАГРОЗИ 148

Ю.І.Сінько
ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ САПР ТП 150

М.А.Сіренко, М.К.Печурін
ЕНЕРГОВИТРАТИ ПРИЙОМО-ПЕРЕДАЮЧОГО ОБЛАДНАННЯ БПЛА ПРИ НАВЧАННІ МЕРЕЖІ ХОПФІЛДА..... 152

О.І.Скіцько
РОЗВІДКА З ВІДКРИТИХ ДЖЕРЕЛ ДЛЯ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ 154

К.В.Степанець
РОЗВИТОК МЕТОДІВ АНАЛІЗУ ТА ПЕРЕДБАЧЕННЯ ЗАГРОЗ КІБЕРБЕЗПЕЦІ, ВРАХОВУЮЧИ СПЕЦИФІКУ УКРАЇНСЬКОГО КІБЕРПРОСТОРУ ТА ГЕОПОЛІТИЧНІ КОНТЕКСТИ..... 156

В.Ф.Сураєв, В.І.Мазур, Н.Б.Фоміна
ОРГАНІЗАЦІЯ ПОТОКІВ ДАНИХ В СИСТЕМІ ФОРМУВАННЯ ЗАВДАНЬ НА ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ ЛІТАКІВ 158

І.В.Телешко
ОСОБЛИВОСТІ ВИКОРИСТАННЯ МАСОК ЗМІННОЇ ДОВЖИНИ В МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ 160

А.О.Трєгуб, Г.О.Шеїна, О.В.Вовна
РОЗРОБКА КОМП`ЮТЕРНОЇ СИСТЕМИ МОНІТОРИНГУ КОНЦЕНТРАЦІЇ СІРКОВОДНЮ В АТМОСФЕРІ ПРОМИСЛОВИХ ПІДПРИЄМСТВ 162

І.І.Тугай
ЄВРОПЕЙСЬКИЙ ДОСВІД ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ 165

О.В.Чалий
АЛГОРИТМИ ВИМІРЮВАННЯ НА КООРДИНАТНО-ВИМІРЮВАЛЬНІЙ МАШИНІ 167

А.М.Чернюк, Д.Ю.Каліновський, Р.С.Савіцький
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ПСИХОЛОГІЧНОЇ ПІДТРИМКИ 169

Т.Р.Чура, Н.Р.Чура
ІНТЕГРАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МЕТОДИ AGILE РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ПРИКЛАДІ SECURE SCRUM 172

О.М.Шаповал, В.В.Цуркан
РИЗИК-ОРІЄНТОВАНА АРХІТЕКТУРА БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ 174

Р.А.Ширшов
РИЗИКИ ВИКОРИСТАННЯ СИСТЕМ ШІ 176

УДК 005.2::004.04::004.67/656::004.9/338.1

І.В.Апаренков,
А.В.Хилевич
Національна академія Служби безпеки України, Київ

ЗАСОБИ МОДЕЛЮВАННЯ КІБЕРАТАК У СУЧАСНОМУ КІБЕРПРОСТОРІ

Зростання інтелектуальних технологій в автоматизації документообігу та управлінні процесами відкриває перед зловмисниками нові шляхи обходу захисних систем. Це робить кібератаки на інформаційні ресурси однією з найактуальніших проблем сьогодення. Боротьба з ними потребує значних ресурсів від державних та комерційних структур, як в фінансовому, так і в часовому та кадровому аспектах.

Особливістю сучасних технологій роботи з великими даними є відсутність усталеної математичної теорії, що визначає процедури пошуку і оброблення інформації. Це дозволяє зловмисникам будувати складні алгоритми атак, що можуть досягати своєї мети різними способами, в залежності від ситуації в кіберпросторі. Для реалізації атак у мережному середовищі зазвичай використовуються троянські програми, кінцевою метою яких є впровадження у програмний код атакованої системи додаткових прихованих функцій. Основною проблемою є те, що зазвичай факт втручання може бути виявлений вже після здійснення атаки. Зазвичай, такі несанкціоновані втручання до інформаційної системи не мають чітко визначеної часової закономірності, а їх тривалість є недостатньою для належного реагування. Таким чином, задача полягає у створенні такої стратегії боротьби, яка б дозволяла визначати зловмисні дії вже на перших кроках реалізації кібератак [1].

Однією із умов створення ефективної системи захисту у кібернетичному просторі є володіння інформацією про всі її слабкі місця, а також розуміння формальних моделей організації сучасних атак у середовищі експлуатації інформаційних систем. І самі моделі, і визначення переліку уразливостей ґрунтується на постійному моніторингу можливих джерел загроз, з точки зору їх мотивів та наявності ресурсів для реалізації цих загроз, а також аудиту системи захисту на наявність у ній уразливостей. Відповіді на ці питання дає використання ромбовидної моделі. Ця модель

враховує чотири основних елементи: супротивника і його ресурси, інфраструктуру, здатність до нападу і ціль. Для прогнозування дій порушника найчастіше використовується модель послідовних вторгнень. Порушник крок за кроком виконує спроби подолання системи захисту, намагаючись подолати механізми захисту через уразливості там, де він їх знаходить. Основними елементами моделі послідовних вторгнень є індикатори, під якими розуміється будь-яка інформація, що об'єктивно описує кожний етап вторгнення. Зазвичай, послідовність вторгнення включає сім етапів: розвідку, озброєння, доставку, виконання, створення "чорного входу", установка таємного каналу і зловмисні дії по відношенню до об'єкту атаки [2]. Незважаючи на тип обраної моделі атак, автоматизація процесів протидії нападу на інформаційну систему з боку зовнішнього кібернетичного середовища передбачає створення досить складного програмного коду. Графи атак являють собою концептуальні діаграми і використовуються для аналізу можливих шляхів реалізації конкретної загрози. Найчастіше – це багаторівневі деревовидні структури, що мають дочірні елементи з одним коренем. У випадку опису сучасної атаки вони мають тисячі вузлів і шляхів подолання механізмів захисту. Тому генерація графів для атак у складних мережах є дуже складною в обчислювальному сенсі. На основі проведеного аналізу існуючих моделей реалізації мережних атак можна зазначити, що перевага має надаватись таким, які дозволяють, по-перше, оцінити вірогідність нападу з боку можливих джерел загроз, по-друге, визначити стратегію розпізнавання атаки на початку спроби її реалізації порушником безпеки. Модель повинна легко піддаватись формальному опису для подальшого її використання у процедурах автоматизації управління захистом.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," DTIC Document, Tech. Rep., 2013. 2. E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Leading Issues in Information Warfare & Security Research, vol. 1, p. 80, 2011.

УДК 004.056.

А.С.Биков
Національна академія Служби безпеки України, Київ

ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ У ВИЯВЛЕННІ ТА ПРОТИДІЇ КІБЕРАТАКАМ

Впровадження нейронних мереж як інструменту виявлення та протидії кібератакам є надзвичайно актуальним і перспективним напрямком у сучасних реаліях зростаючої кількості та складності кіберзагроз.

Здатність нейронних мереж до навчання, адаптації та виявлення складних закономірностей у великих обсягах даних робить їх ідеальним рішенням для швидкої ідентифікації аномалій та потенційно шкідливої активності в комп'ютерних системах та мережах.

Нейронні мережі мають значні переваги порівняно з традиційними методами виявлення вторгнень, заснованими на чітких правилах та сигнатурах. Вони здатні аналізувати різноманітні типи даних, зокрема мережевий трафік, журнали подій, файли та інші цифрові артефакти, для виявлення невідомих раніше векторів атаки.

Завдяки своїй гнучкості та адаптивності, нейронні мережі можуть ефективно протидіяти новим та складним кібератакам, що постійно еволюціонують, на відміну від статичних систем виявлення вторгнень, які часто відстають від нових загроз.

Крім того, використання нейронних мереж дозволяє зменшити навантаження на людські ресурси в процесі моніторингу та реагування на інциденти інформаційної безпеки. Автоматизація процесів виявлення та класифікації атак за допомогою нейронних мереж забезпечує швидке реагування та мінімізує ризики, пов'язані з людським фактором.

Одним з прикладів успішного використання нейронних мереж для виявлення та протидії кібератакам є система Cisco Cognitive Threat Analytics (CTA). Ця система застосовує глибокі нейронні мережі для аналізу великих обсягів даних мережевої активності, журналів подій та іншої інформації з метою виявлення аномалій та потенційних загроз.

Ключовою перевагою CTA є її здатність навчатися на даних та динамічно адаптуватися до нових типів атак. Система постійно оновлює свої моделі машинного навчання, використовуючи як локальні дані організації, так і глобальну інформацію про нові загрози з хмарної платформи Cisco.

Це дозволяє CTA ефективно виявляти невідомі раніше атаки, такі як цілеспрямовані атаки на організації або експлойти для нових вразливостей. Згідно з даними Cisco, CTA продемонструвала високу ефективність у виявленні різноманітних типів кібератак, включаючи шкідливе програмне забезпечення, спроби фішингу, експлойти вразливостей.

За оцінками компанії, система здатна виявляти до 96% загроз з низьким рівнем хибних спрацювань, що значно перевищує показники традиційних систем виявлення вторгнень.

Однією з ключових переваг CTA є її здатність інтегруватися з іншими рішеннями кібербезпеки Cisco, такими як брандмауери, системи запобігання вторгненням та інструменти для реагування на інциденти. Це забезпечує комплексний захист організації та швидке реагування на виявлені загрози.

Хоча впровадження CTA може бути складним і вимагати значних ресурсів, особливо для великих організацій, ця система демонструє величезний потенціал нейронних мереж у сфері кібербезпеки.

Подальший розвиток та вдосконалення таких рішень, а також їх поширення у різних галузях та організаціях, є перспективним напрямком для підвищення загального рівня кібербезпеки.

ВИКОРИСТАНІ ДЖЕРЕЛА

Buhas, Vasyl and Ponomarenko, Ihor and Bugas, Valeriy and Ramskyi, Andrii and Sokolov, Volodymyr (2021) Using Machine Learning Techniques to Increase the Effectiveness of Cybersecurity Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). pp. 273-281. ISSN 1613-0073

УДК 004.056 (045)

А.І. Вавіленкова
Національна академія Служби безпеки України, Київ

ФУНКЦІЇ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕННЯМ

Крім типових обов'язкових заходів кібергігієни, для уникнення DDoS-атак використовують спеціально розроблені системи виявлення вторгнень та системи запобігання вторгненням.

Система виявлення вторгнень (IDS) – це програмне забезпечення, що використовується для виявлення атак та шкідливих дій, а також контролює мережеве середовище для виявлення підозрілої поведінки, про що сповіщає адміністратора мережі. Система виявлення вторгнень моніторить і аналізує активність користувачів, перевіряє цілісність системних файлів та файлів даних, здійснює аудит операційної системи та конфігурації системи, виявляє її слабкі місця.

Система виявлення вторгнень містить:

- детекторну систему, що дозволяє накопичувати події комп'ютерної мережі;
- підсистему аналізу, яка безпосередньо виявляє DDoS-атаки та аномальну поведінку системи;
- сховище для накопичення інформації про події та результати аналізу кібератак та несанкціонованих дій;
- консоль управління – дає змогу задавати параметри системи виявлення вторгнень, стежити за станом мережі, організувати доступ до інформації про виявлені та проаналізовані атаки і несанкціоновані дії.

В цілому, системи виявлення вторгнень можуть працювати за двома принципами:

– на основі виявлення аномалій, тобто працює шляхом відстеження та порівняння типової поведінки системи та аномальної щодо кількості пакетів, інтенсивності сканування портів, таким чином відстежуючи ще й нові, не описані раніше атаки;

– на основі перевірки сигнатур – має велику базу даних сигнатур атак, тобто правил, що описують способи боротьби з вторгненнями, аналізуючи при цьому кожен пакет, порівнюючи з сигнатурами бази даних та генеруючи попередження у випадку виявлення сигнатури.

Система запобігання вторгненням (IPS) – це програмне забезпечення, що використовується для забезпечення безпеки мережі, може виявляти, записувати, сповіщувати про атаку та

виконувати захисні функції, на зразок, блокування пакетів трафіку, можуть працювати онлайн та автоматично блокувати DDoS-атаки. До основних функцій системи запобігання вторгненням належать:

- виявлення відомих експлойтів;
- упередження уразливостей, включаючи відомі та невідомі інструменти експлойтів;
- виявлення неправильного використання протоколів, які можуть містити потенційні загрози;
- виявлення та упередження спроб тунелювання, які можуть вказувати на витік інформації;
- фіксування та виявлення вихідних зловмисних повідомлень.

Під час розгортання системи запобігання вторгненням використовуються чотири основні технології:

- встановлення виділених пристроїв за периметром корпоративної мережі та всередині неї;
- інтеграція системи запобігання вторгненням в маршрутизатор;
- оснащення системами запобігання вторгнень точок доступу для виявлення та протидії різним атакам, а також знаходження несанкціоновано встановлених точок доступу та клієнтів;
- встановлення системи запобігання вторгненням на робочій станції або сервері як прикладне програмне забезпечення поверх операційної системи.

Неодмінною складовою систем виявлення та запобігання вторгнень є міжмережевий екран, фаєрвол, який дозволяє або блокує мережеве з'єднання на основі правил, визначених адміністратором чи користувачем персонального комп'ютера або комп'ютеної мережі, фактично реєструючи інформацію про мережевий трафік, що допомагає адміністратору запобігати атакам.

ВИКОРИСТАНІ ДЖЕРЕЛА

Вавіленкова А.І. Методи і моделі протидії кібератакам / А.І. Вавіленкова: навчальний посібник. – К.: НА СБУ, 2023. – 136 с.

УДК 004.056

В.С.Васильєва
Національна академія Служби безпеки України, Київ

ІННОВАНЦІЙНІ ПІХОДИ ДО НАПИСАННЯ КОДІВ ПРОГРАМ У БОРОТЬБІ ПІД ЧАС КІБЕРВІЙНИ

Кібервійна – це все більш поширена загроза, яка може мати серйозні наслідки для країн, організацій та окремих осіб. Кібератаки можуть призвести до крадіжки даних, перебоїв у роботі систем, шкоди репутації та навіть фізичних руйнувань.

Програмне забезпечення відіграє ключову роль у кібервійні. З одного боку, воно може використовуватися для здійснення кібератак. З іншого – може використовуватися для захисту від таких атак. Тому **а**ктуальність теми дослідження полягає в тому, що воно може допомогти у розробці нових та інноваційних програм, які допоможуть захистити від кібервійни.

Кібервійна – це конфлікт, що триває у цифровому просторі за допомогою комп'ютерних технологій. Його мета – дестабілізація інфраструктури супротивника, збирання розвідданих, а також знищення або пошкодження критично важливих комп'ютерних систем і мереж. Це застосування атак заради отримання переваги над противником або завдання шкоди його економіці, обороні та національній безпеці. На відміну від інформаційних атак, що зосереджені на поширенні дезінформації, пропаганди або на впливі на громадську думку, кібервійна охоплює ширший спектр, як-от злами систем, шпигунство, зараження шкідливим програмним забезпеченням (ПЗ), викрадення даних.

Кібервійна стає дедалі складнішою, і традиційні методи захисту стають все менш ефективними. У боротьбі з кібервійною важливо розробляти програми, що ефективно захищають системи від кібератак і забезпечують їхню безпеку. Тому розробники шукають нові, інноваційні підходи до написання кодів, щоб краще протистояти кібератакам.

1. Підхід щодо застосування штучного інтелекту (ШІ). ШІ може використовуватися для автоматичного виявлення та реагування на кібератаки. Алгоритми машинного навчання можуть аналізувати великі обсяги даних, щоб знаходити аномальні patterns, які можуть свідчити про кібератаку. ШІ також може використовуватися для автоматичного блокування атак або для їхнього перенаправлення.

2. Підхід з використанням блокчейн-технологій. Блокчейн може використовуватися для створення більш безпечних та стійких до атак систем. Ця технологія може використовуватися для зберігання кодів та даних у зашифрованому вигляді, що робить їх недоступними для хакерів.

3. Застосування методів обфускації. Обфускація – це метод, який робить код складнішим для читання та розуміння. Це може ускладнити хакерам завдання виявлення вразливостей у коді.

4. Використання принципів Secure by Design – підходу до розробки програмного забезпечення, який передбачає вбудовування заходів безпеки на всіх етапах розробки. Це може допомогти запобігти появі вразливостей у коді.

5. Застосування методології DevOps – поєднує розробку (Dev) та експлуатацію (Ops) програмного забезпечення. Цей підхід може допомогти усунути недоліки в системі безпеки, які можуть виникати через розрив між розробниками та операторами програмного забезпечення.

Також дієвими підходами протистояння у кібервійні є постійне навчання та оновлення, співпраця та обмін інформацією, підвищення обізнаності, використання кращих практик кодування, регулярне тестування та аудит.

Використання цих інноваційних методів написання кодів може допомогти програмістам створювати більш стійкі до кібератак програми. Розробка програм, які використовують новітні технології, може допомогти у захисті від кібератак та зробити світ кращим.

ВИКОРИСТАНІ ДЖЕРЕЛА

2. Шевченко, О. О. Інноваційні методи написання кодів для програм у боротьбі з кібервійною. Вісник Національного технічного університету України «Київський політехнічний інститут», 2, С.12-18.

Національний координаційний центр кібербезпеки при РНБО України. (2023, 14 листопада). Кібервійна: виклики та шляхи протидії. https://cybercenter.gov.ua/kcybervijna-vyklyky-ta-shlyahi-protydiyi/

УДК 004.7

О.О.Волобуєв
Національний авіаційний університет, Київ

СПОСІБ КОРЕКТНОЇ ПЕРЕДАЧІ ДОКУМЕНТІВ ПІД ЧАС ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ МІЖ СИСТЕМАМИ

У наш час, коли електронний документообіг все більше витісняє традиційні паперові документи, коректна передача усіх атрибутів документів між різними системами набуває першочергового значення. Адже від точності та повноти інформації, що міститься в електронних документах, залежить ефективність взаємодії між установами, підприємствами та організаціями. Тому питання забезпечення надійності, конфіденційності та цілісності електронного документообігу стають ключовими в сучасному діловодстві.

Сучасні технології дозволяють автоматизувати більшість процесів, пов'язаних з обігом документів, проте це вимагає ретельної розробки протоколів та стандартів для коректної передачі усіх необхідних реквізитів між різними програмними системами. Недотримання цих вимог може призвести до помилок, втрати важливої інформації чи навіть порушення законодавства.

Тож розгляд особливостей коректної передачі документів під час електронного документообігу між системами є актуальним і затребуваним завданням, вирішення якого сприятиме підвищенню ефективності та безпеки сучасного діловодства.

Частою проблемою при міграції документів між різними системами є невідповідність типів документів або ситуація, коли в одній системі існують загальні типи, а в іншій - більш деталізовані.

Наприклад, під час передачі документів з системи "Вчасно" в електронний архів "SharePoint Online" можуть виникати складнощі. У "SharePoint Online" можна налаштувати безліч типів документів, тоді як у "Вчасно" кількість типів є обмеженою. Так, у системі "Вчасно" існує лише один тип "Акт надання послуг", а в "SharePoint Online" - "Акт наданих послуг" та "Акт отриманих послуг". Під час звичайної міграції документів із "Вчасно" з типом "Акт надання послуг" до "SharePoint Online" вони можуть зберігатися з некоректним типом у папках організації.

Вирішенням цієї проблеми є вдосконалення логіки міграції. На момент передачі документа з системи із загальними типами

необхідно реалізувати перевірку організації, до якої передається документ у систему з більш детальною класифікацією типів. Якщо організація є адресантом, то в систему з деталізованими типами документ має передаватися як "Акт наданих послуг". Якщо ж організація є адресатом, то в другій системі має проставлятися тип "Акт отриманих послуг".

Такий підхід дозволить уникнути невідповідності типів документів під час міграції між системами та забезпечить коректне збереження документів у електронному архіві. Це, у свою чергу, сприятиме підвищенню ефективності, надійності та прозорості електронного документообігу.

Підсумовуючи вищенаведене, коректна передача атрибутів документів між різними системами електронного документообігу є ключовим завданням сучасності. Від точності та повноти інформації в електронних документах залежить ефективність взаємодії організацій. Недотримання стандартів передачі реквізитів призводить до помилок, втрати даних і порушень законодавства.

Типовою проблемою є невідповідність типів документів між системами з загальними та деталізованими класифікаціями. Вирішенням є вдосконалення логіки міграції з урахуванням особливостей адресантів та адресатів. Забезпечення коректної передачі документів у електронному документообігу сприятиме підвищенню ефективності, надійності та прозорості діловодства.

ВИКОРИСТАНІ ДЖЕРЕЛА

1.Основна інформація про систему «Вчасно» URL: https://help.vchasno.com.ua/loadingdoc/ (Last accessed: 07.04.2024).

2.Електронний документообіг. URL: https://portfel.ua/shho-take-elektronnij-dokumentoobig/ (Last accessed: 07.04.2024).

3.Система електронного документообігу. URL: https://expresssoft.com.ua/uk/sistemi-elektronnogo-dokumentoobigu-vidi-prikladi-gotovi-rishennja/ (Last accessed: 16.03.2024).

4.Основна інформація про систему «SharePoint Online» URL: https://www.microsoft.com/uk-ua/microsoft-65/sharepoint/collaboration (Last accessed: 06.04.2024).

УДК 004.23

В.І.Воронцов
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ СТАНДАРТУ МОВИ ОПИСУ АПАРАТУРИ VERILOG ПРИ ПРОЕКТУВАННІ RISC ІНСТРУКЦІЙ

В роботі по модифікації сучасного RISC процесора шляхом реалізації нових інструкцій використовується стандарт IEEE Verilog[1]. Він визначає, які інструкції мають гарантований порядок виконання, а які оператори не мають гарантованого порядку виконання. При проектуванні апаратних модулів перед розробником виникає проблема стану гонитви. Стан гонитви виникає, коли два або більше операторів, виконання яких заплановано на одному і тому самому етапі моделювання, дадуть різні результати та у випадку зміни порядку виконання операторів, як це дозволяє стандарт. Відповідно до CWE-1298, стан гонитви в апаратній логіці призводять до виникнення вразливостей у безпеці системи. При розробці апаратних інструкцій важливо забезпечити безпеку виконання апаратних модулів.

Щоб уникнути стану гонитви, важливо розуміти планування блокуючих і неблокуючих присвоєнь Verilog.

Оператором блокуючого присвоєння є знак рівності ‘=’. Призначення блокування отримує свою назву, тому що блокуюче призначення має оцінити аргументи правої частини виразу і завершити призначення без переривання будь-яким іншим оператором Verilog. Кажуть, що присвоєння "блокує" інші призначення, доки поточне присвоєння не буде завершено. Єдиним винятком є присвоєння блокування із затримками часу на виразі з лівого боку оператора блокування.

Виконання блокуючих призначень можна розглядати як одноетапний процес, а саме обчислення рівняння правого боку та оновлення виразу лівої сторони блокування без переривання будь-яким іншим оператором Verilog.

Блокуюче присвоєння обмежує кінцеві присвоєння в тому самому блоці завжди від виконання до завершення поточного присвоєння.

Проблема з блокуванням призначень присвоєння, коли змінна правої сторони одного присвоєння в одному

процедурному блоці також є змінною лівої сторони іншого присвоювання в іншому процедурному блоці, і обидва рівняння заплановано виконувати на тому самому кроці часу моделювання, наприклад, на передньому фронті тактового сигналу. Якщо завдання блокування не впорядковано належним чином, може виникнути стан гонитви. Якщо блокування призначено для виконання на одному і тому самому етапі часу, порядок виконання невідомий.

Для ілюстрації блокуючих присвоєнь можна використати наступний код:

```
module m1 (a1, a2, clk, rst);
output a1, a2;
input clk, rst;
reg  a1, a2;
always @(posedge clk or posedge rst)
if (rst) a1 = 0;
else a1 = a2;
always @(posedge clk or posedge rst)
if (rst) a2 = 1;
else a = a1;
endmodule
```

Відповідно до стандарту IEEE Verilog, два блоки завжди можна запланувати в будь-якому порядку. Якщо перший блок завжди виконується першим після скидання (передній фронт сигналу rst), обидва a1 і a2 набудуть значення 1. Якщо другий блок завжди виконується першим після скидання, обидва блоки a1 і a2 набудуть значення 0. Це чітко ілюструє стан гонитви у Verilog.

Неблокуючий оператор присвоєння такий самий, як оператор менше або дорівнює “<=". Неблокуюче присвоєння отримує свою назву, тому що присвоювання оцінює вираз правої частини неблокуючого оператора на початку часового кроку і планує оновлення лівої частини на кінець часового кроку. Між оцінкою виразу правої частини та оновленням виразу лівої частини можна оцінювати й оновлювати інші оператори Verilog, а також обчислювати вираз правої частини інших неблокуючих присвоєнь Verilog та планувати оновлення лівої частини операторів. Неблокуюче присвоєння не блокує обчислення інших операторів Verilog.

Виконання неблокуючих присвоєнь можна розглядати як двоетапний процес:

1) Обчислення правої частини виразу неблокуючих операторів на початку кроку часу.

2) Оновлення лівої частини виразу неблокуючих операторів наприкінці часового кроку.

Неблокуючі присвоєння виконуються лише для реєстрації типів даних і тому дозволені всередині процедурних блоків, таких як початкові блоки та “always” блоки.

Для ілюстрації неблокуючих присвоєнь можна використати наступний код:

```
module m2 (a1, a2, clk, rst);
output a1, a2;
input clk, rst;
reg  a1, a2;
always @(posedge clk or posedge rst)
if (rst) a1 <= 0;
else a1 <= a2;
always @(posedge clk or posedge rst)
if (rst) a2 <= 1;
else a2 <= a1;
endmodule
```

Відповідно до стандарту IEEE Verilog, два блоки завжди можна запланувати в будь-якому порядку. Незалежно від того, який блок завжди починається першим після скидання, обидва неблокуючі вирази правої частини буде оцінено на початку кроку часу, а потім обидві неблокуючі змінні лівої частини виразу оновлюватися в кінці того ж етапу часу. З точки зору користувачів, виконання цих двох неблокуючих операторів відбуваються паралельно.

Розуміючи нюанси розробки апаратних модулів, розробник може запобігти проблем, викликаних станом гонитви.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. “IEEE Standard Verilog Hardware Description Language," in IEEE Std 1364-2001, vol., no., pp.1-792, 28 Sept. 2001. DOI: 10.1109/IEEESTD.2001.93352.

УДК 621.391

В.П.Гамаюн, д.т.н.
Національний авіаційний університет, Київ

ТЕХНОЛОГІЯ ОБРОБКИ ВЕЛИКИХ МАСИВІВ ДАНИХ

Одним з головних напрямів розвитку високопродуктивних комп'ютерних засобів є розвиток алгоритмів з природним паралелізмом та властивостями розподілу на багато процесорні масиви .

При цьому необхідною умовою є високоточна арифметика та загальна точність представлення даних та робота у великому діапазоні чисел. На практиці алгоритм обробки у паралельному режимі може реалізовуватись для різних діапазонів обчислень з обов'язковим. дотриманням точності. Результат визначається за час , пропорційний кількості діапазонів – в залежності від коефіцієнту паралелізму комп'ютерних засобів. Для таких цілей було запропоноване спеціальне кодування даних числових операндів – розрядно-логарифмічне при якому основні положення розрядно-логарифмічного кодування даних полягають у застосуванні спеціальних кодів для позначення розрядів цифрових операндів , які не є нульовими, тобто значущих розрядів: операнд A = Арл={ N_1 N_2 N_3 N_4 ,,,,,,,,N_Q}.

Кожен код значущого N_i =(a_i p_i $\neq 0$) обчислюється як логарифм від кількості , яка визначається цим розрядом: N_i = $\log_2 a_i p_i$ =i. Таке кодування є однозначним та виконується без функціонального перетворення. Діапазони даних операндів значно в збільшуються : чотири розрядна ЕОМ перетворюється на 32 –х розрядну , 8 розрядна на 511 розрядну ЕОМ та інше.

Такі властивості дозволяють розширити набір алгоритмів розвитку , для паралельних систем нового покоління, а також розв'язувати актуальні завдання наприклад криптографії. Методи розкриття ключів допускають паралельне використання комп'ютерів. Така задача розглядалась у 1977 році як розшифрування на множники -

114381----------(-загалом 129 цифр) ----------79543541.

За допомогою алгоритмів шифрування була представлена фраза, для прочитання якої треба було знайти прості числа . Ця історія закінчилася через рік та результат був наступним

P= 3490---------- ----------820577 та

q = 327691---------- ----------8288533.

Для факторізації була допомога абонентів комп'ютерної мережі . Було організовано часовий суперкомп'ютер з 1600 машин від найпростіших персональних комп'ютерів до станцій Cray C90.

Для розв'язання задачі на кафедрі прикладної інформатики НАУ було запропоновано наступну технологію розв'язання - розділення всього діапазону пошуку на СМ кількість учасників (студентів групи) для кожного діапазону виконувати пошук простих чисел по наступному алгоритму.

На кожному кроці алгоритму перевіряється добуток множників . Робота алгоритму виконується паралельно для кожного діапазону, чим більше засобів, тим менше діапазон та швидше пошук.

Продемонструємо пошук простих множників на прикладі M=119.

Перший крок визначення кореню M = 119 та подальші кроки зведені до наступної таблиці.

Номер кроку	**Значення параметрів**	**Значення параметрів**	**Значення параметрів**
1	M=119		
2 I=0	P1= √M = 10		
	P2= M/(P1-i)=11,9	P2=11,9	P3=[P2]=11
	P2≠ P3		
3	P2= M/(P1-i)=12,3	P2= 12,3	P3=[P2]= 12
I=1	P2≠ P3		
4	P2= M/(P1-i)=14,3	P2=14,3	P3=[P2]=14
I=2	P2≠ P3		
5	P2= M/(P1-i)= 17	P2=17	P3=[P2]=17
I=3	P2= P3 Результат знайдено 7,17		

Таблиця з розрядно-логарифмічним кодуваннням буде наступною

Номер кроку	Значення параметрів 2	Значення параметрів	Значення параметрів
1	M=6.5.4.2.1.0.		
2 I=0	P1= √M = 3.1.		
	P2= M/(P1-i)	P2=3.1.0.-1,	P3=[P2]=3.1.0.
	P2≠ P3		
3	P2= M/(P1-i)	P2= 3.2. -2.	P3=[P2]=3.2.
I=1	P2≠ P3		
4	P2= M/(P1-i)	P2= 3.2.1.-2	P3=[P2]=3.2.1.
I=2	P2≠ P3		
5 I=3	P2= M/(P1-i)	P2= 4.0.	P3=[P2]=4.0.
	P2=P3 Результат знайдено 2.1.0., 4.0.		

При обчисленні простих множників 129 –розрядного числа було виповнено розподілення діапазону на значення кратні 500 - 0,,,,,,500, 501,,,,, 1001, 1002,,,,,1502, 1503…..2003, і т.д. По кожному діапазону було виповнене обчислення за алгоритмом, який розглянуто вище.

Для виконання були задіяні звичайні комп'ютерній засоби – персональні комп'ютери . За час , який не перевищував 40 годин були знайдені правильні результати.

Таким чином технологія реалізується за рахунок:

– високоточної розрядно-логарифмічної арифметики;

– технології розділення всього діапазону обчислень на рівні об'єми;

– паралельну роботу по однаковим алгоритмам ;

– удосконалення загального керування масивом комп'ютерів.

УДК 004.272

[1]**В.В.Гамоля,**
[2, 3]**В.А.Мельник,** д.т.н.,
[4]**А.О.Мельник,** д.т.н.,
[1]ТОВ MacPaw, Львів
[2]Національний університет «Львівська політехніка», Львів
[3]Люблінський католицький університет Яна Павла II, Люблін
[4]IT СТЕП Університет, Львів

ПРОБЛЕМНІ ПИТАННЯ РОЗПОДІЛУ ОБЧИСЛЮВАЛЬНОГО НАВАНТАЖЕННЯ В ГЕТЕРОГЕННИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

У процесі розвитку гетерогенних комп'ютерних систем (ГКС) спостерігається виразний перехід від викликів, пов'язаних із апаратним забезпеченням, до викликів переважно на рівні організації виконання програм. Раніше акцент був зроблений на розробці єдиної архітектури пам'яті та інтеграції різних обчислювальних блоків у кристал. Сучасні виклики включають в себе потребу в оптимізованих програмних моделях, ефективному управлінні ресурсами, портабельності коду на різних платформах та розширених інструментах для відлагодження та профілювання, адаптованих для багатопристроєвих середовищ.

В рамках цього дослідження авторами був проведений детальний аналіз проблемних питань ефективного застосування і покращення технічних характеристик ГКС та ідентифіковано основні виклики їх подальшому розвитку, представлені нижче.

В перших ГКС однією з головних проблем на рівні організації апаратних засобів було *застосування окремих блоків пам'яті* для обчислювальних компонентів, зокрема CPU та GPU - дані для обробки в GPU спочатку повинні були передані з пам'яті CPU до пам'яті GPU, що не лише зумовлювало додаткову затримку, але й ускладнювало розробку програм. Прикладом є Cell Broadband Engine, де кожен елемент SPE має свою локальну пам'ять, ізольовану від прямого доступу від ядра PowerPC або інших SPE. З часом цю проблему було подолано, зокрема, впровадженням концепції уніфікованої віртуальної пам'яті в CUDA 6.0 [1].

Іншою проблемою була *низька пропускна спроможність інтерфейсів*, що сполучають гетерогенні обчислювальні модулі. Проте протягом останнього десятиліття вдосконалення технічних

характеристик шин NVLink та PCIe стало дуже значним.

Ще одною значущою для ГКС проблемою була різноманітність архітектур та необхідність глибоких модифікацій або повного переписання написаного для однієї платформи програмного забезпечення для роботи на іншій. Сьогодні ці проблеми в значній мірі вирішені створенням фреймворків для надання уніфікованої моделі програмування для різного обладнання, серед яких одним з перших став OpenCL, а також стандартизацією різних аспектів гетерогенних обчислень.

Якщо згадані вище виклики сьогодні частково або повністю подолано, питання ефективного автоматичного розподілу обчислювального навантаження (АРОН) залишається відкритим для більшості систем. Серед існуючих реалізацій систем АРОН в ГКС варто відзначити бібліотеку StarPU для розробки програм, які використовують різні архітектури (CPU, GPU, FPGA), без прямої специфікації місця виконання кожного завдання, та фреймворків PaRSEC, HPX і Charm++. Проте існуючі реалізації систем АРОН мають ряд недоліків, які знижують їх ефективність, зокрема:

- недостатня адаптивність до змін у навантаженні або характеристиках системи, наприклад, у швидкості мережі або у розмірі навантаження.
- проблеми зі збереженням консистентності даних, особливо при розподілі завдань між різними архітектурами, що може призвести до втрати даних або невідповідності результатів.
- недостатня ефективність планувальника, що може призводити до неоптимального розподілу завдань та незадовільної використання ресурсів.

Ці недоліки можуть бути вирішені за допомогою покращень у алгоритмах розподілу завдань та розробці більш ефективних планувальників.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. T. Allen, R. Ge. In-depth analyses of unified virtual memory system for GPU accelerated computing. In Proc. of Int. Conf. for High Performance Computing, Networking, Storage and Analysis (SC'21). Article 64, p. 1–15. https://doi.org/10.1145/3458817.3480855

УДК 004.054.15:336.7:004.73.05

І.Г.Гіваргізов, к.е.н.,
М.О.Ковальчук
Поліський національний університет, м. Житомир

КОНЦЕПЦІЇ ПОБУДОВИ ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ LLM У БАНКІВСЬКОМУ СЕРЕДОВИЩІ

У сучасних ринкових умовах банки витрачають багато часу на аналіз та узагальнення інформації під час операційної діяльності, що може негативно вплинути на клієнтський досвід. Регуляторні політики, такі як фінансовий моніторинг та грошово-кредитна політика, спричиняють значне операційне навантаження для банків. За таких умов постає питання в пошуку ефективних інструментів та систем які зможуть зменшити за рахунок автоматизації навантаження на операційну діяльність банків, що в свою чергу дозволить банкам заощаджувати ресурси та приймати виважені управлінські рішення.

Дослідження та пошук підходів в оптимізації діяльності банків присвячена велика кількість праць вітчизняних вчених, зокрема: А. Матвійчука [1], С. Устенка [2], А. Камінського [3], які досліджують підходи у моделюванні фінансово – економічних процесів та аналізують шляхи зменшення фінансово – операційних ризиків використовуючи класичний математичний інструментарій та моделювання за допомогою нечіткої логіки. Серед зарубіжних вчених можна виділити праці О. Вільянса та Л. Квока [4] з запропонованими в них методами побудови моделей розмовного машинного навчання з використанням нейронних мереж.

Large Language Models (LLMs) - це штучні нейронні мережі, які автоматично розуміють і генерують мовний контент, використовуючи великі обсяги текстових даних. Вони виконують завдання, такі як генерація тексту, відповіді на запитання, переклад та аналіз зображень. Найбільш відомі LLM базуються на архітектурі трансформерів, яка дозволяє моделі обробляти всі елементи вхідних даних одночасно, а не

послідовно. LLM навчаються на великому обсязі даних методом навчання без вчителя, що дозволяє їм адаптуватися до мовних закономірностей у тренувальних даних. [5].

Також слід наголосити, що Large Language Models можуть мати різні типи архітектур, які відрізняються за способом обробки вхідних та генерації вихідних даних. Основні їх типи:

– Моделі лише з енкодером приймають послідовності даних та кодують їх у внутрішнє представлення для різних завдань, як BERT.

– Моделі лише з декодером генерують послідовності даних з внутрішнього представлення, відомі також як "sequence-to-sequence" (seq2seq), наприклад, GPT.

– Моделі з енкодером і декодером працюють разом для перетворення та генерації вхідних та вихідних даних, часто використовуються для машинного перекладу або генерації тексту зображень.

Ґрунтуючись на визначених характеристиках LLMs можна запропонувати основні задачі для їх використання в банківському середовищі, а саме:

Аналіз документів клієнта. Мультимодальна обробка даних дозволяє використовувати модель у банківських фронт-системах для ідентифікації та вилучення необхідної інформації з фінансових договорів.

• **Відстеження підозрілих транзакцій.** LLM моделі можуть використовуватися для зменшення фінансових ризиків шляхом звірки контрагентів з санкційними списками та відстеженням підозрілої активності клієнтів.

• **Системи підтримки користувачів та співробітників банку.** Використання великих мовних моделей дозволяє створювати системи підтримки клієнтів та співробітників, що дозволяють отримати необхідну інформацію без тривалого пошуку.

Аналізуючи характеристики та використання LLMs у банківському середовищі, виокремлюються наступні переваги:

• Економія часу та ресурсів: автоматизація завдань звільняє час для стратегічної роботи.

• Підвищення точності: зменшення ризику людського фактору та забезпечення послідовного розуміння інформації.

• Покращення ефективності: оперативний доступ до інформації сприяє у прийнятті кращих та швидших управлінських рішень.

• Підвищення продуктивності: автоматизація завдань та надання необхідної інформації у потрібний час сприяє більшій продуктивності співробітників банків.

Впровадження інструментів та систем, що автоматизують процеси, може значно зменшити операційне навантаження на банки. Саме тому, Large Language Models (LLMs) стають цінним інструментом для банківської сфери: по-перше – це може забезпечити економію часу та ресурсів, оскільки LLMs можуть автоматизувати багато рутинних операційних завдань; по-друге, використання LLMs допоможе підвищити точність обробки інформації та знизити ризик людського фактору; по-третє, це збільшить ефективність роботи банків через оперативний доступ до необхідної інформації.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Matviychuk A. Bankruptcy prediction in transformational economy: discriminant and fuzzy logic approaches [Електронний ресурс] / Andriy Matviychuk // Vol. XIV, No. 2. – 2009. – Режим доступу до ресурсу: https://www.researchgate.net/publication/46529692*

2. *Інформаційні управляючі системи та технології : монографія / За заг. ред. докт. екон. наук, професора Устенко С. В. – Київ : КНЕУ, 2019. – 419 с., [5] с.*

3. *Kaminsky A.B. Credit bureau benchmarking as a tool for estimation of bank's position at the market // Вісник Київського національного університету імені Тараса Шевченка. Серія «Економіка». – 2015. – Випуск 1 (166). – С. 68 – 73.*

4. *Vinyals O. A Neural Conversational Model [Електронний ресурс] / O. Vinyals, V. Quoc // ICML. – 2017. – Режим доступу до ресурсу: https://arxiv.org/pdf/1506.05869.pdf*

5. *Attention Is All You Need [Електронний ресурс] / [A. Vaswani, N. Shazeer, N. Parmar та ін.] // Advances in Neural Information Processing Systems 30. – 2017. – Режим доступу до ресурсу: https://arxiv.org/pdf/1706.03762.pdf*

УДК 004.274:004.056

С.Я.Гільгурт, д.т.н.,
І.А.Жуков, д.т.н.
Національний авіаційний університет, Київ

ПІДХІД ДО РЕАЛІЗАЦІЇ АДАПТИВНИХ МОЖЛИВОСТЕЙ РЕКОНФІГУРОВНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ СИГНАТУРНОГО ТИПУ

У зав'язку з активним розвитком кіберзагроз останнім часом традиційні заходи запобігання зловмисним діям в кіберпросторі вже не впораються з поставленими завданнями. Від підходу, орієнтованого на відомі засоби кібербезпеки фокус уваги дослідників зсувається до поняття кіберстійкості. Кіберстійкість або кіберрезильєнтність – це здатність системи кіберзахисту долати небезпеки, загрози та збої в роботі кіберресурсів всередині організації та її екосистеми для впевненого виконання своєї місії та підтримки бажаного спосіб роботи [1]. Але кіберстійкість – це здатність організації не тільки захищатися від кібератак, але й адаптуватися, відновлюватися та продовжувати роботу в умовах, що постійно змінюються. Отже важливою складовою концепції кіберстійкості є забезпечення адаптивності систем кіберзахисту, підвищення їх гнучкості та зміни функціональних можливостей в залежності від обставин.

Відомо, що високою гнучкістю та розвинутими адаптивними здібностями відрізняються реконфігуровні системи, тобто системи, побудовані на базі програмованих логічних інтегральних схем (ПЛІС), зазвичай типу FPGA. Шляхом завантаження в ПЛІС реконфігурації (програмуючої послідовності бітів – bitstream) всередині програмованої мікросхеми майже миттєво може бути створено (фактично – виготовлено) дуже складний цифровий пристрій довільної структури та довільного призначення, в тому числі – спрямований на виконання задач кіберзахисту критичної інфраструктури. Саме здатність швидко оновлювати внутрішню структуру згідно мінливих вимог надає реконфігуровним пристроям безпрецедентну гнучкість та адаптивність, потенційно збільшуючи можливості підвищення резильєнтності систем, що захищаються. В світі здійснюється багато досліджень щодо створення реконфігуровних засобів захисту інформації [2]. Але аналізу питань та розвитку наукових засад застосування теорії

побудови реконфігуровних систем для ефективного використання їх адаптивних здібностей для підвищення кіберстійкості критичної інформаційної інфраструктури поки приділялося замало уваги.

В даному дослідженні розглядається підхід до реалізації адаптивних можливостей реконфігуровних систем захисту інформації сигнатурного типу на прикладі мережевих систем виявлення вторгнень (МСВВ) [3, 4].

На рис. 1. наведено узагальнену структуру аналізатора (основної складової частини МСВВ), синтезованого всередині ПЛІС. Його ключовим компонентом є модуль розпізнавання (МР), в якому безпосередньо вирішується обчислювально складна задача множинного розпізнавання патернів (multi-pattern matching) [5].

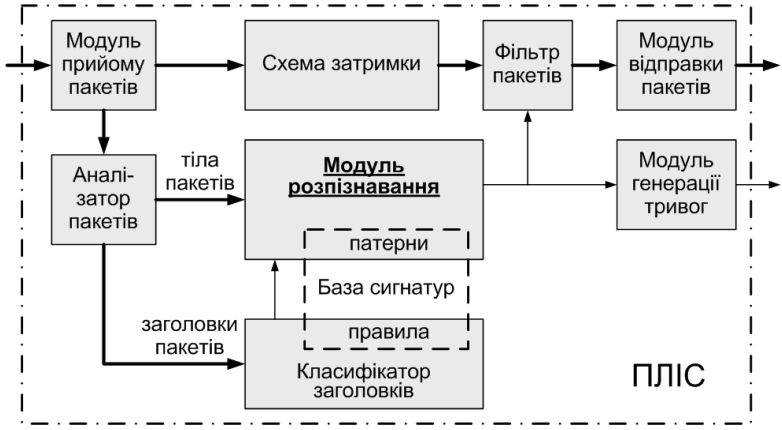


Рис. 1. Узагальнена структура аналізатора МСВВ на базі ПЛІС

Сутність підходу полягає в організації обчислювального процесу під час функціонування реконфігуровної системи таким чином, щоб забезпечити можливість в будь який момент часу здійснити так звану процедуру оперативного оновлення (ПОО). У випадку МСВВ ініціювати ПОО може, наприклад, поява нових класів атак, для протидії яким в склад МР потрібно додати нові апаратні схеми розпізнавання. Виконувати чергову ПОО може змусити й зміна умов роботи інформаційної системи, що захищається (модифікація локальної мережі, оновлення її складу або структури, модифікація програмного забезпечення тощо). Нарешті, здійснення спроби гібридної багатоплановової атаки призводить до необхідності суттєво міняти алгоритми

функціонування всіх компонентів систем захисту об’єкта критичної інфраструктури, але для реконфігуровних підсистем ці зміни зводяться лише до штатного виконання ПОО. До недоліків підходу можна віднести необхідність мати потрібні на подібні випадки конфігурації, заздалегідь створені та перевірені.

У зв'язку з тим, що в процесі оперативного оновлення змінюється лише частка обладнання (яке у випадку МСВВ пов'язане з обробкою сигнатур – МР та класифікатор заголовків), здійснення повного циклу створення цифрової схеми в ПЛІС не потрібно. Більшу частину роботи можна виконати завчасно та уникнути під час проведення ПОО, що прискорює процес синтезу МР та скорочує загальні часові витрати.

Загалом процедура синтезу цифрової схеми для ПЛІС під час виконання ПОО складається з двох етапів (рис. 2): формування обчислювальних структур оновлених компонентів у вигляді тексту на мові опису апаратури, та автоматичної генерації bitstream-файлів – конфігурації для ПЛІС.

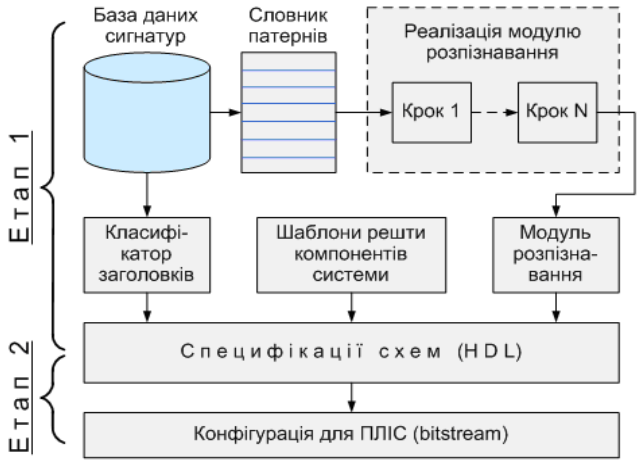


Рис. 2. Етапи автоматизованого синтезу реконфігуровної системи

На першому етапі по змісту бази даних сигнатур генерується опис схеми класифікатора заголовків та формується словник патернів. Процедура реалізації модулю розпізнавання виконується із застосуванням певних методів та засобів і в загальному випадку складається з кількох кроків. До згенерованих блоків змінної складової – класифікатора та МР, додаються схемні заготовки

постійної складової компонентів. На другому етапі отримані описи всіх підсхем мовою опису апаратури (hdl-файли) доповнюється файлами обмежень (ucf-файлами) та іншими складовими проекту створення цифрового пристрою, який виконується із застосуванням пакета САПР для конкретного типу ПЛІС.

Висновки. В результаті дослідження розвинуто теорію реконфігуровних обчислень стосовно використання властивостей гнучкості та адаптивності для підвищення кіберстійкості засобів захисту інформації. Запропоновано та апробовано на прикладі сигнатурних мережевих систем виявлення вторгнень підхід, що базується на виконанні процедур оперативного оновлення.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Худинцев М.М., Хоменко О.А. Методологічні засади індексу кіберрезильєнтності критичної інфраструктури. Резильєнтність критичної інфраструктури — 2023: Матеріали науково-практичної конференції, м. Київ, 21 червня 2023. — К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2023. — С. 52-55.

2. Rouget P., Badrignans B., Benoit P., Torres L., "FPGA Implementation of Pattern Matching for Industrial Control Systems," 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). — 2018. — Vancouver, BC, Canada. — P. 210-213.

3. Жуков И.А., Балакин С.В. Исследование эффективности метода обнаружения вторжений в компьютерные сети на основе искусственных иммунных систем. Проблеми інформатизації та управління: зб.наук.праць. — К.: НАУ, 2017. — № 3(59). — С. 65-69.

4. Hilgurt S. A Concise Review of FPGA-Based Hardware Solutions for Network Intrusion Detection. Proceedings of the 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T'2021). — 2021. — Vol. 36. — IEEE, Kharkiv, Ukraine. — P. 164-168.

5. Smyth B. Computing Patterns in Strings. — 2003. — Essex: Pearson Addison Wesley. — 429 p.

УДК 004.056

Є.А.Гупало
Національна академія Служби безпеки України, Київ

НЕЙРОННІ МЕРЕЖІ У ЗАХИСТІ ІНФОРМАЦІЇ

Сучасний стан розвитку вітчизняних інформаційних систем (ІС), інтегрованих у глобальну мережу Інтернет, характеризується підвищеним рівнем вимог до безпеки інформації, який вже складно забезпечити за допомогою систем захисту, у підсистемах контролю та управління яких використовуються винятково класичні методи оцінювання параметрів безпеки (ПБ).

Штучні нейронні мережі – математичні моделі, а також їх програмні або апаратні реалізації, побудовані за принципом організації й функціонування біологічних нейронних мереж – мереж нервових кліток живого організму. Це поняття виникло при вивченні процесів, що протікають у мозку, і при спробі змоделювати ці процеси. Першою такою спробою були нейронні мережі Мак-Каллока й Піттса. Згодом, після розробки алгоритмів навчання, одержувані моделі стали використовувати у практичних цілях: у завданнях прогнозування, для розпізнавання образів, у завданнях керування та ін.

Принципи роботи нейронних мереж нейролінгвісти та нейрофізіологи, які досліджували ідею про те, що людський мозок – це свого роду комп'ютер, сформували ще у 40-х роках минулого століття. Трохи пізніше американський вчений Френк Розенблатт розробив прабатька сучасних нейромереж – перцептрон, на основі якого було створено перший у світі нейрокомп'ютер. Нейросети використовують для аналізу гігантських масивів даних, прогнозування, зіставлення та класифікації інформації в різних сферах: від економіки до астронавтики. Як приклад ШНМ регулювання може бути представленою розповсюджена комерційна програмна платформа ANFIS (Adaptive Network-based Fuzzy Inference System), яка реалізує нечітку нейронну продукційну мережу. ANFIS входить до складу пакета Fuzzy Logic Toolbox середовища Matlab-Simulink. Дана мережа дозволяє реалізувати нечіткий регулятор динамічних об’єктів із попереднім навчанням і подальшим набуттям властивостей адаптації. При цьому можливі модифікації мережі ANFIS в залежності від застосування алгоритмів нечіткого виведення. Нейромережі, або штучні

нейронні мережі (ШНМ), можуть відігравати важливу роль у захисті інформації з різних точок зору.

Ось деякі способи, які можуть бути використані:

1. Виявлення аномалій: Нейромережі можуть використовуватися для виявлення аномальних патернів або зловмисних дій у мережі. Наприклад, вони можуть аналізувати мережевий трафік для виявлення незвичайних активностей, що може свідчити про кібератаки або порушення безпеки.

2. Виявлення загроз безпеки: ШНМ можуть бути натреновані для розпізнавання відомих патернів в атаках, таких як DDoS атаки, SQL ін'єкції та інші, що дозволяє швидко реагувати на потенційні загрози.

3. Кібербезпека в пристроях IoT: В розумних пристроях і "Internet of Things" (IoT) системах, де захист від кібератак є критичним, нейромережі можуть використовуватися для виявлення аномальних дій або спроб вторгнення.

4. Шифрування та дешифрування: Нейромережі також можуть бути використані для розробки нових методів шифрування та дешифрування даних, що може підвищити безпеку комунікацій.

5. Аутентифікація: Біометричні системи аутентифікації, які використовують нейромережі для розпізнавання облич, відбитків пальців тощо, можуть забезпечити високий рівень захисту від несанкціонованого доступу.

6. Прогнозування загроз: Нейромережі можуть аналізувати великі обсяги даних для виявлення тенденцій і прогнозування можливих кіберзагроз.

Отже, нейромережі можуть бути потужним інструментом у боротьбі з кіберзагрозами та захисті інформації, завдяки своїй здатності аналізувати великі обсяги даних, виявляти аномалії та вдосконалювати методи шифрування та аутентифікації.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Олійник В.В. Комплексний підхід до розв'язання задачі вибору засобів упорядкування середовища у гнучких комп'ютерно-інтегрованих системах // Адаптивні системи автоматичного управління: міжвід. наук.-тех. збірник. — Дніпропетровськ: ДНВП Системні технології. — 2014. - Т.2, №25. — С. 25-32.

УДК 004.056.53

А.Д.Данилов,
Харківський національний університет радіоелектроніки, Харків

ОГЛЯД СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ДАНИХ

Життя сучасної людини нерозривно пов'язане з використання інформаційних технологій. Кілька років тому пересічні користувачі використовували в своєму житті лише прості інструменти та системи, але суспільство та технології розвиваються та потреби користувачів постійно змінюються.

Впровадженням нових інформаційних технологій та систем призводить до необхідності впровадження та удосконалення методів та технологій захисту інформації та персональних даних. Все частіше поширюються випадки незаконного отримання, накопичення, використання, видалення, розповсюдження персональних даних, проведення незаконних фінансових операцій та махінацій у мережі Інтернет. Для забезпечення захисту інформації доцільно використовувати комплексний підхід до захисту даних та інформаційних ресурсів. В роботі розглянуто деякі методи та інструменти захисту даних.

Data Leak Prevention (DLP) − це набір інструментів і процесів, які використовуються для захисту інформаційних ресурсів. Сюди входять функції захисту конфіденційних даних від втрати та запобігання їх використання для вчинення шкідливих дій. Втрата, витік, або порушення цілісності конфіденційних даних може призвести до серйозних наслідків. Програмне забезпечення, що відноситься до класу DLP дозволяє відстежувати та контролювати діяльність кінцевих точок, фільтрувати потоки даних у корпоративних мережах та відстежувати дані в хмарі, з метою захисту інформації у будь-кому стані [1].

Інструменти, що використовуються для моніторингу та фільтрації мережного трафіку, наприклад Брандмауери, що дозволяють забезпечити передачу даних або доступ до них лише авторизованим користувачам

Шифрування даних. Виділяють симетричне, асиметричне та гібридне шифрування. Доступ до файлу можливо отримати лише використовуючи заздалегідь заданий пароль та ключ шифрування. До переваг шифрування можна віднести умовний захист даних навіть у разі викрадення, крім отримання доступу до

інформаційних ресурсів зловмисник також повинен розшифрувати отримані данні, що іноді є занадто складним та знецінює важливість отриманої інформації.

Видалення не потрібних або не актуальних даних. Важливим процесом є знищення застарілих, або непотрібних даних.

Створення систем відмовостійкості в рамках програмного та апаратного забезпечення інформаційної системи організації для забезпечення безпеки у разі надзвичайних ситуацій, або навмисного нанесення системі шкоди.

Для забезпечення збереження та цілісності інформації доцільним є резервне копіювання даних, що дозволяє уникнути, або мінімізувати шкоду у разі збою або стороннього впливу. Для цього формуються плани резервного копіювання.

Для повноцінного захисту організацій важливо запровадити структуру захисту даних, що містить рекомендації щодо захисту всіх робочих процесів.

Розробка ефективної стратегії захисту веб-ресурсів є важливою задачею та повинна включати одночасне здійснення системного, евристичного та статистичного аналізу вразливостей веб-ресурсу, що дозволяє здійснити якісний захист від зловмисників, які використовують декілька типів атак.

Методи незаконного вилучення інформації можуть бути дуже різноманітними і складними, тому потрібно розробляти ефективні методи протидії. Для цього необхідно розуміти потенційні загрози та використовувати відповідні методи захисту даних, щоб забезпечити їх конфіденційність, цілісність та доступність. Також важливо постійно оновлювати методи протидії відповідно до нових загроз та викликів, які постійно змінюються[2].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Запобігання втраті даних. https://octava.ua: веб сайт URL https://octava.ua/zapobigannya-vtrati-danyh (дата звернення: 29.02.2024).

2. Іващенко Д.О., Данилов А.Д. Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VII Міжнар. наук.-практ. конф. (м. Дніпро, 17 бер. 2023 р.). - Дніпро : ДДУВС, 2023. – 558 с.

УДК 004.056.5

К.Дахал,
О.П. Мартинова, к.т.н.,
А.А.Крайносвіт
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

СУЧАСНІ ПІДХОДИ ДО УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЇ: ТЕХНОЛОГІЯ SIEM

Управління безпекою інформації стає надзвичайно актуальною сферою в контексті сучасного цифрового світу, де інформація – це не лише цінний актив, але і основний об'єкт атак та порушень безпеки. Завдяки стрімкому розвитку технологій, особливо систем управління подіями та безпекою інформації (SIEM), організації отримують нові можливості для виявлення, аналізу та реагування на загрози та інциденти безпеки.

Розглянемо дві категорії інструментів кібербезпеки: SIM (управління інформацією про безпеку) та SEM (управління подіями безпеки) [1]. SEM забезпечує моніторинг в реальному часі та управління подіями для підтримки операцій з інформаційною безпекою. SIM забезпечує більше історичного аналізу та звітності для даних про події безпеки. Об’єднавши ці категорії – отримуємо технологію SIEM. Вона надає можливість в реальному часі аналізувати сповіщення безпеки, що генеруються мережевим обладнанням та програмними додатками. Мета: допомогти компаніям реагувати на атаки швидше та впорядковувати величезні обсяги журнальних даних. Можливості продуктів SIEM включають збір, аналіз та відображення інформації з мережевих та безпекових пристроїв; програм для управління ідентифікацією та доступом; інструментів управління вразливостями та виконанням політики; журналів операційної системи, баз даних та додатків; та зовнішніх даних про загрози [2].

Визначною характеристикою технології SIEM є кореляція: таким чином встановлюються взаємозв'язки між записами журналу або подіями, які генеруються пристроями, системами або програмами на основі характеристик, таких як джерело, призначення, протокол або тип події. Однією з основних переваг кореляції є фільтрація дублікатів та зайвих даних для зменшення шуму подій та надання адміністраторам можливості негайно вирішувати проблеми високого пріоритету з правильною інформацією для прийняття обґрунтованих рішень щодо виправлення. Для ефективної роботи SIEM-інструменту

потрібно попереднє впровадження та інтеграція з декількома засобами безпеки: дані звітності від брандмауера, датчика виявлення вторгнень (IDS), служби аутентифікації (AAA, LDAP, AD) та даних сканування на вразливості.

Таким чином, визначимо чотири основні функції SIEM [3]:

1. Централізоване ведення журналів активності на сервері.
2. Кореляція загроз – штучний інтелект, який використовується для аналізу кількох журналів та записів у журналах для ідентифікації зловмисників.
3. Управління інцидентами – процеси від ідентифікації загрози до її утримання та ліквідації.

a. повідомлення – електронна пошта, пейджери, інформація для менеджерів підприємства;

b. створення заявок на вирішення проблем;

4. Ведення звітності відповідей та ліквідації проблеми.

Основною перевагою використання SIEM є здатність зменшувати кількість інцидентів безпеки, які трапляються протягом дня, до керованого та ефективного списку, завдяки автоматизації аналізу. Це дозволяє вчасно виявляти реальні атаки та вторгнення. Хоча традиційний підхід, що базується на людському факторі, може включати десятки висококваліфікованих інженерів з безпеки, які вивчають індивідуальні журнали подій для виявлення загроз, SIEM намагається замінити цей процес автоматизацією, що може призвести до значного зменшення кількості даних про події безпеки та покращення ефективності виявлення інцидентів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. SIEM: A Market Snapshot. Dr.Dobb's Journal. Internet Archive WayBack Machine. – 2007. Доступно за посиланням: [https://web.archive.org/web/20120625003150/http://www.drdobbs.com/197002909]

2. Jamil A.. The difference between SEM, SIM and SIEM. Internet Archive WayBack Machine. – 2010. Доступно за посиланням: [https://web.archive.org/web/20170203010221/http://www.gmdit.com/NewsView.aspx?ID=9IfB2Axzeew=]

3. Swift D.. A Practical Application of SIM/SEM/SIEM Automating Threat Identification. SANS Institute. – 2006 – P. 4 –5.

УДК 519.816(004.056)

Ю.Є.Добришин, к.т.н.
Національна академія Служби безпеки України, Київ

КЛАСИФІКАЦІЯ ТА ОПИС ІНФОРМАЦІЇ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ЩОДО ВИЯВЛЕННЯ, ПОПЕРЕДЖЕННЯ КІБЕРАТАК

Останнім часом серйозна увага приділяється питанням проектування та створення систем підтримки прийняття рішень (далі - СППР), що застосовуються в підрозділах для виявлення, попередження та усунення вторгнень в комп'ютерні системи та мережі. На думку фахівців, поки відсутній формалізований математичний опис багатьох процесів, що відбуваються під час виявлення та застосування сучасних кібератак, способів їх усунення, що заважає здійснювати достовірно процес проектування компонентів та програмних модулів СППР щодо захисту інформації.

Аналізуючи роботи фахівців у галузі захисту інформації [1-2], можна зробити висновок, що проектування СППР щодо захисту інформації, має безліч особливостей, головними з яких є інформація, яка приймає участь у проектуванні та складається з керуючої, вихідний та термінальної.

Керівна інформація I_y регламентує технологічний процес проектування на підставі вимог керівних та методичних матеріалів з проектування. Вихідна I_o складається з нормативної інформації та інформації щодо об’єкту проектування. У свою чергу термінальна інформація I_t є результатом безпосереднього проектування і містить відомості щодо текстових, табличних, графічних матеріалах, які, як правило, зберігається на змінних носіях інформації.

Враховуючи зміст термінальної інформації, представимо її компоненти у вигляді певних складових, об’єднаних між собою

$$I_t = \{I_1 \cup I_2 \cup I_3\} \quad (1)$$

де, I_1 – складові інформації, які раніше використовувалися для розробки СППР та застосовується для проектування без змін;

I_2 – складові інформації, отримані за результатами об’єднання елементів вихідної інформації;

I_3 – складові інформації, отримані за результатами попередньої обробки елементів вихідної інформації.

Процес проектування характеризується у функціональному відношенні як процес якісних та кількісних змін інформації, а у відношенні її структури – як сукупність взаємопов'язаних операцій. На підставі чого функцію (F_p) технологічного проектування СППР щодо захисту інформації, можна формалізувати у вигляді:

$$F_p = J_y \times J_o \rightarrow J_t \quad (2)$$

де термінальна інформація J_t є відображенням вихідної J_o та керівної інформації J_y. Структурні компоненти проектування $\{CK\}$ можна представити у вигляді наступного рівняння $CK = \{B_i\}$, де B_i задача, для якої виконується проектні процедури, наприклад, пошук інформації, попередня обробка інформації, класифікація кібератаки, оцінювання стану загроз, підготовка варіантів рішень щодо усунення кібератак.

Таким чином, проектування включає сукупність проектних процедур, які виконуються для кожної задачі. Функції кожної процедури f_i передбачають перетворення інформації з одного проміжного стану в інший. У свою чергу структура кожної проектної задачі B_i визначається за результатами застосування операції об'єднання графів - функцій процедур, а саме:

$$B_i = f_1 \cup f_2 \cup f_3 \ldots \cup f_n \quad (3)$$

Остаточно структуру технологічного процесу проектування СППР щодо захисту інформації можна описати графом, який представляє об'єднання графів-функцій проектних задач:

$$G(J, Q) = B_1 \cup B_2 \cup B_3 \ldots\ldots \cup B_n \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Азарова А.О., Дьогтєва І.О., Шиян А.А. Система підтримки прийняття рішень щодо підвищення рівня інформаційної безпеки підприємства. Інформаційні технології та комп'ютерна інженерія. 2022. №1. С. 12-18.

2. Яцишин А.В., Попов О.О., Артемчук В.О., Ковач В.О., Зінов'єва І.С. Автоматизовані інформаційні системи підтримки прийняття управлінських рішень у галузі екологічної безпеки. Інформаційні технології і засоби навчання. 2019. №4. С. 286-300.

УДК 004.94:519.85:681.5

Б.І.Долінце
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ОБРОБКИ ІНФОРМАЦІЇ В БАГАТО-СУПУТНИКОВИХ СИСТЕМАХ ПОЗИЦІОНУВАННЯ З ВИКОРИСТАННЯМ LEO-СУПУТНИКІВ

Інтеграція сигналів з різних супутникових сузір'їв у багатошарових системах є одним з найперспективніших напрямків у розробці сучасних систем позиціонування. Як вказано у [1], цей підхід дозволяє компенсувати слабкі сторони окремих сузір'їв, забезпечуючи більш надійне та точне позиціонування.

Система, що інтегрує сигнали з низько-орбітальних (LEO), середньо-орбітальних (MEO) та геостаціонарних (GEO) супутників, створює багатошарову "систему систем" (рис. 1), що оптимізує взаємодію між різними рівнями сигналів для підвищення точності даних про позиціонування. Аналіз збурень у даних супутників, спричинених різними джерелами перешкод, підкреслює значення інтеграції інформації з різних сузір'їв.

Особливість таких рішень полягає у злитті даних від різних сузір'їв для формування оптимізованої оцінки позиціонування об’єкта для досягнення високої точності, зменшуючи вплив індивідуальних недоліків кожної системи, таких як затримка сигналу або обмежене покриття сигналами супутників.

Основні виклики, з якими стикаються розробники систем, включають потребу у створенні гнучких методів адаптивного позиціонування, що можуть швидко реагувати на змінні умови. Розвиток таких систем є особливо актуальним у світлі швидкого розвитку безпілотних технологій та розширення географії їх використання.

Даний підхід побудови адаптивних підсистем позиціонування [2] що дозволяють будувати системи із надзвичайною стійкістю та точністю отримуваної інформації про позиціонування. Велика кількість супутників забезпечує кращу геометрію визначення координат, ніж GPS, і дозволяє використовувати дешевші приймачі отримуючи вищу точність інформації позиціонування.

Вдосконалений метод оцінки похибок у підсистемах прийому та обробки даних передбачає кілька ключових етапів:

- спочатку необхідно ідентифікувати та виміряти похибки

кожної із супутникових систем окремо, тобто e_{GPS}, e_{LEO} та e_{INS}. Це включає в себе збір даних з кожного джерела та оцінку їхньої точності і надійності.

- отримані похибки інтегруються за допомогою функції f, яка враховує не тільки величину окремих похибок, але й їх взаємозв'язок, кореляцію та потенційну компенсацію одна одної.
- через процес оптимізації визначаються вагові коефіцієнти w_{GPS}, w_{LEO} та w_{INS}. Дані коефіцієнти відображають внесок кожної системи в загальну точність моделі та дозволяють балансувати вплив кожної системи на кінцеву похибку e_{LeGNSS}.
- використовуючи отримані вагові коефіцієнти, формується оптимізована сукупна похибка e_{LeGNSS}, яка має мінімізувати підсистема загальну похибку підсистеми для досягнення найкращої можливої моделі точності позиціонування.

Наукове дослідження та застосування багаторівневих інтегрованих систем обробки інформації про позиціонування відкривають нові можливості для забезпечення більшої точності та надійності при застосуваннях в складних умовах експлуатації.

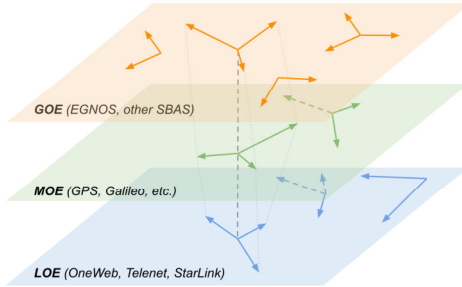


Рис.1. Ілюстрація принципу багатошарової "системи систем".

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Zhukov I., Dolintse B., Balakin S. Improving the Accuracy of Air Navigation Systems for Unmanned Aerial Vehicles. Dependable Systems, Services and Technologies (DESSERT). – 2023. – IEEE Xplore, Athens. – P. 1-7.

2. Dolintse B. Architecture of integrated navigation systems with enhanced coordinate accuracy and fault detection. Problems of Informatization and Management. 2023. Vol. 2(74). – P. 31-37.

УДК 004.056.53

В.А.Дорогань
Національний авіаційний університет, Київ

ВИЯВЛЕННЯ ТА ЗАХИСТ ВІД SQL-ІН'ЄКЦІЙ У ВЕБ-ДОДАТКАХ

SQL-ін'єкція є однією з найбільш поширених та небезпечних вразливостей веб-додатків, яка дозволяє зловмисникам маніпулювати базою даних та отримувати несанкціонований доступ до конфіденційної інформації. Ця проблема привертає серйозну увагу фахівців з кібербезпеки, оскільки більшість веб-додатків взаємодіють з базами даних на основі SQL. Тому важливо розуміти принципи та методи виявлення і протидії таким атакам.

Ручна перевірка є першим кроком у виявленні вразливостей веб-додатків до SQL-ін'єкцій. Вона полягає у ретельному аналізі всіх форм та інтерактивних елементів, де користувачі можуть вводити дані, та введенні спеціальних символів і рядків, які можуть впливати на структуру SQL-запиту. Проведення такої перевірки вимагає уважності та ретельного тестування, оскільки деякі типи SQL-ін'єкцій, такі як "time-based" або "blind", можуть бути складними для виявлення вручну.

Для більш ефективного виявлення SQL-ін'єкцій використовуються автоматизовані сканери вразливостей. Ці інструменти, такі як Acunetix, Burp Suite, Nessus, OpenVAS, SQLMap, OWASP ZAP та Nikto, дозволяють автоматизувати процес пошуку вразливостей та виявляти навіть складні типи атак. Сканери застосовують різні методи, зокрема тестування вводу, тестування виводу, тестування на зміну запиту та тестування на множинне виконання запитів. Кожен сканер має свої переваги та недоліки, тому при їх виборі важливо враховувати функціональні можливості, вартість, швидкість та надійність виявлення вразливостей, а також інтеграцію з іншими інструментами безпеки.

Для захисту веб-додатків від SQL-ін'єкцій необхідно застосовувати комплексний підхід, що включає в себе наступні заходи:

1. Ретельно перевіряти та фільтрувати вхідні дані користувачів, оскільки будь-які дані, що передаються до бази даних, повинні бути належним чином перевірені та очищені від потенційно небезпечних символів.

2. Замість безпосереднього вбудовування даних користувачів у SQL-запити, слід використовувати параметризовані запити, які чітко розділяють дані та код.

3. Застосовувати списки дозволених значень (whitelist) замість списків заборонених (blacklist). Це дозволяє створити більш надійний захист від нових типів атак.

4. Дотримуватися принципу «найменших привілеїв», тобто надавати обліковим записам, що використовуються для підключення до бази даних, лише мінімально необхідні права доступу.

5. Регулярно оновлювати програмне забезпечення та встановлювати найактуальніші оновлення безпеки. Використання застарілих версій може призводити до вразливостей, які можуть бути використані для SQL-ін'єкцій.

6. Застосовувати мережеві екрани веб-застосунків (WAF), які фільтрують шкідливі SQL-запити на основі сигнатур та аналізу поведінки.

Вразливості до SQL-ін'єкцій становлять серйозну загрозу для безпеки веб-додатків, оскільки можуть призвести до несанкціонованого доступу, компрометації та викраденню даних і навіть повної втрати контролю над системою. Для ефективного захисту необхідно поєднувати ручну перевірку, використання автоматизованих сканерів вразливостей та впровадження комплексних заходів безпеки, таких як ретельна перевірка вхідних даних, використання параметризованих запитів, застосування списків дозволених значень та оновлення програмного забезпечення. Лише комплексний підхід дозволить забезпечити надійний захист веб-додатків від цього класу вразливостей.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. K.R.Veerabudren and G. Bekaroo, "Security in Web Applications: A Comparative Analysis of Key SQL Injection Detection Techniques," in 2022 4th International Conference on Emerging Trends in Electrical, Electronic and Communications Engineering (ELECOM), Mauritius, 2022.

УДК 004.738 (043.2)

В.І.Дрововозов, к.т.н.,
С.В.Водоп'янов., к.т.н.,
О.В.Андреєв, к.т.н.,
А.Б.Коцюр
Національний авіаційний університет, Київ

ЕВОЛЮЦІЯ КЛЮЧОВИХ ПАРАМЕТРІВ КОМП'ЮТЕРНИХ МЕРЕЖ ПРИ ПЕРЕХОДІ ДО БЕЗПРОВОДОВИХ РЕЖИМІВ РОБОТИ

Ключовою проблемою у безпроводових інформаційно-комунікаційних мережах є наскрізна якість сервісу (*End-to-End QoS*). В задачах оптимізації безпроводових мереж важливою є розподіл обмеженого числа радіоресурсів між користувачами, у інформаційно-комунікаційних безпроводових мережах має важливе значення в наслідок природних обмежень частотно-енергетичного ресурсу для великого числа користувачів та мультимедійного характеру мережного трафіку. Потрібна якість сервісу *QoS* треба розглядати, тому що вона є комплексною характеристикою, яка включає декілька ключових параметрів. Забезпечення гарантій якості є важливою метою розробки безпроводових мереж [1-3, 8].

У даній роботі розглянуті та надані результати аналізу стосовно даної якості сервісу [1-3, 8] та її власні результати [4, 5, 8]. Однією з ключових проблем у наданні мультимедійних послуг через мобільну безпроводову мережу є підтримка якості обслуговування (QoS) за наявності мінливих мережних з'єднань через мобільність користувачів і спільних, зашумлених, дуже мінливих і обмежених каналів безпроводового зв'язку. Об'єктом дослідження, результати якого представлені у роботі, є процес аналізу енергетичних та інформаційних характеристик безпроводових мереж критичного застосування.

Специфіка безпроводових мереж, зокрема, мереж критичного застосування полягає у наступному.

За результатами аналізу методів організації та забезпечення якості обслуговування в перспективних інформаційно-комунікаційних та комп'ютерних мережах критичного застосування виявлено, що різнорідність мережного трафіку та перевантаження,

які погіршують показники QoS, створюють певні технічні та організаційні проблеми.

Інформаційно-телекомунікаційні системи критичного застосування вміщують автономні мережні сегменти, які є безпроводовими за визначенням. Отримання будь-якої інформації у точці доступу вже здійснюється через безпроводові канали – від мереж *Wi-Fi, WiMAX* до супутникових мереж.

Специфікою безпроводових мереж є розповсюдження сигналів через вільне середовище, тобто принципово відкритий доступ до сигналів як до носіїв інформації, яка передається від одного абонента іншому. Тому, окрім загальних проблем управління інформаційно-телекомунікаційними мережами, у безпроводових мережах досить гостро стоять проблеми захисту від несанкціонованих втручань та зовнішніх завад самого різного походження.

Дана робота присвячена аналізу пропускної спроможності неоднорідних безпроводових мереж при обмеженнях на співвідношення сигнал/(завади плюс шуми). Оскільки пропускна спроможність є невід'ємною складовою загальної продуктивності мережі, проблема, яку тут розглянуто, є вельми актуальною.

Зазвичай розглядають радіо аспект, мережний аспект та інші аспекти безпроводових мереж [6]. Тоді як мережний та інші аспекти, на відміну від радіо аспекту, не мають принципових відмінностей від таких аспектів проводових мереж, розглянемо більш докладно саме радіо аспект.

Об’єм мережі не фіксований: $L_{netw} \le L_{netwmax}|_{q=q_{min}}|$, де $L_{netwmax}$ - максимальна відстань між вузлами мережі, обумовлена мінімальним співвідношенням *SINR* – сигнал/(завади + шуми). Об’єм мережі неперервно змінюється випадковим чином. Зміни залежать від різних (внутрішніх та зовнішніх) чинників. При перевищенні припустимого об’єму мережі система управління мережею намагається негайно повернути мережу до початкового стану. Механізм управління – триплет якості сервісу *QoS*. Для забезпечення норм на *QoS* у відповідності до рекомендацій *Y*.1564-201602-III – паспортизація потоку трафіку – зазвичай використовують наступні параметри (ключовий триплет *QoS*): пропускна спроможність C_{th}; затримка передачі τ_{lt} та її

імовірнісний розподіл $w(\tau_{lt})$; середня кількість бітових помилок у потоці f_{err}.

Дуже важливою характеристикою продуктивності систем зв'язку є відношення сигнал-шум (ОСШ). ОСШ - це відношення енергії сигналу на 1 біт до щільності потужності шумів на 1 герц. Розглянемо сигнал, що містить двійкові цифрові дані, що передаються з певною швидкістю - *R* біт/с. Нагадаємо, що 1 Вт = 1 Дж/с і обчислимо питому енергію одного біта сигналу: $E_b = S \cdot T_b$

(де S - потужність сигналу; T_b - час передачі одного біта).

Врахуємо, що тепловий шум, що є присутнім у смузі шириною 1 Гц, для будь-якого пристрою або провідника, становить

$$N_0 = kT \left(\frac{\text{Вт}}{\text{Гц}}\right), \quad (1)$$

де N_0 – щільність потужності шумів у ватах на 1 Гц смуги; *k* - постійна Больцмана; Т - температура в градусах Кельвіна (абсолютна температура). Отже,

$$\frac{E_b}{N_0} = \frac{\frac{S}{v}}{N_0} = \frac{S}{kTv}. \quad (2)$$

Відношення $\frac{E_b}{N_0}$ має велике практичне значення, оскільки швидкість появи помилкових бітів є функцією даного відношення. При відомому значенні, необхідному для отримання бажаного рівня помилок, можна вибирати інші параметри в наведеному рівнянні. Слід зазначити, що для збереження необхідного значення при підвищенні швидкості передачі даних *R* доведеться збільшувати потужність сигналу, що передається по відношенню до шуму.

Досить часто рівень потужності шуму достатній зміни значення одного з бітів даних. Якщо ж збільшити швидкість передачі вдвічі, біти будуть «упаковані» вдвічі щільніше, і той самий сторонній сигнал призведе до втрати двох бітів інформації. Отже, при постійної потужності сигналу і шуму збільшення швидкості передачі тягне за собою зростання рівня виникнення помилок.

Для розрахунку дальності візьмемо класичну формулу розрахунку дальності зв’язку у вільному просторі [7]:

Потужність сигналу на вході приймача, що знаходиться на дальності r, дорівнює

$$P_{\text{прм}} = \Pi_{\Sigma G} A_{\text{еф}} = \frac{P_{\Sigma} G_{\Sigma} A_{\text{еф}}}{4\pi r^2}. \quad (3)$$

З урахуванням співвідношення $A_{\text{еф}} = \frac{G\lambda^2}{4\pi}$, де λ – довжина хвилі випромінюваного сигналу, можна записати (3) в наступному вигляді:

$$P_{\text{прм}} = \frac{P_{\Sigma} G_{\Sigma} G_{\text{прм}} \lambda^2}{(4\pi r)^2}. \quad (4)$$

Для врахування впливу внутрішніх шумів та зовнішніх завад введемо поняття «еквівалентний рівень шуму на вході приймача». Виразимо його через коефіцієнт шуму $k_{ш}$:

$$k_{ш} = \frac{\frac{P_{\text{прм}}}{k_B T \Delta f}}{\left(\frac{P_{\text{прм}}}{N_{ш}}\right)_0}, \quad (5)$$

де $k_B = k = 1{,}38 \cdot 10^{-23}$ (Вт/Гц) · ° К - постійна Больцмана;

T – абсолютна температура джерела випромінювання, ° К;

Δf – еквівалентна шумова смуга пропускання приймача; $\frac{P_{\text{прм}}}{N_{ш}}$ – відношення потужності сигналу, обчисленої за формулою (4), до потужності шуму, наведеної до входу приймача.

Приймемо $T_0 = 290°K$. Тоді

$$\left(\frac{P_{\text{прм}}}{N_{ш}}\right)_0 k_{ш} = \frac{P_{\text{прм}}}{k_B T \Delta f \cdot k_{ш}}. \quad (6)$$

З рівняння (6) отримаємо

$$N_{ш} = k_B T \Delta f \cdot k_{ш}. \quad (7)$$

Поєднуючи рівняння (4) з рівнянням (7) та вводячи множник втрат L_s для системи зв'язку в цілому, отримаємо рівняння дальності зв'язку у простій та зручній формі:

$$\frac{P_{прм}}{N_ш} = \frac{P_Σ G_Σ G_{прм} \lambda^2}{(4\pi r)^2 k_B T_0 \Delta f \cdot k_ш L_s}. \quad (8)$$

Видно, що відношення сигнал/шум на вході приймача обернено пропорційно квадрату відстані між передавачем і приймачем.

Позначимо S_{OM} (*System Operating Margin*) – запас в енергетиці радіозв'язку (дБ). За допомогою S_{OM} враховуються ключові фактори, що негативно впливають на дальність зв'язку, такі як:

– температурний дрейф чутливості приймача та вихідний потужності передавача;

– різні атмосферні явища: туман, сніг, дощ;

– неузгодженість антени, приймача, передавача з антенно-фідерним трактом.

Цей параметр зазвичай береться рівним 10 дБ [3]. Вважається, що 10-децибельний запас посилення достатній для інженерного розрахунку [7].

У роботі [4, 8] показано, що при збільшенні дальності ймовірність виявлення сигналу з розподілом Парето меншає повільніше, ніж сигналу з нормальним (гаусівським) розподілом. Використовуючи наведені вище формули, можна розраховувати потрібну потужність передавальних пристроїв, число та чутливість приймальних пристроїв, при яких забезпечується необхідна ймовірність доставки повідомлень.

Отримані результати можна використовувати для дослідження залежності ймовірності доставки повідомлення від числа комутаційних вузлів, які приймають повідомлення та пересилають його далі.

Таким чином, можна переконатися, що при переході на передавання даних через безпроводові мережі ключові показники ефективності еволюціонують у напряму залежності від радіотехнічних проблем. Врахування цих проблем – не проста задача, але переваги безпроводових мереж компенсують ці труднощі.

При рішенні задачі забезпечення вимог до якості сервісу (*QoS*) сучасних інформаційно-комунікаційних мереж при функціонуванні у реальному часі необхідно розробляти нові моделі та методи організації безпроводових каналів зв’язку.

У подальших дослідженнях планується розвивати методи управління радіоресурсами з метою оптимізації функціоналу якості сервісу *QoS*.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Khaleel Ahmad, Nur Izura Udzir, Ganesh Chandra Deka (Eds.) Opportunistic Networks Mobility Models, Protocols, Security, And Privacy. Chapman and Hall/CRC; 1st ed., 2019. - 314 p.

2. Anshul Verma, Pradeepika Verma, Sanjay Kumar Dhurandher, Isaac Woungang (Eds.) Opportunistic Networks Fundamentals, Applications and Emerging Trends, CRC Press, 2021 - 330 p.

3. Radio Resource Management White Paper. Cisco Systems, Inc., 2018. – 52 p.

4. Vodopianov S., Martynova O., Krainosvit A. Development of a method of analysis of energy and information characteristics of wireless networks of critical application under conditions of limitations on the signal/(interference plus noise) ratio. Technology Audit and Production Reserves, 2 (1(70)), 2023. P. 26–30. https://doi.org/10.15587/2706-5448.2023.278280

5. Водоп'янов С.В. Алгоритм вибору оптимальної топології комп'ютерної мережі для автоматизованої системи управління повітряним рухом. – К.: НАУ, Проблеми інформатизації та управління, 3(39), 2012. – с. 35 – 38.

6. Huan Chen, Lei Huang, Sunil Kumar, C.-C. Jay Kuo. Radio Resource Management for Multimedia QoS Support in Wireless Networks. - Kluwer Academic Publishers, 2004. (e-version Springer 2012 - 256 pp. DOI: https://doi.org/10.1007/978-1-4615-0469-6

7. Frenzel L. Principles of Electronic Communication Systems. McGraw Hill; 5th Ed., 2022. – 946 p.

8. Дрововозов В.І., Аль-Шаммарі Ахмед Аршед, Журавель Н.В. Підхід до обгрунтування основного методу забезпечення QoS мережі з міжрівневою взаємодією. Комп'ютерні системи та мережні технології (CSNT-2021): XIII міжнар. наук. – прак. конф., 15–17 квітня 2021 р.: тези доп. – К., 2021. – С. 30-31.

УДК 004.8(043.2)

О.В.Дубчак,
Н.К.Гулак, к.т.н.
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ УБЕЗПЕЧЕННЯ КОМУНІКАЦІЙНИХ МЕРЕЖ

Відповідно до статистичних даних Державного центру кіберзахисту ДССЗЗІ України, у 2023 році аналітиками безпеки було зафіксовано та оброблено 1105 кіберінцидентів, що на 62,5% більше, ніж за результатами 2022 року[1]. Прогнозований вплив кіберзлочиності на бізнес у різних галузях у 2025 році може становити 10,5 трл. доларів [2]. Як зазначають фахівці, щорічно зростає кількість кіберінцидентів, пов'язаних із використанням передових технологій, зокрема, штучного інтелекту (ШІ). Водночас зростає і потужність засобів протидії зловмисницькій діяльності – передбачається, що до 2030 року світовий ринок продуктів кібербезпеки на основі ШІ досягне 133,8 млр. доларів [3].

Спеціалісти з кібербезпеки відзначають такі ключові напрямки використання алгоритмів ШІ в галузі кіберзахисту, як: автоматична обробка та аналіз звітів з безпеки; детектування вторгнень у систему; моніторинг і аналіз трафіку; боротьба із хибними спрацюваннями систем виявлення/запобігання вторгнень; прогнозування загроз тощо [4].

Засоби ШІ, слідкуючи за потоками даних у мережах і системах, шляхом проведення аналізу мережевого трафіку, можуть виявляти шкідливу активність, фіксувати спроби несанкціонованих вторгнень, використовуючи, зокрема, метод розпізнавання сигнатур, який передбачає пошук уже відомих алгоритмів [5].

Прикладом ефективного використання технології ШІ є системи виявлення вторгнень (Intrusion Detection Systems, IDS) та системи запобігання вторгненням (Intrusion Prevention Systems, IPS), вбудовані у рішення Cisco Systems. Фактично, технології IDS та IPS можуть доповнювати одна одну, наприклад, IDS - реалізована для перевірки роботи IPS, оскільки IDS можна налаштувати для поглибленої перевірки пакетів в автономному режимі, що дозволяє IPS зосередитись на більш важливих шаблонах трафіку. Реалізація систем можлива шляхом додавання: до маршрутизатора ISR з використанням

модуля розширеної інтеграції IPS (Advanced Integration Module, AIM) або вдосконаленого мережевого модуля (Network Module Enhanced, IPS NME); до пристрою брандмауера ASA (Adaptive Security Appliance) з використанням модуля служб розширеного контролю та запобігання (Advanced Inspection and Prevention Security Services Module, ASA AIP-SSM); до комутатора Catalyst 6500 з використанням модуля системних служб виявлення вторгнень (Intrusion Detection System Services Module, IDSM-2) [6].

Висновки: Засоби ШІ, дозволяючи автоматизувати значну кількість завдань у кібербезпеці, можуть використовуватися для проведення моніторингу та аналізу кіберінцидентів, виявлення поведінкових аномалій та прискорення процесу виявлення загроз, що сприяє зняттю навантаження зі спеціалістів і підвищенню рівня кіберзахисту. Рішення про те, якими засобами користуватися, має ґрунтуватися на цілях організації, визначених політикою безпеки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Державний центр кіберзахисту ДССЗЗІ України. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році [Електронний ресурс] - Режим доступу: https://scpc.gov.ua/uk/articles/334

2. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам [Електронний ресурс] - Режим доступу: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/

3. Штучний інтелект. Статистичні дані, 2023 р. [Електронний ресурс] - Режим доступу: https://uk.blogpascher.com/Ressources/статистика-штучного-інтелекту

4. *Використання ШІ в кібербезпеці: роль та переваги [Електронний ресурс] - Режим доступу: https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi*

5. Вплив ШІ на сферу кібербезпеки[Електронний ресурс] - Режим доступу: https://softico.ua/uk/news/vpliv-shtuchnogo-intelektu-na-sferu-kiberbezpeki/

6. Cisco Networking Academy. CCNA Security [Електронний ресурс] - Режим доступу: https://www.netacad.com/

УДК 004.738.5(043.2)

О.В.Дубчак,
Є.С.Тимофіїв
Національний авіаційний університет, Київ

АНАЛІЗ ЗАСОБІВ ЗАХИСТУ WI-FI РОУТЕРІВ

Кожного року в світі збільшується частка користувачів послугами Інтернет. Зокрема, протягом 2023 р. в Україні кількість споживачів, які щоденно використовують всесвітню мережу, зросла з 72% до 80%, причому за останні три роки цей показник збільшився на понад 10% [1].

Основним обладнанням для виходу до Інтернет є роутер (маршрутизатор), який, з'єднуючи мережеві компоненти та мережі, в основному, виконує три функції: пошук оптимального маршруту; пересилання даних; балансування навантаження. Ефективність мережевої комунікації підвищується за рахунок маршрутизації, що дозволяє керувати трафіком, мінімізуючи мережеві збої [2].

Останнім часом суттєво збільшився попит на бездротові роутери, широко використовувані в домашніх та IoT-мережах. Прогнозований обсяг ринку роутерів у 2024 р. становитиме 15,22 млрд. дол., а до 2029 р. сягне 23,64 млрд. дол. при середньорічному зростанню у 9,2% [3]. Злам такого важливого мережевого обладнання домашніх і корпоративних споживачів може спричинити збитки в десятки й сотні млн. дол., оскільки вразливості роутерів дозволяють зловмисникам, зокрема, виконувати шкідливий код та отримувати доступ до конфіденційних даних [4].

Фахівці пропонують низку кроків, що певною мірою дозволять підвищити рівень убезпеченості роутерів, серед яких: установлення надійного пароля Wi-Fi мережі; захист паролем налаштувань роутера; відключення функції WPS (Wi-Fi Protected Setup); відключення широкомовного SSID (Service Set Identifier); налаштування фільтрації за MAC-адресами; відключення віддаленого керування роутером; налаштування гостьового режиму тощо [5].

Результати проведеного аналізу заходів щодо зниження рівня вразливості роутерів дозволили виокремити проєкт OpenWRT (Open Wireless Router) з відкритим вихідним кодом (Open Source) — вбудовувану операційну систему, засновану

на ядрі Linux, як одне із рішень щодо підвищення надійності та безпеки функціонування мережі. Експерти та фахівці акцентують на таких характеристиках OpenWRT, як: безпека; продуктивність та стабільність; відкритий вихідний код; підтримка спільноти тощо. Розробники отримують зручну платформу для створення додатків, а споживачі – можливість вільного вибору засобів для повного налаштування і використання роутера способами, які не передбачені виробником [6].

Висновок: Пропонується використання OpenWRT як одного із засобів підвищення рівня убезпеченості роутера, оскільки він надає придатну для запису файлову систему з керуванням пакетами, що дозволяє: звільнити користувачів і адміністраторів від необхідності вибору наданих постачальником програм і конфігурацій; налаштувати вбудований пристрій за допомогою пакетів для будь-якої програми. Але слід врахувати необхідність наявності певних фахових знань і навичок для реалізації налаштувань.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Українці стали частіше користуватися інтернетом [Електронний ресурс] - Режим доступу: https://www.undp.org/uk/ukraine/press-releases/ukrayintsi-staly-chastishe-korystuvatysya-internetom-80-onlayn-shchodnya-sotsopytuvannya*
2. *What is the routing [Електронний ресурс] - Режим доступу: https://aws.amazon.com/what-is/routing/*
3. *Wireless Router Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029) [Електронний ресурс] - Режим доступу: https://www.mordorintelligence.com/industry-reports/wireless-router-market*
4. *Вразливості в роутерах ConnectedIO відкрили доступ хакерів до тисяч компаній [Електронний ресурс] - Режим доступу: https://internetua.com/vrazlivosti-v-routerah-connectedio-vidkrili-dostup-hakeriv-do-tisyacs-kompanii*
5. *Maximum protection of your Wi-Fi network and router from other users and hacking [Електронний ресурс] - Режим доступу:https://help-wifi.com/*
6. *Open WRT Project [Електронний ресурс] - Режим доступу: https://openwrt.org/*

УДК 004.738.5(043.2)

О.В.Дубчак,
О.О.Левченко
Національний авіаційний університет, Київ

ПРОБЛЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ КОРИСТУВАЧА ВЕББРАУЗЕРІВ

Послугами всесвітньої мережі для спілкування та виконання рутинних завдань, станом на січень 2024 р., користувалися 5,3 млрд. споживачів, що становить 66% усього світового населення [1].

Функціонування більшості широко використовуваних інтернет – застосунків ґрунтується на складних взаємодіях між різними серверами та клієнтами, на яких має бути встановлене спеціалізоване програмне забезпечення, зокрема, веббраузер (ВБ).

За статистичними даними, станом на лютий 2024 р., частина ринку ВБ у Європі за усіма платформами розподілялася таким чином: Google Chrome (61,15%); Apple Safari (19,1%); Edge (6,6%); Mozilla Firefox (5,14%); Samsung Internet (3,23%); Opera (2, 86%). В Україні, незважаючи на втрату 3% у порівнянні з попереднім періодом, стабільно найпопулярнішим залишається Google Chrome (63,29%); далі - Opera (10,16%), Safari (7,16%) та Firefox - 6,72% [1].

Зазначимо, що критичні вразливості мають майже третина ВБ, зокрема, і популярний в Україні Google Chrome. Зловмисники можуть діяти шляхом атак для отримання або дистанційного керування пристроєм, або доступу до функціонуючої мережі. Крім того, рекламодавці чи інші сторонні компанії можуть збирати через ВБ особисті дані користувача. Найбільший відсоток мають саме ті вразливості, що спрямовані на отримання конфіденційної інформації [2].

За даними проведеного аналізу найпоширеніших уразливостей ВБ виявлено, що технологія вебвідстеження - відбиток ВБ (ВВБ) є підґрунтям загрози порушення конфіденційності даних користувача і, відповідно, багато в чому небезпечніше інших уразливостей ВБ [3].

ВВБ є глобальним ідентифікатором, який робить його власника таким, що найбільш упізнається не тільки на часто

відвідуваних інтернет-ресурсах, а й в інших електронних джерелах. ВВБ збирає значний обсяг інформації та залишається практично незмінним, що дозволяє ідентифікувати користувача майже стовідсотково. У результаті зловмисних дій дані про пристрій можуть використовуватися для застосування експлойтів або «цифрового двійника», що завдає значного збитку споживачеві [4].

Результати проведеного аналізу методів, використовуваних для зменшення унікальності ВВБ, зокрема, Chameleon, User-Agent, Canvasblocker, Canvas Defender дозволили зробити висновок, що найбільшої уваги заслуговує інструментарій спеціалізованих розширень, оскільки це рішення надає: різноманітність вибору та можливість застосування до будь-якого ВБ; зручний і зрозумілий в більшості випадків інтерфейс; можливість налаштувань захисту від ВВБ за власним розсудом; відсутність потреби щодо налаштувань безпосередньо ВБ. Але жодне з них не надає комплексного захисту [5].

Отже, як одне з можливих вирішень проблеми захисту конфіденційності користувача ВБ, пропонується удосконалення інструментарію розширення за рахунок: перехоплення інформації, що збирається на стороні клієнта; подальшої зміни зібраних даних таким чином, щоб мінімізувати їхню унікальність; надсилання вже опрацьованих даних серверу для формування відбитка ВБ.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Statistical report StatCounter [Електронний ресурс] - Режим доступу: https://gs.statcounter.com/browser-market-share/desktop-tablet-console/worldwide

2. Top 10 actual vulnerabilities from OWASP[Електронний ресурс] - Режим доступу: https://qagroup.com.ua/publications/tpo-10-vulnerability-owasp/

3. Дубчак О.В. Аналіз уразливостей веббраузера / О.В. Дубчак, О.О. Левченко, І.А. Кравчук// CSNT-2023: XIV міжнародна науково-практична конференція,13-14 квітня 2023:тези доп. - К., 2023.- С.84-85.

4. What is browser fingerprinting and how does it work? [Електронний ресурс] - Режим доступу: https:// multilogin.com/blog/what-is-browser-fingerprinting-and-how-does-it-work

5. *Дубчак О.В. Засоби протидії вебвідстеженню / О.В. Дубчак, О.О. Левченко, Я.С. Мазур // CSNT-2023: XIV міжнародна науково-практична конференція, 13-14 квітня 2023:тези доп. - К., 2023 .- С.86-87.*

УДК 004.5

Т.С.Дьячук
Національний університет «Запорізька політехніка», Запоріжжя

АВТОМАТИЗОВАНА ПЕРЕВІРКА ЗАВДАНЬ ПРИ НАВЧАННІ ПРОГРАМУВАННЮ

Автоматизована перевірка завдань при навчанні програмуванню дозволяє ефективно контролювати виконання завдань студентами, автоматично перевіряти правильність коду, виявляти помилки та надавати зворотний зв'язок без необхідності ручної перевірки кожного завдання. Такий підхід дозволяє економити час викладачів та студентів, сприяє швидшому виявленню та виправленню помилок, а також забезпечує більш об'єктивну оцінку робіт студентів.

На рис.1 наведена архітектура автоматизованої перевірки завдань, яка була розроблена та апробована у рамках дисципліни «Основи програмування на Kotlin» (базовий репозиторій для навчання доступний за посиланням [1]). Вона базується на можливостях GitHub, таких як Pull requests (PR) та GitHub Actions. Git та GitHub є дуже потужними інструментами для контролю версій та спільної роботи над проєктами. Автоматизована перевірка є частиною більш складної системи для дистанційної освіти, тому завдання, які надаються студентам також генеруються автоматично, придатні для подальшої автоматизованої перевірки та мають чітко визначену специфікацію.

Розглянемо більш детально принцип роботи автоматизованої перевірки. Після виконання завдання для кожної нової функції або задачі, студенти створюють PR, щоб викладач міг переглянути та залишити коментар. А GitHub Actions дозволяє використовувати засоби автоматичного тестування після змін у коді, що забезпечує моментальну відповідь студенту. При автоматичному тестуванні валідатор генерує набори вхідних даних, наприклад 100 значень, проходить цей набір і кожне значення віддає на блок виконання завдання та програмний код студента, потім порівнює результати. Якщо вони не співпадають, то вважається, що студент припустив помилку. Але завжди є можливість студенту звернутись до викладача. Викладач в свою чергу має результати автоматичної перевірки, не витрачає зайвого часу на рутинну роботу та може переглянути код та залишити свої зауваження, додаткові коментарі

та поради з удосконалення коду.

Таким чином автоматичне тестування допомагає впоратися з первинною перевіркою великої кількості типових завдань та заощадити час викладача. А оволодіння сучасними засобами розробки допомагає студентам вирішувати складні завдання та стати конкурентоспроможними на ринку праці у майбутньому, студенти опановують нові технології та здобувають навички спільної роботи над великими програмними продуктами. В подальшому планується створити додаткові тести для перевірки якості коду (такі як відповідність стандартам коду, якість коментарів тощо).

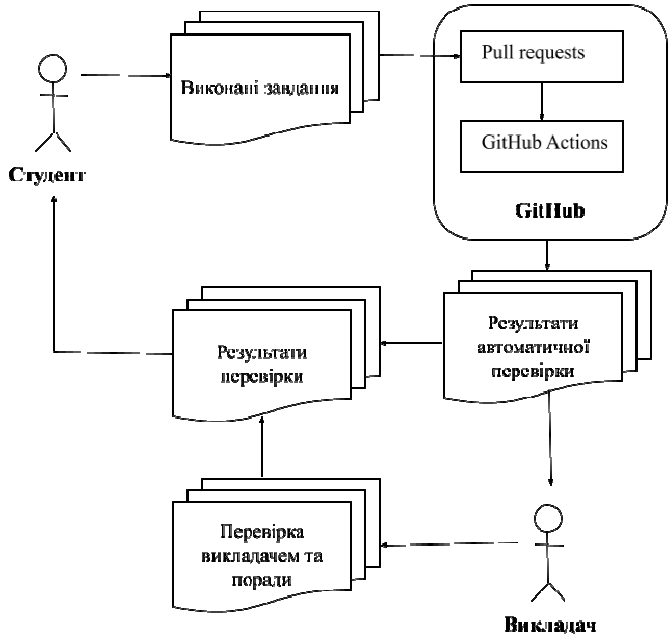


Рис.1. Архітектура автоматизованої перевірки завдань.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. DiachT/KotlinLabsNUZP – Репозиторій з кодом. URL: https://github.com/DiachT/KotlinLabsNUZP (date of access: 10.04.2024).

УДК 351/354

В.В.Дяк
Національна академія СБ України, Київ

ЩОДО ПИТАННЯ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Нині розвиток державного регулювання протидії кіберзлочинності в Україні перебуває на активному етапі формування. У багатьох країнах ця система працює давно і дала позитивні результати, хоча кіберзлочинність все ще випереджає рівень розвитку інструментів протидії їй. Тому, аналізуючи сучасні українські реалії, є можливість наголосити на незавершеності цього процесу на сьогодні і необхідності подальших трансформацій.

До стратегічних цілей кібербезпеки відносяться захист кіберпростору України, її суверенітету, обороноздатності, політичної та соціальної систем, територіальної цілісності, а також прав та законних інтересів громадян [1].

В умовах збільшення розвідувальної активності організацій щодо органів державної та виконавчої влади, оборонних, промислових, сировинних підприємств, медичних, страхових та туристичних компаній України, надання психологічного впливу, у тому числі з елементами нейролінгвістичного програмування з використанням ІТ технологій, етнічних, релігійних особливостей, масова свідомість для дестабілізації політичної ситуації, забезпечення релевантної системи захисту виглядає вкрай необхідним.

Кібербезпека є необхідною умовою розвитку інформаційного суспільства. Її можна було б визначити як сукупність стратегій та дій, які мають бути вжиті для захисту з'єднаних мереж (включаючи апаратні та програмні засоби, збережену та передану інформацію) від несанкціонованого доступу та зміни, крадіжки, руйнування та інших зловмисних дій при гарантії безперервної якості безпеки, незважаючи на характер і природу загроз, що змінюються. Забезпечуючи кібербезпеку, необхідно зберігати доступність, цілісність та конфіденційність середовища для авторизованих користувачів [2].

У контексті захисту можна виділити три рівні захищеності: низьку, середню і високу. Диференціація за ними визначається використанням сучасних захисних ІТ технологій, апаратних

комплексів та програмного забезпечення, що дозволяють купірувати та усувати організовані кримінальні атаки, у тому числі із застосуванням модифікованих шкідливих програм, комп'ютерних вірусів, а також запобігати, своєчасно реагувати та усувати кіберзагрози та виклики.

Займаючи лідируючі позиції, держава та приватні корпорації зможуть підвищити попит на експорт українського продукту у цифровій сфері. Також удосконалення технологій допоможе поширити український вплив та авторитет серед світової спільноти шляхом імплементації інформаційних технологій у «м'яку силу» держави. Крім цього, є можливість збільшити «жорстку силу» країни через створення нової кіберзброї чи кібервійськ. Ця перспектива також може сприяти економічному зростанню, оскільки зброю можна експортувати до країн-партнерів України. Заключною можливістю для України є стрибок у четверту промислову революцію. В України є перевага перед розвиненими країнами, яка найчастіше розглядається як головний недолік: її не гальмує сегмент, зайнятий у промисловій сфері та не готовність до переходу до цифровізації, оскільки всі активи зосереджені у своїй галузі.

Найефективнішим рішенням щодо вдосконалення кібербезпеки є державне заохочення ініціатив у кібербезпеці. Це може бути як економічна підтримка, так і політичний захист. Держава повинна сама визначити інструменти такого стимулювання ініціатив, ідей та винаходів.

Наступні три пропозиції компенсують одна одну і для більшої ефективності мають бути запроваджені разом. Скорочення військових витрат на розвиток кібербезпеки покликане перенаправити кошти на розвиток переваги в новій галузі безпеки. Водночас, ці кошти можуть компенсувати збитки держави від створення пільгових умов для цифрових корпорацій та їх співробітників. Більше того, просування українських стандартів на міжнародний ринок дозволить надати міжнародного характеру вжитим у країні заходів.

Менш ефективними, отже, і менш підходящими нині для України виступають кроки по взаємодії держав до створення міжнародних правил і структурування державної нормативно-правової бази. Незважаючи на те, що концентрація на внутрішніх проблемах кібербезпеки отримала найменшу оцінку ефективності,

цей факт має логічне пояснення. Запропоновані заходи акцентуються на внутрішній політиці держави та змінам усередині країни. В українській реальності це можливо лише за перерозподілу ресурсів із зовнішньої політики на внутрішню.

Більшість державних структур, задіяних у процесі управління, повинні сформулювати свої програми дій, що забезпечують протистояння інформаційним диверсіям та шпигунству.

Так, Міністерству надзвичайних ситуацій України доцільно виявити галузі інформаційної діяльності, схильні до найбільшого ризику шкідливого впливу ззовні. До них можна віднести: формування управлінських баз даних, планування операцій та контроль за здійсненням реальних аварійно-рятувальних технологій, планування заходів цивільної оборони, інформаційну взаємодію з населенням, реалізація міжнародних гуманітарних акцій у «гарячих точках» тощо.

У цих областях мають бути розроблені програмні продукти, насамперед моніторингового характеру, а також такі, що дозволяють виявити негативні інформаційні «вкидання», що локалізують інформацію про їх джерело і дають можливість своєчасного блокування за потреби.

На сучасному етапі найбільше себе проявили загрози, що мають характер організованої злочинності, проте найбільша небезпека, що відзначається світовою експертною спільнотою, походить від останньої з перерахованих категорій загроз, від активізації інформаційної агресії, що проводиться державами. Подібна небезпека принципово нового характеру мала б сприяти побудові конструктивного міжнародного діалогу, однак, прагнення частини держав зайняти домінуючі позиції в кіберпросторі, ґрунтуючись на принципах розглянутої вище політики, що передбачає вжиття подібних заходів як єдино можливого гаранта національної безпеки, були дуже неоднозначно сприйняті, що змусило багато держав перейти на національний шлях побудови кібербезпеки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Якщо уявити кіберзлочинність як країну це була б третя економіка світу – https://10guards.com/ua/articles/cybercrime-as-empire-would-be-the-worlds-third-largest-economy/.

2. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д.В. Дубов. – К. : НІСД, 2014. 328 с.

УДК 004.492.2 (043.2)

М.С.Жижкін,
М.В.Куклінський, к.т.н.
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА НАДІЙНОСТІ ОБМІНУ ДАНИМИ

На сьогоднішній день безпека веб-сайтів, додатків та інших онлайн ресурсів стала однією з найважливіших проблем, яка турбує як державні установи, так і громадянське суспільство. Щорічно з'являються нові загрози в Інтернеті, і для їх запобігання постійно розробляються нові методи захисту. Такий підхід вимагає постійного удосконалення, гнучкості та творчого підходу. Тому наразі актуальною є розробка нових моделей та програм для ефективної протидії зловмисникам.

Одним з можливих варіантів такої моделі може бути модель блокчейн. Логіка цієї системи полягає в постійному обміні пакетами даних та ключами шифрування між всіма учасниками. Це дозволяє зробити процес обміну швидким, анонімним та безпечним у порівнянні з іншими системами захисту.

Блокчейн є децентралізованою системою, що означає, що дані зберігаються на різних комп'ютерах, що робить їх важкими до зміни або втрати. Ця технологія забезпечує прозорість, оскільки всі операції зберігаються у вигляді блоків даних, які можуть бути переглянуті всіма учасниками мережі.

На сьогодні блокчейн використовується для фінансових операцій в Інтернеті, де він є безаналоговим. У той час як веб-ресурси частіше використовують статичні системи захисту, такі як хостинг або резервний сервер.

Проте, завдяки своїм можливостям блокчейн може бути використаний не лише для фінансових операцій, а й для забезпечення цілісності даних у сферах, де важлива безпека та надійність.

Модель блокчейну дасть змогу створити нову систему захисту веб-ресурсів, яка дозволить використати її принцип обміну інформацією між серверами. Цей механізм зможе забезпечити надійний захист від DDOS атак, оскільки вони спрямовані на сервера, де розміщуються файли. Якщо

місцезнаходження файлів буде заховане від зловмисника, час відновлення після атаки скоротиться, порівняно з традиційним відновленням веб-сайту. Це унікальне рішення дозволить зменшити витрати на відновлення даних, у порівнянні з орендою резервного сервера [1], який наразі є основною альтернативою для захисту від DDOS атак.

У зв'язку з цим, стає можливим розроблення системи, що включатиме у себе логічно пов’язану мережу серверів. При розміщені у різних частинах планети вони будуть синхронізуватися в реальному часі.

Основним аспектом також буде те, що розташування серверів, їх кількість та можливості будуть відомі лише власнику веб-ресурсу, а порядок їх виконання вирішуватиметься рандомайзером, який буде подібним до системи блокчейн.

Іншими словами, коли DDOS атака починається в одному місці, сервер автоматично вмикається в іншому з завантаженням останньої версії сайту з резервного копіювання на резервних серверах, які також вибираються випадковим чином. Так як ці процеси автоматизовані, доменне ім'я без змін зможе мігрувати на дзеркальне ім'я або переспрямовувати трафік на перевірку через додаток Cloudflare [2].

Висновок. Веб-додатки та веб-сайти потребують удосконалення систем захисту, які мають успішно відбивати кібератаки зловмисників. Тому важливо займатися розробкою нових моделей систем захисту, а також вдосконалювати вже наявні, використовуючи результати флагманських систем з подібних сфер діяльності. Блокчейн система гарно зарекомендувала себе як для роботи з анонімними фінансовими транзакціями, так і в захисті даних веб-ресурсів.

ВИКОРИСТАНІ ДЖЕРЕЛА:

1. Протокол DHCP [Електронний ресурс]. URL: https://learn.microsoft.com/windows-server/networking/ technologies/dhcp/dhcp-top (Last accessed: 21.03.2024).

2. *Система захисту Cloudfare [Електронний ресурс]. URL: https://developers.cloudflare.com/dns/?_gl=1*1iod0uk*_ga*NTEw OTc0NzgzLjE3MTA5NDk0MDA.*_ga_SQCRB0TXZW*MTcxMDk0 OTQwMC4xLjEuMTcxMDk0OTQ4MS4wLjAuMA (Last accessed:* 21.03.2024)

УДК 004.056

А.В.Закружний
Національна академія Служби безпеки України, Київ

ПРОГРАМНІ СЕРВІСИ МОНІТОРИНГУ ТРАФІКУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

У сучасному світі комп'ютерні мережі відіграють важливу роль у забезпеченні зв'язку та обміну даними між користувачами та різними пристроями. Однак контроль та моніторинг трафіку в комп'ютерних мережах є ключовими завданнями для забезпечення їхньої ефективності та безпеки. Програмні сервіси моніторингу трафіку відіграють важливу роль у забезпеченні цих завдань.

Сьогодні на ринку існує багато програмних рішень для моніторингу трафіку в комп'ютерних мережах. Ці рішення надають можливість збору, аналізу та візуалізації даних про трафік у реальному часі, що дозволяє адміністраторам мережевих систем ефективно контролювати та управляти мережею.

Ми розглянемо деякі з найпопулярніших програмних засобів моніторингу мережі та їхнє практичне використання в контексті виявлення проблем та підвищення загальної надійності мережі.

Wireshark – це інструмент, який забезпечує можливість захоплення та аналізу пакетів даних, що передаються по комп'ютерній мережі. Він використовується для виявлення проблем з'єднання та аналізу безпеки мережі, дозволяючи адміністраторам мережі отримувати детальну інформацію про трафік, що проходить через мережеві пристрої [1]. PRTG Network Monitor - ця програма призначена для моніторингу мережевих пристроїв та збору статистики використання мережевих ресурсів. Вона дозволяє виявляти проблеми у роботі мережі та вчасно реагувати на них, що допомагає забезпечити неперервну роботу мережі та уникнути виникнення серйозних проблем [2]. Nagios - цей програмний продукт використовується для моніторингу систем та мережевих пристроїв. Він надає можливість встановлення різних правил моніторингу та відслідковування стану мережі, що допомагає виявляти та вирішувати проблеми в роботі мережі з метою забезпечення її ефективної та надійної роботи.

Програмні сервіси моніторингу трафіку відіграють критичну роль у забезпеченні безпеки мережі. Вони дозволяють виявляти потенційні загрози та атаки, спостерігаючи за незвичайними

патернами трафіку, надсилаючи аларми та сповіщення про потенційні проблеми. Програмні сервіси моніторингу трафіку надають детальну статистику використання мережевих ресурсів, що дозволяє виявляти проблемні ділянки мережі та оптимізувати їх роботу. Це дозволяє забезпечити ефективне використання ресурсів та уникнути перевантажень.

Програмні сервіси моніторингу трафіку дозволяють контролювати та розподіляти пропускну здатність мережі для оптимального використання ресурсів. Шляхом аналізу використання ресурсів мережі, вони допомагають управляти пропускною здатністю для забезпечення оптимальної продуктивності.

Проте, при використанні програмних сервісів моніторингу трафіку виникають збір та аналіз великих обсягів даних про трафік може спричиняти велике навантаження на систему. Встановлення оптимального рівня деталізації аналізу трафіку, що дозволить ефективно виявляти проблеми, але не завдасть зайвого навантаження на систему.

Під час аналізу трафіку важливо забезпечити конфіденційність особистих даних користувачів та конфіденційність корпоративної інформації.

Програмні сервіси моніторингу трафіку в комп'ютерних мережах відіграють рішучу роль у забезпеченні безпеки, ефективності та оптимізації мережевих інфраструктур. Їхнє практичне використання дозволяє адміністраторам мережевих систем ефективно контролювати, управляти та оптимізувати роботу мережі, що є критичним у сучасному інформаційному суспільстві. Однак, для успішного впровадження програмних сервісів моніторингу трафіку важливо вирішувати проблеми, пов'язані з обробкою великих обсягів даних, забезпеченням конфіденційності та знаходженням балансу між деталізацією та продуктивністю.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *https://uniteddc.net.ua/news/i/net-monitoring/*
2. *https://www.softinventive.com.ua/best-network-monitoring-tools*

УДК 629.7.014.16

[1]**А.Л.Зірка,** к.т.н.,
[1]**М.В.Зірка,** к.т.н.,
[2]**Н.П.Кадет**
[1]*Центральний науково-дослідний інституту озброєння та військової техніки Збройних Сил України, Київ*
[2]*Національний авіаційний університет, Київ*

ТЕОРЕТИЧНІ ОСНОВИ СТРУКТУРНОГО СИНТЕЗУ ЛІНІЙНИХ ТА НЕЛІНІЙНИХ МАТЕМАТИЧНИХ МОДЕЛЕЙ АЕРОДИНАМІКИ В ЗАДАЧАХ ОЦІНКИ АЕРОДИНАМІЧНИХ ХАРАКТЕРИСТИК БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Забезпечення високого ступеню гарантії успіху програми створення сучасного безпілотного авіаційного комплексу (БпАК), особливо класів II та III в умовах часового та ресурсного обмежень, потребує більш високого ступеню точності прогнозування характеристик БпАК при його проєктуванні. При цьому в сучасних умовах більш широкого використання ініціативних розробок приватних виробників знижується роль науково-дослідних та дослідно-конструкторських робіт. За таких умов збільшується роль прикладних методів аналізу та прийняття проєктних рішень на базі математичних моделей, що адекватно відтворюють характер та закономірності об'єктів та процесів, що досліджуються, також збільшується роль напівнатурних та натурних експериментів на можливо-ранніх етапах розробки проєкту. Одним зі складних та відповідальних етапів реалізації ТТХ майбутнього зразка БпЛА вважається етап визначення його аеродинамічного компонування [1], яке безпосередньо пов'язане з аеродинамічними характеристиками (АХ) зразка.

АХ, у першій ітерації визначаються завдяки параметричним дослідженням при попередньому проєктуванні (етап синтезу обрису перспективного БпЛА), та є попередніми вихідними даними для подальшого ескізно-технічного проектування.

Необхідність високої точності при таких дослідженнях пояснюється необхідністю прийняття до 80% концептуальних рішень на зазначених стадіях проекту (до початку робочого проєктування) , і допущені тут помилки, а також різного роду

неточності пов'язані зі значними ризиками додаткових часових та матеріальних витрат на їх усунення при виконанні наступних етапів або взагалі не досягнення поставленої мети розробки [1].

У доповіді пропонується до розгляду комплексний підхід щодо обґрунтування основних АХ перспективного БпЛА на основі розробленого науково-методичного апарата (НМА), що на етапі теоретичних досліджень являє собою синтез різноманітних методів та методик визначення АХ зразка. З метою оцінки достовірності розрахункових значень АХ пропонований НМА на послідуючому етапі досліджень передбачає їх експериментальні підтвердження а уточнення шляхом застосування метода літаючої моделі. Передбачається, що такий підхід забезпечить отримання значень АХ БпЛА з приємною для прийняття проектних та технічних рішень точністю. У практиці проектних досліджень частіше за інші вирішуються завдання визначення льотно-технічних характеристик (ЛТХ) літальних апаратів (ЛА) при наявності попереднього обрису планеру ЛА та силової установки. Результати вирішення зазначених задач співвідносяться із тактико-технічними вимогами (ТТВ) до ЛА за його ЛТХ, та з врахуванням значення оцінювального критерію робиться висновок про задовільність або незадовільність проектних параметрів, а також про можливі шляхи їх покращення [1].

Таким чином, мова йде про ітераційний процес, ускладнений тим, що параметричний аналіз та розрахунки проводяться у момент, коли процес проектування ще не замкнений прийняттям, будь якого з проектно-конструкторських рішень.

Для аналізу впливу проектних параметрів на ЛТХ БпЛА перш за все проводяться параметричні розрахунки його технічних характеристик. До основних технічних характеристик проекту БпЛА на рівні технічних пропозицій входять наступні:

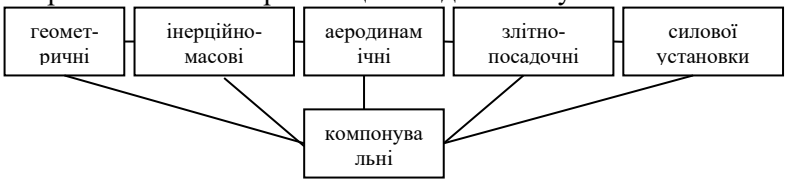


Рис. 1. Основні технічні характеристики проекту БпЛА на рівні технічних пропозицій

У подальшому зосереджено увагу на АХ, що не можуть бути прийнятими за постійні, адже серед перелічених, вони у меншій мірі визначаються при обґрунтуванні ТТВ.

Під АХ слід розуміти, перш за все, поляру ЛА на крейсерському та злітно-посадочному режимах польоту C_x (C_y, H, V) та відповідні цим режимам значення $C_{y\max}$, де наведені коефіцієнти це коефіцієнти лобового опору, підіймальної сили та максимальної підіймальної сили, а також висота та швидкість польоту.

На основі аналізу відомих підходів для розрахунку основних АХ запропонований до використання в НМА для чисельної реалізації лінійних моделей аеродинаміки МДВ, що досить широко використовується в задачах розрахунку АХ. Для розрахунків АХ, запропоновано використовувати інженерні методики, створені на основі експериментальних даних у лінійному діапазоні зміни кінематичних параметрів, а для врахування впливу гвинта на АХ БпЛА вихрову математичну модель повітряного гвинта та теоретичні положення теорії ідеального гвинта.

З метою підтвердження достовірності попередньої оцінки АХ, НМА пропонується використання метода літаючої моделі ЛА з електричним двигуном, що є альтернативним засобом дуже коштовним та менш інформативним продувкам моделі в аеродинамічній трубі. Розроблена в роботі методика інтегрована у загальний запропонований НМА, що реалізований у вигляді алгоритму послідовних наближень для отримання потрібної інформації.

Запропонований НМА дозволить оперативно вирішувати завдання з отримання АХ БпЛА, оптимізації його аеродинамічного компонування та оцінці динаміки на попередніх етапах проектування.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Проектирование самолетов / С.М. Егер, В.Ф. Мишин, Н.К. Лисейцев и др.; под ред. С.М. Егера // М.: Машиностроение, 1983. – 616 с.2

2. БПЛА. Обоснование и расчет основных параметров и характеристик. под редакцией В.И. Силкова. – К.:ЦНИИ ВВТ ВС Украины, 2016. – 268 с.

3. Сілков В.І. Літаюча модель замість аеродинамічної труби // ОВТ. – 2020. – № 4 (28). – С. 66 – 74.

УДК 004.0560523:342.8:091.5(043.2)

О.М.Зудов, к.т.н.,
В.В.Горіна,
Н.О.Рибасова
Національний авіаційний університет, Київ

ПРОТОКОЛИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ КРИПТОГРАФІЧНОЇ СХЕМИ "СЛІПОГО ПІДПИСУ" І БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Електронне голосування (E-voting) стає ключовим елементом демократії. Нещодавня пандемія кинула новий виклик в цій області, хоча інтерес до проблеми існує давно. Основи принципів електронного голосування було закладено ще наприкінці двадцятого століття, разом із розвитком сучасних основ криптографії. Відомі науковці, що заклали основи сучасних криптографічних систем, такі як Аді Шаимір, Девід Чаум, Брюс Шнайєр та інші приділяли увагу і цьому важливому застосунку криптографії [1].

Актуальність електронного голосування виросла, зокрема через потребу в безконтактних методах голосування та підвищення ефективності виборчих процесів. І якщо електронна комерція, банкінг та інші подібні технології швидко стали популярними, а надійність їх викликає довіру споживачів, саме завдяки криптографічним методам захисту інформації, то електронне голосування все ще знаходиться на стадії дослідження, розробок, удосконалень і модифікацій алгоритмів і протоколів, а рівень довіри серед громадськості, політиків і фахівців суспільних наук не дуже високий. Причиною є суперечливість вимог до процесу голосування, який повинен одночасно бути прозорим і анонімним.

Зазвичай, авторами пропонується використання технології сліпого підпису для підписування виборчих бюлетенів. Такий підхід застосовується у найбільш відомих схемах електронного голосування, а саме у *схемі Фудзіок-Окамото-Оти* [2] і *протоколі SENSUS* [3].

Але даний підхід не вирішує проблеми конфіденційності, яка висвітлена вище. Якщо ж замість “осліплення” бюлетеня підписувати наосліп відкритий ключ потенційного виборця, таємність його голосу зберігається. Даний підхід вперше було

запропоновано Ци Хе і Чжунмінь Су, технологія зараз відома під назвою *протокол He-Su* [4]

Отже, основна ідея полягає в тому, що виборець підписує свій відкритий ключ, а не голос. Для шифрування голосу використовується криптографічна схема RSA. Цей підхід гарантує, що навіть недоброчесна виборча комісія не може співставити конкретного виборця з його вибором, навіть після розшифрування та оприлюднення результатів. Крім того, оскільки публікуються у відкритий доступ списки виборців і їх авторизовані ключі, достатньо проблематично для зловмисників використовувати неіснуючі голоси, а публікація можливість перевірки результатів голосування унеможливлює зарахувати голоси виборців, які зареєструвалися, але не проголосували.

Схема виборів за протоколом He-Su багатьма дослідниками вважається найбільш досконалою. Дійсно, вона на перший погляд задовольняє усім основним вимогам, що пред'являються до електронних виборів. Але все ж таки дана схема не гарантує відсутність продажу голосів недоброчесними учасниками. Дійсно в ситуації, коли зловмисник пропонує викупити не голос виборця, а його приватний ключ ще на етапі реєстрації, зловмисник може повністю діяти від імені виборця, віддаючи його голос на власний розсуд.

Зазвичай, такий сценарій рідко розглядається спеціалістами з криптографії. Тому було поставлено задачу унеможливити саму процедуру продажу приватного ключа в протоколі He-Su (оскільки купувати голос, як зазначалося, не має сенсу за відсутності можливості підтвердити свій вибір у даній схемі, або ж за наявності можливості переголосувати таємно від покупця пізніше). Ключовою ідеєю запропонованого підходу є використання подвійної біометричної ідентифікації (наприклад на основі відбитка пальця).

Пропонується наступний алгоритм проведення виборів на основі комбінації протоколу He-Su і біометрії.

1) На етапі особистої реєстрації виборець пред'являє не тільки свої документи/ідентифікатори, але й авторизується за допомогою відбитку пальця в застосунку. Надалі за допомогою застосунка підписує наосліп свій криптографічний ключ.

2) На етапі голосування виборець також анонімно голосує із застосунка, використовуючи біометрію, що ускладнює продаж

голосу без фізичної присутності виборця (наприклад, продаж через анонімний месенджер).

3) Нарешті на етапі підрахунку і публікації результатів виборці відправляють ключі розшифрування також через застосунок.

Звичайно, даний підхід не дає гарантії повного виключення продажу голосів (або примусу до голосування певним чином), оскільки залишається можливість присутності “людини за спиною”. Тобто виборець свідомо може голосувати в присутності іншої особи. Тому бажано комбінувати криптографічні методи з юридичною відповідальністю. Підвищення технічної складності торгівлі голосами підвищує загальну якість процесу виборів і рівень довіри результатам у суспільстві.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. B. Schneier. Applied Cryptography. Protocols, Algorithms, and Source Code in C // John Wiley & Sons. - 1996. - 784 p.

2. Fujioka, Atsushi; Okamoto, Tatsuaki and Ohta, Kazuo. A practical secret voting scheme for large scale elections // Lecture Notes in Computer Science. - 1993. - Vol. 718. - pp. 244-251.

3. Cranor, L., Cytron, R.K. Sensor: A Security-Conscious Electronic Polling System for the Internet // Proc. of HICSS. - 1997. - pp.561-570.

4. He, Q. and Su, Z. A New Practical Secure e-Voting Scheme // Proceedings of the 14th International Information Security Conference (IFIP/SEC’98), Austrian Computer Society. - Austria, 1998. - pp.196-205.

УДК 004.03 (043.2)

А.В.Ільєнко, к.т.н.,
С.С.Ільєнко, к.т.н.,
О.Л.Яковенко
Національний авіаційний університет, Україна

ПІДХІД ЩОДО ПЕРЕВІРКИ ЦИФРОВИХ СЕРТИФІКАТІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ BLOCKCHAIN

На сьогодні актуальність захищеної передачі даних між користувачами та веб-сторінками, зокрема використання HTTPS, HSTS, Certificate pinning та HTTP Public Key Pinning для забезпечення безпеки є дуже важливим. Забезпечення безпеки комунікацій у мережі залежить від ефективного процесу верифікації цифрових сертифікатів. Основною проблемою є некоректна верифікація цифрових сертифікатів, що призводить до вразливостей, які можуть бути використані зловмисниками. Метою роботи є розробка методу верифікації сертифікатів з використанням технології blockchain для захисту операційної системи Windows від вразливостей, пов'язаних із передачею цифрових сертифікатів. Об'єктом дослідження є недоліки та вразливості використання операційної системи Windows, пов'язані з передачею цифрових сертифікатів та розробка децентралізованої інфраструктури відкритих ключів. Завданням дослідження є аналіз основних проблем, таких як ненадійні сертифікати, слабкі алгоритми хешування та RSA ключі менше 2048 біт, а також неправильно підписані сертифікати SSL; розробка підходу до організації інфраструктури відкритих ключів (PKI) з використанням технології blockchain для усунення існуючих недоліків традиційної технології цифрових сертифікатів; опис технології децентралізованої інфраструктури відкритих ключів (DPKI) і пояснення, як вона працює за відсутності централізованої структури; деталізація формування транзакцій у межах децентралізованої інфраструктури, включаючи створення нульових транзакцій, наступних транзакцій і використання різних типів пар ключів (звичайних і службових пар ключів).

Запропоноване в роботі рішення зосереджено на підвищенні безпеки даних у відкритих мережах шляхом використання технології blockchain для передачі цифрових сертифікатів.

Запроваджуючи новий підхід до організації інфраструктури відкритих ключів за допомогою blockchain, дослідження має на меті усунути існуючі недоліки традиційної технології цифрових сертифікатів, зокрема залежність від центральних органів видачі. Виділено ключові компоненти blockchain, такі як записи транзакцій і використання хеш-функцій для забезпечення цілісності даних. Запропонована децентралізована інфраструктура відкритих ключів використовує blockchain для забезпечення безпеки та надійності обміну цифровими сертифікатами. «Нульова транзакція» є центральним елементом цієї інфраструктури. Ідея полягає в тому, що перша транзакція в мережі blockchain, або «нульова транзакція», створюється для прив'язки всіх публічних ключів до конкретного власника. Ця транзакція діє як якір для всіх подальших транзакцій, які містять інформацію про публічні ключі. Такий підхід забезпечує децентралізовану та надійну систему підтвердження ідентичності та автентичності.

Для досягнення поставленої цілі була розроблена власна програмна реалізація для перевірки цифрових сертифікатів з використанням децентралізованої інфраструктури відкритих ключів з використанням технології blockchain , що може бути використана на операційній системі Windows, врахувавши уразливості, які наявні у сучасних методах верифікації цифрових сертифікатів. Програма реалізована на мові програмування Python і використовує Visual Studio як першочергове середовище розробки.

Актуальність запропонованого рішення полягає в його інноваційному підході до підвищення безпеки даних за допомогою технології blockchain, вирішення проблем довіри, пов’язаних із централізованими центрами сертифікації. Завдяки децентралізації управління відкритими ключами та використанню blockchain для забезпечення цілісності даних рішення пропонує альтернативу традиційним системам PKI.

Загалом робота підкреслює важливість рішень на основі blockchain для покращення захисту даних у відкритих мережах. Тому використання blockchain для перевірки цифрових сертифікатів на операційній системі Windows може бути ефективним методом підвищення рівня захисту. Реалізація такого програмного комплексу дозволяє не лише заглибитися у принципи роботи blockchain, але й переконатися в його можливостях на практиці.

УДК 656.71:629.735.05:621.396.946:004.056(043.2)

Є.Є.Карпов,
О.В.Вовна, д.т.н.
Національний авіаційний університет, Київ

ПІДВИЩЕННЯ БЕЗПЕКИ ТА НАДІЙНОСТІ КОМП'ЮТЕРНО-ІНТЕГРОВАНОЇ СИСТЕМИ МОНІТОРИНГУ В МЕЖАХ АЕРОПОРТУ НА БАЗІ РАДІОМЕРЕЖІ LORAWAN

Безпека в аеропортах України є однією з найважливіших та найбільш контрольованих сфер. Українські аеропорти дотримуються стандартів Міжнародної організації цивільної авіації, а також наступних документів: Інструкція [1]; Повітряний кодекс України [2]; Правила руху [3]; інші документи.

В Правилах руху [3] визначено, що на транспортних засобах має бути система контролю швидкості та місцезнаходження. Також, на території аеропорту знаходиться багато інших систем, які потребують моніторингу задля своєчасного обслуговування обладнання різних систем аеропорту.

Проблемою сучасних систем моніторингу в аеропортах є те, що в них є підсистеми, які залежать від каналів зв’язку сторонніх компаній, а також підсистем: зберігання, обробки та відображення даних, які знаходяться во власності сторонніх компаній.

Метою цього дослідження є підвищення безпеки та надійності комп’ютерно-інтегрованої системи моніторингу в межах аеропорту завдяки розробці нової схеми системи моніторингу, переходу на технологію передачі даних LoRaWAN, та повну незалежність від послуг сторонніх компаній по передачі, зберіганню, обробці та відображенню даних.

Об'єктом дослідження обрано процеси передачі, зберігання, обробки та відображення даних комп’ютер-інтегрованої системи моніторингу в межах аеропорту.

Предметом дослідження є вдосконалення схеми системи моніторингу з метою підвищення безпеки та надійності.

Методологія дослідження заснована на використанні математичного моделювання для аналізу характеристик радіомережі з подальшим тестуванням прототипу макетного зразка.

На теперішній час системи моніторингу використовують

локальні мережі на базі витої пари, оптичної мережі, або мережі провайдерів стільникового зв'язку (GPRS). Ці мережі або не дають гнучкість розташування (мобільності) датчиків, або залежать від сторонніх компаній. Це впливає на безпеку та надійність системи моніторингу, а також на своєчасне отримання даних з датчиків для швидкого прийняття рішень.

В роботі було виявлено, що існуючі системи моніторингу в підсистемі радіозв'язку використовують модулі GPRS для зв'язку з операторами стільникового зв'язку. Підсистема передачі даних до бази даних виконується через канали зв'язку сторонніх компаній (інтернет-провайдерів). Підсистеми збору, обробки та відображення даних знаходяться на серверах постачальників систем моніторингу. Також, все це впливає на ціну обслуговування системи моніторингу.

Розроблена схема системи моніторингу на базі LoRaWAN дозволяє уникнути впливу негативних факторів, які зазначені вище, а саме:

- Залежність від каналів зв'язку сторонніх компаній;
- Залежність від підсистем збору, обробки та відображення даних, якими керують сторонні компанії;
- Мобільність розташування датчиків в межах аеропорту;
- Безпека та надійність передачі, збереження та обробки даних.

На рис.1 наведена розроблена схема системи моніторингу. Підсистема радіозв'язку складається з радіомодуля, розташованого на мікроконтролері з датчиками та радіомодуля, розташованого на шлюзі до локальної мережі. Вся територія аеропорту повинна бути покрита радіомережею шлюзів. Підсистеми збору, обробки та відображення даних знаходяться на сервері в серверній кімнаті аеропорту. Тобто, вся система моніторингу стає повністю незалежною від сторонніх компаній. Таким чином, виключаючи негативний вплив, який зазначено вище, зростає надійність та безпека системи моніторингу.

Рис.1. Схема комп'ютерно-інтегрованої системи моніторингу

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Верховна Рада Укріїни : Про затвердження Авіаційних правил України «Інструкція з організації та здійснення контролю на безпеку в аеропортах України». URL : https://zakon.rada.gov.ua/laws/show/z0594-19 (дата звернення: 12.04.2024).

2. Верховна Рада Укріїни: Повітряний кодекс України. https://zakon.rada.gov.ua/laws/show/3393-17 (дата звернення: 12.04.2024).

3. Державне підприємство «Міжнародний аеропорт «Бориспіль»: Правила руху транспортних засобів на аеродромі «Київ» (Бориспіль) (ПРТЗА) URL: https://kbp.aero/wp-content/uploads/2020/11/ПРТЗА_Ел.примірник.pdf (дата звернення: 12.04.2024).

УДК 629.782:001.5 (045)

А.С.Климова, к.т.н.
Національний авіаційний університет, Київ

БАГАТОКРИТЕРІАЛЬНИЙ ПАРАМЕТРИЧНИЙ СИНТЕЗ АВІАЦІЙНО-КОСМІЧНИХ СИСТЕМ

Сучасна економічна обстановка в країні вимагає раціонального використання матеріальних ресурсів, для чого необхідне глибоке теоретичне осмислення завдання на розробку авіаційно-космічної техніки і пошуку прикладних методів вирішення проблемних питань, що виникають в ході військово-технічних досліджень, з метою істотного скорочення витрат на їх проведення.

Важливими напрямами підвищення ефективності проведення наукових досліджень авіаційно-космічної систем (АКС) є удосконалення існуючих і розробка нових підходів, методик, засобів збезпечення синтезу АКС на основі багатокритеріальної оптимізації і математичного моделювання.

Якість рішення задачі багатокритеріальної оптимізації оцінюється за сукупністю суперечливих частинних критеріїв, що є функціями від заданих концептуальних параметрів $y = \{y_i\}_{i=1}^{n} \in Y$, що визначають концепцію її побудови. Задані для кожного параметра обмеження утворюють допустимій простір параметрів Y. Обмеження на параметри виявляються на підставі аналізу прогнозованих умов створення і застосування АКС і мають вигляд $\alpha_{iн} \leq y_i \leq \alpha_{iв}$, $j = \overline{1,q}$, де $\alpha_{iн}$, $\alpha_{iн}$ - відповідно допустимі нижня і верхня межі зміни чисельного значення у-го параметра.

Сукупність функцій частинних критеріїв $f_k(y)$, $k = 1,m$ утворюють вектор цільової функції $f = f(y) = \{f_k(y)\}_{k=1}^{m}$, який повинен знаходитись в області допустимих значень. Передбачається, що зовнішні умови, які впливають на функціонування системи, відомі і фіксовані. Тоді векторний критерій є функцією тільки концептуальних параметрів. Потрібно визначити оптимальний набір (вектор) концептуальних параметрів системи $y' \in Y$, якій оптимізує вектор критеріїв при відомих обмеженнях на параметри. Рішення задачі припускає виділення області ефективних варіантів системи (множини Парето) і вибір з

цієї множини єдиного компромісного варіанта. Цей вибір здійснюється на основі додаткової суб'єктивної інформації (про відносну важливість частинних критеріїв в заданій ситуації) від особи, яка приймає рішення. На основі цієї інформації, формулюється схема компромісів $F_{\text{узаг}}[f(y)]$ - узагальнена функція скалярної згортки частинних критеріїв.

Відповідна модель векторного параметричного синтезу АКС за умови мінімізації функції $F_{\text{узаг}}[f(y)]$ полягає у визначенні вектора концептуальних параметрів системи y', який задовольняє векторному критерію $f(y)$ і мінімізує узагальнений критерій (згортку частинних критеріїв за нелінійною схемою компромісів) при заданих обмеженнях $y = \underset{y \in Y}{argmin} F_{\text{узаг}}[f(y)]$. При цьому потрібно переконатися, що мінімізація функції $F_{\text{узаг}}[f(y)]$ призводить до оптимального за Парето рішення. Для побудови функції узагальненого критерію, найчастіше застосовується лінійна згортка частинних критеріїв (перевага: простота).

Основними етапами вирішення задачи векторної оптимізації є нормалізація (приведення до єдиної міри) частинних критеріїв, виділення множини компромісів (ефективних за Парето рішень) та вибір схеми компромісів і єдиного рішення.

В основі алгоритму виділення множини ефективних точок лежить числове дослідження (зондування) простору концептуальних параметрів проектованої системи, яке проводиться у декілька етапів. На першому етапі здійснюється зондування простору параметрів за допомогою послідовності рівномірно розподілених псевдовипадкових $ЛП_t$ точок. Послідовності $ЛП_t$ точок є найбільш рівномірно розподіленими серед відомих у теперішній час послідовностей. Для генерації псевдовипадкових $ЛП_t$ точок використовуються генератори пробних точок, наприклад модуль генерації $ЛП_t$ чисел інтегрований в Microsoft ExceI. Отримана сукупність $ЛП_t$ точок в натуральних значеннях являє собою матрицю початкових значень незалежних змінних. Межі зміни кожного з параметрів (параметричні обмеження) виділяють в просторі параметрів гіперпаралелепіпеда.

Виділення ефективних точок засновано на вирішенні задачі параметричного програмування і формуванні множини ефективних

рішень в нормалізованому просторі критеріїв. Визначаються точки за формулою

$$y' = \bigcup_{c \in X} \operatorname*{agrmin}_{y \in Y} \sum_{k=1}^{m} C_k f_k^0(y)$$, де

$f_k^0(y)$ - нормалізоване значення к-го частинного критерію,

$C = \{C_k\}_{k=1}^{m}$ - формальний векторний параметр, визначений на множині

$$X_c = \{c | \sum_{k=1}^{m} C_k = 1, C_k \geq 0\}.$$

Отримати наближену компромісну криву можна з'єднавши ламану, що сполучає (за порядком) всі ефективні точки (вона завжди безперервна). Коли кількість вихідних $ЛП_t$ точок зростає наближена компромісна крива в деякому розумінні наближається до точної компромісної кривої. На практиці, зазвичай, використовують не ділянки наближеної компромісної кривої, а оптимальні за Парето точки, яким завжди відповідають реальні ефективні варіанти побудови системи.

Остаточний вибір оптимального варіанта покладається на суб'єкт досліджень і значною мірою залежить від вдалого вибору схеми компромісів і коефіцієнтів важливості (ваги) частинних критеріїв. У результаті оцінки альтернативних варіантів комплексу множина ефективних рішень звужується і закінчується вибором єдиного оптимально-компромісного варіанта.

Отже для отримання єдиного рішення на першому етапі необхідно, підставляючи аналітичні залежності частинних критеріїв від параметрів, отримати функцію узагальненого критерію у вигляді нелінійної згортки компромісів. Скалярна функція векторного критерію $F_{узаг}[f(y)]$ в різних ситуаціях є виразом різних принципів оптимальності, яка повинна задовольняти вимоги:

- бути гладкою і монотонною;
- у напружених ситуаціях виражати принцип мінімакса;
- у спокійних умовах - принцип інтегральної оптимальності;
- у проміжних випадках призводити до оптимальних за Парето рішень.

Найбільш простою функцією і такою, що задовольняє викладені вимоги, є

$$F_{узаг}[f(y)] = \alpha_1 * \left(1 - f_1(y)\right)^{-1} + (1 - \alpha_1) * \left(1 - f_2(y)\right)^{-1}, \alpha_1 = 0, \ldots, 1.$$

На другому етапі обчислюються значення функції $F_{узаг}[f(y)]$ у всіх точках нормалізованого простору критеріїв при заданих значеннях коефіцієнтів важливості критеріїв $\alpha_k \geq 0, \sum_{k=1}^{m} \alpha_k = 1$.

На третьому етапі вирішується задача пошуку точки A', для якої $F_{узаг} = \min_{A \in V} F_{узаг}(A)$.

Відомо, що координати точок A є ділянкою послідовності, рівномірно розподіленої в просторі параметрів. Це забезпечує хорошу швидкість збіжності при чисельному рішенні задачі пошуку мінімуму $F_{узаг}(A)$. Можна скористатися будь-яким методом локального пошуку екстремумів, вибираючи, як початкові, всі точки A_i, що належать допустимій області.

Знайшовши точку мінімуму в нормалізованому просторі критеріїв, можна визначити відповідну їй точку в натуральному просторі критеріїв. Цій точці відповідає точка в просторі параметрів, координатами якої є шукані параметри (вектор) значень, що задовольняють векторному критерію $f(y)$.

Розглянута методика, заснована на методах і алгоритмах багатокритеріальної оптимізації і математичного моделювання. Вона забезпечує вирішення широкого спектру завдань, починаючи з проведення процедури побудови моделей критеріальних функцій на основі даних експерименту, обчислень за моделями допустимих варіантів системи і закінчуючи вибором остаточного компромісно-оптимального рішення. Методика може знайти застосування при дослідженнях на початкових етапах розробки і проектування авіаційно-космічних комплексів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Зіатдінов Ю.К., Климова А.С., Полухін А.В. Проблеми багатокритеріального синтезу складних технічних систем і методи їх вирішення. Проблеми інформатизації та управління: зб. наук. праць. – К.: НАУ, 2023. – Вип. 4(76). – С.28-34. DOI: 10.18372/2073-4751.76.18237.

УДК 004.78

А.М.Козуб, к.т.н.,
Д.П.Кучеров, д.т.н.,
О.М.Пошивайло
Національний авіаційний університет, Київ

РЕКОМЕНДАЦІЙНА СИСТЕМА ДЛЯ ЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ ПОВІТРЯНОГО ТРАНСПОРТУ В СКЛАДНИХ УМОВАХ ПОЛЬОТУ

Авіатранспорт відіграє у сучасному житті важливу роль. Цей факт підтверджується даними Міжнародної асоціації повітряного транспорту (IATA), яка встановила зростання авіаперевезень у світі перевезень пасажирів та вантажів за останні два роки. Це спостереження пов'язують із скасуванням обмежень, запроваджених з оголошенням пандемії.

Крім того, авіатранспорт є ефективним засобом вирішення соціальних та міждержавних проблем, до яких належать доставлення гуманітарної та військової допомоги, евакуація постраждалих з осередків стихійних лих, дипломатичні візити тощо.

Оскільки роль авіатранспорту зростає, все більша увага приділяється покращенню якості самих літаків та ефективного їх використання. Сучасні тенденції у розвитку авіатранспорту спрямовані на скорочення викидів в атмосферу та зменшення рівня шуму авіаційних двигунів, розробляються оптимальні стратегії у формуванні маршрутів, що сприяє скороченню вартості перевезень, вивчаються різноманітні сценарні підходи, підвищується якість підготовки пілотів, вивчаються технологічні та поведінкові стратегії. вирішення потреб перевізників та пасажирів.

На підвищення якості використання авіатранспорту впливає вивчення авіакатастроф і усунення їх причин. Авіакатастрофи мають не стільки технічне походження, скільки пов'язані з неправильною діяльністю екіпажу. Так, людський фактор за оцінками ICAO становить близько 80% усіх авіакатастроф [1].

Таким чином, проблемним стає правильність дій екіпажу в складних умовах польоту. Одним із можливих рішень щодо беззбійного функціонування авіатранспорту може бути створення бортових помічників або рекомендаційних експертних систем, які б виробляли рішення на основі прогнозу розвитку ситуації та пропонували екіпажу ефективні на даний момент рішення. Основою для аналізу поточного стану літака може бути не тільки інформація від системи, що діагностує, а й інтегральні показники руху по маршруту, що дозволяють забезпечити політ без збоїв.

Мета дослідження полягає у проектуванні та створенні ефективних бортових рекомендуючих експертних систем, що дозволяють їх впровадження на будь-який літак з метою створення стійкого та прийнятного в експлуатації авіатранспорту.

Формування рекомендацій ґрунтується на основі даних зовнішнього світу та внутрішнього технічного стану літального апарату. Ці дані групуються за обмеженим набором ознак, серед яких визначаються пріоритети. За кожною ознакою формуються рекомендації та пропонуються дії як екіпажу, так і систем керування літального апарату. Пропонуються також деякі підходи та алгоритми щодо оцінки пріоритетності поточної ситуації. Тут можуть бути застосовані сучасні підходи до оцінки ситуації на основі апріорної невизначеності щодо вихідних даних. Передбачається оснащення такими системами сучасних літальних апаратів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. ICAO Safety Report, 2019. URL: https://www.icao.int/safety/Documents/ICAO_SR_2019_final_web.pdf.

УДК 004.056

В.В.Константиненко,
Є.В.Куляк
Національна академія Служби безпеки України, Київ

TRELLO ПРОГРАМА ДЛЯ ІТ-ПРОЄКТУВАННЯ ТА УПРАВЛІННЯ

Системи проектування та управління проектами (СПУП) – це програмні інструменти, які допомагають командам планувати, організовувати та контролювати виконання проектів. Вони можуть використовуватися для проектів будь-якого розміру та складності, від невеликих завдань до масштабних підприємств.

Trello – це безкоштовна багато платформна система управління проєктами й робочими процесами, за допомогою якої можна відстежувати виконання завдань. Ця програма використовує систему дошок, в яких знаходяться списки та картки.

Переваги Trello:

1. Візуальна організація: Trello не показує одразу всі завдання в купі, а дає можливість ієрархічно розкласти їх. На дошці ви можете бачити списки всіх завдань, а відкривши їх, вам постануть картки, на яких відображені всі завдання та необхідна робоча інформація.
2. Відстежування прогресу: За допомогою дошок ви можете упорядкувати завдання й виконати свою роботу. В одну мить можете побачити завдання на всіх етапах включно від «проект ще в розробці» до «данний проект вже виконано».
3. Співпраця: Списки відображають етапи виконання завдання. Тут буде вся інформація, така як: «Що треба зробити», «У роботі», «Готово». Таким чином дізнаєтесь чи дану роботу вже хтось виконує чи ви можете взятись за неї і не переживати що хтось вже робить те саме і виявиться що хтось з вас марно згаяв свій час. Ну або навпаки ви зі своїм колегою можете взятись за роботу разом і допомагати один одному.
4. Інформативність: Картки містять інформацію про завдання та всю необхідну для роботи інформацію. Якщо ви виконуєте роботу з кимось разом, то можете побачити його вкладення та додати свій коментар, щоб вказати на недоліки зробленої роботи.
5. Зручність використання: Trello має приємний інтерфейсом drag-and-dop що перекладається як «тягни та кинь» тобто ви швидко можете перетягнути вашу виконану роботу на цю програму,

а так як всі данні динамічно оновлюються ви можете не переживати що ваша робота десь не збережеться.

Додаткові можливості Trello:

3. Підтримка команд: Trello дозволяє створювати команди та призначати завдання членам команди.

4. Інтеграція: Trello можна інтегрувати з багатьма іншими програмами, такими як Slack, Jira, Google Drive та багато іншими.

5. Мобільні додатки: Trello має мобільні додатки для iOS та Android, що дозволяє вам керувати своїми проектами на ходу.

6. Безпека: Trello використовує шифрування даних та інші заходи безпеки для захисту ваших даних. Працюйте та не переживайте що хтось крім вашої команди побачить цю роботу.

Отже підведемо підсумок: Trello - це потужний та гнучкий інструмент управління проектами, який може бути корисним для команд будь-якого розміру. Її візуальний інтерфейс, функції співпраці та мобільні додатки роблять її ідеальним вибором для команд, які прагнуть покращити організацію та продуктивність.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Trello (2024)*. https://uk.wikipedia.org/wiki/Trello
2. *Trello (2023). https://trello.com/uk/tour*

УДК 65.012.27

В.А.Копитов

Національний авіаційний університет, Київ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ В СУЧАСНІЙ УКРАЇНСЬКІЙ ЕНЕРГЕТИЦІ З УРАХУВАННЯМ НАСЛІДКІВ ВІЙСЬКОВОЇ АГРЕСІЇ

Ще на початку 2019 року енергетична сфера України активно розвивалась у напрямку цифровізації і поступового впровадження новітніх технологій. Саме тоді компанією ДТЕК було запущено програму цифрового перетворення MODUS. Довгостроковий проект стосується використання інноваційних цифрових систем у всіх виробничих і адміністративних процесах енергетичного бізнесу. Більше 30 проектів першої та другої хвилі представники компанії ДТЕК успішно запустили наприкінці 2020 року.

Без ефективного управління і надшвидкого реагування на критичні зміни і руйнування країна могла давно вже опинитися в страшних умовах блекаутів. Але фатальних наслідків і досі вдається уникати.

За допомогою програми MODUS створено інфраструктуру безпровідного зв'язку на шахті «Ювілейна» у Павлограді. Це – унікальний для нашої країни приклад успішного облаштування «Wi-Fi у шахті», адже зв'язок працює на глибині 500 метрів. У 2021 році на Ювілейній впроваджено інноваційну систему позиціювання персоналу. Для цього під землею розміщено систему з більш ніж 1700 радіо маячків Bluetooth для покриття приблизно 80 км гірничих виробіток. Шахтарі отримали індивідуальні smart-лампи, які передають сигнал тривоги у критичних ситуаціях.

Створюється математична модель вентиляції підземних виробіток. Використовується штучний інтелект при завантаженні вагонеток. За офіційними даними компанії, з моменту запуску системи MODUS вдалося заощадити більше 37 млн. грн. власних коштів підприємства.

Модернізуються не тільки шахти. У 2019 році впроваджено систему дронового моніторингу ліній електропередач на підприємстві Дніпровські електромережі. Водночас проводилися роботи по зменшенню тривалості аварійних відключень для споживачів на 10-15% при масштабуванні на всю компанію. Ці надбання зіграли надважливу роль під час ракетних обстрілів енергетичної системи України з боку росії.

Не менш важливим виявилося впровадження систем автоматичного визначення оптимальних режимів роботи енергоблоків на кількох українських ТЕС, серед яких була і Запорізька станція в Енергодарі. Ці нововведення допомагають автоматично управляти режимами роботи енергоблоків станції за допомогою сучасних технологій IoT, Machine Learning, Data Lake. Економічний ефект від скорочення витрат палива за перші 21 місяці роботи станції склав 170 млн. грн. Після ударів ворога по машинних залах Дніпровської ГЕС наявність працездатної та добре контрольованої Запорізької ТЕС є надважливою.

Отже, високі витрати на цифровізацію є обґрунтованими і швидко окупаються. Згідно офіційних звітів ДТЕК, від 2019 року загальний економічний ефект використання цифрових технологій склав біля 230 млн. грн.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Нові горизонти: як українська енергетика використовує цифрові технології [Електронний ресурс]. – Режим доступу: https://dtek.com/media-center/news/skachok-tsivilizatsii-kak-tsifrovye-tekhnologii-menyayut-energeticheskuyu-otrasl-ukrainy/

2. Найглибша Wi-Fi-мережа у країні, яка знаходиться на шахті «Ювілейна», відсвяткувала свою першу річницю [Електронний ресурс]. – Режим доступу: https://www.5632.com.ua/news/3105573/samaa-glubokaa-wi-fi-set-v-strane-raspolozennaa-na-sahte-ubilejnaa-otmetila-pervuu-godovsinu

УДК 004

Р.І.Кормиш,
Р.С.Савіцький
Державний університет "Житомирська політехніка", Житомир

АНАЛІЗ ПРОЦЕСІВ АВТОМАТИЗАЦІЇ МЕНЕДЖМЕНТУ БУДІВЕЛЬНИХ ПРОЕКТІВ

Автоматизація систем управління проектами в будівельних компаніях не є лише тенденцією; це стає необхідністю в сучасному динамічному бізнес-середовищі. Процес автоматизації виходить далеко за межі зручності, надаючи конкретні переваги, що можуть революціонізувати спосіб, яким плануються, виконуються та завершуються будівельні проекти. У дослідженні розглянемо необхідність автоматизації систем управління проектами в будівельних компаніях, вивчаючи безліч переваг і вирішуючи виклики, що супроводжують цю трансформаційну подорож.

Ефективність є основою успішного будівельного проекту, де автоматизація виступає каталізатором максимізації оперативної ефективності. Шляхом оптимізації процесів та мінімізації ручного втручання автоматизовані системи управління проектами дозволяють будівельним компаніям оптимізувати розподіл ресурсів, оптимізувати графіки робіт та покращувати управління бюджетом. Це не лише призводить до значного збереження часу, але й дозволяє компаніям стратегічно розподіляти ресурси, що сприяє підвищенню прибутковості та загальної успішності проекту [1].

Більше того, автоматизація сприяє покращеному співробітництву між учасниками проекту, перевищуючи географічні бар'єри та організаційні обмеження. Реальний час доступу до даних проекту, централізовані канали комунікації та інструменти спільної роботи сприяють безшовному обміну інформацією та прийняттю рішень. Незалежно від того, чи є це архітектори, інженери, підрядники чи клієнти, всі учасники проекту можуть залишатися синхронізованими, сприяючи прозорості, відповідальності та, в кінцевому підсумку, успіху проекту.

Однією з найбільш серйозних перешкод є опір змінам, що глибоко вкорінений в організаційній культурі. Працівники, звиклі до

традиційних методів управління проектами, можуть виявити неохочість або страх перед прийняттям нових технологій.

Фінансові обмеження є ще однією важливою перешкодою, особливо для будівельних компаній малого та середнього розміру з обмеженими бюджетами. Хоча довгострокові переваги автоматизації беззаперечні, початкові витрати на придбання та впровадження автоматизованих інструментів управління проектами можуть бути пугачем. Подолання цієї перешкоди вимагає ретельного фінансового планування, дослідження вартісних рішень та демонстрації конкретного повернення інвестицій (ROI), пов'язаного з автоматизацією [2].

Технічні складнощі також стоять на шляху до автоматизації, особливо щодо інтеграції з існуючою програмною інфраструктурою та міграції даних. Проблеми сумісності, виклики інтероперабельності та синхронізації даних можуть завдати шкоди безшовності інтеграції, порушуючи робочі процеси та заважаючи продуктивності. Подолання технічних бар'єрів потребує міцних знань з IT, дотепного планування та гнучкості у вирішенні проблем.

Конкурентні тиски сучасного бізнес-середовища вимагають гнучкості, ефективності та інновацій. Автоматизація — це не просто розкіш; це стратегічна необхідність для зберігання попереду кривої, підвищення оперативної ефективності та досягнення виняткових результатів для клієнтів.

Переваги автоматизації систем управління проектами в будівельних компаніях є покращення ефективності та співпраці, мінімізація ризиків та конкурентної переваги. Хоча викликів вдосталь, їх вирішення завчасно за допомогою ефективного управління змінами, фінансового планування та технічних знань може покрити шлях до успішної реалізації та трансформаційного потенціалу автоматизованих систем управління проектами.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Досвід з автоматизації будівельних компаній від Kamala Software [Електронний ресурс]. – Режим доступу: https://kamala soft.com/uk/blog/avtomatizatsiya-stroitelnykh-kompaniy/.

2. Суть і переваги автоматизації будівельного бізнесу [Електронний ресурс]. – Режим доступу: https://www.netsoft*. com.ua/ articles-soft/bas news/avtomatizacija-biznjesa-sut-i - prjeimushhjestvaU.html*

УДК 004.415

С.В.Костюков,
О.П.Мартинова, к.т.н.,
О.О.Кучмій
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

КОНТЕЙНЕРИЗАЦІЯ ТА ЇЇ ВПЛИВ НА ПРОЦЕС РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Контейнеризація, особливо представлена такими інструментами як Docker, Kubernetes та іншими, стала основним інструментом у розробці програмного забезпечення. Ця технологія змінює парадигму створення, розгортання та управління додатками. Контейнеризація помітно впливає на процес розробки програмного забезпечення.

Контейнери — це тип технології віртуалізації, який дозволяє запускати кілька програм в одній операційній системі (ОС), ізолюючи кожну програму та її процеси один від одного. Ця ізоляція досягається за рахунок використання ОС, яка контролює розподіл ресурсів, таких як ЦП, пам’ять і диск для кожного процесу [1].

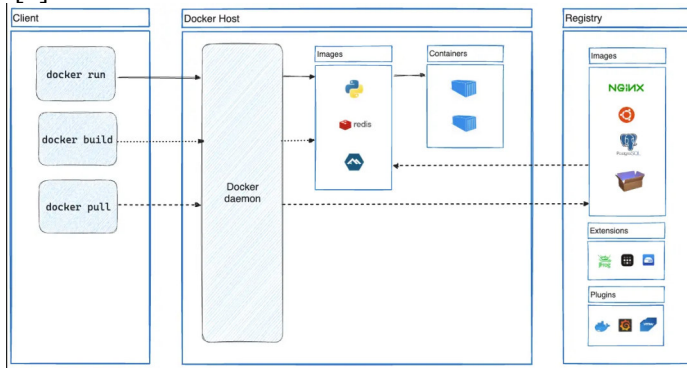


Рис. 1 Архітектура докера [2]

Однією з основних переваг контейнеризації є здатність швидко розгортати додатки у будь-якому середовищі [4]. За допомогою контейнерів, розробники можуть упаковувати всі необхідні залежності та бібліотеки разом з самим додатком, забезпечуючи консистентність середовища розгортання від розробки до продукції.

Контейнеризація дозволяє розробникам легко масштабувати свої додатки, запускаючи кілька контейнерів одного і того ж додатку на різних серверах або в хмарних середовищах. Це робить процес масштабування більш простим і ефективним, оскільки контейнери можуть бути легко розгортані та керовані за допомогою інструментів оркестрації, таких як Kubernetes.

Ця технологія спрощує розробку та тестування програмного забезпечення, оскільки дозволяє розробникам створювати ізольовані середовища для своїх додатків [3]. Це означає, що розробники можуть запускати та тестувати свої додатки в однаковому середовищі, що використовується у замовника, зменшуючи ризик виникнення проблем при розгортанні.

Контейнеризація також дозволяє розробникам створювати більш гнучкі та адаптивні додатки. Завдяки контейнерам, додатки можуть бути розроблені таким чином, що їх можна легко переносити з одного середовища в інше, незалежно від того, чи це власний сервер, хмарне середовище або локальний комп'ютер розробника.

Забезпечення безпеки та ізоляції додатків також є перевагою контейнеризації, оскільки кожен контейнер має власне ізольоване середовище виконання. Це дозволяє запобігти можливим конфліктам між додатками та забезпечити, що в разі вразливостей або атак контейнер може бути легко відокремлений та виправлений без впливу на інші компоненти системи.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Гонтаренко С.С. Аналіз технологій контейнеризації та оптимізації розгортання масштабованого застосунку на платформі Kubernetes: кваліфікаційна магістерська робота: URL: https://krs.chmnu.edu.ua/jspui/bitstream/123456789/2729/1/Гонтаренко.pdf

2. Docker Owerview: URL: https://docs.docker.com/get-started/overview/

3. Навіщо нам контейнеризація: перевага для DevOps: URL: https://itedu.center/ua/blog/articles/navishho-nam-kontejnerizaciya-perevagi-dlya-devops/

4. Олександр Ю. Що таке Docker: простими словами про контейнеризацію: URL: https://blog.ithillel.ua/articles/shcho-take-docker-prostimi-slovami-pro-konteynerizatsiyu

УДК 004.42

М.М.Котенко,
Т.А.Вакалюк, д.п.н.
Державний університет «Житомирська політехніка», Житомир

МЕТОДИКИ ВИМІРЮВАННЯ ТА АНАЛІЗУ ВЗАЄМОДІЇ МІКРОСЕРВІСНИХ КОМПОНЕНТІВ

Архітектура мікросервісів, яка передбачає розбиття комплексних програм на малі, автономні сервіси, відіграє важливу роль у сучасному програмуванні. Вона дозволяє сервісам комунікувати за допомогою легковагових протоколів, забезпечуючи тим самим підвищену масштабованість, адаптивність та надійність системи. Проте, децентралізована структура мікросервісів ускладнює взаємодію між компонентами, потребуючи застосування сучасних методик вимірювання та аналізу для ефективного управління міжкомпонентною взаємодією. Дане дослідження фокусується на аналізі цих методик.

Методи, такі як розподілене трасування, агрегація журналів подій та збір метрик, являються ключовими для вимірювання та аналізу взаємодії мікросервісних компонентів [1]. Розподілене трасування дозволяє виявляти затримки та діагностувати несправності через детальний аналіз шляхів запитів у мережі мікросервісів. Водночас, агрегація та аналіз журналів подій з усіх компонентів системи сприяє діагностиці системних відхилень, надаючи змогу отримати цілісне розуміння стану системи. Впровадження метрик розширює можливості вимірювання взаємодій між компонентами мікросервісів. Збір даних про ключові показники ефективності, як-от час відповіді, швидкість обробки запитів, частота помилок та використання ресурсів, дозволяє зацікавленим сторонам відслідковувати тенденції протягом часу. Комбінування метрик та інструментів аналізу часових рядів дозволяє ефективно виявляти аномалії та встановлювати моделі, які можуть вказувати на приховані проблеми.

В архітектурі мікросервісів картографування та аналіз залежностей допомагає в розумінні складних взаємозв'язків між компонентами. Ці методи полегшують аналіз впливу змін або несправностей на екосистему, сприяють ризик-менеджменту та розробці адаптивних систем. Такі процеси дозволяють виявляти та

ліквідувати потенційні недоліки, забезпечуючи надійність системи. У контексті картографування залежностей варто звернути увагу на дослідження Гамажа та Перери [2], що застосовує розподілене трасування і теорію графів для побудови дерева залежностей між сервісами. Це дослідження допомагає виявити та виміряти проблеми в дизайні системи, такі як надмірне зв'язування, циклічні залежності, коефіцієнт кластеризації та інші.

Синтетичний моніторинг і інженерія хаосу є новаторськими методами в розробці та підтримці взаємодії мікросервісних компонентів, що спрямовані на підвищення стабільності та продуктивності. Синтетичний моніторинг використовується для систематичного аналізу продуктивності мікросервісів шляхом симуляції користувацьких запитів та трафіку в контрольованих умовах, що дозволяє детально аналізувати реакцію системи на різні типи навантажень. З іншого боку, інженерія хаосу зосереджується на випробуванні стійкості системи через навмисне введення збоїв у роботу системи. Цей метод дозволяє ідентифікувати слабкі місця в механізмах відновлення та обробки помилок, сприяючи розробці більш надійних стратегій для забезпечення неперервної роботи сервісу в умовах непередбачуваних збоїв.

Досліджені методи демонструють ефективність у контексті аналізу та вимірювання взаємодії мікросервісних компонентів, але їх використання в основному обмежене етапами розробки та періодом після впровадження. Майбутні дослідження можуть бути направлені на розробку методологій для моделювання взаємодії мікросервісів на ранніх етапах проектування, беручи до уваги практики, що описані у даному аналізі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Newman S. Building Microservices: Designing Fine-Grained Systems. O'Reilly Media, Incorporated, 2021. 616 p

2. Gamage I. U. P., Perera I. Using dependency graph and graph theory concepts to identify anti-patterns in a microservices system: A tool-based approach. 2021 Moratuwa Engineering Research Conference (MERCon), Moratuwa, Sri Lanka, 27–29 July 2021. 2021. URL: https://doi.org/10.1109/mercon52712.2021.9525743 (date of access: 24.03.2024).

УДК 004.8

Є.В.Красовська, к.т.н.,
О.Д.Красовський
ВСП «Фаховий коледж інженерії, управління та землевпорядкування НАУ», Київ

ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ 3D МОДЕЛЮВАННЯ

Штучний інтелект (ШІ) відноситься до моделювання людського інтелекту в машинах, які запрограмовані думати як люди та імітувати їхні дії. Підмножиною ШІ є машинне навчання, яке стосується концепції, згідно з якою комп'ютерні програми можуть автоматично вчитися на нових даних і пристосовуватися до них без допомоги людей. Машинне навчання – найпопулярніша галузь ШІ. Інші класи ШІ включають імовірнісні моделі, системи штучних нейронних мереж, глибоке навчання тощо. Методи глибокого навчання дозволяють автоматично навчатися шляхом поглинання величезної кількості неструктурованих даних [1].

Глибоке навчання (ГН) є формою машинного навчання, що моделює моделі в даних як складні, багатошарові мережі. Оскільки ГН є найбільш загальним способом моделювання проблеми, воно має потенціал для вирішення складних завдань, таких як комп'ютерне бачення та обробка природної мови, які перевершують як звичайне програмування, так і інші методи машинного навчання [2].

Глибоке навчання не тільки може принести корисні результати там, де інші методи виходять з ладу, але також можуть створювати більш точні моделі, ніж інші методи, і може скоротити час, необхідний для створення корисної моделі. Однак навчання моделей ГН вимагає великої обчислювальної потужності. Іншим недоліком ГН є складність інтерпретації глибоких моделей навчання. Визначальною ознакою ГН є те, що навчальна модель має більше одного прихованого шару між входом і виходом. У більшості випадків ГН означає використання глибоких нейронних мереж.

Комп'ютерний зір – це міждисциплінарна наукова область, яка займається питанням того, як комп'ютери можуть отримати розуміння на високому рівні задопомогою цифрових зображень чи відео. З точки зору інженерії, він прагне зрозуміти та автоматизувати завдання, які може виконувати зорова система людини [3]. Завдання комп'ютерного зору включають методи

отримання, обробки, аналізу та розуміння цифрових зображень, а також вилучення даних із великих розмірів реального світу з метою отримання числової або символічної інформації, наприклад у формах рішень.

Рекурентні нейронні мережі (*RNN*) — це найсучасніші алгоритми послідовної обробки даних, які використовуються в *Siri* від *Apple* і голосовому пошуку *Google*. Це перший алгоритм, який запам'ятовує вхідні дані через внутрішню пам'ять, що робить його ідеальним для завдань машинного навчання з послідовними даними.

Існує кілька архітектур нейронних мереж, призначених для виявлення об'єктів. Вони в основному поділяються на «дворівневі», такі як *R-CNN*, *fast R- CNN* і *faster R-CNN*, і «однорівневі», такі як *YOLO*.

Створення 3*D*-об'єктів може бути важким і трудомістким для людей, які не мають попереднього знання 3*D*-моделювання. Для досягнення автоматичної генерації 3*D* необхідно виконати три вимоги, щоб зробити програму простою у використанні:

- якість, вихідна роздільна здатність;
- швидкість, час генерації;
- простота і зручність використання.

Можна створити тривимірний об'єкт, використовуючи одне вхідне зображення та згорткові нейронні мережі. Це буде вважатися досить простим для третьої вимоги, зручної для споживача, при цьому потрібно перевірити обмеження вихідної роздільної здатності та часу генерації.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Müller A. Introduction to Machine Learning with Python*: *A Guide for Data Scientists* / *Müller A.*, *Guido S. – USA*: *O'Reilly Media*. – 2020. – 400 *p*.

2. *Glassner A. Deep Learning: A Visual Approach* / *A. Glassner*; *San Francisco*: *No Starch Press*. – 2021. – 776 *p*.

3. *Lakshmanan V. Practical Machine Learning for Computer Vision: End- to-End Machine Learning for Images* / *V. Lakshmanan*; *Boston: O'Reilly Media*. – 2021. – 482 *p*.

УДК 004.77

С.О.Кудренко, к.т.н.,
А.Л.Столяр
Національний авіаційний університет, Київ

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМІ ДИСТАНЦІЙНОГО СПІЛКУВАННЯ

Система дистанційної комунікації – це сукупність технологій та інструментів для віддаленого спілкування, незалежно від географічного розташування користувачів.

Безпека цих систем має критичне значення через зростаючу загрозу хакерських атак і витоку даних. Важливими аспектами є розвиток методів шифрування, антивірусного захисту та навчання цифровій безпеці адже недостатній рівень захисту може мати серйозні наслідки, включаючи втрату конфіденційності та фінансові втрати.

Виділимо наступні аспекти захисту інформації у системах дистанційного спілкування:

1. ***Використання криптографічних методів***. Криптографія – це наука про забезпечення секретності інформації [1]. Основні принципи криптографії гарантують, що лише авторизовані особи мають доступ до зашифрованих даних, що дані залишаються незмінними під час передачі, ідентифікують сторони, що комунікують між собою, та унеможливлюють відкидання факту відправлення або отримання повідомлення.

Криптографія використовує ключі для шифрування та розшифрування даних. Ключі можуть бути симетричними (один ключ для шифрування та розшифрування) або асиметричними (два ключі: публічний для шифрування та приватний для розшифрування) [1].

Процес шифрування розпочинається з вибору шифрувального алгоритму, наприклад, AES, RSA або DES. Після цього генерується ключ для шифрування і розшифрування. Для симетричного шифрування, це може бути випадковий набір символів або пароль. Для асиметричного – генерація ключової пари, яка складається з публічного та приватного ключів. Шифрування перетворює вихідні дані у шифротекст, який може бути безпечно переданий чи збережений. Розшифрування відбувається за допомогою відповідного ключа, що перетворює шифротекст у зрозумілі дані.

2. ***Захист мережевого сполучення.***

VPN захищає конфіденційність даних шляхом шифрування передачі інформації, запобігаючи підслуховуванню та зловживанням. Вона також дозволяє користувачам обходити обмеження на доступ до певних веб-ресурсів і зберігати конфіденційність під час перегляду веб-сторінок; VPN маскують IP-адреси і надають віртуальні адреси, які приховують вашу особистість, зберігаючи вашу конфіденційність і анонімність в Інтернеті. VPN забезпечує безпечне і приватне з'єднання через незахищену мережу, гарантуючи конфіденційність і безпеку передачі даних забезпечується конфіденційність і безпека передачі даних.

Фірмові файєрволи контролюють та фільтрують трафік мережі, застосовуючи набір правил на основі характеристик пакетів даних. Вони захищають мережу від несанкціонованого доступу та атак і допомагають у запобіганні перехоплення пакетів. Наприклад, Cisco ASA, Palo Alto Networks Next-Generation Firewall та Fortinet FortiGate - популярні файєрволи на ринку.

Інтрузійні системи виявлення моніторять мережевий трафік та виявляють небажані або зловмисні активності, аналізуючи пакети даних. Вони сповіщають адміністратора про підозрілу діяльність та можуть приймати заходи для блокування зловмисних дій. Популярні інтрузійні системи виявлення включають Cisco ASA, Palo Alto Networks Next-Generation Firewall та Fortinet FortiGate.

3. ***Автентифікація та авторизація.***

Автентифікація та авторизація є критичними аспектами інформаційної безпеки, оскільки вони контролюють доступ користувачів до ресурсів системи. Для надійної автентифікації рекомендується використовувати методи, такі як двоетапна перевірка, біометричні дані або апаратні ключі, замість простих паролів. Принцип найменшого доступу допомагає уникнути надання зайвих прав користувачам, тим самим запобігаючи можливим зловживанням.

Ведення журналу подій допомагає виявляти аномалії та спроби несанкціонованого доступу, а аналіз цих журналів допомагає виявити вразливості у захисті системи.

Додатковим методом захисту є обмеження часу доступу, яке запобігає можливості несанкціонованого доступу через тривалий період неактивності.

4. ***Захист даних та конфіденційності.***

Шифрування даних на рівні файлової системи дозволяє забезпечити конфіденційність інформації, збереженої на зовнішніх носіях, таких як жорсткі диски або флеш-накопичувачі. Основні переваги зашифрованої файлової системи включають збереження даних в зашифрованому вигляді, що унеможливлює доступ до них без правильного ключа шифрування; захист від випадкової втрати даних шляхом обмеження доступу до них без відповідного ключа; контроль доступу до даних шляхом вимоги правильного ключа шифрування.

Популярні зашифровані файлові системи включають BitLocker, FileVault та VeraCrypt.

5. ***Планування та управління інцидентами безпеки***.

Планування та управління інцидентами безпеки включає наступні етапи [2]:

1. Підготовка: імплементація методів захисту і оцінка ризиків.
2. Виявлення: спостереження за аномальною поведінкою системи та змінами даних.
3. Оцінка: аналіз можливих наслідків та впливу інциденту.
4. Реагування: розробка та втілення планів протидії інциденту.
5. Аналіз та вдосконалення: аналіз слабких місць та упередження подібних інцидентів у майбутньому.

Вище висвітлено загальний підхід, але кожна організація може розробити власний план з урахуванням своїх потреб та ресурсів.

Далі наведені практичні рекомендації щодо захисту інформації в системах віддаленого зв'язку:

1. Використовуйте надійні паролі: створюйте складні паролі з комбінацією великих і малих літер, цифр і спеціальних символів. Використовуйте унікальні паролі для кожної онлайн-платформи або сервісу та регулярно змінюйте їх.
2. Увімкніть двоетапну перевірку: використовуйте функції двоетапної перевірки, такі як одноразові паролі та автентифікація мобільних пристроїв, щоб підвищити безпеку при вході в систему.
3. Оновлюйте програмне забезпечення: регулярно оновлюйте всі програми, в тому числі ті, що використовуються для віддаленого спілкування.
4. Використовуйте безпечні канали зв'язку: використовуйте зашифровані з'єднання HTTPS для передачі інформації та уникайте використання відкритих або незахищених мереж Wi-Fi.

5. Керуйте правами доступу: дозволяйте доступ до системи лише необхідним користувачам і встановлюйте права доступу відповідно до їхніх ролей та обов'язків. Регулярно переглядайте та відкликайте непотрібні права доступу.

6. Створюйте резервні копії даних: регулярно створюйте резервні копії важливих даних і зберігайте їх на захищених носіях або в хмарі, щоб запобігти втраті даних у разі інциденту.

7. Навчайте користувачів: розповідайте користувачам про основи кібербезпеки та небезпеки, пов'язані з віддаленим спілкуванням.

8. Моніторинг та виявлення: встановіть механізми моніторингу та виявлення вторгнень для своєчасного виявлення підозрілої активності.

9. Аудит безпеки Проводьте регулярний аудит безпеки систем віддаленого зв'язку, щоб виявити вразливі місця та вжити заходів.

Таким чином, використання основних методів захисту інформації в системах дистанційного спілкування є важливим елементом безпечного та конфіденційного обміну даними. Забезпечення безпеки вимагає комплексного підходу, що включає технічні, організаційні та людські аспекти, а також постійного вдосконалення для адаптації до нових загроз і ризиків.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Гомонай О. В. Криптографія. URL: https://esu.com.ua/article-1576 (дата звернення: 08.04.2024).

2. Швець О. Ю., Лазаренко В. В. Аналіз методів і засобів захисту інформації та сучасних вимог до них. URL: http://www.rusnauka.com/25_DN_2008/Informatica/28842.doc.htm (дата звернення: 08.04.2024).

УДК 681.3

Ю.О.Кулаков, к.т.н.,
Д.В.Коренко
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ

МЕТОД БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В МЕРЕЖАХ SDN З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Підходи штучного інтелекту (AI) та машинного навчання (ML) відіграють ключову роль в розв'язанні широкого спектру складних проблем, що виникають у сучасних мережах. Серед цих завдань можна відокремити маршрутизацію, класифікацію трафіку, кластеризацію потоків, виявлення вторгнень, балансування навантаження, виявлення збоїв, оптимізацію якості обслуговування (QoS), поліпшення якості користування (QoE), контроль доступу та розподіл ресурсів.

У контексті Software-Defined Networking (SDN) взаємодія між AI та ML стає особливо важливою. Дослідження [1] вказує на те, що зростання ролі AI в SDN є значущим та відображає напрямок розвитку промисловості та наукового співтовариства. Цей рух відзначається впровадженням різноманітних підходів AI в архітектуру SDN.

Серед найбільш поширених методів вирішення проблем в мережах можна визначити машинне навчання (ML), мета-евристику та вибірковий пошук (FS). Ці підходи відзначаються високою ефективністю та гнучкістю у вирішенні різноманітних завдань, таких як адаптація до змін у трафіку, оптимізація роботи маршрутизації, та підвищення загальної продуктивності та надійності мережевого середовища. Такий симбіоз ШІ та SDN відкриває нові можливості для ефективного керування та оптимізації мережевих систем у сучасних інформаційних технологіях.

Нинішні дослідження в сфері балансування навантаження у багатошляхових мереж активно розглядають проблематику балансування навантаження. У низці наукових досліджень, що стосуються оптимізації балансування мережевого навантаження в архітектурі SDN, були висунуті різноманітні системи

балансування [2-3]. У таких системах контролер використовується для аналізу інформації, отриманої від комутаторів OpenFlow, та вносить зміни в таблиці потоків відповідно до стратегії балансування навантаження.

Проте, більшість досліджуваних стратегій відносяться до статичних методів балансування навантаження, що обмежує їхню здатність адаптивно реагувати на динамічні зміни у стані навантаження мережі в режимі реального часу. Важливо відзначити, що ці методи не використовують на повну можливість SDN, оскільки не враховують глобальний погляд на структуру мережі та не взаємодіють із всіма її компонентами.

Однією з найважливіших аспектів подальшого дослідження в цьому напрямі є розробка більш адаптивних та гнучких стратегій балансування навантаження в архітектурі SDN, які використовують всі переваги цієї технології та здатні ефективно враховувати та реагувати на динамічні зміни у мережевому середовищі.

Авторами запропоновано використовувати систему підвищення ефективності використання ресурсів мережі SDN за рахунок використання модуля балансування навантаження на базі штучного інтелекту для обрахунку оптимальних маршрутів передачі пакетів у мережі спираючись на особливості корпоративних SDN мереж.

Для належного відображення стану завантаження кожного маршруту використовуються критерії оцінки, такі як коефіцієнт використання пропускної здатності, втрати пакетів, затримка передачі та кількість стрибків для передачі пакетів. Ці параметри є основними для визначення ефективність та навантаження на кожному маршруті, що дозволяє системі адаптивно реагувати на зміни в умовах мережі та обирати оптимальні шляхи для передачі даних. Застосування цих критеріїв оцінки сприяє вдосконаленню стратегії балансування навантаження, забезпечуючи оптимальні рішення у реальному часі.

Для вибору оптимального маршруту з найменшим завантаженням в мережі, необхідно аналізувати інтегровану інформацію про стан завантаження шляхів. Використання

методів машинного навчання в цьому процесі важливо для покращення продуктивності та якості обслуговування мережі. Обчислювальна модель штучної нейронної мережі, яка є нелінійною та самоадаптивною, може бути ефективним інструментом для цієї задачі. У порівнянні з іншими методами машинного навчання, такими як логістична регресія, штучна нейронна мережа не обмежена векторами введення, що робить її ефективною для обробки невизначених даних трафіку в мережі.

Застосування запропонованої схеми сприяє підвищенню ефективності використання ресурсів мережі SDN та забезпечує оптимальне розподілення навантаження, що в результаті сприяє підвищенню продуктивності та якості обслуговування у системах передачі даних.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Y.O. Kulakov, D.V. Korenko (2023). Methods of applying artificial intelligence in software-defined networks. Problems of Informatization and Control, Vol. 1 No. 73 (2023).

2. Kulakov, Yurii, and Dmytro Korenko. "Modified Method of Traffic Engineering in DCN with a Ramified Topology." International Journal of Advanced Computer Science and Applications 12.12 (2021).

3. Korenko, Dmytro, et al. "Creation of the method of multipath routing using known paths in software-defined networks." Technology audit and production reserves 4.2 (66) (2022): 19-24.

УДК 004.77

Ю.О.Кулаков, д.т.н.,
О.В.Череватенко
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

ДИНАМІЧНА РЕКОНФІГУРАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЇ SDN

Практика використання комп'ютерних мереж останніми десятиліттями демонструє декілька основних моментів. По-перше, на будь-якому рівні та масштабі мережі ручне управління є малоефективним, а з погіршенням якості обладнання проблеми з мережею стають дедалі частішими. По-друге, пропускна можливість мереж досі є некомфортною для користувачів, що активно перейшли на використання мобільних пристроїв та більш потужних комп'ютерів. Накладаючись одне на одного, ці недоліки перетворюють процес адміністрування на довгу проблемну роботу системного адміністратора.

Це означає, що існує необхідність виконати, щонайменше, два важливих завдання – спроектувати мережу таким чином, щоб була можливість безперебійного обслуговування користувачів та якомога менша ймовірність виходу з ладу елементів мережевої системи, а також створити таке управління, щоб нічого не залежало від людського фактору, що, в свою чергу, знизить ймовірність помилок при підключеннях.

При цьому існує очевидна проблема з тим, що чим більше ускладняється конфігурація мережевих елементів, тим збільшується ймовірність виходу з ладу окремих ланок мережі, що буде спричиняти порушення роботи усієї мережі, особливо тієї, що має багато сусідніх з'єднань. Іншим проблемним моментом є швидкість з'єднання на перевантажених точках доступу, що через певні апаратні обмеження не мають змоги обслуговувати усіх користувачів з необхідною швидкістю. Тому пошук можливостей автоматизації конфігурування обладнання та виключення людського фактору є однією з найбільш пріоритетних задач у галузі мережевих технологій станом на сьогодення.

Подібні проблеми вирішує технологія SDN, або мереж, що програмно конфігуруються. Її суть полягає в тому, що роботу по конфігуруванню мережевих елементів виконує спеціальне

програмне забезпечення, яке регулює маршрутизацію, оптимізує трафік, та виконує динамічне переналаштування (реконфігурацію) тих ланок, що перестали відповідати. Це дозволяє перевести регулювання усією системою в повністю автоматичний режим та вирішити проблеми, зазначені вище [1].

Переведення адміністрування мережі у автоматичний режим передбачає не лише встановлення з'єднання між частинами мережі за допомогою програмних засобів, які має в своєму розпорядженні центральний контролер, а й формування валідної та правильно структурованої маршрутної інформації, від якої буде залежати взаємозв'язок у мережі та правильність надсилання пакетів від одного елементу до іншого.

Авторами був запропонований метод динамічної реконфігурації комп'ютерної мережі, що дозволяє при малих часових витратах виконати переналаштування вузлів мережі та перебудову каналів зв'язку таким чином, щоб обійти проблемну ділянку. Проведені експерименти на SDN-контролері ONOS довели ефективність обраного рішення порівняно з існуючими методами вирішення проблеми періодичних виходів з ладу ланок мережі (рис. 1) [2].

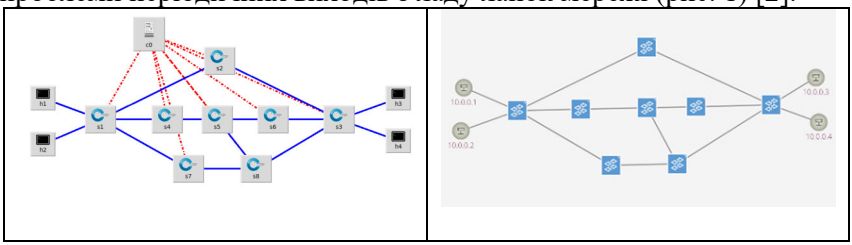


Рис.1. Представлення топології мережі при моделюванні.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Череватенко О., Кулаков Ю. Моделювання маршрутизації з використанням відомих маршрутів за допомогою SDN-контролера ONOS. (2023). Проблеми інформатизації та управління - №2(74). – ст. 55-61. https://doi.org/10.18372/2073-4751.74.17882

2. Cherevatenko, O., Kulakov, Y., Korenko, D., & Rusinov, V. (2022). Creation of the method of multipath routing using known paths in software-defined networks. Technology Audit and Production Reserves, 4(2(66), 19–24.

УДК 004.93’1

Ю.В.Лукаш,
Національний авіаційний університет, Київ

МЕТОД АВТОМАТИЗОВАНОГО СТВОРЕННЯ ДАТАСЕТУ ДЛЯ НЕЙРОМЕРЕЖІ РОЗПІЗНАВАННЯ ОБРАЗІВ

У сучасному світі все більшого поширення набувають різні методи штучного інтелекту, зокрема нейромережі. Цю технологію застосовують для вирішення найрізноманітніших задач. Наприклад, свою ефективність методи ШІ показують у розпізнаванні та детекції зображень. На базі результатів роботи даних алгоритмів вирішують різні прикладні задачі в сфері безпеки, автотранспорті, безпілотній авіації.

Для розробки ефективної моделі для нейронної мережі важливу роль відіграє процес навчання та підготовки великого різноманітного датасету [1] – готових зображень, до яких створюється анотація, що вказує, до якого саме класу відноситься конкретне зображення. Таких зображень потрібно сотні і тисячі на кожен клас, який нейромережа повинна навчитися класифікувати. На ручну підготовку такого набору вхідних даних йде велика кількість часу роботи людини, яка повинна знайти підходящі зображення та розбити їх на категорії[2].

Для навчання спеціальної, легкої нейронки-класифікатора, котра повинна з високою швидкодією працювати на борту БПЛА, було поставлено задачу згенерувати датасет. Вимога до розмірності вхідного зображення повинно бути 64x64 пікселі.

Для того, щоб зекономити затрачений час на підготовку датасету, запропоновано використати інший тип нейронної мережі – детектор об’єктів. Детектор виконує класифікацію та водночас локалізацію об’єкта на зображенні або відео-потоці[3].

Результатом детекції є клас об’єкту, його локалізація у вигляді bounding-box та впевненість з якою алгоритм виявив об’єкт.

Було розроблено програму на мові програмування Python, яка запускає загальнодоступний добре навчений алгоритм детекції об’єктів на наявних відео та оброблює результат детекцій так, щоб на виході отримати набори зображень придатні для використання в якості навчальних даних для нейромережі-класифікатора.

Для реалізації обробки, що описана вище – використано поріг, по якому беруться до уваги лише детекції з високим рівень

впевненості, що об'єкт відноситься саме до цього класу. Реалізовано фільтрування по шуканим класам – так як детектор навчений визначати 40 різноманітних класів об'єктів, а для розроблюваного класифікатора потрібні лише 4 класи об'єктів. І найголовніший процес – нормалізації знайденого зображення. Детектор може виділити результат прямокутником. Якщо його одразу трансформувати в зображення 64x64, необхідне для навчання класифікатора – то отриманий результат буде мати викривлення і погіршить загальний результат навчання. Тому було обрано підхід, де спочатку прямокутник розширюється до розмірів квадрату, а вже потім вся область нормалізується до 64x64.

Такий підхід дозволяє швидко готувати набори зображень для навчання в специфічних умовах – наприклад, залежних від пори року або часу доби. Також цей підхід дозволяє використовувати ефективний, хоч і вимогливий до обчислювальної потужності, алгоритм детекції для точного розпізнавання[3], так як цей процес не вимагає роботи в реальному часі, та може навіть оброблювати відео в великому розширенні.

Запропонований метод та розроблена програма дозволяють суттєво скоротити час на підготовку навчальної вибірки зображень для нейромережі-класифікатора. Це дає можливість змінювати, порівнювати та покращувати навчальні та контрольні вибірки для розроблювальної нейромережі-класифікатора.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Alzubaidi, L., Bai, J., Al-Sabaawi, A., etal. A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications. – 2023 – Journal of Big Data, 10 (1), art. no. 46 - doi: 10.1186/s40537-023-00727-2

2. Dempster, A., Petitjean, F., Webb, G.I. - ROCKET: exceptionally fast and accurate time series classification using random convolutional kernels – 2020 – Data Mining and Knowledge Discovery, 34 (5), pp. 1454-1495 doi: 10.1007/s10618-020-00701-z

3. Zaidi, S.S.A., Ansari, M.S., Aslam, A. etal. A survey of modern deep learning-based object detection models. – 2022 – Digital Signal Processing: A Review Journal – vol. 126 – art. no. 103514 doi: 10.1016/j.dsp.2022.103514

УДК 004.056.53

А. А.Малахова,
А.Д.Данилов
Харківський національний університет радіоелектроніки, Харків

ЮРИДИЧНІ ТА ЕТИЧНІ АСПЕКТИ ЗБОРУ МЕРЕЖЕВИХ АРТЕФАКТІВ: БАЛАНС МІЖ БЕЗПЕКОЮ ТА КОНФІДЕНЦІЙНІСТЮ

Збір мережевих артефактів стає все більш поширеним явищем у міру зростання кіберзлочинності та кібератак. Ці дані можуть бути цінними для розслідувань, кібербезпеки та аналізу даних. Однак збір мережевих артефактів також викликає ряд юридичних та етичних питань, пов'язаних з конфіденційністю та безпекою.

Юридичні аспекти включають у себе закони про конфіденційність, комп'ютерні злочини та про захист даних [1].

Багато країн мають закони, які захищають конфіденційність особистої інформації. Збір мережевих артефактів може призвести до збору особистої інформації, тому важливо дотримуватися цих законів. GDPR - це закон Європейського Союзу, який захищає особисті дані. GDPR може застосовуватися до організацій, які збирають мережеві артефакти, навіть якщо вони не знаходяться в ЄС. ЗПД - це закон України, який захищає персональні дані.

Деякі країни мають закони, які забороняють несанкціонований доступ до комп'ютерних систем. Збір мережевих артефактів може призвести до несанкціонованого доступу, тому важливо дотримуватися цих законів. Конвенція про кіберзлочинність - це міжнародний договір, який визначає комп'ютерні злочини. Конвенція може застосовуватися до організацій, які збирають мережеві артефакти, які є доказами комп'ютерних злочинів [3].

Деякі країни мають закони, які вимагають від організацій зберігати дані протягом певного періоду часу. Це може мати наслідки для організацій, які збирають мережеві артефакти. Директива про збереження даних - це директива ЄС, яка вимагає від провайдерів телекомунікаційних послуг зберігати метадані про телефонні дзвінки та текстові повідомлення протягом певного періоду часу. Директива може застосовуватися до організацій, які збирають мережеві артефакти, які містять метадані [2].

Етичні аспекти говорять про конфіденційність, безпеку та прозорість. Збір мережевих артефактів може призвести до

вторгнення в приватне життя людей. Важливо збирати лише необхідні дані, вживати заходів для захисту зібраних даних, бути прозорим щодо того, які дані збираються, як вони використовуються та хто отримує до них доступ.

Важливо знайти баланс між безпекою та конфіденційністю при зборі мережевих артефактів. Рекомендується використовувати політику мінімальних даних, псевдонімізацію та анонімізацію, шифрування, вживати заходів для кібербезпеки, таких як регулярне оновлення програмного забезпечення, використання сильних паролів, проведення регулярних перевірок безпеки [5].

Збір мережевих артефактів є цінним інструментом для розслідувань, кібербезпеки та аналізу даних. Однак важливо знати про юридичні та етичні аспекти, пов'язані з цією діяльністю. Організації, які збирають мережеві артефакти, повинні вжити заходів для захисту конфіденційності даних та дотримання відповідних законів [4].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Boiko A. M. Legal regime of biometric personal data protection california consumer privacy act. Juridical scientific and electronic journal. 2021. No. 10. P. 369–370. URL: https://doi.org/10.32782/2524-0374/2021-10/94 (дата звернення: 05.03.2024).

2. Califf R. M., Muhlbaier L. H. Health Insurance Portability and Accountability Act (HIPAA). Circulation. 2003. Vol. 108, no. 8. P. 915–918. URL: https://doi.org/10.1161/01.cir.0000085720.65685.90 (дата звернення: 05.03.2024).

3. GDPR ENFORCEMENT. EU General Data Protection Regulation (GDPR), third edition. 2019. P. 285–297. (дата звернення: 05.03.2024).

4. Vilasau M. Directive 2006/24/EC on the retention of electronic communications traffic data: security v. privacy. IDP Revista de Internet Derecho y Política. 2006. No. 3. URL: https://doi.org/10.7238/idp.v0i3.398 (дата звернення: 05.03.2024).

5. Авраменко А. В. Принципи захисту персональних даних працівників. Актуальні проблеми держави і права. 2019. № 82. С. 3–9. URL: https://doi.org/10.32837/apdp.v0i82.39 (дата звернення: 05.03.2024).

УДК 004.2

[1]**А.О.Мельник,** д.т.н.,
[2]**Ю.В.Морозов,** к.т.н.,
[2]**Б.І.Гаваньо,** д.ф.,
[3]**П.А.Гупало**
[1]ІТ СТЕП Університет, Львів
[2]Національний університет «Львівська політехніка», Львів
[3]ТОВ Інтрон, Львів

СПОСІБ АНОНІМІЗАЦІЇ ДАНИХ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

Розробка моделей і алгоритмів для анонімізації даних (АД) у сервісах на основі Інтернету речей (IoT) має важливе значення [1], чому є кілька причин:

- Захист конфіденційності: пристрої IoT генерують великі обсяги даних, які часто містять конфіденційну або особисту інформацію.
- Відповідність нормативним вимогам: багато регіонів і країн прийняли правила захисту даних і конфіденційності, наприклад Загальний регламент захисту даних (GDPR) Європейського Союзу.
- Обмін даними та співпраця. Методи АД дозволяють організаціям обмінюватися даними IoT із зовнішніми сторонами, такими як дослідницькі інститути або сторонні постачальники послуг, зберігаючи при цьому конфіденційність.
- Зменшення ризиків: до надання послуг на основі IoT задіяні багато зацікавлених сторін, включаючи виробників пристроїв, постачальників послуг і кінцевих користувачів.
- Довіра та прийнятність користувачів: жорсткі засоби захисту конфіденційності, такі як АД, підвищують довіру користувачів і сприймають служби IoT.

Організації повинні запровадити комплексну стратегію конфіденційності, яка включає крім АД додаткові засоби захисту, такі як контроль доступу, шифрування та мінімізація даних, щоб забезпечити загальну безпеку та конфіденційність служб із підтримкою Інтернету речей. Етапи способу АД у сервісах на основі IoT:

1. Уся ідентифікаційна інформація в системі збору та обробки даних зберігається та обробляється лише на сервері автентифікації довіреної третьої сторони.

2. Усі сеанси зв'язку в системі збору та обробки даних шифруються за допомогою протоколу TLS.

3. Дані анонімізують шляхом видалення всіх ідентифікаторів і заміни їх на зашифрований маркер JWT із коротким часом життя.

4. Після отримання на сервері дані повторно анонімізують шляхом додавання динамічного ідентифікатора.

5. Щоб протидіяти диференціальному аналізу, динамічний ідентифікатор узагальнюється, змінюючись щогодини.

Вищеописаний спосіб дозволяє протистояти атакам на конфіденційність, до числа яких належать наведені нижче.

Атака на розкриття особи. Ми використовуємо узагальнення, щоб протистояти атаці розкриття особи. Навіть якщо супротивник має додаткову інформацію про особу, розкрити особу неможливо, оскільки неможливо відновити ідентифікаційну інформацію.

Атака на розкриття членства. Запропонована модель є ефективною для захисту таблиці записів від розкриття членства за допомогою методів повторної АД.

Атака на розкриття атрибутів. Ми протидіємо такій атаці за допомогою методів узагальнення, де сіль змінюється щогодини.

Атака схожості. Ми протидіємо такій атаці за допомогою методів повторної АД, коли сіль змінюється для кожного запису.

Напад косоподібності. Запропонована модель протистоїть атакам з перекосом, розподіляючи конфіденційні атрибути в узагальненому наборі записів ближче до загального розподілу атрибутів у таблиці.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *A.Melnyk, Y.Morozov, B.Havano, B.J.Le, P. Hupalo, "Protection of data transmission in remote monitoring tools by anonymization // CEUR Workshop Proceedings". – 2023. – Vol. 3373: Proceedings of the 4th International workshop on intelligent information technologies & systems of information security, Khmelnytskyi, Ukraine, March 22–24, 2023. – P. 452–463.*

УДК 004.4

П.І.Мельниченко
Національний авіаційний університет, Київ

АНАЛІЗ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ БЕЗПЕЧНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Життєвий цикл розробки програмного забезпечення (ЖЦ) – це структурований процес, який дозволяє створювати високоякісне недороге програмне забезпечення витрачаючи якнайменше часу [1]. Метою ЖЦ є створення якісного програмного забезпечення, яке відповідає та перевершує всі очікування та вимоги клієнтів. ЖЦ визначає та окреслює детальний план із етапами або фазами, кожна з яких охоплює власний процес та результати.

Початкова концепція та створення ЖЦ розглядали діяльність із забезпечення безпеки лише як окреме та єдине завдання, яке виконується в рамках етапу тестування. Недоліками такого підходу була неминуча велика кількість вразливостей чи помилок, виявлених надто пізно у процесі, а в деяких випадках не виявлених взагалі. На даний час є зрозумілим, що безпека має вирішальне значення для успішного ЖЦ, та що інтеграція заходів безпеки в рамках ЖЦ допомагає створювати більш надійне програмне забезпечення. Завдяки включенню методів та заходів безпеки на більш ранні етапи ЖЦ виявлення вразливостей та їх усунення буде відбуватись значно раніше, тим самим зменшуючи загальний час та вартість виправлення на більш пізніх етапах життєвого циклу.

Життєвий цикл розробки програмного забезпечення включає в себе наступні етапи: аналіз вимог, проєктування, розробка, тестування, розгортання, експлуатація та підтримка.

Для подальшого аналізу можемо записати математичну модель життєвого циклу розробки програмного забезпечення у загальному вигляді, як множину елементів розробки:

$$ММ_{\text{ЖЦ}} = \{X_{\text{ав.}}, X_{\text{пр.}}, X_{\text{розроб.}}, X_{\text{тест.}}, X_{\text{розгор.}}, X_{\text{екс.}}\},$$

де $X_{\text{ав.}}$ – аналіз вимог, $X_{\text{пр.}}$ – проєктування, $X_{\text{розроб.}}$ – розробка, $X_{\text{тест.}}$ – тестування, $X_{\text{розгор.}}$ – розгортання, $X_{\text{екс.}}$ – експлуатація та підтримка.

Оскільки кожен етап життєвого циклу розробки програмного забезпечення складається з певних дій, то можемо записати математичну модель життєвого циклу розробки програмного

забезпечення, як множину з елементів, які, у свою чергу, також є множинами:

$MM_{\text{жц}} = \{\{X_{\text{ав}}\}, \{X_{\text{пр.}}\}, \{X_{\text{розроб.}}\}, \{X_{\text{тест.}}\}, \{X_{\text{розгор.}}\}, \{X_{\text{екс}}\}\}$,

Кожна множина при цьому складається з наступних елементів:

$\{X_{\text{ав}}\} = \{X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8\}$,

де X_1 – це планування, X_2 – визначення об'єму проєкта, X_3 – процес навчання розробників, X_4 – постановка цілей та завдань, X_5 – визначення вимог безпеки, X_6 – визначення показників та звітність про відповідність, X_7 – планування ресурсів, X_8 – моделювання загроз.

$\{X_{\text{пр.}}\} = \{X_3, X_5, X_6, X_8, X_9, X_{10}, X_{11}, X_{12}, X_{13}, X_{14}\}$,

де X_9 – це визначення функціональних вимог, X_{10} – це визначення технічних вимог, X_{11} – перегляд вимог та їх схвалення, X_{12} – встановлення вимог безпеки щодо проєктування, X_{13} – визначення та використання стандартів криптографії, X_{14} – управління ризиком безпеки, пов'язаним із використанням сторонніх компонентів.

$\{X_{\text{розроб.}}\} =$

$= \{X_3, X_5, X_6, X_8, X_{12}, X_{13}, X_{14}, X_{15}, X_{16}, X_{17}, X_{18}, X_{19}, X_{20}, X_{21}, X_{22}\}$

де X_{15} – написання стандартного коду, X_{16} – написання масштабованого коду, X_{17} – створення бази даних, X_{18} – інтеграція необхідних сервісів, X_{19} – використання безпечних інструментів, X_{20} – виконання тестування безпеки статичного аналізу, X_{21} – перегляд коду, X_{22} – створення функціональної та технічної документації.

$\{X_{\text{тест.}}\} = \{X_3, X_6, X_8, X_{13}, X_{14}, X_{19}, X_{20}, X_{23}, X_{24}, X_{25}, X_{26}, X_{27}, X_{28}\}$,

де X_{23} – проведення функціонального тестування коду, X_{24} – перевірка відповідності вимогам технічного завдання, X_{25} – перевірка на продуктивність, X_{26} – виконання тестування безпеки динамічного аналізу, X_{27} – проведення тестування на проникнення, X_{28} – створення стандартного процесу реагування на інциденти.

$\{X_{\text{розгор.}}\} = \{X_3, X_8, X_{19}, X_{20}, X_{26}, X_{27}, X_{28}, X_{29}, X_{30}, X_{31}\}$,

Де X_{29} – планування релізу, X_{30} – автоматичне розгортання, X_{31} – навчання користувачів.

$\{X_{\text{екс}}\} = \{X_3, X_8, X_{20}, X_{26}, X_{27}, X_{28}, X_{32}, X_{33}, X_{34}, X_{35}, X_{36}\}$,

де X_{32} – виправлення помилок, X_{33} – підтримка користувачів, X_{34} – внесення змін та створення нового функціоналу, X_{35} – нагляд

за програмним забезпеченням, X_{36} – аналіз роботи програмного забезпечення.

Кожному етапу життєвого циклу розробки програмного забезпечення відповідає одна або декілька дій, що пов’язані з забезпеченням безпеки [2]. На рис. 1 зображено теплову карту відношення безпекових дій до кожного етапу життєвого циклу. Найяскравішим помаранчевим кольором позначено етапи, на яких приділяється найбільша увага безпековим діям, у міру спадання використання колір змінюється до більш світлішого. Синім кольором позначаються етапи, на яких безпекові дії зовсім не відбуваються.

Рис.1. Теплова карта відповідності дій безпеки до етапів життєвого циклу розробки програмного забезпечення

Проведений аналіз дав змогу сформувати математичну модель життєвого циклу розробки безпечного програмного забезпечення з урахуванням безпекових дій, що є базисом безпечної розробки. Створена на основі математичної моделі теплова карта відповідності дій безпеки до етапів життєвого циклу відтворює процес розробки безпечного програмного забезпечення, як множини елементів, що починаються на перших етапах роботи над проєктом та продовжуються весь цикл розробки, до того ж більшість дій виконуються одночасно. Це дає можливість оцінити наскільки процес забезпечення безпеки є неперервним впродовж усього життєвого циклу розробки, та яку значну роль у розробці він займає.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Software Development Life Cycle (SDLC) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.synopsys.com/glossary/what-is-sdlc.html

2. What are the Microsoft SDL practices? [Електронний ресурс]. – Режим доступу до ресурсу: https://www.microsoft.com/en-us/securityengineering/sdl/practices

3. Сеспедес Гарсія, Н., & Сеспедес Гарсія, П. (2023). МОДЕЛІ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ. Молодий вчений, 2 (114), 17-20. https://doi.org/10.32839/2304-5809/2023-2-114-4

УДК 004.056.53

Н.А.Москвичова, к.т.н.,
Н.О.Шибаєва, д.т.н.
Національний університет «Одеська політехніка», Одеса

ІНТЕГРОВАНА ЕЛЕКТРОННА ПЛАТФОРМА ДЛЯ ОПТИМІЗАЦІЇ ПРОЕКТУВАННЯ ТА УПРАВЛІННЯ КОМП'ЮТЕРНИМИ СИСТЕМАМИ В УМОВАХ ЗМІНИ ПАРАДИГМИ НАВЧАННЯ

У сучасному освітньому середовищі, яке постійно зазнає змін, виникає необхідність в інноваційних підходах до проектування та управління комп'ютерними системами. Однією з ключових стратегій є використання інтегрованих електронних платформ, які сприяють оптимізації цих процесів. Зокрема, в контексті зміни парадигми навчання, що передбачає більший акцент на самостійному навчанні та співпраці, електронні платформи стають ключовим інструментом для забезпечення якісної освіти.

В [1] розглядається роль технологій у сучасному навчальному процесі та виклики, пов'язані з утриманням студентів на онлайн платформах з огляду на фактори впровадження технологій та результатів навчання. Було зазначено, що, незважаючи на численні переваги онлайн-навчання, важкість збереження студентів на цих платформах є серйозною проблемою з високим рівнем відпаду. Щоб залучити студентів до онлайн-навчання та забезпечити їхню активність, автори розглядають інтеграцію віртуальних спільнот у навчальний процес.

Основний акцент робиться на необхідності залучення студентів до навчання за допомогою віртуальних спільнот, що може покращити їхню активність та результати. Автори обговорюють стратегії залучення, такі як надання зворотного зв'язку та співпраця, а також вказують на необхідність подальших досліджень щодо використання віртуальних спільнот у навчальному процесі.

Цілі дослідження [2] включають у себе організацію порівняльного аналізу платформ дистанційного навчання відповідно до критеріїв (функції системи, підтримка контенту, створення контенту, керування користувачами, звітність), проведення консультацій з викладачами університету з метою висвітлення переваг систем дистанційної освіти з точки зору

викладача, а також аналізи результатів тестування онлайн-платформ для навчання студентами, щоб з'ясувати їх вплив на академічну успішність.

Консультуючись із 40 викладачами університетів по всьому світу, були виділені наступні переваги дистанційних платформ:

- більша свобода доступу до матеріалів;
- нижча вартість навчання;
- можливість поділу змісту електронного курсу на модулі;
- гнучкість навчання;
- здатність не відставати від сучасного темпу життя;
- можливість визначення чітких критеріїв оцінювання знань.

Результати тестування студентів після користування електронною освітньою платформою показали, що учасники покращили свої результати, при цьому найбільш суттєве покращення відбулося серед студентів з «незадовільними» оцінками

Аналіз результатів впровадження систем дистанційного навчання дозволяють стверджувати, що такі платформи допомагають зробити освіту доступнішою та зручнішою. Інтегровані електронні платформи виявляються необхідним інструментом для сучасного освітнього процесу, зокрема в галузі комп'ютерних систем. Вони сприяють покращенню якості навчання, забезпечуючи студентам та викладачам зручні та ефективні інструменти для співпраці та досягнення навчальних цілей.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Ritanjali Panigrahi, Praveen Ranjan Srivastava, Dheeraj Sharma, Online learning: Adoption, continuance, and learning outcome—A review of literature, International Journal of Information Management, Volume 43, 2018,Pages 1-14.

2. Liu, Z.Y., Lomovtseva, N. & Korobeynikova, E. (2020). Online Learning Platforms: Reconstructing Modern Higher Education. International Journal of Emerging Technologies in Learning (iJET), 15(13), 4-21. Kassel, Germany: International Journal of Emerging Technology in Learning.

УДК 004.415

М.О.Московко,
О.П.Мартинова, к.т.н.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SDN В ПОЛЬОВИХ УМОВАХ

Ідея створення та використання програмно-визначених мереж (англ. SDN або Software Defined Networks) виникла ще давно та користується популярністю вже більше 10 років [4]. SDN є парадигмою програмування, що полягає в відокремленні рівня управління від рівня передавання інформації (control and data plane). Зокрема OpenFlow протокол надає стандартизований інтерфейс для управління даними рівнями.

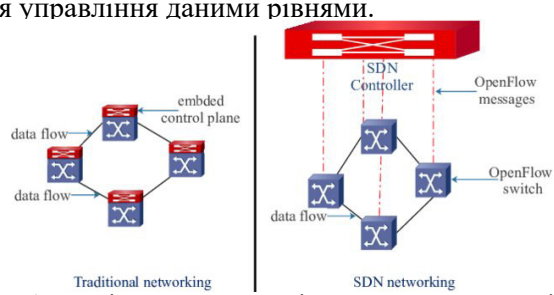


Рис. 1. Порівняння традиційної та SDN мережі [5]

Сьогодні SDN мережі почали привертати до себе багато уваги у військовій сфері. Чітко розмежовуючи площини управління і пересилання даних, SDN стали програмованим методом забезпечення і управління мережевими ресурсами [1]. Їх застосування для зв'язку на полі бою забезпечує наскрізний обмін даними і підтримує використання можливостей периферійних обчислень для оперативної обробки даних.

Ключовими перевагами SDN виступають:

- швидка розробка та розгортання мережевих додатків [2], що забезпечує маневреність і адаптивність в динамічних сценаріях поля бою;
- розділення мережевого обладнання та програмного забезпечення дозволяє мережевим адміністраторам централізовано керувати поведінкою мережі[3];
- високий ступінь програмовості та легкість реконфігурування мережі, що дозволяє «на льоту» коригувати поведінку мережі і полегшує адаптацію до мінливих умов [1];

- централізоване управління забезпечує кращу видимість мережевого трафіку та загроз безпеці мережі [3];
- оптимізація розподілу ресурсів шляхом динамічного налаштування мережевих шляхів, пропускної здатності та параметрів приорітезації QoS [2];

SDN відіграють вирішальну роль у вирішенні проблем відмовостійкості в умовах бойових дій, а саме у разі збоїв площини управління (наприклад, - недоступність контролера), SDN може використовувати такі механізми, як механізм груп швидкого переходу (Fast Failover groups) [6], щоб перенаправити трафік, не використовуючи контролера. Також при застосуванні декількох контролерів або розподільних контролерів, SDN забезпечує повну роботоздатність навіть якщо один з контролерів є недоступним[1]. Це досягається за рахунок постійного моніторингу всіх мережевих пристроїв та шляхів, налаштування альтернативних шляхів відводу в разі збою пристрою; швидкому реагуванню і перелаштуванню таблиць потоків та відновлення нормального потоку даних при відновленні функціонування втрачених пристроїв.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Mahmud, R., Toosi, A. N., Rodriguez, M. A., Madanapalli, S. C., Sivaraman, V., Sciacca, L., ... & Buyya, R. (2021). Software-defined multi-domain tactical networks: Foundations and future directions. Mobile Edge Computing, (pp. 183-227)

2. Doshi, B., & Cansever, D. (2018). Software defined networking for army's tactical network: Promises, challenges, and an architectural approach. CSIAC Journal, 6(3), 30-38..

3. Dorsch, N., Kurtz, F., Georg, H., Hägerling, C., & Wietfeld, C. (2014, November). Software-defined networking for smart grid communications: Applications, challenges and advantages. In 2014 IEEE international conference on smart grid communications (SmartGridComm) (pp. 422-427). IEEE.

4.Feamster, N., Rexford, J., & Zegura, E. (2014). The road to SDN: an intellectual history of programmable networks. ACM SIGCOMM Computer Communication Review, 44(2), 87-98.

5. Maaloul, R., Taktak, R., Chaari, L., & Cousin, B. (2018). Energy-aware routing in carrier-grade Ethernet using SDN approach. IEEE Transactions on Green Communications and Networking, 2(3), 844-858.

6. Yamansavascilar, B., Baktir, A. C., Ozgovde, A., & Ersoy, C. (2020). Fault tolerance in SDN data plane considering network and application based metrics. Journal of Network and Computer Applications, 170, 102780.

УДК 004(088.2)(043.2)

В.В.Нікітін,
М.М.Козуля, к.т.н.
Національний технічний університет «Харківський політехнічний інститут», Харків

ZKSNARKS ТЕХНОЛОГІЯ ДЛЯ СЕРТИФІКАЦІЇ ЦИФРОВОГО КОНТЕНТУ

Однією з характеристик сертифікованого цифрового контенту у NFT є повна публічність у Blockchain мережі. З одного боку це є перевагою, але з іншого постає питання яким чином сертифікувати документи або інший контент який може мати приховані характеристики, наприклад сертифікат з унікальною перепусткою що надає доступ до ресурсу. На сьогоднішній день не існує можливості сертифікації контенту з приватними властивостями, що значно поширює ризик крадіжки авторських прав на цифрову власність.

Метою дослідження є створення унікальної платформи для сертифікації, купівлі, продажу, обміну, захисту цифрового контенту у вигляді NFT. Головні проблеми для вирішення включають в себе застосування смарт-контрактів для забезпечення стійкості, захист авторських прав на NFT та можливість створення та підтвердження володіння сертифікатами з конфіденційними даними без їх розголошення. Це досягається за допомогою використання технологій zkSnarks та криптографічного шифрування для сертифікації контенту на блокчейні, щоб забезпечити повний захист особистої інформації та надійність процесів обробки NFT.

Генерація zkSnarks доказу відбувається за наступною формулою [1]:

1. $A = \alpha + t_0 u_0(\tau) + t_1 u_1(\tau) + \ldots + t_m u_m(\tau) + r\delta;$
2. $B = \beta + t_0 u_0(\tau) + t_1 u_1(\tau) + \ldots + t_m u_m(\tau) + s\delta;$
3. $C = \frac{t_{\varphi+1} L_{\varphi+1}(\tau)}{\delta} + \frac{t_{\varphi+2} L_{\varphi+2}(\tau)}{\delta} + \ldots \frac{t_{\varphi m} L_{\varphi m}(\tau)}{\delta} + \frac{H(\tau) Z(\tau)}{\delta} + As + Br - rs\delta.$
4. Доказ $\pi = ([A]_1, [B]_2, [C]_1)$.

Верифікація zkSnarks доказу відбувається за наступною формулою [1]:

$$[A]_1 * [B]_1 = [\alpha]_1 * [\beta]_1 + \left[\frac{c_0 L_0(\tau)}{\gamma} + \frac{c_1 L_1(\tau)}{\gamma} + \ldots + \frac{c_l L_{\varphi}(\tau)}{\gamma}\right]_1 * [\gamma]_2 + [C]_1 * [\delta]_2$$

.

На рис.1 наведено приклад NFT сертифікату з зашифрованими властивостями та zkSnarks доказ, який було згенеровано для підтвердження того що значення поля «English grade» більше ніж 85, без його розголошення. Потім даний zkSnarks доказ валідується у Blockchain мережі.

Рис.1. Генерація zkSnarks доказу
для сертифікованих цифрових даних

Отже, запропонований підхід до сертифікації має великий потенціал для забезпечення безпеки та конфіденційності сертифікованого цифрового контенту, що може сприяти подальшому розвитку ринку NFT та цифрової власності взагалі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. T. Minh. Theoretical and practical introduction to ZK-SNARKs and ZK-STARKs. — Brno, 2022. — P. 32—37.

УДК 004.056: 519.766.23

М.К.Печурін, д.т.н.,
Л.П.Кондратова, к.т..н.,
С.М.Печурін, к.т.н.
Національний авіаційний університет, Київ

МОВА ВЗАЄМОДІЇ ДЛЯ НАДЛЕГКИХ БПЛА

Вибір методів захисту мови взаємодії (комунікацій) для систем надлегких БПЛА у значній мірі залежить від того, що легкі, малопотужні літальні апарати з невеликими значеннями таких кількісних характеристик, як максимальна злітна вага, потужність передавача, доступна висота і радіус дії, рівень енергоспоживання тощо, мають суттєві обмеження в доступних інформаційно-обчислювальних та телекомунікаційних ресурсах. Невисока швидкість передачі даних через безпроводове середовище, необхідність використовувати економні обчислювальні алгоритми призводять до відносно низького рівня безпеки функціонуючих надлегких БПЛА. Способам підвищення рівня захищеності, розв'язанню проблеми організації безпечного функціонування систем взаємоповязаних БПЛА, присвячено багато публікацій, наприклад [1].

Існуюча класична універсальна методологія побудови (криптографічно) захищеної обчислювально-телекомунікаційної інфраструктури системи взаємодіючих літальних апаратів, основана на Еталонній моделі взаємодії відкритих систем, враховує вищенаведені обставини. Це «провокує» проектувальників комп'ютерного забезпечення обчислювально-телекомунікаційної інфраструктури вимагати адекватні, існуючому інструментарію реалізації протоколів Еталонній моделі взаємодії відкритих систем, ресурси програмно-апаратного забезпечення, що може не відповідати технічним можливостям обладнання літальних апаратів, зокрема – можливостям енергетичних потужностей.

Подібна ситуація, наприклад, мала місце при розробці архітектури «skatternet» Bluetooth, де обмеження на параметр вартості виробництва апаратної складової спровокували вимушене обмеження функціональних системи шляхом виключення деяких

традиційних функцій захисту на нижньому рівні Еталонної моделі взаємодії відкритих систем.

Природнім є спроби врахувати, при проектуванні систем криптографічного захисту для малопотужних літальних апаратів, ресурсні параметри шляхом (вимушеного ж) обмеження функціональних можливостей на їнших рівнях Еталонної моделі.

В доповіді розглядається один зі способів розв'язання проблеми захисту процесів взаємодії (комунікацій) між авіаційними об'єктами, що вони взаємодіють в автономному режимі, - спосіб криптографічного захисту взаємодії (комунікацій) в умовах малої потужності взаємодіючих безпілотних апаратів.

Для вивчення питання використане моделювання в класах теорії формальних граматик і мов, а також теорії кінцевих автоматів.

Пропонується релевантна (слабій доступності інформаційно-обчислювальних ресурсів), асиметрична криптографічна система захисту, основана на використанні регулярної мови взаємодії (комунікацій).

Обмеження семантичних можливостей мови компенсується простотою пропонованого однонаправленого відображення (функції), для асиметричної криптографічної системи, на множину речень мови шляхом застосування продукційних правил регулярної граматики.

Ефект криптографічного захисту мови взаємодії для надлегких БПЛА суть використання її неоднозначності при спробах несанкціонованого дешифруючого граматичного розбору.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Печурін М.К., Боярінова Ю.Є., Кондратова Л.П., Воронін М.Г., Сіренко М.А. Моделі топологій слабовипромінюючої телекомунікаційної системи взаємодіючих БПЛА. Проблеми інформатизації та управління: зб. наук. праць. — 2022. — Вип. 4 (72). — С.48-54. — DOI: 10.18372/2073-4751.72.17461.

УДК 004.056.53

П.А.Поліщук

Національний університет «Одеська політехніка», Одеса

СТРАТЕГІЯ РОЗРОБКИ ВЕБ-ЗАСТОСУНКІВ

У сучасному світі веб-застосунки відіграють важливу роль у багатьох аспектах комерційної діяльності. Від інтернет-магазинів до систем управління клієнтами, веб-застосунки дають змогу підприємствам взаємодіяти з клієнтами, управляти даними та покращувати свою ефективність. Розробка веб-застосунків, які відповідають потребам комерційного призначення, потребує ретельного планування, використання сучасних технологій та дотримання принципів проектування користувацького інтерфейсу.

Для досягнення цих мет цілком доцільно використовувати передові підходи до розробки програмного забезпечення. Ключові аспекти розробки веб-застосунків для комерційного призначення:

1. Функціональність: веб-застосунок повинен мати всі необхідні функції для підтримки бізнес-процесів підприємства.
2. Продуктивність: веб-застосунок повинен бути швидким, надійним та масштабованим, щоб задовольнити потреби користувачів.
3. Безпека: веб-застосунок повинен бути безпечним для захисту даних користувачів та підприємства.
4. Дизайн: веб-застосунок повинен мати зручний та інтуїтивно зрозумілий інтерфейс користувача.
5. Інтеграція: веб-застосунок повинен бути інтегрований з іншими системами підприємства, такими як CRM, ERP та платіжні системи.

Технології розробки веб-застосунків існує безліч, кожен з них має свою особливість, але загалом зараз найпопулярніші такі технології:

Фронт-енд: JavaScript, HTML, CSS, фреймворки (React, Angular, Vue.js).

Бек-енд: Node.js, Python, Java, PHP, .NET.

Бази даних: MySQL, PostgreSQL, MongoDB.

Розробка веб-сайту є складним завданням, схожим на створення будь-якого іншого додатку, і вимагає чіткого планування та реалізації окремих етапів. Основні кроки розробки веб-застосунку включають наступне:

Збір вимог: визначення потреб користувачів та бізнес-вимог до проекту.

Проектування: створення дизайну веб-застосунку та архітектури проекту.

Розробка: написання коду веб-застосунку.

Тестування: перевірка веб-застосунку на наявність помилок та відповідність вимогам.

Впровадження: розгортання веб-застосунку в робочому середовищі.

Підтримка: обслуговування та вдосконалення веб-застосунку.

Розробка веб-застосунків для комерційного призначення може допомогти підприємствам покращити свою ефективність, знизити витрати та збільшити прибуток. Завдяки широкому спектру доступних технологій та інструментів підприємства будь-якого розміру можуть розробити веб-застосунки, які відповідають їхнім потребам.

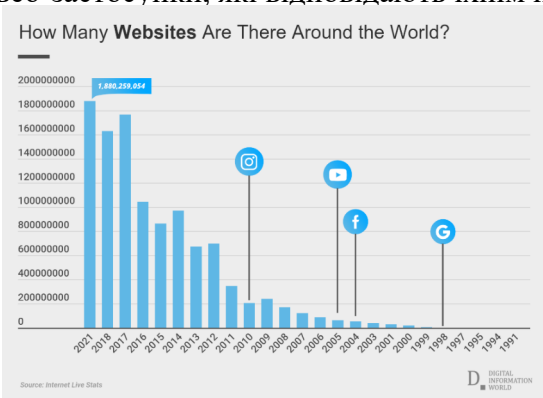


Рис. 1. Кількість веб-застосунків у світі

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Developing web applications, by IBM Corporation, Feb 26, 2024 (https://www.ibm.com/docs/en/wasdtfe?topic=developing-web-applications)*

2. *How Many Websites Are There In 2021?, by Arooj Ahmed, Aug 10, 2021 (https://www.digitalinformationworld.com/2021/08/how-many-websites-are-there-in-2021.html)*

УДК 004.056.5

[1]**О.І.Полотай,** к.т.н.,
[1]**А.П.Тераз,**
[2]**Б.В.Шаповалов**
[1]Львівський державний університет безпеки життєдіяльності, Львів
[2]Національний університет «Львівська Політехніка», Львів

СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

Тенденція останніх років свідчить про збільшення використання комп'ютерних мереж саме безпровідного типу. Мова йде про смартфони, ноутбуки, пристрої розумного будинку, тощо. Саме тому зростають ризики інформаційної безпеки таких технологій.

Відомо, що бездротовий зв'язок працює за допомогою передавання сигналів у повітрі. Бездротові сигнали можуть проникати крізь тверді об'єкти, такі як стеля, підлога і стіни, і виходити за межі будинку або офісу. Без належних заходів безпеки встановлення бездротової локальної мережі може бути синонімом встановлення портів Ethernet скрізь, навіть на вулиці.

Щоб запобігти втручанню зловмисників у бездротову мережу і захистити дані, більшість маршрутизаторів і точок доступу все ще мають дві традиційні функції безпеки: маскування SSID і фільтрацію MAC-адрес.

Маскування SSID.

На точках доступу та деяких бездротових маршрутизаторах є можливість вимикати сигнальні кадри SSID. Для під'єднання до мережі бездротові клієнти повинні налаштувати SSID вручну.

Фільтрація MAC-адрес.

Адміністратор може вручну дозволити або заборонити клієнтам бездротовий доступ на основі фізичних MAC-адрес їх апаратних засобів. На рисунку показано налаштований на маршрутизаторі дозвіл для двох MAC-адрес. Пристрої з різними MAC-адресами не зможуть приєднатися до WLAN 2,4 ГГц.

Однак, дані способи не є надійними і забезпечують слабий захист. Найкращий спосіб захистити бездротову мережу – використовувати системи аутентифікації та шифрування [1].

Відомо про два типи аутентифікації:

Відкрита аутентифікація системи – сприяє легкому під'єднанню бездротових клієнтів; повинна використовуватися тільки у випадках, коли безпека не має значення, наприклад, у кафе, готелях чи у віддалених районах при наданні вільного доступу до мережі Інтернет.

Аутентифікація зі спільним ключем – забезпечує такі механізми, як WEP, WPA, WPA2 та WPA3, для аутентифікації та шифрування даних між бездротовим клієнтом та точкою доступу. Однак для під'єднання обом сторонам потрібно попередньо надати пароль.

Шифрування використовується для захисту даних. Зловмисник, який перехоплює зашифровані дані, не може розшифрувати їх протягом певного часу [2].

Стандарти WPA і WPA2 використовують такі протоколи шифрування:

TKIP (Temporary Key Integrity Protocol) – метод шифрування, який забезпечує попакетне шифрування, що включає перевірку цілісності повідомлень та механізм повторного шифрування.

Розширений стандарт шифрування (AES) – це метод шифрування, який використовується в WPA2. Йому надається перевага, оскільки це більш надійний метод шифрування; він використовує протокол блочного шифрування CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) який дозволяє вузлам призначення розпізнати, чи були змінені зашифровані та незашифровані біти.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Belej O., Nestor N., Sadeckii J., Polotai O. Features of Application of Data Transmission Protocols in Wireless Networks of Sensors. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019. Proceedings. 2019. Article ID 8847878. P. 317–322.

2. Kukharska N.P., Lagun A.E., Polotai O.I. The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 2020. Article ID 9204108. P. 174–177.

УДК 004.056

Д.О.Пономаренко,
П.І.Іванчук
Національна академія Служби безпеки України, Київ

СУЧАСНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ: КОМПЛЕКСНИЙ ПІДХІД ДО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У сучасному світі, де інформація стає все більш цінною, кібербезпека виходить на перший план. Захист даних, мереж та систем від кіберзагроз стає життєво необхідним для приватних осіб, підприємств та урядів.

1. Класифікація кіберзагроз:

-Шкідливе програмне забезпечення (Malware): це будь-який програмний код або комп'ютерна програма, «навмисно написана з метою завдати шкоди комп'ютерній системі або її користувачам»

-Фішинг (Phishing): це спроба отримати конфіденційну інформацію, таку як імена користувачів, паролі та дані кредитної картки, безпосередньо від користувачів шляхом обману користувачів.

-Соціальна Інженерія (Social engineering): В контексті комп'ютерної безпеки спрямована на те, щоб переконати користувача розкрити такі секрети, як паролі, номери карток тощо, або надати фізичний доступ, наприклад, видаючи себе за керівника вищої ланки, банку, підрядника чи клієнта.

-Програма-вимагач (Ransomware): Програмне забезпечення, яке блокує доступ до даних та вимагає викупу за їх розблокування.

-Атака на відмову в обслуговуванні (Denial-of-service attacks): призначені для того, щоб зробити машину або мережевий ресурс недоступними для призначених користувачів.

2. Захист від кіберзагроз:

-Антивірусне програмне забезпечення:це програма, яка призначена для захисту пристроя від шкідливих програм.

-Системи виявлення вторгнення (IDS): програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу до комп'ютерної системи чи мережі або несанкціонованого управління ними в основному через Інтернет.

-Системи запобігання вторгненням (IPS): це програмний або апаратний засіб, який здійснює моніторінг мережі та комп'ютерної системи в реальному часі з метою, запобігання або блокування несанкціонованого доступу .

-Шифрування: це метод перетворення даних, щоб їх могли читати лише ті особи, в кого є доступ. У процесі шифрування відкритий текст перетворюється в зашифрований за допомогою криптографічного ключа.

3. Технології кібербезпеки: штучний інтелект (AI): Використовується для швидкого аналізу загроз та запобігання їх виникнення; машинне навчання (ML): це процес, який за допомогою машини вчаться на наданій інформації та будуючи логіку та прогнозуючи вихід для даного входу; Blockchain: ця технологія, яка дозволяє користувачам самостійно зберігати дані та редагувати і контролювати їх передачу; квантова криптографія: Використовує принципи квантової механіки для забезпечення стійкого до злому шифрування.

Роль CISA. У світі ризиків і потенційних наслідків кібернетичних подій CISA зміцнює безпеку та стійкість кіберпростору, що є важливою місією внутрішньої безпеки. CISA пропонує ряд послуг із кібербезпеки та ресурсів, зосереджених на операційній стійкості, практиках кібербезпеки, організаційному управлінні зовнішніми залежностями та інших ключових елементах надійної та стійкої кіберструктури. CISA допомагає окремим особам і організаціям повідомляти про поточні кібертенденції та атаки, керувати кіберризиками, посилювати захист і впроваджувати превентивні заходи. Кожен зменшений ризик або попереджена атака зміцнює кібербезпеку нації.

Системи та технології кібербезпеки постійно розвиваються, щоб протистояти новим та витонченим кіберзагрозам. Важливо використовувати комбінацію цих методів для забезпечення комплексного захисту інформаційних ресурсів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1) Cybersecurity & Infrstructure Security Agency https://www.cisa.gov/topics/cybersecurity-best-practices*;*

2) Computer security *https://en.wikipedia.org/wiki/Computer security*

УДК 004.032.26:621.391.8

І.Г.Прокопенко, д.т.н
А.С.Савченко, д.т.н.,
К.І.Прокопенко, к.т.н.,
А.Ю.Дмитрук
Національний авіаційний університет, Київ

ПОРІВНЯННЯ ЕФЕКТИВНОСТІ НЕЙРОМЕРЕЖЕВОГО ТА СТАТИСТИЧНОГО ПІДХОДІВ ДО ЗАДАЧІ ВИЯВЛЕННЯ СИГНАЛІВ

Проблема ефективного виявлення сигналів залишається актуальною для багатьох сфер застосування, оскільки синтез оптимальних процедур виявлення особливо ускладнюється при дії сигналів та завад, які характеризуються складним частотним спектром. За таких умов однією з альтернатив вирішення задачі, враховуючи зростаючий інтерес до технології штучного інтелекту, є застосування нейромережевих технологій виявлення при апріорній невизначеності розподілів ймовірності сигналів та завад.

Однак, використання нейронних мереж в задачі виявлення сигналів поки що не набуло широкого поширення, відповідно їх ефективність досліджено недостатньо. Таким чином для розуміння доцільності їх застосування було проведено синтез двох алгоритмів виявлення гармонічного сигналу з невідомою фазою, та виконано порівняльний аналіз їх ефективності.

Синтез першого алгоритму ґрунтується на статистичному описі суміші сигналу і завад та процедурі статистичного синтезу адаптивного алгоритму виявлення. Побудова алгоритму полягає в тому, що відносно реалізації вибірки, розглядаються умовні щільності розподілів ймовірностей (ЩРІ) гіпотез H_0 та H_1, про відсутність і наявність сигналу, відповідно, згідно з якими формується перевірна статистика адаптивного алгоритму виявлення сигналу у вибірці $x_1,..,x_n$, що визначається відношенням правдоподібності (1).

$$L(x_1,..,x_n,b)=\frac{f(x_{k+1},..,x_n \mid x_1,..,x_k,a^*_1,..,a^*_n,b,H_1)}{f(x_{k+1},..,x_n \mid x_1,..,x_k,a^*_1,..,a^*_n,b=0,H_0)} \qquad (1)$$

де $f(x_{k+1},..,x_n \mid x_1,..,x_k,a^*_1,..,a^*_n,b,H_1)$ - багатовимірна ЩРІ суміші сигналу та завади; $f(x_{k+1},..,x_n \mid x_1,..,x_k,a^*_1,..,a^*_n,b=0,H_0)$ -

багатовимірна ЩРІ завади; b - сигнальний параметр.

Згідно з (1) синтезується алгоритм виявлення сигналу на тлі марківської корельованої завади, адаптивність якого забезпечується алгоритмом оцінювання параметрів завади $a^*_1,..,a^*_n$, що ґрунтується на методі максимальної правдоподібності, та формується структурна схема виявлювача (Рис.1) [1].

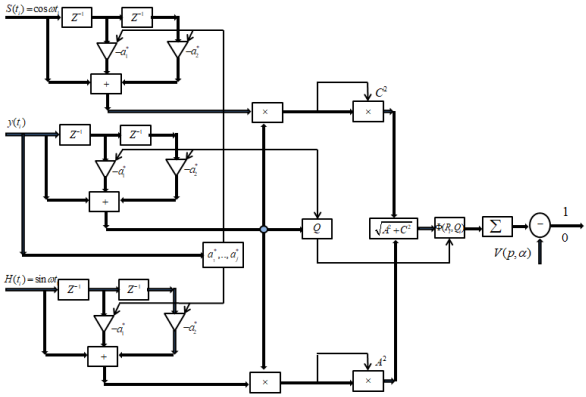


Рис.1. Блок-схема адаптивного виявлювача

Другий підхід ґрунтується на застосуванні нейромережі в комбінації з перетворенням Фур'є, архітектура якої наведена на Рис.2 [1].

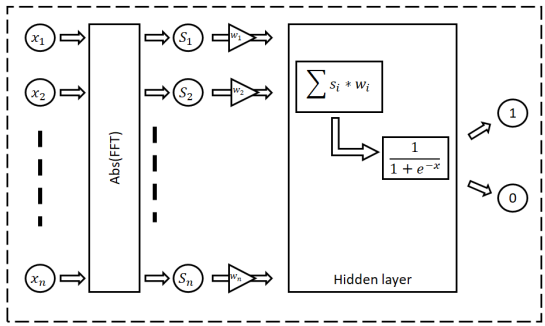
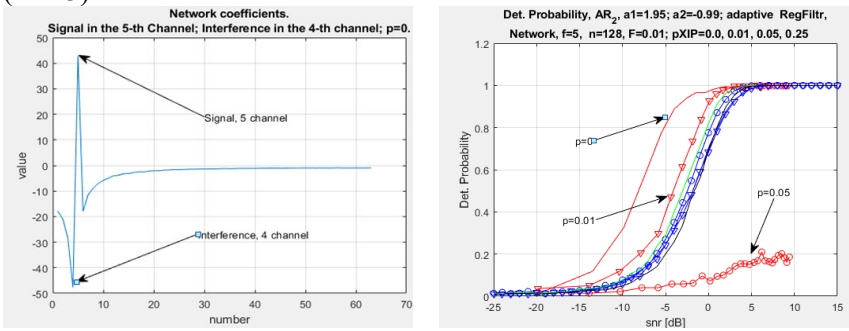


Рис.2. Архітектура нейромережевого виявлювача

Нейромережевий виявлювач складається з передпроцесора, який застосовує перетворення Фур'є вхідної вибірки $x_1,...,x_n$, що є сумішшю сигналу та завади. Коефіцієнти перетворення $S_1,...,S_n$ складають вхідний шар нейромережі і подаються на єдиний прихований шар з єдиним вузлом логістичної регресії.

Відповідно до синтезованих алгоритмів за допомогою комп'ютерного моделювання, було побудовано характеристики виявлення алгоритмів та проведено аналіз ефективності їх роботи (Рис.3).



а) б)

Рис. 3. а) коефіцієнти нейромережі; б) зведені характеристики виявлення двох алгоритмів – оптимального адаптивного (червоні лінії) та нейромережевого (сині лінії) при різних ймовірностях виникнення імпульсних завад

Слід зауважити, що відповідно до Рис.3(а) коефіцієнти нейромережі по суті, повторюють собою амплітудну-частотну характеристику фільтра Вінера. Таким чином, згідно з результатами порівняльного аналізу обох алгоритмів (Рис. 3(б)), варто відзначити, що обидва алгоритми забезпечують стійкість характеристик виявлення до дії інтенсивних імпульсних перешкод, однак при близькому розташуванні сигналу до завади (5 канал), нейромережевий алгоритм проявляє більшу стійкість, в той час як адаптивний за таких умов втрачає ефективність.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Prokopenko I., Prokopenko K., Dmytruk A. Comparison of neural network and statistical approaches to the problem of signal detection. In: "Proceedings of the 2nd International Workshop on Advances in Civil Aviation Systems Development," Lecture Notes in Networks and Systems, Volume 992, 2024, Springer, Cham, pp. 1–19.

УДК 004.056.5

В.А.Пургін,
О.П.Мартинова, к.т.н.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ LANGCHAIN З ВЕКТОРНОЮ БАЗОЮ ДАНИХ PINECONE ДЛЯ ГЕНЕРАЦІЇ ВІДПОВІДІ ШТУЧНИМ ІНТЕЛЕКТОМ ДЛЯ КОРИСТУВАЧА

Штучний інтелект в сучасному світі розвинувся до серйозних розмірів, він представляє інтелектуальні системи, спроможні виконувати завдання, які традиційно вимагають наявність людини поєднує здатність глибокого розуміння мови з передовими технологічними рішеннями, загалом наростає в своїх можливостях та застосуваннях. Це показує значні досягнення у цій сфері.

LangChain – це платформа з відкритим вихідним кодом для створення додатків на основі великих мовних моделей (LLM). Моделі LLM навчаються за великими обсягами даних і використовуються для глибокого навчання, щоб генерувати відповіді на запити користувачів, наприклад відповідати на запитання або створювати зображення на основі текстових підказок. Процес створення повідомлень з використанням Langchain здійснюється відносно швидко та ефективно, алгоритмічно враховуючи контекст та індивідуальні особливості комунікативної ситуації. Він надає інструменти та абстракції для розширення можливостей налаштування, підвищення точності та актуальності генерованої інформації. Наприклад, розробники можуть за допомогою готових компонентів LangChain створювати нові ланцюжки підказок або налаштовувати наявні шаблони. Також у LangChain є компоненти, які дозволяють застосовувати LLM до нових наборів даних без повторного навчання [1].

На сьогоднішній день ми потребуємо ефективного надійного зберігання та швидкого пошуку інформації. Реляційні або старіші бази даних є найбільш важливими базами даних для будь-якої комп'ютерної програми, але вони не здатні обробляти дані в різних формах, таких як документи, пари ключ-значення та графіки. Векторна база даних – це новий підхід, який використовує векторизацію для ефективного пошуку, зберігання та аналізу даних.

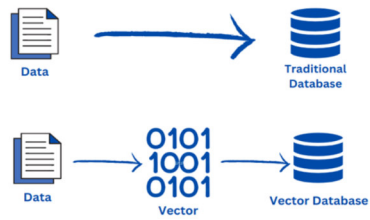


Рис.1 Порівняння традиційної бази даних з векторною

Pinecone – одна з таких векторних баз даних, яка широко використовується в галузі для вирішення таких проблем, як складність і розмірність. Pinecone – це хмарна векторна база даних, яка обробляє векторні дані високої розмірності. Основний підхід Pinecone базується на пошуку наближеного найближчого сусіда (ANN), який ефективно знаходить найшвидші збіги та ранжує їх у великому наборі даних [2].

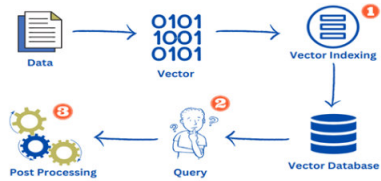


Рис.2 Принцип запитів до векторної бази даних

Підключення Langchain до Pinecone, побудоване через інтеграцію їх API та взаємодії між ними за допомогою зовнішніх запитів, може бути створене для масштабної системи обробки текстів та генерації контенту на обрану тему. Pinecone демонструє виняткову масштабованість, він легко керує мільярдами багатовимірних векторів і може пропонувати можливості горизонтального масштабування, що і робить його придатним для обробки навіть найвимогливіших робочих навантажень машинного навчання.

Перше, що треба зробити – це побудувати модель обробки текстів, саме вона буде використовувати Pinecone для індексації та пошуку матеріалів. Pinecone безперешкодно підтримує приймання даних у режимі реального часу, даючи змогу користувачам зберігати й індексувати нові дані в міру їхньої появи без будь-яких простоїв або перебоїв [3]. Після того як потрібні матеріали завантажені і розбиті на вектори, можна використовувати Langchain для генерації текстів на основі матеріалів, знайдених у

базі даних. Langchain використовує ці векторизовані представлення текстів для розуміння контексту та структури інформації. Після аналізу текстових даних у Langchain можна використати генераційні моделі, такі як GPT (Generative Pre-trained Transformer), для створення нових текстів, відповідей або контенту на основі цього аналізу.

Підсумовуючи вище сказане можна зробити висновок, що ці технології можуть бути використаними в широкому спектрі нашого життя. Маючи якийсь обсяг матеріалів, можна створити бота, який буде чудово відповідати на питання користувачу у цій сфера. На даний момент це дуже важливо, так як це можна використати у серйозних цілях. Наприклад, створення ботів для психічного здоров'я військових може стати кроком до покращення допомоги та підтримки військовослужбовців у зоні бойових дій або після повернення до цивільного життя. Боти, побудовані на базі Langchain та Pinecone, можуть аналізувати тексти та надавати індивідуальні поради, підтримку або посилання на необхідні ресурси для поліпшення психологічного стану. Крім того, ці технології можуть бути використані для створення інтелектуальних систем аналізу та передбачення в сферах фінансів, маркетингу та бізнесу. Наприклад, системи аналізу соціальних мереж можуть використовувати дані з Pinecone для ідентифікації та аналізу групової динаміки, а Langchain може генерувати рекомендації для підвищення ефективності маркетингових кампаній або оптимізації бізнес-процесів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Що таке Langchain.* https://aws.amazon.com/en/what-is/langchain/
2. *Everything you need to know about Pinecone – A vector database* https://www.packtpub.com/article-hub/everything-you-need-to-know-about-pinecone-a-vector-database
3. *Mastering Vector Databases with Pinecone Tutorial: A Comprehensive Guide. https://www.datacamp.com/tutorial/mastering-vector-databases-with-pinecone-tutorial.*

УДК 004.451.44

О.В.Русанова, к.т.н.,
О.В.Корочкін, к.т.н.,
О.П.Шевело
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

ПРОБЛЕМА АВТОМАТИЗАЦІЇ ПЛАНУВАННЯ РОБІТ У IT БІЗНЕС ПРОЄКТАХ

Системи управління проєктами дозволяють мінімізувати час, витрачений на організацію виконання проєктів. Підвищення ефективності таких систем пов'язані з автоматизацією планування робіт між співробітниками. Саме цій проблемі для IT галузі і присвячується дана робота.

На сьогодні існує більше 30 систем управління проєктами. У роботі розглянуто і проаналізовано найбільш відомі серед них,такі, як *Any.Do, Asana, Google Tasks*, *Wrik, Microsoft Project, Monday work management* та інші. Усі відомі системи мають зручний функціонал щодо стану виконання проєктів, прогресу співробітників, статистичних даних, тощо. На жаль жоден з них не має функції автоматичного планування робіт, яка підвищує ефективність управління проєктами, спрощує роботу менеджерів і в результаті впливає на час виконання проєкту.

У роботі розглядається класифікація підходів та особливості автоматичного планування робіт між співробітниками, а саме: статичне, динамічне та балансове планування.

Далі розглядаються вихідні дані до планування. До вихідних даних відносяться опис робіт проєкту, склад команди та їх характеристики, а також критерії оптимізації планування робіт і представлення результатів у вигляді діаграми Ганта..

Авторами аналізуються варіанти опису робіт проєкту, що можуть бути представленя у вигляді графу задачі *(task graph)*, де вершинам відповідають завдання проєкту, а дугам – зв'язки між завданнями. У якості ваг вершин можуть бути застосовані середній час виконання задачі або їх складність на базі оцінок *Story Points.* Перший варіант опису графу задачі застосований авторами у роботі [1]. Поява методології *Scrum* [2] спричинила вагомі зміни в IT-індустрії і принесла не лише продуктивність і ефективність в розробці програмного забезпечення, а й нові стандарти в

проєктуванні. Завдяки *Scrum*, здобула популярність оцінка задач проєкту не в людино-годинах, а у *Story Points* [3]. Тому такий варіант при описі графу задач є більш перспективним.

Розглядаються можливі варіанти опису складу команди для проєкту, починаючи від їх кількості [1] до врахування індивідуальних можливостей кожного співробітника у вигляді таких показників, як швидкість розробки *(velocity)*, яка вимірюється у *Story Points* за тиждень, спеціалізація та зарплата.

Враховуючи різні критерії оптимізації, можливі наступні постановки задачі планування робіт: визначення мінімального часу виконання проєкту при заданому складі команди; визначення часу виконання проєкту при його мінімальній вартості; визначення мінімальної кількості людей у команді, яка виконає проєкт за обмежену(задану) вартість; визначення мінімальної кількість людей у команді, яка виконає проєкт за обмежений(заданий) час; визначення мінімальної вартості проєкту при обмеженій кількості людей. Авторами запропоновано і реалізовано [1] деякі з вищезазначених задач. Обгрунтовується можливість застосування методів планування обчислень для паралельних КС з певною модифікацією для автоматичного розподілу задач між співробітниками у бізнес проєктах.

Обговорюються відкриті питання динамічного планування, пов'язані зі зміною складу учасників команди під час виконання проєкту, а також із запізненням виконання певних задач проєкту

ВИКОРИСТАННІ ДЖЕРЕЛА

1. Спосіб управління проєктами на основі мережевого планування / О.В.Русанова, О.В.Корочкін, Ю.І.Медведкова// Проблеми інформатизації та управління-2022.-№3(71)-С.51-56

2. What is Scrum? [Електронний ресурс] // Scrum.org – Режим доступу: https://www.scrum.org/learning-series/what-is-scrum

3. Rad, Nader K.. Agile Scrum Handbook – 3rd edition. Netherlands: Van Haren, 2021.

УДК 004.738 (043.2)

А.С.Савченко, д.т.н.,
О.В.Толстікова, к.т.н.,
С.В.Водоп'янов, к.т.н.
Національний авіаційний університет, Київ

СИСТЕМНИЙ ПІДХІД ДО РОЗВ'ЯЗАННЯ КОНФЛІКТІВ МІЖ КЛЮЧОВИМИ ПАРАМЕТРАМИ БЕЗПРОВОДОВИХ МЕРЕЖ

Сучасні концепції розвитку інформаційних та телекомунікаційних технологій, їх впровадження пов'язані з розробкою та побудовою складних та розвинених інформаційно-обчислювальних систем. Вони стали невід'ємною частиною інформаційно-управляючих систем авіаційного призначення [1]. Це стосується, у першу чергу, корпоративних мереж крупних аеровузлів. Такі мережі за визначенням є складеними гетерогенними мережами з різнорідним трафіком типу *Triple Play* (мова – відео – дані) або *Quadruple Play* (мова – відео – дані плюс мобільні абоненти). В останньому випадку мобільні абоненти – це повітряні судна, на борту яких розташовані мережні вузли.

З розширенням меж застосування технологій взаємодії відкритих систем і міжнародних стандартів функціонування інформаційно-обчислювальних структур зростають і вимоги до їх швидкодії та надійності. При розгляді завдань інформаційно-комунікаційного обслуговування крупного аеровузла треба брати до уваги той факт, що збільшення ефективності мережі неминуче супроводжується зростанням вимог до її провідних технічних характеристик (ключових параметрів ефективності – *Key Performance Indicators, KPIs*), а внаслідок природних обмежень мережного ресурсу, звичайно, виникають технічні та організаційні конфлікти.

У відповідності з системним підходом у виробничо-технічних системах конфлікти різної природи виникають при розробці тих чи інших методів обміну даними між мережними вузлами та опрацювання інформації у мережних вузлах:

– моделювання автономних сегментів та/або мережі в цілому – виникають конфлікти між адекватністю та складністю моделі;

– вибір та аналіз системи – виникають конфлікти між

ефективністю та вартістю;

– забезпечення енергоефективності та завадозахищеності на фізичному рівні еталонної моделі *ISO* – виникають суперечності між щільністю розташування вузлів, зоною дії мережі та якістю обслуговування (*Quality of Service – QoS*);

– прокладання маршрутів від відправника до отримувача на мережному рівні еталонної моделі *ISO* – виникають конфлікти між справедливістю та оптимальністю [2].

При розгляді та аналізу цих задач виявлено, що при намаганні досягти 100% адекватності потребує створення моделі, абсолютною ідентичної реальному об'єкту – до усіх вузлів, елементів та зв'язків між ними, підсистем енергопостачання, генерації сигналів та зняття даних тощо [3]. Аналітичні результати дають корисну інформацію про компроміси серед параметрів. Однак нинішні інформаційно-комунікаційні системи є складними за визначенням. У цьому сенсі прагнення моделювати до останньої деталі часто призводить до математично нерозв'язних проблем. Іншими словами, створена за такою вимогою модель системи буде представляти, по суті, дублікат об'єкту, а задача моделювання просто лишається змістовного сенсу.

Для розв'язання цього конфлікту доцільно вводити ключові показники ефективності, які є найважливішими для загального оцінювання продуктивності системи.

Відповідно, при побудові довільної технічної, інформаційної або будь-якої іншої системи за критерієм «ефективність/вартість» можна було б намагатися якнайбільше знижати вартість. Оскільки вартість знаходиться у знаменнику, обране співвідношення, здавалося б, буде необмежено зростати. Більш того, при зниженні вартості до нуля воно прагнутиме до нескінченності. Однак здоровий глузд підказує, що при цьому й саме система буде відсутня. Знову ж таки задача лишається сенсу.

Такі ж міркування справедливі для усіх різновидів конфліктів, що виникають у наукових дослідженнях, включаючи згадані енергоефективність та завадозахищеність, справедливість та оптимальність тощо.

Єдино можливим засобом розв'язку конфліктів є системний підхід:

– аналіз асимптотичної поведінки процесу розвитку конфлікту,

вибір простору прийнятних рішень з відкиданням свідомо безглуздих варіантів;

– обирання раціональних компромісів між суперечливими сторонами конфлікту.

Саме такий підхід і використовується у представленій роботі.

Крім того, авіаційна комп'ютерна мережа з наявними мобільними абонентами, по суті, є системою з випадковими параметрами. Тому для побудови моделі мережі та розробки методів розв'язання внутрішніх конфліктів треба застосовувати статистичні методи [1].

У роботі [1] проведено порівняльний аналіз методів опису процесів появи та зникнення довільних об'єктів у термінах математичної статистики і доведено, що найбільш придатною є модель неоднорідного альтернуючого процесу відновлення. Дамо короткий опис цієї моделі.

Нехай мають місце послідовності появи та зникнення мережних вузлів. Припустимо, що в результаті появи *i*-го мережного вузла ймовірність штатного функціонування мережі знижується, можливо, на величину одного порядку порівняно з імовірністю, яка спостерігалася до цього моменту, а в результаті зникнення *j*-го $(i \neq j)$ вузла ймовірність функціонування мережі підвищується, можливо, на величину другого порядку малості порівняно з імовірністю, яка спостерігалася до цього моменту. Таким чином, у кожний момент часу система може перебувати в одному з N можливих фазових станів $\varphi_1, \varphi_2, \dots, \varphi_N$, що характеризують ймовірність функціонування об'єкта. Відомі початковий стан системи (в початковий час вона перебуває у стані $\psi_0 = \varphi_i$) і однокрокові ймовірності переходу $\rho_{lk} = P\{\psi_l = \varphi_k | \psi_{l-1} = \varphi_i\}$, $i, k = \overline{1, N}$. Отже, якщо враховувати випадковий характер часу очікування та цікавитися моментами переходу, то процес $\psi_l = \psi(t_l)$ є вкладеним однорідним ланцюгом Маркова. Імовірність переходу ρ_{lk} визначається *i-м* станом об'єкта і результатами змін кількості вузлів. Запізнення і в системах і є дискретними процесами, які не обов'язково є марківськими.

Запізнення τ_1 в τ_2 мережі є дискретними процесами, які не обов'язково є марківськими. Однак це не критично для подальшого аналізу, оскільки самі величини $\rho_{mn}, m, n \in M$ дають вичерпну інформацію про еволюцію мережі.

Співставимо кожному ненульовому елементу матриці ймовірностей переходу випадкову величину ζ_{ik} з функцією розподілу $F_{ik}(t) = F_{ik}(\tau_{ik} \leq t)$. У розглянутій задачі випадкову величину ζ_{ik} будемо трактувати як час перебування мережі в стані φ_i за умови, що наступним станом, в який перейде мережа, буде φ_k. При цьому величина ζ_{ik} вважається невід'ємною із щільністю ймовірності $w_{ik}(t)$. При такій інтерпретації величину ζ_{ik} можна назвати інтервалом знаходження мережі у стані φ_i до переходу у станφ_k.

Припустимо, що точка, яка відображає поведінку мережі в просторі станів $\Phi, \varphi_1, \varphi_2, \dots, \varphi_N \subset \Phi$, залишиться в стані φ_j протягом часу ζ_{ij}, перш ніж вона перейде в стан φ_j (рис. 1,2). Після досягнення стану φ_j «миттєво» (відповідно до матриці ймовірностей переходу $\{\rho_{ik}\}$) вибирається наступний стан. Тут «миттєвість» трактується у тому сенсі, що тривалість переходу є величиною другого порядку малості проти мінімальної тривалістю перебування у поточному стані.

Як відомо [1], коефіцієнт використання мереж не може бути близьким до одиниці, інакше корисна пропускна здатність мережі різко впаде. Мережа або повторно передаватиме загублені пакети і квитанції, або оброблятиме колізії, тобто. працюватиме «на себе». Тому для управління ресурсами та підтримки пропускної спроможності мережі в цілому на необхідному рівні необхідно перерозподіляти навантаження на окремі сегменти вже при появі найперших симптомів навантаження, поки воно ще контрольоване. Структуризація та сегментація мереж може бути доведена до виродженого стану (режим «мікросегментації», коли кожен

термінальний вузол фактично є окремим автономним сегментом). Тоді число вузлів комутації практично дорівнює числу термінальних вузлів [1].

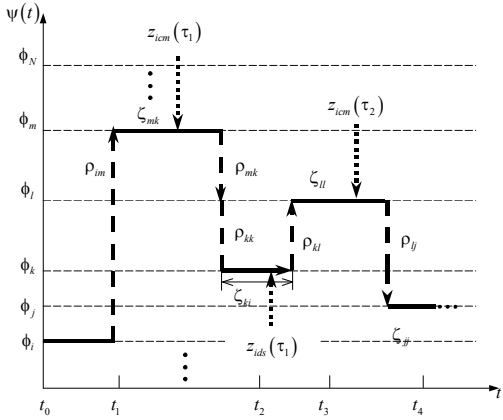


Рис. 1. Зміни імовірностей станів мережі. Імовірність появи нових вузлів переважає імовірність зникнення існуючих вузлів:

$$z_{icm}(\tau_n) \succ z_{ids}(\tau_n)$$

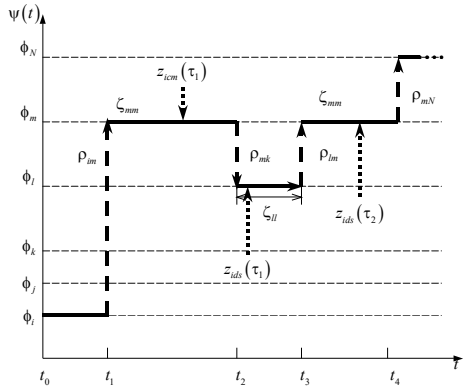


Рис. 2. Зміни імовірностей станів мережі. Імовірність зникнення існуючих вузлів переважає імовірність появи нових вузлів:

$$z_{ids}(\tau_n) \succ z_{icm}(\tau_n)$$

Основні підходи до моделей мобільності наступні:

– випадкова мобільність: мобільність вузлів є випадковою та незалежною в різних аспектах (швидкість, час паузи, напрямок...). Ця модель може бути придатною для ряду конкретних застосувань, але, не є повною;

– моделі з часовою залежністю: щоб протистояти виникненню різких і раптових змін швидкості, деякі моделі припускають, що вузли мають певну «пам'ять», яка дозволить оцінити поточний стан із попередніх станів, виміряних протягом останніх кількох одиниць часу;

– моделі з просторовою залежністю: цей вид моделі вирішує проблему вузлів, рух яких залежить від інших вузлів, наприклад, у ситуації, коли вузол рухається позаду іншого і може рухатися так само швидко, як і передній вузол; при цьому потрібно дуже ретельно моделювати вектор напрямку з урахуванням існуючої топології;

– моделі з географічними обмеженнями зони дії мережі: параметри входу-виходу рухомих вузлів залежать від застосованої топології.

Використання адекватних математичних моделей дозволяє отримати асимптотичні оцінки імовірностей стану комп'ютерної мережі у широкому діапазоні змін кількості мережних вузлів, процесів еволюції конфліктів та пошуку компромісів [1-3].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Толстікова О.В., Водоп'янов С.В., Андреєв О.В., Коцюр А.Б. Модель системи управління опортуністичною комп'ютерною мережею. Проблеми інформатизації та управління: зб. наук. праць. – К.: НАУ, 2024. – Вип. №77 (1). – С. 47 – 51.

2. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. – Pearson Education, Inc., Old Tappan, New Jersey, 2016. – 538 pp.

3. Soret B., Mogensen P., Pedersen K.I., Carmen Aguayo-Torres M. Fundamental tradeoffs among reliability, latency and throughput in cellular networks. – 2014 IEEE Globecom Workshops (GC Wkshps) – Ultra-Low Latency and Ultra-High Reliability in Wireless Communications, Austin, TX, USA. – pp. 1391 – 1396.

https: // DOI: 10.1109/GLOCOMW.2014.7063628

УДК 004.056

Д.О.Сак
Національна академія Служби безпеки України, Київ

АНАЛІЗ МІЖНАРОДНИХ ДОКУМЕНТІВ З УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

З розвитком інформаційних технологій та їх всеосяжним проникненням практично в усі сфери діяльності сучасних держав і компаній питання захисту інформації стають ключовими: так звана четверта наукова революція немислима без використання наукомістких інформаційних технологій, які з усіма перевагами привносять і пов'язані з ними ризики, оскільки одночасно з проникненням ІТ в життя держав, компаній і звичайних громадян зростають і множаться загрози інформаційній безпеці.

Ось декілька різних методологій ризик-менеджменту.

Фреймворк «NIST Risk Management Framework» на базі американських урядових документів NIST (National Institute of Standards and Technology (NIST SP 800-39, NIST SP 800-37, NIST SP 800-30, NIST SP 800-137). Стандарти Міжнародної організації зі стандартизації ISO (International Organization for Standardization): стандарт ISO/IEC 27005: 2018, ISO / IEC 27102: 2019, ISO/IEC 31000:2018. Методологія FRAP (Facilitated risk Analysis Process) є відносно спрощеним способом оцінки ризиків, з фокусом тільки на найбільш критичних активах. Якісний аналіз проводиться за допомогою експертної оцінки. Методологія OCTAVE сфокусована на самостійній роботі членів бізнес-підрозділів. Вона використовується для масштабної оцінки всіх інформаційних систем і бізнес-процесів компанії. Стандарт AS / NZS 4360 є австралійським і новозеландським стандартом з фокусом не тільки на IT-системах, але і на бізнес-здоров'я компанії, тобто пропонує більш глобальний підхід до управління ризиками, зараз замінений на стандарт AS/NZS ISO 31000-2009. Методологія FMEA пропонує проведення оцінки системи з точки зору її слабких місць для пошуку ненадійних елементів. Методологія CRAMM пропонує використання автоматизованих засобів для управління ризиками. Методологія Fair – пропрієтарний фреймворк для проведення кількісного аналізу ризиків, що пропонує модель побудови системи управління ризиками на

основі економічно ефективного підходу, прийняття поінформованих рішень, порівняння заходів управління ризиками, фінансових показників і точних ризик-моделей.

Концепція COSO ERM описує шляхи інтеграції ризик-менеджменту зі стратегією та фінансовою ефективністю діяльності компанії та акцентує увагу на важливості їх взаємозв'язку. У документі описані такі компоненти управління ризиками, як стратегія і постановка цілей, економічна ефективність діяльності компанії, аналіз і перегляд ризиків, корпоративне управління і культура, а також інформація, комунікація і звітність.

Впровадження різних технічних засобів захисту доцільно проводити тільки після проходження основних етапів побудови комплексної системи управління інформаційною безпекою: розробки внутрішніх нормативних документів в області ризик-менеджменту і кібербезпеки, інвентаризації та класифікації активів, оцінки та аналізу ризиків, техніко-економічного обґрунтування впровадження конкретних типів засобів захисту.

Отже, розвиток і користь від застосування сучасних інформаційних технологій йдуть рука об руку з асоційованими з ними ризиками і загрозами. Тільки цілісне розуміння компонентів актуальних загроз інформаційній безпеці укупі із застосуванням методик оцінки ризиків впровадження та експлуатації тих чи інших інформаційних систем, а також розуміння сучасних способів нейтралізації загроз захисними заходами принесе вам користь при виборі IT-стратегії розвитку компанії та її цифрової трансформації, а також при впровадженні та використанні тих чи інших інформаційних технологій, продуктів і сервісів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Кавин О., Кавин С., Кавин Б., Кавин Я. Застосування інтеракивного програмного середовища для оцінки ризиків інформаційної безпеки. Scientific Collection «InterConf». № 123. Pp. 312-319. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/1280

2. Dobson S., Galbraith D., Legrow J. An Adaptive Attack on 2-SIDH. The University of Auckland, New Zealand, 2020. 17 p.

3. Demertzis K., Iliadis L. Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks. Journal of Computations & Modelling. 2019. Vol. 9, no. 2. Pp. 1-26.

УДК 004.9:[629.05:623.746-519]

В.С.Сахно,
О.П.Мартинова, к.т.н.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

ПРОБЛЕМАТИКА ПОЛЬОТНОГО КОНТРОЛЮ В СУЧАСНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Військові конфлікти сучасності відзначаються швидким розвитком технологій, що призводить до появи нових інновацій, зокрема в сфері використання безпілотних літальних апаратів (БПЛА). Наслідком цього є постійне модернізування та вдосконалення систем керування дронами, а також виклики, пов'язані з захистом від радіочастотних впливів та перехопленням. Завдяки розвитку технологій, використання БПЛА стало широкою практикою у збройних силах різних країн, забезпечуючи нові можливості для розвідки, наведення ударів та моніторингу ворожої активності. Однак, разом зі зростанням числа БПЛА на бойовому полі, зростає і загроза для їхньої системи керування.

Однією з основних загроз для систем управління БПЛА є засоби реактивно-електронної боротьби (РЕБ), які призначені для перешкоджання або блокування сигналів керування. РЕБ можуть використовуватись противником для перехоплення сигналів керування БПЛА, що може призвести до втрати зв'язку з ним або навіть до повного втрати контролю.

Наразі, кожна з воюючих сторін старається використовувати певні частоти для управління своїми БПЛА. Але, до сих пір існує загроза перехоплення сигналу та взяти дрон під свій контроль. Механізм перехоплення працює як шум радіохвиль, який в основному, атакує приймач сигналу. Як наслідок, дрон втрачає керування і не виконує поставлену задачу.

Для подолання проблеми перехоплення дронів, шукають рішення в застосуванні двохчастотної (або мультичастотної) передачі даних. Ці системи дозволяють розділити передачу даних на кілька частот, зменшуючи тим самим вразливість до атак РЕБу та забезпечуючи більшу надійність управління

БПЛА. На разі, засоби РЕБу покривають певну площину частот, через що перемикання частоти керування, є ефективним методом протидії РЕБ.

Переваги використання мультичастотого управління:

- недосяжність певними засобами РЕБу до ураження;
- гнучкість польоту в радіозасміченому середовищі, менший вплив інтерференції інших радіохвиль на сигнал;
- розширення функціоналу керування, адже втрата одного пакету при маневрі не впливає на прийом інших пакетів.

Недоліки:

- більше апаратне забезпечення, збільшення кошту;
- збільшення енергопотужності передевача, швидша розрядка пульта.

Система польоту контролю на мультичастоті являє собою комплекс апаратних рішень, а саме:

1. Пульт керування.
2. Система приймачів.
3. Польотний контролер.
4. Антени та їх підсилювачі.

Загалом рішення розраховане на передачу двох паралельних сигналів на систему приймачів, де визначається сигнал до польотного контролера. Така система є гнучкою до перехоплення одного з сигналів керування, і може покращити характеристики керування БПЛА. Сама система має бути виконана певним набором трансміторів і ресиверів, які не мають конфліктувати один з одним і за допомогою грамотного розміщення паралельно виконувати задачі. Це реалізується як розробкою пульта управління, його модулів передачі, антенним комплексом, і системою прийому сигналу на польотний контролер.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Jane's International Defence Review. (2021). "Unmanned Aerial Vehicles (UAVs) in Modern Warfare: Trends and Challenges."

2. Smith, J. (2020). "Radio Frequency Jamming and Countermeasures in Military Operations." Journal of Electronic Warfare.

3. NATO Science for Peace and Security Series. (2019). "Counter-UAS Technologies: Emerging Trends and Future Perspectives."

УДК 004.056 (045)

С.М.Сидоренко
Національна академія Служби безпеки України, Київ

ДЕЗІНФОРМАЦІЯ ЯК СИНДРОМ ВИНИКНЕННЯ КІБЕРЗАГРОЗИ

Згідно з опитуванням, проведеним у 2023 році, 62% учасників отримують інформацію з соціальних мереж і 48% з новинних сайтів. Дезінформація може легко поширюватися в соціальних мережах через відсутність редакційного контролю, свободу публікацій для будь-якого користувача та можливість швидко створювати та поширювати інформацію безкоштовно.

Неправдива інформація є одним із засобів маніпулятивного впливу, який здійснюють за допомогою прихованих технік [1]:

- Клікбейт – перебільшені, сумнівні або оманливі заголовки, зображення чи описи в соціальних мережах для створення веб-трафіку.
- Пропаганда – поширення інформації, чуток чи ідей, щоб завдати шкоди країні, групі людей чи окремій особі, зазвичай з політичною метою.
- Фейк – імітація новинних або інших сайтів, що містять вигадані історії.
- Упереджені новини – контент, що спонукає читачів підтвердити власні упередження та переконання.
- Джинса – новини, опубліковані під контролем уряду, для створення та поширення дезінформації серед громадян.
- Сатира – створення фейків заради пародії чи розваги.

Дезінформація – це лише один з елементів величезного набору ворожих інформаційних дій, який може включати в себе багато тактик, методів та процедур. Наприклад, пропагандистські журналісти дуже часто закидають в новинні телеграм канали інформацію, яка не перевірена або трактована так, як вигідно російським ЗМІ (рис. 1). Розрізняють три основі методи дезінформації.

Пропаганда – це інформація, що призначена для маніпулювання конкретною цільовою аудиторією з метою схилити її до певної поведінки або думки, що часто проводиться в рамках довготривалої компанії державним суб’єктом з політичними цілями.

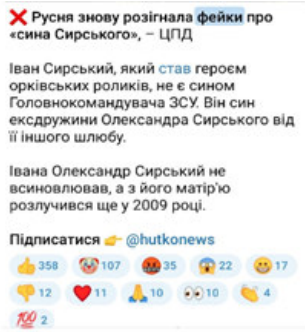


Рис. 1. Приклад поширення брехливих даних

Ворожий наратив – це певна історія, що розроблена з метою дискредитації конкретного об'єкта. Наративи можуть впливати на громадську думку, сприяти певному сприйняттю подій, фактів та персонажів.

Ворожа інформаційна діяльність – широкий спектр скоординованих дій, спрямованих на породження недовіри та маніпулювання думкою, наприклад, вирвані з контексту цитати або брехня.

Маніпулювання та втручання в іноземну інформацію – це модель поведінки, що загрожує або здатна негативно впливати на цінності, процедури або політичні процеси.

Іноді дезінформація покликана не лише для того, щоб змусити людину повірити у ту чи іншу брехню, а щоб заплутати, внести дисонанс за допомогою протиріч, щоб люди не могли розрізними факти від вигадки. У такому випадку одні люди потраплять під вплив дезінформації та будуть її поширювати, а у іншому випадку будуть роздратовані та втратять цікавість до новин. Обидва цих результати можуть зіграти на руку ворожим суб'єктам, які намагаються знизити стійкість суспільства.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Деструктивні впливи та негативні наративи: інструменти виявлення та протидії: метод.мат. / Д.В.Дубов, А.В.Баровська, Ю.К.Каздобіна. – К.:УФБС, 2020. – 60 с.

УДК 004.453(076.5)

Ю.І.Сінько, к.пед.н.

Національний авіаційний університет, Київ

ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ САПР ТП

Система автоматизованого проектування технологічних процесів (САПР ТП) дозволяє інженерам створювати технічні проекти, розробляти схеми технологічних процесів, виконувати розрахунки та моделювання різноманітних технологічних систем. Вона спрощує процес проектування, зменшує час на розробку проектів і підвищує їх якість. Розрізняють ефективність створення САПР та ефективність її функціонування.

Виробництво систем автоматизованого проектування (САПР) є унікальним. Ефективність створення САПР розглядають як розробку нової технології, але з урахуванням особливостей самої САПР. САПР відноситься до сучасних організаційно-технічних систем, які характеризуються швидким розвитком методів та засобів. Тому стратегія витрат повинна враховувати, з одного боку, революційний процес створення САПР, а з іншого – еволюційний процес її розвитку, що передбачає періодичні вкладення коштів у модернізацію системи та підвищення її ефективності, яка змінюється з часом. При цьому використовують такі критерії вибору засобів системи:

- максимум продуктивності за обмежених витрат;
- мінімум витрат (В) за обмеженої продуктивності (П);
- максимум відношення П : В (мінімум витрат відносно досягнутої продуктивності);
- максимум різниці економії (Е) і витрат (В) (признак ефективного використовуєте ресурсів) та ін.

Оцінюючи ефективність функціонування САПР ТП застосовуються підходи, що описані вище, а порівняльна економічна ефективність розглядається з двох різних точок: до та після впровадження розробленої САПР ТП. Водночас функціонування САПР ТП дає специфічний непрямий економічний ефект:

$\Delta E = \Delta E_{П} + \Delta E_{НП}$, де $\Delta E_{П}$ – прямий економічний ефект, а $\Delta E_{НП}$ – непрямий економічний ефект.

Введемо такі поняття [1]:

$\Delta E_П = \sum_{i=0}^{n}(B_1M_1 – B_2M_2)$ – прямий економічний ефект від зниження трудомісткості процесу проектування (це безпосередній вплив зменшення витрат на робочу силу та інші ресурси, які витрачаються під час проектування);

B_1, B_2 – вартість обробки одиниці інформації до та після впровадження розробленої САПР ТП;

M_1, M_2 – обсяг річної інформації технологічного завдання до та після впровадження розробленої САПР ТП;

n – число взаємозалежних завдань;

$\Delta E_{НП} = \Delta E_Р + \Delta E_{ПВ} + \Delta E_Ф$ – непрямий економічний ефект,

де $\Delta E_Р$ – економія матеріальних ресурсів;

$\Delta E_{ПВ}$ – економія шляхом підвищення продуктивності під час виготовлення виробів;

$\Delta E_Ф$ – економія внаслідок вивільнення елементів продуктивного фонду (зменшення витрат або оптимізації використання ресурсів).

Коефіцієнт порівняльної ефективності, який використовується для оцінки ефективності різних варіантів діяльності – до та після впровадження розробленої САПР ТП, визначають за формулою

$E_n = \Delta E / K_O$, де K_O – одноразові витрати.

Чим вище значення коефіцієнта порівняльної ефективності, тим ефективнішим вважається варіант з впровадженням розробленої САПР ТП.

Термін окупності капітальних витрат є важливим показником для оцінки економічної ефективності впровадження САПР ТП, а також для прийняття рішень щодо їхньої доцільності.

Термін окупності капітальних витрат (у роках):

$T_{ОК} = K_O / \Delta E_{РІК}$, де $\Delta E_{РІК}$ – річна економія поточних витрат.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Стефанишин О. В. Економічна теорія: навч. посіб. / О. В. Стефанишин, М. В. Квак, М. В. Кічурчак, М. І. Теребух; Львів. нац. ун-т ім. І. Франка. – Л., 2015. – 335 с.

УДК 004.45:629.735-519(043.2)

М.А.Сіренко,
М.К.Печурін, д.т.н.
Національний авіаційний університет, Київ

ЕНЕРГОВИТРАТИ ПРИЙОМО-ПЕРЕДАЮЧОГО ОБЛАДНАННЯ БПЛА ПРИ НАВЧАННІ МЕРЕЖІ ХОПФІЛДА

Однією з нагальних науково-практичних проблем авіаційної сфери є проблема створення інформаційних технологій штучного інтелекту інтегрованої нейрокомп'ютерної системи, розміщеної на борту надлегких БПЛА, тобто в умовах, коли мають місце суттєві обмеження на допустимі енерговитрати обладнання, що забезпечує інтеграцію компонентів системи [1]. Суттєва доля енерговитрат припадає на прийомо-передаюче обладнання БПЛА, котре використовується для налагодження телекомунікаційної інфраструктури [2].

В доповіді пропонується модель для оцінювання величини сумарних енерговитрат прийомо-передаючого обладнання нейрокомп'ютерної системи, що має архітектуру, подібну архітектурі мережі Хопфілда, де допускаються аномалії у вигляді відсутності окремих безпосередніх точка-точка зв'язків.

Алгоритм навчання нейромережі реалізує стандартну функцію навчання, при чому враховується обставина, що витрати енергії для підтримки потужності прийомо-передаючого обладнання нейрокомп'ютерної системи мають місце лише при умові наявності безпосередньої комунікації між парою вузлів. Введенням припущення про тип функції затухання сигналу в комунікаційному середовищі, а також про характер залежності сумарних енерговитрат від потужностей прийомо-передаючого обладнання компонентів нейрокомп'ютерної системи, вдалося побудувати просту нормативну модель в класі моделей задач блокового лінійного програмування.

Вихідними даними для формування параметрів моделі є дані про поточне розташування кожного з m компонентів нейромережі, розміщених на взаємодіючих у тривимірному просторі БПЛА.

Суть цільової функції розробленої моделі є у відшуканні мінімального значення загальної потужності прийомо-передаючого

обладнання P при збереженні достатнього ступеня інтегрованості системи, тобто функція мети має вигляд:

$$P_{\Sigma} = C * P ,$$

де $P = (P_1, P_2, \dots P_m)^T$ – вектор-стовпчик (m·1);

C – вектор-рядок ($1 * m$).

Обмеження моделі:

$$A * P \geq L(k),$$

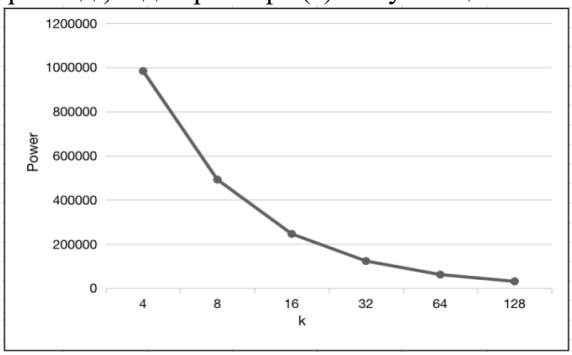
$$P \geq 0 ,$$

де A – блочно-діагональна матриця ($m^2 * m$);

$L(k)$ – вектор-стовпчик ($m^2 * 1$);

k - константа, яка характеризує властивості комунікаційного середовища.

Модель досліджено за допомогою інструментарію *Python* та бібліотек: *scipy*, *numpy*, *random*, *pulp, matplotlib* та ін. В результаті чого маємо ілюстрацію залежності мінімально потрібної сумарної потужності прийомо-передаючого обладнання нейромережі (на умовному прикладі) від параметра (*k*) комунікаційного середовища.



ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Pechurin M.K., Boyarinova Yu.Ye., Kondratova L.P., Voronin M.G., Sirenko M.A. (2022). Models of the topologies for the weak-emitting telecommunication system of interacting UAVs. Problems of Informatization and Management, 4(72), 48-54.*

2. *Chinedu A.E., Aniekan A.U., Valentine I.I., Abimbola O.A. (2024). Telecommunications energy efficiency: optimizing network infrastructure for sustainability. Computer Science & IT Research Journal, 4(1), 26-40.*

УДК 351/354

О.І.Скіцько, к.т.н.
Національна академія СБ України, Київ

РОЗВІДКА З ВІДКРИТИХ ДЖЕРЕЛ ДЛЯ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ

Однією з складових частин забезпечення державної безпеки є забезпечення контррозвідувальної діяльності. Основними завданнями такої діяльності (визначені Законом України «Про контррозвідувальну діяльність» від 31.03.2023) є:

добування, аналітична обробка та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України;

протидія розвідувальній, терористичній та іншій діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України;

розроблення і реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян.

Важливу роль для виконання цих завдань відіграє здобуття та своєчасне надання релевантної, повної та достовірної інформації, яка дозволить якісно їх виконувати. Одним з механізмів отримання такої інформації є OSINT (Open Source Intelligence) – розвідка з відкритих джерел.

OSINT - це методологія, яка зосереджена на зборі та аналізі відкрито доступної інформації для цілей, пов'язаних із військовою, політичною, економічною та іншими сферами. Цей підхід широко застосовується у сферах національної безпеки та оборони, роботі спецслужб, а також при проведенні різноманітних розслідувань, наукових досліджень, а також виконанні завдань зі збору розвідданих та проведенні контррозвідувальних операцій.

На сучасному етапі Інтернет виступає як головна платформа для дослідників у сфері OSINT. Основними ресурсами для збору інформації є:

Засоби масової інформації, включаючи традиційні газети, журнали, а також радіо та телебачення з різноманітних країн.

Ресурси інтернету, такі як онлайн-статті, блоги, форуми, контент, створений користувачами (наприклад, відео з мобільних телефонів), відеохостинги типу YouTube, вікіпедії та інші платформи соціальних медіа (Facebook, Twitter, Instagram тощо), що виділяються своєю

актуальністю та доступністю.

Публічні дані від урядів, включаючи офіційні звіти, бюджети, записи слухань, телефонні довідники, прес-конференції та інші урядові вебсайти, які доступні для загального користування.

Професійні та академічні матеріали, отримані з наукових журналів, конференцій, симпозіумів, наукових робіт, дисертацій.

Комерційні дані, включаючи зображення, фінансові звіти та бази даних.

Так звана "сіра література", до якої відносять технічні звіти, патенти, робочі документи, непубліковані матеріали та інші інформаційні бюлетені.

Ключові вимоги до здійснення досліджень за методом OSINT

Формування комплекту інструментів та джерел для OSINT.

Ефективний інструментарій для OSINT повинен обов'язково включати доступ до соціальних мереж (для аналізу зображень, перегляду особистих профілів, застосування соціальної інженерії), картографічних сервісів (як-от Google Maps, Bing Maps, Yandex Maps), публічних реєстрів (тендерні платформи, реєстри послуг тощо), відкритих баз даних, інформації з форумів та спеціалізованих груп, а також ресурсів темної мережі (Dark Web).

Аналіз контексту дослідження.

Для вірного тлумачення отриманих даних необхідно здійснити глибокий аналіз контексту об’єкта дослідження. Важливо мати чітко визначені цілі та критерії в рамках задач OSINT.

Застосування геоданих.

Важливо забезпечити, щоб всі знайдені дані, де це можливо, були прив'язані до конкретних географічних локацій. Це допомагає уточнити контекст зображень чи відео, які часто діляться в соціальних мережах і містять інформацію про місцезнаходження.

Перевірка інформації.

Вся зібрана інформація має бути ретельно перевірена та підтверджена за допомогою декількох незалежних джерел, що значно підвищить достовірність та точність дослідження.

Забезпечення конфіденційності.

Під час проведення дослідження необхідно забезпечити конфіденційність особистості дослідника, використаних методик та отриманих результатів для збереження їх цінності та забезпечення безпеки дослідника.

УДК 004.056

К.В.Степанець
Національна академія Служби безпеки України, Київ

РОЗВИТОК МЕТОДІВ АНАЛІЗУ ТА ПЕРЕДБАЧЕННЯ ЗАГРОЗ КІБЕРБЕЗПЕЦІ, ВРАХОВУЮЧИ СПЕЦИФІКУ УКРАЇНСЬКОГО КІБЕРПРОСТОРУ ТА ГЕОПОЛІТИЧНІ КОНТЕКСТИ

Кібербезпека є одним з найактуальніших питань у сучасному світі, що впливає на національну безпеку, економічний розвиток та суспільство. Україна, як і багато інших країн, за останні роки зіткнулася з безпрецедентними кібератаками, які завдали значної шкоди державним і приватним підприємствам та поставили під загрозу критично важливу інфраструктуру. Геополітична ситуація навколо України робить цю проблему особливо гострою. Окрім збройних конфліктів, російська агресія супроводжується масштабними кібератаками, спрямованими на дестабілізацію українського суспільства та послаблення країни на світовій арені.

Сучасне українське суспільство стикається з низкою кіберзагроз, які становлять значні ризики для національної безпеки та безпеки громадян. Кібератаки становлять серйозну загрозу для критичної інфраструктури України. Такі атаки призводять до перебоїв у наданні критично важливих послуг, значних економічних втрат та загрози безпеці громадян. На даний момент Україна залишається гарячою точкою для кібершпигунства, особливо з боку інших країн з геополітичними амбіціями. Цілями кібершпигунства є крадіжка конфіденційної інформації, політичні маніпуляції та соціальна дестабілізація. Кіберзлочинці активно використовують фішинг, шкідливе програмне забезпечення та крадіжку даних, щоб порушити цілісність даних приватних компаній та громадян. Все це свідчить про те, що Україна перебуває під постійним кібертиском з боку зловмисників та необхідність розробити ефективні механізми для аналізу, моніторингу та протидії цим загрозам [1].

Удосконалення способів аналізу та моніторингу кіберзагроз є важливим викликом в умовах сьогодення. Ефективне виявлення, ідентифікація та прогнозування кіберзагроз вимагає використання сучасних аналітичних інструментів та інтеграції даних з різних джерел. Використання сучасних аналітичних інструментів, таких як машинне навчання, великі дані та

кіберрозвідка, є ключовим для виявлення та аналізу кіберзагроз. Вони виступають в якості потужних інструментів для аналізу цифрових даних та ідентифікації вразливостей у кібернетичному просторі.

Україна постійно стикається з різними загрозами, що впливають на функціонування держави в цілому. Для забезпечення високого рівня кіберстійкості та захисту від цифрових загроз необхідно зосередити зусилля на кількох пріоритетних напрямах. По-перше, важливо вдосконалити механізми оперативного обміну інформацією про кіберзагрози між державними органами, приватним сектором та міжнародними партнерами. Це дозволить швидко виявляти та вчасно реагувати на нові види кібератак і зменшити потенційні втрати. По-друге, необхідно проактивно впроваджувати найкращі практики кіберзахисту в об'єктах критичної інфраструктури та державних системах. Це включає використання новітніх технологій безпеки, регулярний аудит безпеки та розробку та впровадження стратегій відновлення після кібератак. По-третє, важливо посилювати міжнародне співробітництво у сфері кібербезпеки. Україна має активно співпрацювати з міжнародними організаціями та партнерами, обмінюватися досвідом, розробляти спільні стратегії та проводити спільні навчання і тренування. Тільки такий комплексний підхід дозволить ефективно захищати національну кіберінфраструктуру та забезпечувати кібербезпеку країни [2]. Розвиток методів аналізу та прогнозування загроз кібербезпеці є невід'ємною складовою сучасного цифрового світу, особливо в умовах, коли кіберзагрози постійно зростають і впливають на різні аспекти життя суспільства.

Важливими напрямами подальших досліджень у майбутньому є більш глибокий аналіз взаємозв'язку між кібербезпекою та геополітичними процесами, а також розробка нових методів та інструментів для ефективного виявлення та протидії кіберзагрозам у кіберпросторі України.

ВИКОРИСТАНІ ДЖЕРЕЛА

1.Кіберзагрози для України: аналіз та рекомендації / Національний інститут стратегічних досліджень. - Київ, 2020. - 52 с.

2.Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.2021 № 447/2021.

УДК 004.725.7

В.Ф.Сураєв, к.т.н.,
В.І.Мазур,
Н.Б.Фоміна
Національний авіаційний університет, Київ

ОРГАНІЗАЦІЯ ПОТОКІВ ДАНИХ В СИСТЕМІ ФОРМУВАННЯ ЗАВДАНЬ НА ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ ЛІТАКІВ

Змінне завдання на виконання технічних робіт по обслуговуванню та/або ремонту обладнання, встановленому на літаках, готується за алгоритмом обробки даних, що імпортуються з систем Departure Control System (DCS) та Maintenance, Repair and Overhaul (MRO). Зазвичай такі системи мають розвинуті можливості створення інтерфейсів [1].

Для автоматизації експорту даних треба лише зробити опис змісту даних, обрати формат, налагодити розклад стартів експорту та визначити місце призначення, куди дані будуть вивантажуватись. Для формування змінних завдань організовуються два потоки.

Перший має містити дані з оперативного розкладу польотів у вигляді множини елементів leg:

$$leg = (ac, ap\_dep, dep, ap\_arr, arr),$$

де ac - реєстровий номер літака, ap_dep – аеропорт вильоту, dep – дата і час вильоту, ap_arr – аеропорт приземлення, arr – дата і час приземлення. Ці дані будуть використані для визначення переліку літаків, що опиняться у базовому аеропорту і будуть доступні для проведення робіт по технічному обслуговуванню на протязі деякого часу впродовж зміни, на яку формується завдання. Джерелом для цього потоку є система DCS.

Другий потік постачає з системи MRO інформацію про роботи event, які треба виконати на кожному з літаків. Ці роботи включаються до пакетів wp, які і є основними одиницями для планування робіт і мають показники часу, необхідного для виконання всіх робіт пакету:

$$wp = (ac, ap, wpno, wp\_start, wp\_end),$$

де ac - реєстровий номер літака, ap – базовий аеропорт, wpno - ідентифікатор пакету, wp_start і wp_end - дати і години початків та завершення виконання пакетів. Наповнення пакетів роботами дається у вигляді множини елементів з описом event_description та ємністю роботи event_mh у людиногодинах:

$$event = (wpno, event\_description, event\_mh).$$

Опис змісту цих потоків можна зробити у термінах запитів до бази даних, які можуть бути доступними для експорту завдяки наявності у таких системах відповідних процедур Application Programming Interface (API). Найбільш поширені формати в системах авіаційного направлення – це CSV та XML, але можливі і інші. Наявність модулів автоматичного старту процедур за встановленим розкладом дозволяє організувати регулярний експорт даних, наприклад раз на добу вранці, або кожні 15 хвилин, тощо. Для прийому експортованих даних найбільш вірогідніше буде використовуватись файл-сервер авіакомпанії.

Система формування змінних завдань теж стартує за розкладом. Оскільки дані в потоках можуть змінитись в будь-яку хвилину, а змінне завдання має діяти на протязі всієї зміни, процедуру формування слід запускати одразу після завершення експортів. Зважаючи на структуру даних, реалізація системи може бути виконана у середовищі сервера баз даних за допомогою процедури, що зберігається у базі даних. В ній можна передбачити імпорт даних з файл-серверу, обробку інформації, створення документу у форматі HTML або XML та відправлення його поштою на заздалегідь підготовлені адреси відповідних працівників технічних підрозділів авіакомпанії.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Suraiev V., Mazur V., Ivankevsch O. Effective approach to minimization of the cost of airline's intersystem interfaces creation. The Ninth World Congress "AVIATION IN THE XXI-st CENTURY". – Kyiv, September 22-24, 2020.

УДК 004.738.5.055.7

І.В.Телешко, к.т.н.
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МАСОК ЗМІННОЇ ДОВЖИНИ В МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

У спеціальних або динамічних (Ad-Hoc) мережах, де пристрої динамічно утворюють тимчасові підмережі без потреби у вже існуючій інфраструктурі механізм призначення IP-адрес має вирішальне значення для забезпечення ефективного зв'язку між пристроями. Загальновідомі механізми: динамічна конфігурація хоста, локальна адресація, ручна конфігурація чи розподілене призначення адрес. Вибір конкретного механізму залежить від таких факторів, як топологія мережі, можливості пристрою та сценарії розгортання. Іншим важливим чинником що визначає ефективність розгортання та функціонування мережі, є принцип формування мережевих масок також відомих як маски підмережі.

Зазначені концепції визначають базу алгоритму призначення IP-адрес який має бути ефективними та адаптованим до змінної топології. Типовий алгоритм призначення мережевої адреси в ad hoc мережах включає такі кроки: ініціалізація, пошук сусіда, присвоєння адреси за допомогою вище згаданих механізмів, вивчення топології, вирішення конфліктів адрес, динамічна реконфігурація, обробка помилок і відновлення, масштабування. Дотримуючись цього простого алгоритму пристрої в спеціальних мережах динамічно призначають IP-адреси та адаптуватися до змін у топології мережі, забезпечуючи ефективний зв'язок і з'єднання між пристроями.

Присвоєння IP-адреси є найважливішим кроком на етапі розгортання мережі. Існують різні алгоритми реалізації, але ні один з них не обходиться без визначення масок підмереж. Маски підмережі використовуються для визначення діапазону дійсних IP-адрес, які можна призначити пристроям у сегменті мережі. Загалом маски підмережі є основоположними для роботи спеціальних мереж, дозволяючи ідентифікувати межі мережі, розподіляти IP-адреси та маршрутизувати пакети даних між пристроями в мережі.

Існує два загально відомі підходи до створення масок, а саме, використання фіксованої або змінної довжини маски. Маски підмережі є основоположними для роботи спеціальних мереж,

дозволяючи ідентифікувати межі мережі, розподіляти IP-адреси та маршрутизувати пакети даних між пристроями в мережі. На підставі аналізу різних підходів до використання масок в роботі [1] робиться висновок про високу ефективність використання масок змінної довжини VLSM або технології CIDR.

Переваги використання механізму VLSM: гнучкість, ефективність, масштабованість, ієрархічність. Попри наявність суттєвих переваг цей механізм має й суттєві недоліки, а саме: складність: керування масками підмережі змінної довжини може бути складнішим, ніж використання масок фіксованої довжини, що вимагає ретельного планування та налаштування; наявність накладних витрат на адресацію: VLSM може створити додаткові накладні витрати при керуванні адресами з точки зору розміру таблиці маршрутизації, особливо в мережах із багатьма підмережами; можливість неправильної конфігурації: неправильна конфігурація параметрів VLSM може призвести до винекнення конфліктів або проблем з маршрутизацією, що потребує механізму усунення несправностей та їх виправлення; сумісність: не всі мережеві пристрої можуть підтримувати VLSM або CIDR, що може обмежити взаємодію в неоднорідних мережевих середовищах Ad-Hoc [2].

З метою зменшення накладних витрат на керування адресами при розгортанні мережі пропонується обмежити використання нижнього діапазону масок починаючи з певної кількості сегментів мережі. Для ефективної реалізації такого підходу використовуються типові алгоритми об’єднання сегментів. Підмережі (сегменти) можуть об’єднуватися за принципом географічної приналежності елементів що дає зменшення затримок при маршрутизації пакетів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. SILVA, Pedro Miguel; DIAS, Jaime; RICARDO, Manuel. CIDRarchy: CIDR-based ns-3 routing protocol for large scale network simulation. 2015.

2. ZHOU, Biao; CAO, Zhen; GERLA, Mario. Cluster-based inter-domain routing (CIDR) protocol for MANETs. In: 2009 Sixth International Conference on Wireless On-Demand Network Systems and Services. IEEE, 2009. p. 19-26.

УДК 004.057.8 : 662.613.53

[1]**А.О.Трєгуб,**
[1]**Г.О.Шеїна,** к.т.н.,
[2]**О.В. Вовна,** д.т.н.
[1]*Державний вищий навчальний заклад «Донецький національний технічний університет», м. Луцьк*
[2]*Національний авіаційний університет*

РОЗРОБКА КОМП'ЮТЕРНОЇ СИСТЕМИ МОНІТОРИНГУ КОНЦЕНТРАЦІЇ СІРКОВОДНЮ В АТМОСФЕРІ ПРОМИСЛОВИХ ПІДПРИЄМСТВ

Сірководень відноситься до небезпечних і важливих забруднювачів, що погіршують якість повітря у виробничих зонах промислових об'єктів. Цей газ має характерний гострий запах, що дозволяє його виявляти навіть з мінімальною концентрацією. На підприємствах, що займаються видобутком та переробкою природного газу та нафти, критично важливим є впровадження комп'ютерних систем для моніторингу рівнів сірководню. Превентивні заходи щодо зниження ризиків отруєння токсичними речовинами серед співробітників вимагають регулярного контролю концентрації шкідливих газів у повітрі.

Метою цього дослідження є підвищення швидкодії системи вимірювання концентрації сірководню в атмосфері робочої зони промислового об'єкта та забезпеченні незмінності функціональних характеристик і параметрів сенсорної системи у часі.

Об'єктом дослідження обрано процеси у вимірювальному каналі сірководню в рамках комп'ютеризованої системи моніторингу концентрації газів у промисловій зоні підприємства.

Предмет дослідження сконцентрований на вдосконаленні чутливості вихідного сигналу вимірювального перетворювача у комп'ютерній системі моніторингу.

Методологія дослідження заснована на використанні математичного моделювання для аналізу характеристик вимірювального каналу, а також на тестуванні розробленого прототипу макетного зразка.

У комп'ютеризованій системі як первинний вимірювальний перетворювач застосовується оптичний сенсор [1], поверхня якого покрита полімерним шаром з додаванням барвника (див. рис. 1). Залежно від концентрації газу, що контролюється, відбувається зміна оптичних характеристик цього покриття. Для вимірювання змін прозорості цього шару в сенсорі застосовано оптичну систему, що має в своєму складі світлодіод і фотодіод.

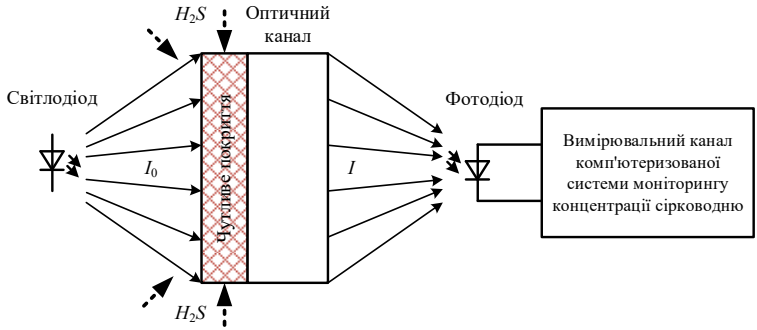


Рис. 1. Принцип визначення вимірювальної концентрації сірководню оптико-хімічним сенсором

Оптичний потік (I), що проходить аналізований об’єм кювети, перетворюється фотодіодом на електричний сигнал. Зміни цього сигналу аналізуються вимірювальним каналом комп’ютерної системи для моніторингу рівня сірководню в атмосфері промислового об'єкта. Діапазон поглинання світлової інтенсивності знаходиться в діапазоні довжин хвиль від 652 нм до 632 нм.

На рис. 2 наведено структурну схему комп’ютерної системи моніторингу концентрації сірководню в повітрі промислового підприємства. Живлення всієї комп’ютерної системи, а також передача результатів вимірювального контролю відбуваються через інтерфейс USB. Для контролю інтенсивності світлового потоку від світлодіода використовується змінний резистор, який включено послідовно із світлодіодом. Фотодіод функціонує в зворотному включенні завдяки застосуванню зворотної напруги. Як світлодіод застосовано модель L-1543SRC-C [2], а фотодіод представлений моделлю VT90N1 [3].

Сигнал падіння напруги, що утворюється на фотодіоді, надходить до вимірювального перетворювача, де відбувається його підсилення та масштабування до стандартного рівня вхідної напруги аналого-цифрового перетворювача. Після обробки, цей сигнал передається до аналого-цифрового перетворювача та далі через RS845 передається для обробки в персональному комп’ютері.

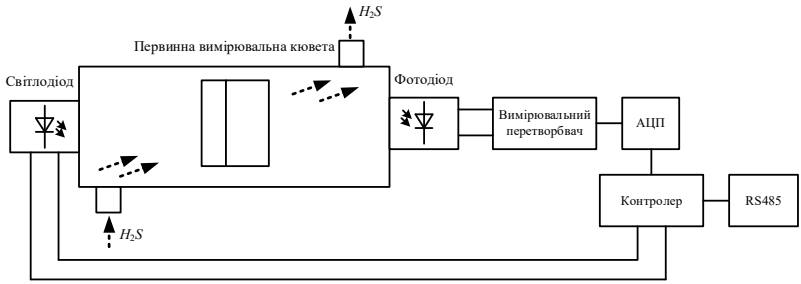


Рис. 1. Структура комп'ютерної системи моніторингу концентрації сірководню в атмосфері промислового підприємства

У персональному комп'ютері виконується обробка отриманих даних за допомогою спеціалізованого програмного забезпечення, розробленого для аналізу даних від прототипу комп'ютерної системи. Це програмне забезпечення дозволяє візуалізувати та аналізувати значення концентрації сірководню, які надходять від контролера, у форматі, що є інтуїтивно зрозумілим для користувача.

Дані приймаються через консоль у форматі ASCII. У програмі також здійснюється запис цих даних до файлу. Частота збору та запису даних становить 5 секунд. Запис вимірювань проводиться в асинхронному режимі у окремому потоці, що дозволяє оптимізувати продуктивність системи. Оновлення графічного відображення даних відбувається після кожного нового циклу обробки даних.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. ТОВ «Оптима-Комплекс» : Датчик сірководню ІПЦ-H2S. URL : https://optima-shop.com.ua/gazoanalizatory/ mnogo kanalnie-cifrovie-gazoanalizatory-dozor-s-c/datchiki-i-kompo nenty-dozor-s-c/datchik-ipc-h2s-serovodorod-dlya-dozor-s-c (дата звернення: 05.04.2024).

2. IMRAD: L-53SRC-C. URL : https://imrad.com.ua/ua/l-53src-c-0 (дата звернення: 05.04.2024).

3. Datasheets PDF: VT90N1. URL : http https://datasheetspdf. com/datasheet/VT90N1.html (дата звернення: 05.04.2024).

УДК 004.056

І.І.Тугай
Національна академія Служби безпеки України, Київ

ЄВРОПЕЙСЬКИЙ ДОСВІД ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Європейський досвід захисту критичної інформаційної інфраструктури базується на комплексному підході до кібербезпеки, який включає в себе різноманітні заходи та стратегії.

Одним з ключових елементів є створення національних та міжнародних стратегій кібербезпеки, які визначають завдання, пріоритети та ресурси для захисту критичної інформаційної інфраструктури. Ці стратегії також визначають основні підходи до виявлення та реагування на кібератаки. Нижче, проаналізуємо сучасний досвід ЄС щодо захисту критичної інформаційної інфраструктури.

У середині грудня 2020 року Єврокомісія представила нову Стратегію кібербезпеки ЄС, яка покликана зміцнити колективну стійкість Європи до кіберзагроз і гарантувати, що всі громадяни і підприємства зможуть використовувати повною мірою надійні послуги, що заслуговують на довіру, і цифрові інструменти. Стратегія покликана закласти нові засади розвитку сектора кібербезпеки на найближче десятиліття [1].

Стратегія також дозволить ЄС встановити міжнародні норми та стандарти кібербезпеки та зміцнити співпрацю з партнерами по всьому світу для просування відкритого, стабільного та безпечного кіберпростору. Єврокомісія також внесла пропозиції щодо підвищення кібербезпеки критично важливих фізичних об'єктів та мереж, включаючи захист інфраструктур, які можуть зазнавати кібернетичних нападів, таких як транспорт, енергетика, охорона здоров'я, фінансова система та багато інших секторів. Таким чином, Стратегія спрямована на усунення поточних та майбутніх онлайн-і офлайн-ризиків, від кібератак до кіберзлочинності або стихійних лих. Наприкінці червня 2021 року Європейська комісія створила нову єдину групу для боротьби з хакерами в рамках Стратегії кібербезпеки ЄС, щоб усі держави-члени були готові до колективної роботи та активного обміну інформацією [2]. Структура під назвою Joint Cyber Unit об'єднає ресурси та досвід головних фахівців ЄС для запобігання, стримування та реагування

на великомасштабні кіберінциденти. Нова група забезпечить відповідні рекомендації та передові методи співробітництва між цивільними правоохоронними органами, дипломатичними відомствами, спільнотами кібербезпеки та приватним сектором. Передбачається, що цей кібер-підрозділ стане «віртуальною та реальною платформою співпраці для протидії великомасштабним кібератакам». 17 липня 2023 року оприлюднено перелік рекомендацій для Європейського Союзу щодо забезпечення захисту держав-членів від кібератак нового типу з використанням квантових обчислень [3].У доповіді Андреа Г. Родрігеса «План забезпечення квантової кібербезпеки для Європи» йдеться про те, що проблеми, які можуть створити квантові системи для сфери захисту інформації, в основному не обговорювалися на рівні політики ЄС. А тому стратегія боротьби з такими загрозами просто відсутня. Тим часом кібербезпека відіграє важливу роль в економічній стабільності Європи. У документі викладено ключові рекомендації щодо забезпечення захисту ЄС від квантових атак: розробка плану скоординованих дій ЄС щодо квантового переходу; створення профільної експертної групи в рамках Агентства з мережевої та інформаційної безпеки Євросоюзу (ENISA) з національними експертами для обміну досвідом; визначення пріоритетів для переходу на постквантове шифрування та забезпечення криптографічної гнучкості для реагування на загрози, що виникають; забезпечення політичної координації між Європейською комісією, державами-членами ЄС, агентствами національної безпеки та ENISA для визначення технологічних пріоритетів та варіантів використання квантово-безпечних технологій.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient.* URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

2. *Creating a single group in the EU to fight hackers.* URL: https://tadviser.com/index.php/Company:Joint_Cyber_Unit

3. *A quantum cybersecurity agenda for Europe.* URL: https://www.epc.eu/en/publications/A-quantum-cybersecurity-agenda-for-Europe~526b9c

УДК 531.7

О.В.Чалий
Національний авіаційний університет, Київ

АЛГОРИТМИ ВИМІРЮВАННЯ НА КООРДИНАТНО-ВИМІРЮВАЛЬНІЙ МАШИНІ

Без належного контролю технології не можуть розвиватись. Розповсюдження верстатів з числовим програмним управлінням у виробництві призвело до зростання вимог до засобів контролю. Це призвело до широкого використання координатних вимірювальних машин (КВМ) для забезпечення ефективного контролю[1].

Основний метод вимірювання КВМ, що базується на координатах, є найбільш універсальним і може ефективно використовуватися для автоматизованого контролю широкого спектру деталей. Сучасні КВМ дозволяють виміряти майже будь-які складні поверхні та деталі в цілому, що не завжди було можливо до їхнього виникнення[2].

Весь процес можна умовно розділити на два етапи. Перший етап включає створення координатної моделі або схеми, в якій визначаються контрольні точки. Найпростіші моделі сканують об'єкт у системі координат X, Y, Z відносно базової точки. Більш технологічна шестикільцева координатно-вимірювальна машина базується на принципі паралельної кінематики. Другий етап передбачає безпосереднє зчитування інформації про геометричні параметри досліджуваного об'єкта. Для цього використовуються щупи або датчики, які сканують цільову деталь. Існують контактні і безконтактні типи щупів – контактні взаємодіють з робочою поверхнею, тоді як безконтактні працюють за принципом хвильового випромінювання.

В залежності від умов експлуатації і завдань обробки можна використовувати горизонтальні, вертикальні і мостові типи КВМ (рис.1) [3]. У горизонтальних моделях забезпечується висока точність, яка обумовлена жорсткістю їх конструкції, а також оператор отримує можливість прямого доступу до внутрішньої структури об'єкта. На практиці горизонтальні установки частіше використовуються для обробки дрібних деталей. Вертикальні координатно-вимірювальні машини вважаються найбільш точними, тому їх використовують у відповідальних метрологічних дослідженнях. Однак для ефективного використання цих установок

потрібно забезпечити термостабільність приміщення і високу витратність на їх обслуговування. Щодо мостових машин, вони завдяки своєму зносостійкому обладнанню дозволяють працювати з великоформатними виробами.

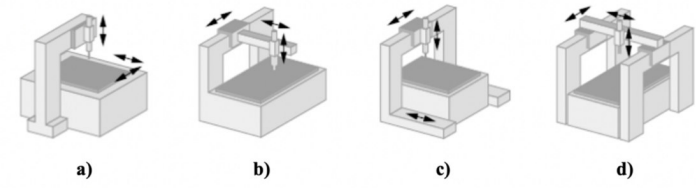


Рис.1 a,b-горизонтальні, c-вертикальні і b- мостові КВМ.

Впровадження КВМ у виробничий процес давно стало ключовим показником сучасного підходу до управління підприємством. Відмова від застарілих методів контролю елементів та використання обладнання з шаблонами підвищує якість збірки та технологічну ефективність робочої ділянки. У той же час нове покоління вимірювальних приладів для контролю геометричних параметрів постійно вдосконалюється у різних аспектах. Наприклад, безконтактні лазерні сканери є передовим напрямком розвитку, оскільки вони відрізняються зручністю використання та високою точністю аналізу. Однак головним недоліком таких прогресивних систем є їх висока вартість та складність обслуговування.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Xiao Muzheng, Jujo satomi, Takahashi Satoru, Takamasu Kiyoshi "nanometer Profile measurement of large aspheric optical surface by scanning deflectometry with rotatable devices" Proc. SPIE 8126, Optical manufacturing and testing IX, 83260R, 2011

2. Savio E, Chiffre L De"An artefect for traceable freeform measurements on coordinate measuring machines", Prec. Eng. Vol.26, 58-68, 2012

3. Chen Xiaomei, Wan Yu, Koenders Ludger and Schilling Meinhard "Measurementsof dimensional standards and etalons with feature size from tens of micrometres tomillimetres by using sensor strengthened nanomeasuring machine" Measurement Vol.43, 1369-1375, 2010.

УДК 004.056.53

А.М.Чернюк,
Д.Ю.Каліновський,
Р.С.Савіцький
Державний університет «Житомирська Політехніка, Житомир

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ПСИХОЛОГІЧНОЇ ПІДТРИМКИ

Штучний інтелект (ШІ) відкриває перед нами неабиякі горизонти можливостей, які раніше вважалися недосяжними. У світі, де психічне здоров'я стає все більшою проблемою, ШІ стає ключовим інструментом для покращення систем психологічної підтримки. У цій статті детально розглянемо, як можна ефективно інтегрувати штучний інтелект у програмні продукти, що надають психологічну підтримку, а також розглянемо етичні аспекти цього процесу та позитивний вплив на психічне здоров'я.

Імплементація штучного інтелекту в програмні продукти для психологічної підтримки охоплює різноманітні ключові функції, спрямовані на аналіз та корекцію поведінки пацієнтів. Це представляє собою інноваційні підходи до психотерапії та консультування, які можуть ефективно вдосконалити результати психологічного супроводу.

Штучний інтелект використовує комплексні алгоритми для аналізу текстових звернень пацієнтів. Здатність розпізнавати емоційні відтінки, виражені у мові, дозволяє системі точніше розуміти стан та потреби користувача. Техніки обробки природної мови та аналізу сентиментів дозволяють ШІ автоматично визначати ключові теми та настрій пацієнта.

Не менш важливою функцією є фіксація поведінки пацієнта у діалозі. ШІ може вивчати структуру та інтонацію мовлення, виявляти зміни у поведінці та автоматично реагувати на них. Наприклад, система може реалізувати техніки емпатії, допомагаючи пацієнту відчути важливість його почуттів та досвіду.

Іншою ключовою функцією штучного інтелекту є надання індивідуалізованих порад та вправ для підтримки психічного здоров'я пацієнтів. Система може аналізувати ефективність різних психотерапевтичних стратегій та адаптувати їх до потреб конкретного користувача. Використовуючи машинне навчання, ШІ

може постійно вдосконалювати свої рекомендації на основі результатів та відгуків пацієнта.

Інтеграція ШІ в область психічного здоров'я відкриває безліч можливостей для покращення надання психологічної підтримки та психотерапії. Зокрема, інтеграція моделей штучного інтелекту дозволяє використовувати різні стратегії психології та психотерапії в автоматизованому режимі. Наприклад, система може використовувати когнітивно-поведінкові техніки для корекції негативних міркувань чи реляційні підходи для вирішення конфліктів, розширюючи тим самим психотерапевтичний арсенал та забезпечуючи більш ефективну допомогу.

Ця інтеграція в системи психологічної підтримки не лише покращує якість надання послуг, але й полегшує роботу операторів. Автоматизація процесів, таких як запис інформації про клієнтів, планування сесій та навіть проведення деяких аспектів терапії, дозволяє фахівцям зосередитися на більш важливих аспектах роботи з клієнтами.

В сучасному світі, де технології стають необхідним інструментом для розвитку різних галузей, штучний інтелект вже вносить значний вклад у сферу психічного здоров'я. Інновації використання штучного інтелекту, такі як чат-боти для цифрового доступу до медичних консультацій та системи для виявлення ризику самогубства, показують великий потенціал у покращенні надання психічної підтримки та забезпеченні доступу до необхідних ресурсів [1].

Навіть у галузі діагностики, ШІ виявляє свій вплив, пропонуючи інтерпретовані глибокі мережі, які з вражаючою точністю діагностують різні психічні розлади. Важливою частиною цього процесу є розгляд етичних, юридичних та регуляторних вимог для забезпечення безпеки та ефективності використання нових технологій.

Додатки з розмовними ШІ-агентами, такі як Woebot, Wysa та Tess, вже впроваджують психотерапію в повсякденне життя, дозволяючи користувачам отримувати підтримку в будь-який час і в будь-якому місці. Це вказує на готовність сучасних людей взаємодіяти з мобільними додатками для психічного здоров'я, що відкриває нові можливості для інтеграції моделей у практику психотерапії та психологічної підтримки. Застосування штучного інтелекту дозволить операторам швидше реагувати на кризові

ситуації. Системи можуть автоматично виявляти сигнали ризику та надсилати повідомлення операторам, щоб вони могли приймати необхідні заходи. Це може врятувати життя та сприяти збереженню психічного здоров'я клієнтів. Крім того, ШІ може надавати операторам рекомендації та аналітику, що допоможе їм краще розуміти потреби користувачів і реагувати на них більш ефективно.

Однак, з впровадженням ШІ в сферу психологічної підтримки виникає ціла низка етичних питань [2]. Збір та збереження великої кількості особистих даних може порушити конфіденційність та приватність пацієнтів. Важливо розробити чіткі стандарти безпеки даних та забезпечити, щоб доступ до цих даних був обмежений та контрольований.

Додатково, важливо враховувати, що технології ШІ можуть бути обмежені в своїй здатності виявляти складні та індивідуальні аспекти психічного здоров'я. Повне покладання на алгоритми може призвести до втрати людського аспекту та непередбачуваності, яка іноді є необхідною в роботі психотерапевтів.

Підбиваючи підсумки, застосування штучного інтелекту в системах психологічної підтримки є не лише технологічним вдосконаленням, але й можливістю покращити психічне здоров'я нашого суспільства. Важливо розробляти та впроваджувати ці технології з урахуванням етичних стандартів та забезпечувати їх відповідальне використання для досягнення максимальної користі для людей. Від усіх нас залежить, як ми використаємо цей потенціал для покращення психологічного благополуччя громади.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Результати досліджень щодо використання ШІ в системах психологічної підтримки [Електронний ресурс]. – Режим доступу: https://web.archive.org/web/20240310230451/https://www.himss.org/resources/role-artificial-intelligence-and-its-impact-mental-health-services.

2. Американська психологічна асоціація [Електронний ресурс]. – Режим доступу: https://web.archive.org/web/20240217160909/https://www.apa.org/monitor/2023/07/psychology-embracing-ai.

УДК 004.056

Т.Р. Чура,
Н.Р. Чура
Національний університет «Львівська Політехніка»

ІНТЕГРАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МЕТОДИ AGILE РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ПРИКЛАДІ SECURE SCRUM

Запропонована методологія Secure Scrum (S-S) пропонує кілька підходів до впровадження безпеки в рамках Scrum.

Компанія Veracode запропонувала два методи: Підхід з безпечного спринту та Кожно-спринтовий підхід. У Кожно-спринтовому підході безпекові історії користувачів включаються в кожний Спринт, що вимагає наявності дорогого фахівця з безпеки в команді Scrum. З іншого боку, у підході з Безпечного Спринту безпекові історії користувачів аналізуються та розробляються у відокремленому Спринті, що може спричинити затримки у розробці.

Mongouei, Sani, та Almasi (2013) ввели S-Scrum, покращену версію Scrum, у якій вони включили "Спайки" як Події Scrum. Ця модифікація змінює основну структуру рамки S-Scrum.

Secure Scrum, який характеризується як легкий і простий підхід, акцентує увагу на розробці безпечного програмного забезпечення протягом усього процесу розробки. Він складається з чотирьох компонентів: Ідентифікації, Впровадження, Верифікації та Визначення Готовності. Ці компоненти інтегруються з шістьма стандартними частинами Scrum для підвищення безпеки розробки програмного забезпечення. Основними поняттями в Secure Scrum є S-Тег та S-Маркер.

Компонент Ідентифікації визначає проблеми безпеки у користувальницьких історіях, наданих Власником продукту та зацікавленими сторонами. Потім безпекові користувальницькі історії пріоритизуються за ризиком і позначаються в Беклогу продукту за допомогою S-Маркера. Для кожної позначеної користувальницької історії створюється S-Тег, який описує проблему безпеки, яка може вплинути на один або кілька елементів Беклогу продукту.

Оскільки елементи Беклогу продукту можуть змінюватися з часом для адаптації розробки, S-Теги можуть бути змінені під час уточнення Беклогу або планування нового Спринту. Компонент Впровадження гарантує усвідомленість команди розробки вимог безпеки, пов'язаних з позначеними S-Маркером користувальницькими історіями.

Компонент Верифікації - це частина завдання, яка забезпечує перевірку членами команди проблем безпеки, виявлених завданнями з позначкою S-Маркером. Цей процес верифікації є частиною Визначення Готовності і здійснюється під час щоденного зустрічі Scrum.

У випадках, коли членам команди не вистачає знань або часу для внутрішньої перевірки проблем безпеки, може знадобитися залучення зовнішніх ресурсів. Отже, створюється нове завдання для верифікації, яке успадковує S-Маркер та всі пов'язані S-Теги з оригінального завдання. Зовнішні ресурси можуть допомогти Команді Scrum у збільшенні знань, подоланні викликів та наданні зовнішнього погляду на це завдання. Компонент Визначення Готовності гарантує, що верифікація безпеки буде проведена або внутрішніми, або зовнішніми ресурсами.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Keramati, H., & Mirian-Hosseinabadi, S.-H. (2008). Integrating Software Development Security Activities with Agile Methodologies. 2008 IEEE/ACS International Conference on Computer Systems and Applications (pp. 749 - 754). IEEE.*
2. *Mougouei, D., Sani, N. F., & Almasi, M. M. (2013). S-Scrum: a Secure Methodology for Agile Development of Web Services. World of Computer Science and Information Technology Journal (WCSIT), 3(1), 15-19.*

УДК 004[056.53::413.4]

О.М.Шаповал,
В.В.Цуркан, к.т.н.,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ

РИЗИК-ОРІЄНТОВАНА АРХІТЕКТУРА БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ

Запорукою діяльності будь-якої організації є наявність вчасної, точної і повної інформації. Вона накопичується, обробляється, зберігається, передається завдяки використанню комп'ютерних мереж. З огляду на це, необхідно забезпечувати непорушність насамперед основних властивостей інформації, зокрема, конфіденційності, цілісності та доступності. Така необхідність обумовлена запобіганням експлуатуванню загрозами вразливостей комп'ютерних мереж. Запобігання таким проявам досягається шляхом обирання відповідних заходів і засобів оброблення неприйнятних ризиків [1, 2].

Комп'ютерні мережі в організаціях характеризуються змішаною архітектурою. При цьому основою внутрішніх комунікацій є мережа інтранет. До того ж як важливий складник виокремлюється бездротовий сегмент. За потреби забезпечення голосового спілкування використовується IP телефонія зі з'єднаннями або телефонною мережею загального користування, або мережею стільникового зв'язку за допомогою GSM-шлюзу. Доступ зацікавлених сторін до внутрішньої мережі організовуються через екстранет. З цим пов'язане виділення демілітаризованої зони з підключенням до глобальної мережі Інтернет. Крім того, у багатьох організаціях є віддалені майданчики (філії, склади, виробництво) [1]. Тому проєктування безпечних комп'ютерних мереж це завжди прагнення до балансуванням між ризиками безпеки та вигодою у поєднанні зі зручністю. Подолання даного протиріччя можливе завдяки формулюванню і задоволенню нефункційних вимог (безпеки). Вони визначаються як заходи оброблення неприйнятних ризиків. Як наслідок, це дозволяє створити архітектуру безпеки комп'ютерної мережі на етапі їх проєктування. Крім того стане можливим урахування особливостей середовища використання комп'ютерних мереж в організаціях [1–3].

Для створення архітектури безпеки комп'ютерних мереж

рекомендовано використовувати ризик-орієнтований підхід. За ним впроваджуються відповідні заходи та засоби оброблення. Їхньому обиранню передує оцінювання ризиків безпеки комп'ютерних мереж. Залежно від обраної шкали вони узагальнено знаходяться як добуток імовірності (вірогідності) і наслідків реалізування загрози. Для цього визначаються метод і критерій прийнятності. За результатами зіставлення оцінок ризиків безпеки комп'ютерних мереж з прийнятним значенням ухвалюється рішення про необхідність оброблення. Така необхідність обґрунтовується наявністю неприйнятних оцінок. Вони ранжуються і пріоритезуються з огляду на черговість оброблення (найбільша оцінка має найвищий (перший) пріоритет). З огляду на встановлені пріоритети обираються відповідні заходи (модифікування, приймання, ухиляння, розподілення) та засоби [2, 3].

Отже, діяльність організацій обумовлюється використанням комп'ютерних мереж. Характерною їх особливістю є проєктування за змішаною архітектурою. Така особливість призводить до необхідності балансування між ризиками безпеки комп'ютерних мереж та вигодою у поєднанні зі зручністю. Подолання даного протиріччя досягається впровадженням заходів оброблення неприйнятних ризиків. Завдяки цьому створюються архітектура безпеки комп'ютерних мереж і, як наслідок, враховуються особливості середовища їх використання в організаціях.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. ISO/IEC 27033-1:2015. Information technology. Security techniques. Network security. Part 1: Overview and concepts. [Valid from 2015-08-10; revised 2021-04-19]. URL: https://www.iso.org/standard/63461.html (accessed on: 14.04.2024).

2. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks. [Valid from 2022-10-25]. URL: https://www.iso.org/standard/80585.html (accessed on: 14.04.2024).

3. ISO/IEC 27033-2:2012. Information technology. Security techniques. Network security. Part 2: Guidelines for the design and implementation of network security. [Valid from 2012-07-27; revised 2023-07-15]. URL: https://www.iso.org/standard/63461.html (accessed on: 14.04.2024).

УДК 004.8

Р.А.Ширшов

Національна академія СБ України, Київ

РИЗИКИ ВИКОРИСТАННЯ СИСТЕМ ШІ

В останні роки використання систем штучного інтелекту (ШІ) стало все більш поширеним у різних секторах, включаючи військову справу, технології, охорону здоров'я, фінанси та транспорт. Незважаючи на переваги, які приносить широке впровадження ШІ, такі як покращення ефективності та продуктивності, підвищення швидкості та точності прийняття рішень, існують також значні ризики, пов'язані з його використанням, які потребують ретельного розгляду.

Одним з основних викликів є відсутність прозорості та відповідальності в процесах прийняття рішень на основі ШІ, що може призвести до непередбачених наслідків та шкоди для окремих осіб або суспільства в цілому.

Останнім часом з’явилися підтвердження використання систем з ШІ в якості керуючого елементу для безпілотних ударних комплексів. Також, збір та використання великих обсягів особистих даних системами ШІ викликає серйозні побоювання щодо конфіденційності.

Крім того, зростаюча залежність від систем ШІ викликає занепокоєння щодо заміщення робочих місць та потенціалу економічної нерівності. Етичні наслідки використання систем ШІ виходять за рамки приватності та упередження, оскільки існує також ризик зловмисного використання та потенційних загроз національній безпеці.

Одним з механізмів зниження ризиків є управління ризиками штучного інтелекту (ШІ) з метою їх вимірювання та зменшення для задоволення визначеному набору вимог. Щоб повною мірою зрозуміти це, необхідно визначити, що таке ризик ШІ.

Значення ризику ШІ може бути виражено як добуток ймовірності помилки моделі ШІ або її експлуатації на потенційний ефект.

Помилки ШІ та вразливості є численними, часто трапляються

і варіюються в залежності від завдань моделі. Приклади включають виконання довільного коду, отруєння даних, ін'єкцію запитів, екстракцію моделі, галюцинації, дрейф даних, неочікувану поведінку, упереджені прогнози та токсичний вивід.

Ефекти помилки моделі в основному залежать від випадку використання. Вони можуть бути фізичними (для кібер-фізичних систем), фінансовими, правовими або репутаційними. Що важливіше, вони можуть мати руйнівні наслідки безпосередньо для користувачів.

Ризики використання систем з ШІ відрізняються від ризиків використання програмного забезпечення. Традиційне програмне забезпечення базується на процедурній логіці для трансформації входу в заданий вихід.

Натомість, перевага ШІ полягає в тому, що воно може «вчитися» логіці з набору даних, а не вимагати від користувача її явного визначення. Оскільки користувач не може безпосередньо спостерігати за цією логікою, це робить тестування систем з ШІ набагато важчим і вимагає нових підходів.

Просте тестування на кількох точках даних і крайніх випадках вже недостатньо для підтвердження «правильності». Тепер користувач повинен тестувати продуктивність моделі за допомогою наборів даних для оцінки та підтверджувати, що модель також може робити правильні прогнози на потенційно нескінченному наборі можливих розподілів даних.

Моделі ШІ представлені у широкому спектрі завдань, починаючи від бінарної класифікації на табличних даних до відповідей від генеративного ШІ.

Кожне завдання має свої унікальні режими збоїв та вимоги до тестування. Більше того, оскільки ШІ передбачає автоматизацію критичних рішень, існують тести, що включають тестування проти упередженості та справедливості, а також зловживань чутливою інформацією, яка може бути закодована у моделі та даних.

Управління ризиками ШІ відноситься до набору інструментів та практик, що застосовуються для проактивного захисту від

ризиків ШІ. Воно передбачає вимірювання ризиків та впровадження рішень для їх мінімізації. Відповідно до визначення ризику ШІ, його можна мінімізувати, зменшивши ймовірність збою або знизивши серйозність наслідків.

Згідно з NIST AI RMF: Управління ризиками ШІ є ключовим компонентом відповідальної розробки та використання систем ШІ. Відповідальні практики ШІ можуть допомогти узгодити рішення про проектування, розробку та використання систем ШІ з призначеною метою та цінностями. Основні концепції відповідального ШІ підкреслюють орієнтованість на людину, соціальну відповідальність та стійкість. Управління ризиками ШІ може спонукати до відповідального використання та практик, заохочуючи організації та їх внутрішні команди, які проектують, розробляють та впроваджують ШІ, більш критично мислити про контекст та потенційні або несподівані негативні та позитивні впливи.

Автоматизація управління ризиками ШІ

Виявлення помилок в системах ШІ та розроблення заходів щодо їх пом'якшення вручну вимагатиме великих ресурсів, як людських, так і фінансових. Використання інструментів для автоматизації управління ризиками ШІ може перетворити пасивні фреймворки на активні практики. Така автоматизація допомагає проактивно вимірювати та зменшувати ризик, надаючи впевненість у розгортанні ШІ у великих масштабах.

Наукове видання

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
XV МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ
ТА МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2024)

25–26 квітня 2024 року

Тези доповідей надруковані в авторській редакції
однією із двох
робочих мов конференції: українською, англійською.