МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
Національний авіаційний університет
Факультет кібербезпеки, комп'ютерної
та програмної інженерії

CSNT 2021

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

XIII Міжнародної науково-практичної конференції

КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖНІ ТЕХНОЛОГІЇ

15-17 квітня 2021 року

Київ 2021

УДК 004.7(043.2)

Збірник тез доповідей XIII Міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2021), м. Київ, 15–17 квітня 2021 р., Національний авіаційний університет. – К.: НАУ, 2021. – 99 с.

Збірник тез доповідей укладено за матеріалами XIII міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2021). У доповідях розглянуті наукові, технічні та технологічні проблеми побудови, проектування сучасних комп'ютерних систем, засоби і методи моделювання комп'ютерних мереж, проблеми захисту ресурсів в інформаційних систмах, технології підготовки авіаційних фахівців.

Рекомендовано до видання вченою радою Факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету (протокол № 5 від 15 березня 2021 р.).

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

ЗМІСТ

УДК 519.218.82 (043.2)

О.В. Андреєв, к.т.н.,
В.І. Андрєєв, к.т.н.
Національний авіаційний університет, Київ

СПОСІБ ВИЗНАЧЕННЯ КОЕФІЦІЄНТА НЕЛІНІЙНОСТІ ВИПАДКОВОГО НЕСТАЦІОНАРНОГО ПРОЦЕСУ

Визначення коефіцієнта нелінійності випадкового нестаціонарного сигналу (ВНС) має важливе значення для аналізу характеристик цього процесу та для екстраполяції значень його характеристик.

Модель НВС для моменту часу t_3, для якого виконується екстраполяція параметрів, має такий вигляд [1]:

$$Y(t_3) = Y_3 = a_0 + a_1 t_3^g + x(t_3), \qquad (1)$$

де α_0 – початкова очка процесу, α_1 – швидкість протікання процесу, γ – коефіцієнт нелінійності, ξ – величина завади.

Цей вираз містить в собі параметр γ – коефіцієнт нелінійності ВНС. Запропонований нижче спосіб дозволить оперативно обчислювати його, маючи два попередні дискретні значення сигналу – Y_1, Y_2.

Аналогічний спосіб з іншою постановкою задачі було запропоновано в статті [2], та він був адаптований під нашу задачу.

На рис. 1 показані всі основні характеристики і параметри для визначення коефіцієнта нелінійності γ.

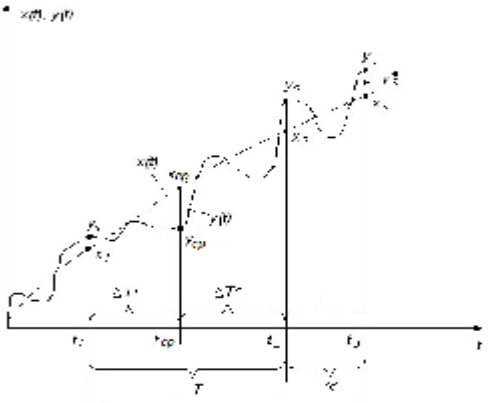

Рис.1. Ілюстрація основних характеристик і параметрів

Для знаходження коефіцієнта нелінійності введемо такі додаткові параметри:

$Y_{ср}$ – середнє арифметичне значення для дискретних значень сигналу Y_1, Y_2.

$X_{ср}$ – середнє арифметичне значення для дискретних значень сигналу без завади X_1, X_2.

$t_{ср}$ – вимір часу, що відповідає середньому арифметичному значенню для дискретних значень сигналу Y_1, Y_2 (з завадою), або X_1, X_2 (без завади).

ΔT_1 – інтервал між вимірами часу $t_{ср}$ та t_1 .

ΔT_2 – інтервал між вимірами часу t_2 та $t_{ср}$.

1. Маємо два дискретні спостереження сигналу – Y_1 та Y_2.

2. Візьмемо середнє арифметичне цих значень для дискретних значень сигналу – Y_1, Y_2. та для відповідних моментів часу t_1 та t_2.

Отримаємо додаткові параметри: середнє значення для величин сигналу $Y_{ср}$ і часу $t_{ср}$. Відповідно відстань між значенням часу $t_{ср}$ та моментів часу t_1 та t_2 запишемо як ΔT_1 та ΔT_2:

$$DT_1 = t_{cp} - t_1, \; DT_2 = t_2 - t_{cp}. \qquad (2)$$

5. Враховуючи проміжки часу ΔT_1 та ΔT_2 (2), запишемо вирази для обчислення $Y_{ср}$ та γ в наступному вигляді для їх практичного знаходження:

$$Y_{cp.пр} = \sqrt[g]{\frac{Y_1 \times DT_2 + Y_2 \times DT_1}{DT_1 + DT_2}}, \qquad (3)$$

$$g_{пр} = \frac{ln(Y_1 \times DT_2 + Y_2 \times DT_1) - ln(DT_1 + DT_2)}{lnYcp}. \qquad (4)$$

Таким чином, ми отримали спосіб оперативного визначення коефіцієнта нелінійності випадкового нестаціонарного сигналу на тлі завад.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Ігнатов В.О. Метод оптимальної екстраполяції випадкових нестаціонарних сигналів на тлі завад / В.О. Ігнатов, О.В. Андреєв, В.І. Андрєєв // Проблеми інформатизації та управління: Зб. наук. праць – К.: НАУ, 2010. – Вип. 2(30). - С. 79-83.

2. Столчнев В.Г. Геометризация месторождений с позиции "неевклидовой" геометрии Текст./Маркшейдерия и недропользование. 2004. – №3. - С. 43-62.

УДК 656.7.022.4

С.В. Балакін, к.т.н.,
Б.І. Долінце
Національний авіаційний університет, Київ

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ ДОГОВОРУ ПРО СПІЛЬНИЙ АВІАЦІЙНИЙ ПРОСТІР

Спостерігається поступове переміщення центру авіаційної галузі з Європи до Азії, поява міжконтинентальних рейсів бюджетних перевізників на далекі відстані та питання щодо конкурентного ефекту глобальних альянсів знову викликали інтерес до питання лібералізації в авіаційній галузі.

Українською стороною було виконано відповідні внутрішні процедури та отримано повноваження на укладання Угоди у травні 2014 року, але через територіальний спір Іспанії та Британії підписання документу кілька разів переносилося [1].

Для уніфікації інформації про спільний авіаційний простір з ЄС перш за все потрібно узгодити продукти аеронавігаційної інформації, що включають в себе:

1. Збірник аеронавігаційної інформації, зміни та доповнення до нього;
2. Циркуляр аеронавігаційної інформації;
3. Аеронавігаційні карти;
4. NOTAM;
5. Масиви цифрових даних.

Авіаційний сектор є життєво важливим для економіки Європейського Союзу, на який припадає 2,1 відсотка (300 мільярдів євро) ВВП [2, 3].

Незважаючи на прогнози подальшого зростання авіаперевезень, повне використання європейського повітряного простору стримується неефективністю європейської системи управління повітряним рухом. Єдине європейське небо охоплює низку законодавчих та регуляторних заходів, що відображають бачення реформування управління повітряним рухом в Європі, щоб остаточно вийти за межі національного контролю повітряного простору.

Для реагування на ці питання у 2004 році Європейською Комісією була створена програма Єдиного європейського неба. Дана ініціатива працює шляхом застосування правових норм до ЄС

та його держав-членів з метою реформування проблемних аспектів операцій у європейському повітряному просторі шляхом пропонування загальноєвропейських законів, спрямованих на посилення міжнародного співробітництва та підвищення ефективності [4].

Важливим елементом побудови такої системи є не тільки внутрішній ринок ЄС, а й розбудова мережі авіаційного сполучення із сусідніми країнами. Основним механізмом для такого співробітництва виступають договори про «відкрите небо».

Із статистичних даних, можна зробити висновок, що подальша лібералізація може принести додаткові вигоди як авіаційній галузі, так і економіці окремих країн в цілому. Найвищий ефект зростання виручки від туризму спостерігається в країнах що мають розвинений внутрішній туристичний ринок. Слід визнати, що на конкурентному ринку повітряного транспорту, як і в будь-якій іншій галузі, завжди знайдуться переможці та ті хто програв.

Майбутні дослідження наслідків лібералізації європейського авіаринку можуть розширити розуміння даних питань, в тому числі розглядаючи наслідки зовнішньої авіаційної політики ЄС на добробут громадян, загальноекономічні ефекти політики, включаючи її вплив на авіаційні вантажі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Коссе Ірина, Кульчицька Катерина. Авіаційний вектор східного партнерства: оцінка прогресу України, Молдови та Грузії у наближенні до авіаційного законодавства ЄС. Київ, 2017. – 17 с.

2. Single European Sky: The progress so far. Journal of Aerospace Technology and Management, University of Huddersfield, 2020.

3. Christopher Lawless. Assembling airspace: The Single European Sky and contested transnationalities of European air traffic management. Durham University, UK, 2020.

4. Megersa Abate, Panayotis Christidis. The impact of air transport market liberalization: Evidence from EU's external aviation policy. Economics of Transportation, 2020.

УДК 004.055.53

А.В. Бикадорова
Національний авіаційний університет, Київ

ЗАХИСТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В КІБЕРПРОСТОРІ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН

У сучасному інформаційному суспільстві об'єкти інтелектуальної власності (ІВ), у тому числі досягнення у науці, літературі, мистецтві, мають велике значення. Із розвитком науково-технічного прогресу з'явились і нові об'єкти ІВ, такі як комп'ютерні програми, цифрові документи, бази даних, тощо, які можуть бути збережені як на матеріальному носії так і у електронному вигляді. З огляду на відносну простоту викрадення інформації виникають нові проблеми у сфері її захисту. Особливості ІВ як цифрового об'єкта (зокрема, легкість копіювання) призвели до зміни підходів, які склалися в правовій сфері використання ІВ, і до необхідності адаптації їх до нових умов. Глобальний технологічний розвиток, створення, розширення та використання існуючих та нових технологій тісно пов'язане із захистом ІВ на міжнародному правовому рівні.

У правовому розумінні "інтелектуальна власність" – це права на результати розумової діяльності людини в науковій, художній, виробничій та інших сферах, які є об'єктом цивільно-правових відносин у частині права кожного володіти, користуватися і розпоряджатися результатами своєї інтелектуальної, творчої діяльності, які, будучи благом не матеріальним, зберігаються за його творцями і можуть використовуватися іншими особами лише за узгодженням з ними, крім випадків, визначених законодавством України[1].

Сьогодні інтелектуальна власність стоїть перед новим етапом розвитку захисту: блокчейн (англ. blockchain) – одна із найактуальніших тем останнього часу. Ця технологія стала настільки широковідомою завдяки тому факту, що на її основі були створені такі криптовалюти, як Біткоїн (англ. Bitcoin) та Ефіріум (англ. Ethereum).

Використання блокчейну надає багато переваг у порівнянні з іншими технологіями захисту ІВ в кіберпросторі. Отже, блокчейн – це розподілена база даних, що зберігає впорядкований ланцюжок

записів (так званих блоків), що постійно довшає. Дані захищено від підробки та спотворення. Кожен блок містить часову позначку, геш попереднього блока та дані транзакцій, подані як геш-дерево[2]. Найчастіше копії блокових ланцюгів зберігаються на безлічі різних комп'ютерів незалежно один від одного. Таким чином, блокчейн – це відкрита книга інформації, яка обмінюється та перевіряється усіма учасниками однорангової мережі. Кожен запис або блок передається всім учасникам мережі і повинна перевірятись кожним вузлом, що бере участь, розв’язуючи складну математичну задачу. Після перевірки блоку він додається до книги або ланцюга. У свою чергу, використання шифрування гарантує що користувачі можуть змінювати лише ті частини ланцюга блоків, до яких у них є приватні ключі, без яких запис у файл неможливий. Крім того, шифрування забезпечує синхронізацію копій розподіленого ланцюга блоків серед усіх користувачів.

В даний час існує декілька сервісів (наприклад, Proof of Existence, Emernotar, Депонент), за допомогою яких завантажений файл з об’єктом ІВ гешується, а результат (унікальний відбиток файлу - геш) заноситься в блокчейн. У разі необхідності перевірки проводиться повторна операція гешування, і отриманий геш порівнюється з гешем, що зберігається в блокчейні. Збіг гешу гарантує, що конкретний файл був внесений в блокчейн в конкретний момент часу.

З точки зору теорії інформації, по-справжньому інноваційний характер технології розподіленої книги пов'язаний з тим, що вона забезпечує цілісність книги за допомогою контролю всіх учасників ланцюга та виключає необхідність центрального регулювання. Іншими словами, транзакції перевіряються та підтверджуються численними комп'ютерами, які зберігають блокчейн. Тому дана технологія вважається абсолютно стійкою, оскільки для зміни будь-якої інформації кібератака повинна бути спрямована (практично) на всі копії книги одночасно.

У порівнянні з іншими технологіями захисту ІВ блокчейн дозволяє суттєво спростити процедуру фіксації факту авторства, скоротити її строки і вартість. Крім того, ці записи залишаються в реєстрі незалежно від існування організації-депозитарію.

Таким чином, застосування блокчейна особливо актуально в даний час, оскільки з розвитком інтернету об'єкти ІВ можуть

використовуватися в різних юрисдикціях, в тому числі і з порушенням прав на їхнє використання. Блокчейн дозволяє будь-якій особі в будь-якій точці світу швидко і без участі будь-яких посередників отримати доступ до відомостей про правовласників і інформаційної власності.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *ПРАВОВЕ РЕГУЛЮАННЯ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В УКРАЇНІ // Заступник начальника відділу Центру правової реформи і законопроектних робіт при Міністерстві юстиції України Костюченко Оксана Миколаївна [Електронний ресурс]. – Режим доступу: https://minjust.gov.ua/m/str_4487*
2. *Блокчейн // Матеріал з Вікіпедії – вільної енциклопедії [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD*
3. *Intellectual Property Protection / Kristina Zaytseva – 14.12.2018. [Електронний ресурс]. – Режим доступу: https://zuykov.com/en/about/articles/2018/12/15/new-technology-and-its-protection-intellectual-pro/*
4. *Объекты интеллектуальной собственности в цифровой форме / Атанасов С. – 16.03.2004. [Електронний ресурс]. – Режим доступу: http://www.i2r.ru/static/504/out_23440.shtml*
5. *Объекты интеллектуальной собственности в век цифровых технологий / Избаш О. О., ОНМА – 2014. [Електронний ресурс]. – Режим доступу: http://dspace.onua.edu.ua/bitstream/handle/11300/1643/Izbash%20Obj eekty%20intel%20sobstv.pdf?sequence=1&isAllowed=y*

УДК 510.635:004.891 (045)

А.І. Вавіленкова, д.т.н.,
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ МЕТОДОЛОГІЇ MSF ДЛЯ СТВОРЕННЯ SCRUM-КОМАНДИ

Порядок виконання задач, структура та функції команди, обрання методів оцінки та контролю визначає обрана методологія розробки програмного забезпечення. Одним із способів реалізації основних ідей гнучкої методології розробки програмного забезпечення Scrum [1] є модель команди Microsoft Solution Framework (MSF), у якій всі члени команди відповідальні та зацікавлені у високому результаті створеного програмного продукту. Це забезпечується завдяки рольовим кластерам MSF[2], кожен з яких представляє собою унікальну точку зору на проєкт та може включати як одного, так і декількох членів команди. Кожен рольовий кластер має зону відповідальності:

- кластер управління програмою – відповідає за управління проєктом, тобто те, щоб вимоги клієнта були правильно сприйняті та проведені через проєкт – у такий рольовий кластер обов'язково повинен входити Product Owner;
- кластер архітектури продукту – відповідає за всю систему в цілому, розробляє архітектуру рішення, включаючи сервіси, технології та стандарти, які будуть використані впродовж роботи – входять представники усіх трьох груп ролей Scrum-команди – Product Owner, Scrum-master та команди розробників;
- кластер розробки – призначений для проєктування та здійснення реалізації – входить вся команда розробників;
- кластер тестування – відповідає за якість отриманого програмного рішення з точки зору замовника та майбутніх користувачів – беруть участь члени команди розробників;
- кластер управління версіями – відповідає за впровадження програмного рішення в інфраструктуру замовника – до кластера входять Product Owner, Scrum-master та представники команди розробників;
- кластер задоволення споживача – відповідає за розуміння потреб та їх коректну реалізацію у розробленому програмному продукті – відповідальні Product Owner та Scrum-master;

- кластер управління продуктом – відповідає за розуміння кінцевого результату – входять Product Owner, Scrum-master та представники команди розробників.

Таким чином, однією із складових успішної розробки програмного забезпечення згідно з методологією MSF є структура команди та розподіл зон відповідальності рольових груп. Із попереднього опису видно, що модель команди MSF можна накласти на структуру Scrum-команди та реалізувати шляхом створення командного проєкту у програмному середовищі Visual Studio на базі використання Team Foundation Server (Рис. 1).

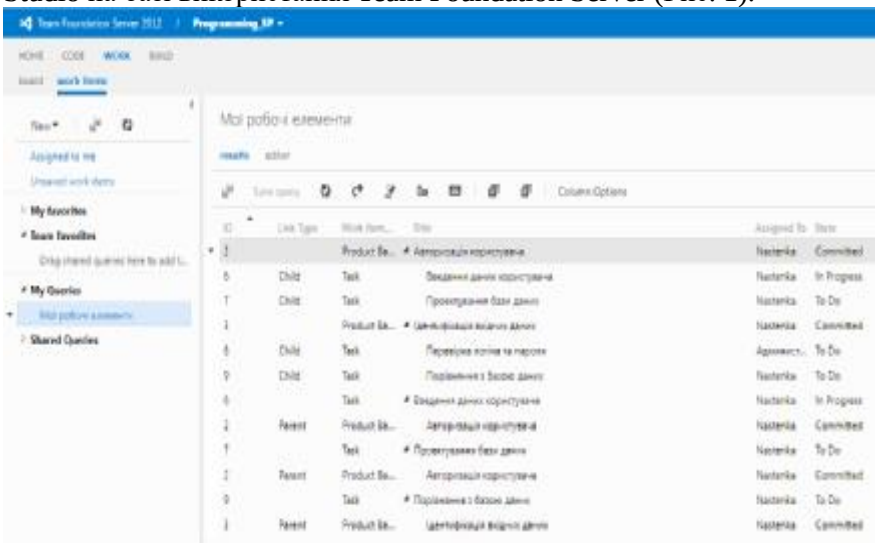

Рис.1. Приклад навчального командного проєкту у Visual Studio

Створення навчальних командних проєктів на основі методології MSF та розподіл членів команди на рольові кластери дає змогу дослідити та отримати візуальні результати процесу створення програмного продукту.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Satherland D. (2015) Scrum. The Art of Doing Twice the Work in Half the Time. Random House, 256 p. 2. Microsoft Solutions Framework. Basic Principles. URL: https://newline.tech/microsoft-solutions-framework-basic-principles.

УДК 004.942: 620.179.18: 621.643.8

О.А. Владимирський, д.т.н.,
І.А. Владимирський, к.т.н.
ІПМЕ ім. Г.Є. Пухова НАН України, Київ

ОРГАНІЗАЦІЯ МОБІЛЬНОГО ПРОСТОРОВО - РОЗПОДІЛЕНОГО, СИНХРОНІЗОВАНОГО ЗБОРУ АКУСТИЧНИХ ДАНИХ ПРО СТАН ПІДЗЕМНИХ ТРУБОПРОВОДІВ

Схема розгортання основного устаткування системи реєстрації РАСТР-1М на ділянці трубопроводу, що діагностується, приведена на Рис. 1. Реєстратори “А” і “В” встановлюються біля двох суміжних місць доступу до трубопроводу, наприклад теплокамер (ТК) уздовж обстежуваного трубопроводу. Вібродатчики ВДМ встановлюються на трубопроводі за допомогою магнітних тримачів і підключаються до реєстраторів.

Для проведення вимірювань в активному режимі додатково встановлюється акустичний випромінювач за допомогою магнітного утримувача. Акустичний випромінювач підключається до виходу блоку РАСТР-ТЕСТ [1], в якому змонтовані підсилювач зондуючих сигналів, генератор і радіопередавач синхронізації.

Для коректного застосування кореляційних методів реалізована синхронізація записів вібросигналів з точністю, не гірше 0,1 мс. Сигнал синхронізації (смуговий шум) надходить до реєстраторів по радіоканалу. При подальшій, попередній обробці записів з реєстраторів спочатку здійснюється їх синхронізація за допомогою кореляційної обробки і формування єдиного файлу даних. Сигнали синхронізації видаляються і в подальшому не використовуються.

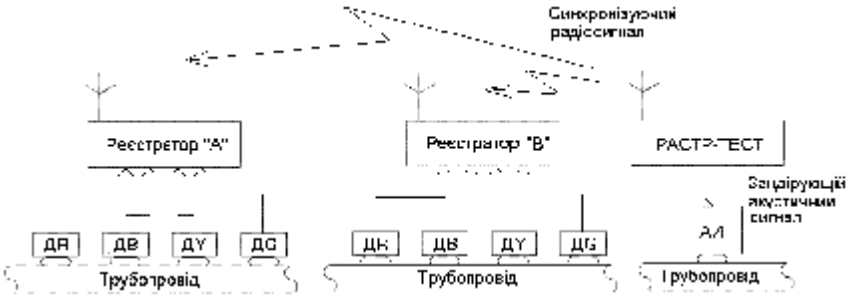

Рис. 1. Розгортання системи РАСТР-1М на трубопроводі.

Система РАСТР-1М призначена, в першу чергу, для роботи в активному режимі. Для роботи в умовах багатохвильового поширення акустичних сигналів (хвиль гідравлічного удару по транспортованому середовищу, поверхневих, поперечних, повздовжних - по стінці трубопроводу та ін.), інтерференційних спотворень, використовується "багатоточковість" як для зондуючих сигналів, так і для реєстрованих. Застосовується синхронна 4-х канальна реєстрація кожним реєстратором для кожного з 5 положень випромінювача у місці доступу, наприклад у ТК. Зондування відбувається з обох сторін ділянки трубопроводу. Схема вимірювань для двох позицій випромінювача наведено на рис.2.

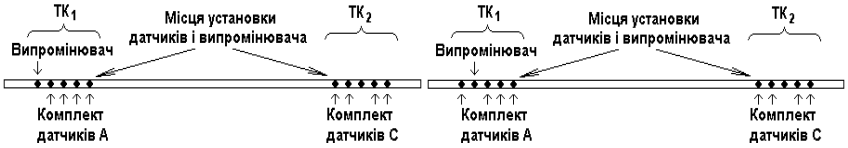

Рис.2. Схема вимірювань для двох позицій випромінювача.

Далі зареєстровані сигнали обробляються за допомогою спеціального програмного забезпечення, яке реалізує вирішення завдань з визначення фактичних характеристик поширення акустичних сигналів по трубопроводу, місць та параметрів його пошкоджень за допомогою кореляційних параметричних методів [2].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. А.А. Владимирский, И.А. Владимирский, И.П Криворучко, Н.П.Савчук. Разработка модернизированной системы низкочастотного диагностирования состояния трубопроводов РАСТР-1М. Моделювання та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 78, Київ, 2017 р. – С. 40-45.

2. Владимирський О.А. Параметричні методи діагностування підземних трубопроводів з урахуванням багатохвильового поширення інформаційних сигналів. Електронне моделювання. 2019. – 41 (1). – С. 3-17.

УДК 004.056.53

В.О. Герценок,
Г.В. Мартинюк, к.т.н.
Національний авіаційний університет, Київ

МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ЛЮДИНИ

Вступ. Однією з актуальних задач розвитку інформаційних технологій на сучасному етапі є забезпечення надійного захисту інформації. Існуючі сьогодні методи захисту інформації поділяють на [1]: апаратні, програмні, змішані. Останні поєднують у собі як апаратні, так і програмні засоби. Задача захисту інформації є особливо актуальною в умовах активного розвитку систем електронної торгівлі та банківських операцій, систем дистанційного навчання та великих корпоративних мереж, де циркулює конфіденційна інформація.

Як альтернатива парольній системі або її доповнення може розглядатися ідентифікація користувачів за біометричними характеристиками. Біометричні технології ідентифікації та автентифікації мають низку переваг перед традиційними і знаходять все більше застосування у системах захисту об'єктів інформаційної діяльності.

Мета. Метою даної роботи є критичний огляд непоширених методів біометричної ідентифікації та визначення переваг та недоліків цих методів.

Розпізнавання по венам руки

Це нова технологія в сфері біометрії, широке застосування її почалося менше 10 років тому. Інфрачервона камера робить знімки зовнішньої або внутрішньої сторони руки. Малюнок вен формується завдяки тому, що гемоглобін крові поглинає інфрачервоне випромінювання. В результаті, ступінь відображення зменшується, і вени видно на камері у вигляді чорних ліній. Спеціальна програма на основі отриманих даних створює цифрову згортку. Не потребує контакту людини з скануючим пристроєм [2].

Переваги методу. Відсутність необхідності контактувати зі скануючим пристроєм. Висока вірогідність - статистичні показники методу можна порівняти з показаннями райдужної оболонки. Прихованість характеристики: венозну сітку для ідентифікації дуже важко отримати від людини «на вулиці», наприклад сфотографувавши його фотоапаратом.

Недоліки методу. Неприпустимо засвічення сканера сонячними променями і променями галогенових ламп. Деякі захворювання, наприклад артрит - сильно погіршують помилки першого (ймовірність помилкового співпадіння білметричних характеристик двох людей) та другого (ймовірність відмови доступу людині, яка має доступ) роду. Метод менш вивчений в порівнянні з іншими статичними методами біометрії.

Розпізнавання по геометрії руки

Цей метод заснований на отриманні геометричних характеристик рук: довжин пальців, ширини долоні і т.д. Метод розпізнавання по геометрії руки вимираючі, але треба виділити, що він може підходити для деяких систем технічного захисту інформації на об'єктах інформаційної діяльності.

На відміну від методу розпізнавання за венами рук, де необхідно робити знімок усієї долоні, у методі, який використовує геометрію руки достатньо зробити тільки знімок пальців [3].

Переваги методу. Легкість у використанні, потребує невеликої кількості даних для ідентифікації користувача (шаблон займає близько 10 байт, коли шаблон ідентифікатору голосу потребує близько 1500 – 3000 байт). Низька відмова реєстрації користувача.

Недоліки методу. Недостатня точність, через що система може використовуватися тільки для верифікації. Великі розміри сканера, а також довгий процес ідентифікації у порівнянні з іншими системами.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Домарев В. В. Безопасность информационных технологий. Методы создания систем защиты/ В. В. Домарев. - К.: ООО ТИД ДС, 2001. - 688 с.

2. Задорожный В. Обзор биометрических технологий [Электронный ресурс] / В. Задорожный. – Режим доступа:. http://www.bre.ru/security/20234.html.

3. Мороз А. О. Біометричні технології ідентифікації людини. Огляд системи / А.О. Мороз // Математичні машини і системи. – 2011. - № 1. – С. 39-45.

УДК 004.274:004.056

С.Я. Гільгурт, к.т.н.
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПІДХОДІВ ДО ПОБУДОВИ КОМПОНЕНТІВ РЕКОНФІГУРОВНИХ ЗАСОБІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Останнім часом у зав'язку зі сталим зростанням мережевого трафіку, кількості та витонченості кібератак, а також через зупинення частоти універсальних мікропроцесорів програмна реалізація складних засобів технічного захисту інформації, таких як системи виявлення вторгнень або додатки проти вірусів та спаму вже не відповідають вимогам щодо їх швидкодії. Тому розробники звертаються до реконфігуровних рішень на базі програмованих логічних інтегральних схем (ПЛІС), які поєднують в собі продуктивність спецпроцесорів і гнучкість програмного забезпечення. Найбільш ресурсномісткою задачею реального часу в апаратних засобах технічного захисту інформації є множинне розпізнавання фіксованих послідовностей символів (патернів). Від того, наскільки успішно вдасться вирішити цю задачу, залежить ефективність системи захисту в цілому.

Існує багато підходів різної природи до побудови апаратних схем множинного розпізнавання патернів. Як свідчить аналіз численних публікацій, найкращі здібності в сенсі ефективності при побудові схем множинного розпізнавання патернів продемонстрували наступні три підходи (а також їх модифікації, технології, на яких вони базуються, та техніки покращення відповідних рішень):

– асоціативна пам'ять на базі цифрових компараторів;

– фільтр Блума на базі геш-функцій;

– алгоритм Ахо–Корасік на базі скінченних автоматів.

Асоціативна пам'ять (АП), є класом пристроїв, які створювалися саме для швидкого розпізнавання кодів і виконують функцію, протилежну традиційному ОЗП – за змістом відшукують місце розташування даних в пам'яті або свідчать про їх відсутність. Швидкодіючою основою АП на ПЛІС є цифрові компаратори.

Фільтр Блума (ФБ) – це абстрактний пристрій, який складається з комплекту з K блоків обчислення геш-функції $h_1(x)$, $h_2(x)$, …, $h_K(x)$ та масиву з M бітових комірок (МБК). В початковому стані МБК

заповнений нулями. На етапі програмування на входи геш-функцій послідовно подаються всі патерни словнику, для кожного з них обчислюється K геш-функцій, значення котрих інтерпретуються як адреси комірок у МБК, в які заносяться одиниці. В процесі функціонування фільтра Блума на його вхід подається фрагмент вхідної послідовності символів, і також обчислюються значення всіх K геш-функцій. По отриманим адресам здійснюється звернення до комірок МБК. Якщо у всіх позиціях, на які вкажуть геш-функції, містяться одиниці, вважається, що вхідна комбінація символів з певною вірогідністю співпадає з одним з патернів, що приймали участь у програмуванні ФБ.

Алгоритм Ахо–Корасік (АК) є прикладом засобу, який на відміну від багатьох відомих алгоритмів одиночного розпізнавання виявляє у вхідних даних одночасно кілька зразків. На етапі побудови АК з наданого набору патернів за певними правилами створюється детермінований скінченний автомат – розпізнавач. Під час функціонування такий автомат на кожному такті в залежності від вхідного символу переходить з одного стану в інший згідно функції переходів поки не опиниться в одному з так званих прийнятних станів, що означає факт розпізнавання певного слова (рядка символів) зі словника патернів.

Щоб оцінювати та порівнювати технічні рішення щодо реконфігуровних засобів технічного захисту інформації, потрібно визначитися з критеріями їх ефективності та відповідними показниками. Аналіз світового досвіду дозоляє створити ієрархію показників ефективності (ПЕ) таких засобів. Всі ПЕ можна поділити на три категорії: основні (вартісні показники, показники продуктивності та функціональні показники), проміжні (що пов'язують деякі з основних) та похідні (що формуються з кількох інших).

Як свідчать результати порівняльного аналізу, жоден з досліджених підходів не демонструє явних переваг перед іншими. Кожен має позитивні риси та недоліки, але не перевершує конкурентні рішення за всіма ПЕ. Отже, виникає потреба в методах поєднання різних підходів в єдиному пристрої із забезпеченням максимальної реалізації переваг кожного з підходів.

УДК 519.7

О.М. Глазок, к.т.н.
Національний авіаційний університет, Київ

НЕЙРОМЕРЕЖЕВИЙ ПРОТОКОЛ ОБМІНУ КЛЮЧАМИ З ВИКОРИСТАННЯМ РОЗШИРЕНОГО ЗСУВНОГО РЕГІСТРУ

Обмін ключами є однією із проблем сучасної криптографії. В сучасному інформаційному середовищі поширеною задачею є встановлення через відкриті канали зв'язку безпечного віртуального каналу зв'язку двох сторін, які до цього не зустрічалися і не мають надійного секретного каналу для передачі таємної інформації в час узгодження ключів. Для цього сторони мають через небезпечний канал зв'язку узгодити сеансовий ключ, який буде відомий тільки легітимним учасникам обміну. За замовчуванням можна вважати, що інформація, яка передається по відкритим каналам, доступна для прослуховування зловмисникові, який намагатиметься отримати узгоджувані ключі. В даний час для розв'язання цієї задачі широко використовується протокол обміну ключами Діффі-Хеллмана. Нейромережеві протоколи обміну ключами розглядаються як можлива безпечна заміна протоколу Діффі-Хеллмана [1]. Розроблені на даний час нейромережеві протоколи обміну ключами в основному засновані на синхронізації двох деревовидних машин парності – це спеціальний тип багатошарової прямої нейронної мережі [2]. Вона складається з K * N вхідних нейронів, K прихованих нейронів та одного вихідного нейрона, де K і N – параметри конкретної архітектури мережі. Входи в мережу можуть отримувати одне з трьох можливих значень: –1, 0, 1. Вихідне значення кожного прихованого нейрона обчислюється як функція його входів: Вихід деревовидної машин парності є двійковим (може дорівнювати +1 або –1). Також може бути використано бінаризований варіант деревовидної машин парності, що називається «машини парності перестановки» [3], де ваги між вхідними та прихованими нейронами є двійковими значеннями, наприклад 0 або 1; вихідні значення прихованих нейронів також є двійковими.

Метою запропонованого протоколу є створення секретного ключа сеансу, спільного для двох сторін A і B, які спілкуються по незахищеному каналу таким чином, що зловмисник, який слухає їх

переговори, не зміг би відтворити вироблений секрет. Для реалізації протоколу дві сторони повинні зберігати загальний секрет (головний ключ), який використовується в розрахунках при створенні сеансових ключів, але не передається по каналу зв'язку. Важливим елементом схеми є генератор псевдовипадкових чисел (PRNG), який створює групу значень для кожного раунду протоколу. У цій схемі пропонується використовувати PRNG на основі схеми розширеного зсувного регістру. Класичний зсувний регістр побудований на основі послідовно сполучених D-тригерах, кожен з яких може зберігати один із двох бінарних станів (0 або 1). Зворотній зв'язок у такому регістрі реалізований у вигляді набору відводів, які беруть значення з виходів деяких елементів регістру; для отримання величини зворотного зв’язку, що подається на вхід регістру на кожному такті його роботи, ці значення додаються за модулем 2. Розширений зсувний регістр складається з елементів, набір станів яких може відрізнятися від бінарної множини. Для визначення величин зворотного зв’язку додавання за модулем 2 замінюється більш загальною функцією, входи та вихід якої є елементами множини набору станів. Таких функцій може бути одна, використана кілька разів, або декілька різних функцій для кожної окремої ланки зворотного зв’язку. Таким чином, робота модуля зворотного зв’язку у розширеному регістрі залежить від набору відводів і набору застосованих функцій відображення. Класичний зсувний регістр є частковим випадком розширеного.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Singh A., Nandal A. Neural Cryptography for Secret Key Exchange and Encryption with AES // Int. J. of Advanced Research in Computer Science and Software Engineering. – 2013. – Vol. 3, Issue 5. – Pp. 376-381.

2. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Червяков Н.И. и др. – М.: Физматлит, 2012. – 279 с.

3. Reyes O., Zimmermann K. Permutation parity machines for neural cryptography. – Physical Review E. 81 (6): 066117. DOI: 10.1103/ PhysRevE.81.066117.

УДК 004.056.53

Н.М. Голего,
В.В. Бедіна
Національний авіаційний університет, Київ

ТЕХНОЛОГІЯ СТВОРЕННЯ MESH-МЕРЕЖ ВИСОКОЇ ПРОДУКТИВНОСТІ І НАДІЙНОСТІ ВСЕРЕДИНІ БУДІВЕЛЬ

В даний момент для створення нормально функціонуючої бездротової мережі всередині будівлі всі точки доступу з'єднуються кабелем через комутатор. Це рішення надійне, але при цьому зовсім не гнучке і ресурсомістке. Крім того, не завжди є можливість протягнути кабель саме туди, де треба розмістити точку доступу (новий ремонт, відсутність кабельних каналів).

Технологія Ruckus Wireless SmartMesh створена для вирішення питань розширення бездротової мережі без протягування додаткових кабелів і додавання в мережу нових комутаторів. Все, що треба зробити для розширення мережі - підключити до живлення точку доступу в необхідному місці. Ніяких більше налаштувань та вивчень не вимагається - все вже передбачено в SmartMesh і відбувається автоматично.

Точки підключаються один до одного через радіоефір. Як правило для цього задіюється окремий радіоінтерфейс з частотою 5 ГГц 802.3ac.

Даний діапазон менш завантажений і забезпечує більшу швидкість передачі даних.

Залежно від обраної концепції точки можуть здійснювати маршрутизацію і пошук оптимального маршруту (реалізовано в обладнанні Motorola), або збирати весь трафік на центральну точку (root), що має з'єднання з інтернет (реалізовано компанією Edimax).

Точки можуть працювати в Mesh-мережі як самостійно (наприклад, інтелектуальні точки - Motorola), так і в якості тонкого клієнта під управління контролера (Blusocket).

«Розумні» точки доступу можуть динамічно перерозподіляти навантаження. Якщо одна точка виявляється перевантажена, вона знижує потужність і передає частину своїх абонентів сусіднім точкам, які збільшують потужність.

Сучасні точки можуть використовувати додаткові радіонтерфейси (2-ий або 3-ий) в якості сенсора навколишнього

радіоефіру, що дозволяє в автоматичному режимі вибирати оптимальні радоіканали і випромінює потужність сигналу для зниження впливу інтерференції. Сенсор також може реєструвати підключення незареєстрованих точок, інформувати про це адміністартора мережі, а також використовувати активне подавлення радіосигналу від незаконно встановлених точок (захист радіоперіметра).

Таким чином значно спрощується проведення пуско-налагоджувальних робіт. Часто ця технолгогія дозволяє виключити трудомістку і дорогу процедуру радіопланування.

SmartMesh об'єднує в собі технологію адаптивних масивів антен BeamFlex і централізоване управління бездротовою мережею. Мережа SmartMesh здатна самостійно організовуватися і оптимізуватися, маючи при цьому підвищену відмовостійкість.

Переваги використання SmartMesh-мереж:

- Висока продуктивність завдяки з'єднанню технологій Smart Wi-Fi і 802.11n;
- Техніки знаходження найкращого шляху і відбудови від перешкод для надійного зв'язку між вузлами Mesh-мережі;
- Адаптація в реальному часі до постійно змінюваних навколишніх умов і забезпечення високонадійних магістральних зв'язків між точками (використання технології ChannelFly підвищує ємність мережі на 50%);
- Використання топології «Дерево» для зменшення ризиків конвергенції і затримок в мережі;
- Просте налаштування в один клік і управління на одній сторінці;
- Удвічі менше часу на установку, вдвічі дешевше і втричі швидше в порівнянні з конкурентами.

УДК 004.451.44

В.В. Демчик,
О.В. Корочкін, к.т.н.,
О.В. Русанова, к.т.н.
Національний технічний університет України
“КПІ ім. І. Сікорського”, Київ

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ WCF ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБЧИСЛЕНЬ В СУЧАСНИХ РОЗПОДІЛЕНИХ КОМП’ЮЕТРНИХ СИСТЕМАХ

В даній роботі досліджуються питання підвищення ефективності високонавантажених обчислень в розподілених комп’ютерних системах за рахунок їх організації із застосуванням технології WCF (Windows Communication Foundation).

Розподілені комп’ютерні системи станом на сьогодні є основними цільовими платформами для проведення високонавантажених обчислень. При цьому основними технологіями для організації паралельних обчислень в розподілених комп’ютерних системах лишаються низькорівнева передача повідомлень (найпопулярнішим втіленням якої є бібліотека MPI) та розпаралелювання за допомогою директив компілятора (яку втілює в собі бібліотека OpenMP).

Не зважаючи на високу швидкодію програм, організованих з використанням цих технологій, та загальну зручність їх застосування, основною проблемою даних технологій лишається їх застарілість, яка з року в рік тільки посилюється. Серед ключових моментів, які вказують на їх застарілість, можна виділити три, кожен наступний випливає з попереднього:

1. Обмеженість цільових мов. Обидві технології перш за все розроблялись для мов Fortran та C. Обидві мови (особливо Fortran) наразі втратили популярність та актуальність в розробці ***прикладного*** програмного забезпечення, про що свідчать статистики за останні роки, зібрані такими сайтами як Google, GitHub, StackOverflow.

2. Орієнтованість на процедурне програмування. Обидві технології розроблялися в часи, коли основною парадигмою, яка застосовувалась в прикладному програмуванні, була процедурна. Проте наразі загальноприйнятими вважаються значно складніші парадигми – об’єктно-орієнтовна, функціональна, реактивна.

3. Низький рівень абстракції, необхідність виділення значного проміжного рівня в програмному комплексі для організації взаємодії між шаром бізнес-логіки та шаром комунікації, приведення інтерфейсів, тощо. Наприклад, в MPI максимальна абстракція, яку можна відправити – завчасно визначена структура.

Від самого початку технологія WCF розроблялась для вирішення описаних вище проблем, що і було врешті-решт зроблено. Окрім того, її застосування дозволяє поєднувати між собою комп'ютери з різною архітектурою, не відволікаючись на вирішення проблем сумісності, оскільки, як і всі технології .NET Framework-у, вона працює в рамках віртуальної машини CLR (Common Language Runtime). За основу в ній прийнята концепція відвантажених обчислень та виклику віддалених методів, що дозволяє організувати значно більш гнучку взаємодію, ніж звичайними технологіями передачі повідомлень. При цьому паралелізм в рамках кожної кінцевої машини може бути реалізований за рахунок супутньої вбудованої в .NET Framework бібліотеки TPL (Thread Parallel Library).

Єдиним і основним недоліком, який можна виділити в технології WCF, порівняно з OpenMP та MPI, є більша складність та об'ємність програмного коду.

В ході роботи було розроблено пакет програм для вирішення декількох класичних для високонавантажених обчислень задач в розподілених комп'ютерних мережах, один з використанням зв'язки технологій MPI+OpenMP, інший технології WCF (з TPL). Проведено порівняльне тестування розроблених програм в декількох розподілених комп'ютерних мережах, як фізичних, так і хмарних (за допомогою сервісу Goolge Cloud). Результати тестування показали можливості до скорочення часу обчислень при застосуванні технології WCF. При цьому варто відмітити, що чим менш інтенсивним був обмін даними, тим більшим був відносний показник скорочення.

УДК 004.056.55

Д.М. Драгоєв
Національний авіаційний університет, Київ

РОЛЬ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ЖИТТІ ЛЮДИНИ

У сучасному суспільстві інформаційні технології пройшли довгий шлях і проникли в усі сфери життя людини. Нові технології дозволяють передавати інформацію з однієї точки земної кулі в іншу за лічені секунди. Крім особистого листування, електронні повідомлення використовуються для передачі інформації між державними органами, органами місцевого самоврядування, військовими частинами тощо. І всі ці повідомлення можна перехопити і використовувати в своїх корисливих цілях. А щоб зловмисники не дізналися інформацію, використовуються різні методи шифрування, які надаються сучасною криптографією. Криптографія - це наука про методи забезпечення конфіденційності (неможливості прочитати інформацію від сторонніх), цілісності даних (неможливості ненавмисної зміни інформації), аутентифікації (перевірки справжності авторства або інших властивостей об'єкта), а також неможливості заперечувати авторство. Ключовою метою криптографічного захисту інформації є забезпечення конфіденційності та захисту інформаційних даних комп'ютерних мереж в процесі їх передачі по мережі між користувачами системи.

Основним видом криптографічного перетворення інформації в комп'ютерних мережах є шифрування. Шифрування відноситься до процесу перетворення відкритої інформації в зашифровану інформацію (зашифрований текст) або до процесу перетворення зашифрованої інформації назад в відкриту інформацію. Процес перетворення відкритої інформації в закриту називається шифруванням, а процес перетворення закритої інформації в відкриту інформацію дешифруванням.

Ефективність шифрування для захисту інформації вимагає таємності ключа і криптографічної стійкості шифру.

Криптографічні методи можна розділити на два класи:

1) обробка інформації шляхом заміни і переміщення букв, які не змінюють обсяг даних (шифрування);

2) стиснення інформації шляхом заміни окремих поєднань літер,

слів чи словосполучень (кодування).

Можливі як апаратні, так і програмні методи шифрування при обміні інформацією між комп'ютерами через телекомунікаційну мережу, а також при роботі з локальними абонентами. Апаратне шифрування використовується для захисту текстової інформації при передачі на віддалені станції в телекомунікаційній мережі. Методи апаратного шифрування використовуються для передачі захищених даних по телекомунікаційної мережі. Програмні методи шифрування використовуються для зберігання інформації на магнітних носіях (дисках, стрічках). Це можуть бути дані з різних інформаційних і допоміжних систем, ACS, ASOD і інших методів програмного шифрування, які зводяться до повторного кодування, впорядкування і додаванню операцій по модулю 2 з використанням ключових слів.

У той же час слід використовувати разом кілька методів шифрування для захисту цілісності та конфіденційності даних. Комбіновані шифри застосовуються з послідовним використанням двох або навіть трьох різних шифрів.

Сьогодні криптографія є невід'ємною частиною всіх інформаційних систем: від електронної пошти до стільникового зв'язку, від доступу до Інтернету до електронних грошей. Криптографія забезпечує підзвітність, прозорість, точність та конфіденційність. Це запобігає спробам шахрайства в електронній комерції та забезпечує юридичну силу фінансових операцій. Криптографія допомагає ідентифікувати вас, але також надає анонімність. Захищає бандитів від зловживання сервером та конкуренції шляхом проникнення у ваші конфіденційні документи. І в майбутньому, оскільки бізнес та комунікації все більше прив'язуються до комп'ютерних мереж, криптографія буде необхідною.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Панасенко С.П., Захист інформації в комп'ютерних мережах // Журнал «Світ ПК» 2002./ – № 2.

2. Введення в криптографію / За заг. ред. В.В. Ященко - М., МЦНМО, 2000 – 272 с.

3. Шнайдер Б. Прикладна криптографія. М. – Світ. – 2004.

УДК 004.7:004.738.5 (043.2)

В.І. Дрововозов, к.т.н.,
Аль-Шаммарі Ахмед Аршед,
Н.В. Журавель
Національний авіаційний університет, Київ

ПІДХІД ДО ОБҐРУНТУВАННЯ ОСНОВНОГО МЕТОДУ ЗАБЕЗПЕЧЕННЯ QoS МЕРЕЖІ З МІЖРІВНЕВОЮ ВЗАЄМОДІЄЮ

До основних завдань оптимізації безпроводових мереж відноситься оптимізація розподілу обмеженого числа радіоресурсів між користувачами. Розподіл, контроль та управління радіоресурсами у безпроводових інформаційно-комунікаційних мережах мають вирішальне значення внаслідок природних обмежень частотно-енергетичного ресурсу за умов великого числа користувачів та мультимедійного характеру мережного трафіку. Щоб забезпечити потрібну якість сервісу (*Quality of Service, QoS*), адаптація до умов передачі по каналу повинна бути реалізована на всіх рівнях стека протоколів. Ключове питання, яке виникає, полягає в тому, чи можуть бути реалізовані методи адаптації на кожному рівні незалежно, у відповідності з класичним підходом до проектування вузлів в моделі взаємодії відкритих систем (*Open System Interconnection Reference Model, OSI*), або оптимізація повинна здійснюватися спільно на декількох рівнях стека протоколів, тобто повинна бути міжрівнева оптимізація. Основним принципом міжрівневої оптимізації є комплексне рішення задачі ефективного використання обмеженого числа радіоресурсів, що враховує ряд першорядних чинників: підвищення пропускної спроможності; забезпечення рівнодоступності - справедливого (*fair*) поділу ресурсів між користувачами; досягнення необхідної або, принаймні, найкращої можливої якості обслуговування.

Проблему управління якістю сервісу треба розглядати більш широко, тому що якість сервісу є комплексною характеристикою, яка включає декілька ключових параметрів. Головною вимогою до мережі є виконання її основної функції – забезпечення користувачам потенційної можливості доступу до ресурсів всіх термінальних вузлів, об'єднаних в мережу, причому доступ має бути забезпечений без затримки, або з прийнятною для користувача затримкою. Всі інші вимоги - продуктивність,

надійність, сумісність, керованість, захищеність, розширюваність і масштабованість – пов'язані з якістю виконання цієї основної задачі.

Розглядаються безпроводові мережі з пакетною комутацією. По мережі циркулює різнорідна мультимедійна інформація, а обмін даними здійснюється як зі стаціонарними, так і з мобільними абонентами. Це обумовлює складну специфіку мережного трафіку та жорсткі вимоги до параметрів мережі. Проаналізовано статистичні характеристики мережного трафіку *Quadruple Play* й ключові параметри (затримку та пропускну спроможність) мереж. Передавання даних, по суті, має бути інформаційною системою жорсткого реального часу. Для забезпечення вимог до якості сервісу (QoS) сучасних інформаційно-комунікаційних мереж, що працюють у реальному часі, потрібно розробляти нові моделі та методи організації безпроводових каналів зв'язку, планування маршрутів з мінімальними затримками опрацювання у комутаційних вузлах, доставляння до отримувачів, малим рівнем бітових помилок тощо. Проведено порівняльний аналіз методів забезпечення QoS безпроводових мереж та розглянуто підхід до основного методу забезпечення QoS мережі з міжрівневою взаємодією.

Надання гарантій якості є важливою метою розробки безпроводових мереж. Різні методи можуть мати дуже різноманітні вимоги до якості щодо термінів передачі даних, міжкінцевої затримки та ймовірностей порушення, пов'язаних із затримкою. Наприклад, програми управління виробничим підприємством вимагають надійної та своєчасної доставки команд управління; отже, важливо гарантувати, що жоден пакет не втрачається чи затримується під час передачі пакету. Цей тип гарантій QoS зазвичай називають детермінованими або жорсткими гарантіями. З іншого боку, для більшості мультимедійних застосунків, включаючи відео телефонію, передачу мультимедіа та Інтернет-ігри, не потрібні такі суворі вимоги до якості QoS, тому що ці застосунки мало чутливі до короткострокових порушень QoS. Цей тип гарантій QoS зазвичай називають статистичними або м'якими гарантіями.

УДК 004.716.(043.2)

О.В. Дубчак,
І.А. Кравчук,
С.І. Ожерельєв,
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ РОЗШИРЕНИХ ACL ОБЛАДНАННЯ CISCO ДЛЯ УБЕЗПЕЧЕННЯ LAN ВІД ЗОВНІШНІХ ЗАГРОЗ

Новітні інформаційні технології, зокрема з підтримкою віддаленого доступу, активно впроваджуються в усі сфери життєдіяльності людини. Кібербезпека наразі має основоположне значення щодо розв'язання нагальних задач із забезпечення цілісності, конфіденційності і доступності ресурсів інформаційних систем і мереж. Враховуючи статистичні дані за 2020 р. щодо суми нанесених кіберзлочинцями збитків, яка становила понад 1% світового ВВП, що на 50% вище, ніж було у 2018 р., можна визначити несанкціонований доступ як одну з найпоширеніших загроз мережевим інфраструктурам [1].

Відповідно до RFC 4949 «InternetSecurityGlossary» [2] Access Control List (ACL) є механізмом реалізації контролю доступу до системних ресурсів. Цілі застосування ACL - обмеження мережевого трафіку для підвищення продуктивності LAN та налаштування відповідного рівня безпеки відносно доступу до різних мережевих пристроїв.

ACL слід налаштовувати на пристроях «брандмауера», які часто розташовані між внутрішньою мережею підприємства та зовнішньою мережею, наприклад, Інтернетом. Також використовуються ACL на роутері, локалізованому між двома частинами мережі, з метою контролювати трафік, що входить або виходить із локальної мережі. [3]

На прикордонних пристроях слід налаштувати ACL для кожного встановленого на інтерфейсах пристрою мережевого протоколу таким чином, що вхідний, вихідний або обидва види трафіка фільтруватимуться через інтерфейс.

Доступ до налаштування пристроїв Cisco, а саме маршрутизатору Cisco 1841 та комутатору Cisco Catalyst 2960 відбувається за допомогою кабелю Cisco Switch Router Console Cable RJ-45 to RS-232 через позасмуговий доступ (консольний порт). Можливості даного мережевого обладнання також

дозволяють використовувати протоколи Telnet та більш захищений його аналог Secure Shell (SSH).

Отже, політики безпеки реалізуються в повній мірі за допомогою вбудованих функцій мережевого обладнання Cisco у вигляді стандартних та розширених ACL. Для обмеження доступу іззовні в середину LAN, пропонується застосовувати розширені ACL. Обмеження такого трафіку можна створити у двох місцях: зі сторони LAN або зі сторони маршрутизатора провайдера (рис. 1.).

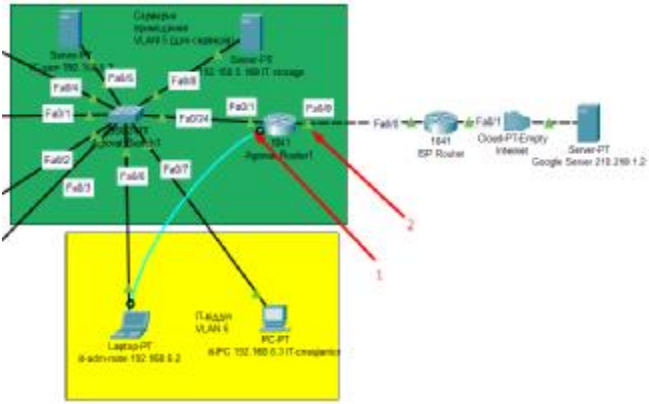

Рис. 1. Місця можливого розташування ACL: інтерфейс до LAN (1) та інтерфейс до провайдера (2)

У результаті ACL надали можливість фільтрувати будь-які Інтернет-з'єднання на 3-му (IP-адреси джерела та призначення), 4-му (TCP, UDP), та 7-му (HTTP, HTTPS, telnet) рівнях моделі OSI.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Кіберзлочини у 2020 р. Дослідження. URL:https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/55857766*

2. *Дубчак О.В. Списки контролю доступу обладнання Cisco як засіб мережевої безпеки / О.В.Дубчак, С.І.Ожерельєв// Materials of XVI Intenational Research And Practice Conference «Cutting-Edge Science – 2020», 30.04.20 – 07.05.20. – Sheffield (UK):"Science&Education Ltd". - V.8.- P.50-52.*

3. *Security Configuration Guide:Access Control Lists. Cisco IOS Release 15M&T. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration*

УДК 004.738.(043.2)

О.В. Дубчак,
А.О. Поліщук,
Національний авіаційний університет, Київ

АВТЕНТИФІКАЦІЯ СКЛАДОВИХ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ПІД ЧАС ЇХ КОМУНІКАЦІЇ

Відповідно до досліджень та висновків експертів мікросервісна архітектура (МСА) на сьогоднішній день перебуває на піку популярності. Як встановлено за результатами проведеного аналізу [1], характерною особливістю МСА є можливість побудувати комплексну систему, яка в подальшому використанні зможе з легкістю масштабуватися, дозволяючи витримати значні навантаження через кількість користувачів. У МСА всі сервіси мають відповідати наступним вимогам: ресурсність; сфокусованість; слабкопов'язаність; погодженість.

Однією з важливих переваг МСА є незалежність від використаних технологій під час розроблення будь - якого сервісу: мова програмування, бібліотека, фреймворки тощо. Однак потребує врахування коректне виділення сервісів та розподіл бізнес-логіки, стандартизація транспорту і протоколу взаємодії між сервісами, оскільки однією з ключових складових МСА є методи комунікації як зовні системи, так і між її компонентами. [2]

Метод комунікації може залежати від потреб, які виникають в системі задля забезпечення стабільної та надійної роботи, збереження консистентності даних, потужностей системи при обслуговування користувачів. За результатами аналізу методів комунікації, таких як: REST API (HTTP запити); з допомогою повідомлень та команд; з допомогою подій, - можна дійти висновку щодо наявності у кожного з них як недоліків, так і переваг, що ускладнює визначення оптимальнішого. При проведенні аналізу існуючих варіантів та методів щодо убезпечення комунікації компонентів системи під час їх взаємодії було виділено найбільш популярні - JWT та взаємна автентифікація за TLS. Але існують недоліки та вразливості даних рішень, через які вони не повністю задовольняють вимогам щодо безпечної комунікації в МСА. Результати проведеного аналізу та досліджень дали змогу дійти висновку щодо необхідності створення власної системи автентифікації компонентів МСА, для реалізації якої використано

наступні технології: мова програмування Java; фреймворк Spring Framework; бібліотека OpenFeign; збірник проєктів Gradle; Docker; Amazon ECS; Apache Kafka.

За основу розробки системи автентифікації компонентів МСА взято декілька підходів та відповідна їх комбінації, а саме JWT - токен з JWKS для генерації токенів доступу, центральний сервіс автентифікації для використання в якості регістра сервісів.

Для демонстрації функціонування запропонованої системи автентифікації створено тестову інформаційну систему на базі МСА: два сервіси User Service та Trip Service, а також контейнер Message Brocker, який використовує Apache Kafka для забезпечення функцій брокера повідомленнь. Кластер запущений в приватній підмережі, що дає змогу зменшити імовірність проникнення зловмисника в систему. Окрім того, доступ до сервісів організований через спеціальний шлюз, який, залежно від параметрів запиту, перенаправляє його на відповідний сервіс.

Запропонована система автентифікації під час комунікації МСА для перешкоджання діям зловмисників дала змогу впровадити додатковий рівень захисту, а саме: на рівні інфраструктури - обмеження доступу до реєстру сервісів глобальної мережі, що ускладнює процес проникнення та отримання доступу до ресурсів; на рівні комунікації - шифрування даних відомими ключами; на програмному рівні - автентифікація та авторизація компонентів системи задля попередження несанкціонованого доступу та дій в системі. Концепція є універсальною для багатьох видів і підходів щодо організації комунікації між компонентами в інформаційних системах, побудованих на базі МСА. Як продовження досліджень планується розширити функціональність системи до авторизації сервісу на основі ролей та надання їм дозволів і заборон.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Дубчак О.В. Аналіз характеристик мікросервісної архітектури / О.В.Дубчак, А.О. Поліщук// Materiály XV mezinárodní vědecko - praktická konference «Aktuální vymoženosti vědy 2019», 22.06.19 – 30.06.19. - Prague, 2019. - V.8.- P. 39-41.

2. Microservice authentication and authorization solutions [Електронний ресурс] - Режим доступу: https://medium.com/tech-tajawal/ microservice-authentication-and-authorization-solutions

УДК 004.94:621.316

В.А. Євдокімов к.н. з держ. упр.
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

КОМП'ЮТЕРНА СИСТЕМА EQUANT CLOUD МОДЕЛЮВАННЯ ПРОЦЕСІВ ЦІНОУТВОРЕННЯ НА РИНКУ ЕЛЕКТРОЕНЕРГІЇ УКРАЇНИ

В роботі [1] до числа актуальних теоретичних і прикладних проблем загальної проблеми вдосконалення методів і засобів математичного і комп'ютерного моделювання, призначених для аналізу функціонування складної організаційно-технічної системи (СОТС), віднесено проблему підвищення ефективності механізмів функціонування СОТС при управлінні ними в швидкозмінних умовах існування і проведення інституційних змін у взаєминах між її підсистемами і з суб'єктами управління господарською діяльністю у зовнішньому середовищі.

Там же було виділено підсистему управління ціноутворенням як окрему СОТС загальної системі організаційного управління (СОУ) ринком електричної енергії (е/е), а процес ціноутворення в цій підсистемі в якості об’єкта дослідження. Обґрунтовано актуальність та необхідність створення імітаційної моделі процесу ціноутворення на ринку е/е з безпосередньою участю суб'єктів ринку, основним призначенням якої є дослідження науково-практичної проблеми удосконалення методичного інструментарію розрахунку цінових показників на різних його сегментах. На основі аналізу сучасних методів імітаційного моделювання процесів управління в виділеної СОТС обґрунтовано вибір мультигентного підходу, в якості основного, для побудови імітаційної моделі децентралізованої взаємодії його суб’єктів на ринку е/е в процесі ціноутворення.

Перехід до нової моделі ринку е/е України відповідно до Закону України «Про ринок електричної енергії» є закономірним результатом його розвитку відповідно до прийнятої раніше Концепції функціонування та розвитку оптового ринку е/е України. І разом з тим, частиною загальної

тенденції зміни основних принципів функціонування ринків е/е в країнах Європейського союзу, США, Австралії, Росії і багатьох інших. Процес реформування ринку е/е України відповідно до світових тенденцій розвитку енергоринків, що почався ще в наприкінці 90-х років, завершився переходом з 01.06.2019 р. до відомої моделі його організації «Конкуренція на всіх рівнях».

У сьогоднішніх умовах, які можна назвати умовами розвитку ринкового ціноутворення на е/е, питання з приводу формування цін продажу е/е виробниками для подальшої подачі у вигляді торгових заявок на різні сегменти ринку е/е є одними з найбільш важливих. Оскільки багато в чому визначають фінансові результати їх роботи на ринку. У зв'язку з цим в нових умовах функціонування ринку е/е постає питання розроблення та дослідження методичного інструментарію для підготовки і прийняття рішень про ціни в торгових заявках на поставку е/е та системних послуг на новоутворені сегменти ринку: на добу наперед (РДН); внутрішньодобової ринок (ВДР); ринок двосторонніх договорів (РДД): ринок допоміжних послуг (РДП); балансуючий ринок (БР). Саме на кожному з цих сегментів ринку існують свої особливості функціонування та ризики при формуванні рівноважних цін. В кінцевому підсумку це є питання формування стратегії ціноутворення генеруючих компаній (ГК) на них і в цілому на ринку, яке набуває особливої важливості як в частині аналізу застосовуваних раніше методик, так і в частині розробки нових алгоритмів та методик на їх основі, що відповідають новим Правилам ринку [2].

Аналіз розвитку даного сегмента ринку України за минулий період його функціонування показує:

- недосконаліть механізмів тарифного регулювання, і, як результат, неконтрольоване зростання тарифів на передачу і розподіл е/е;
- складність процедур і висока вартість приєднання до мереж;
- збереження системи перехресного субсидування («перехрестя» між групами «дешевих виробників» і справді «дорогими виробниками» е/е на підприємствах відновлюваної енергетики закладено в тариф на передачу е/е, але механізм її

ліквідації не передбачений, що істотно спотворює ринкові процеси , і позбавляє частину виробників е/е можливостей використання їх конкурентних переваг і стимулів, як в поточному стані, так і при виробленні стратегії розвитку.

Можна припустити, що саме ці обставини, явно не сприяють зниженню цін на оптовому ринку е/е, а, отже, і тарифів для кінцевих споживачів, і утворюють систему негативних сигналів для споживачів.

Equant Cloud - це інноваційна програмно-апаратна інформаційно-розрахункова комп'ютерна система, яка надає можливість учасникам – агентам ринку е/е України в онлайн-режимі вирішувати завдання інформаційного забезпечення та проведення розрахунків задач моделювання процесів ціноутворення, прогнозування показників динаміки функціонування як оптового, так і роздрібного ринку, а також формувати стратегії поведінки агентів з урахуванням ризиків.
Концептуальний мультиагентний підхід, який закладено в основу розробки програмного забезпечення системи, забезпечує створення мультиагентного середовища для організації інформаційної взаємодії агентів ринку між собою і зовнішнім середовищем - реально діючої інформаційно-технологічною інфраструктурою ринку.

Комп'ютерна система призначена як для вирішення поточних завдань планування виробництва е/е та управління електроспоживанням, так і для досліджування різних сценаріїв еволюційного розвитку системи ціноутворення на оптовому і роздрібному ринках при різних припущеннях про вдосконалення регуляторних механізмів, інституційних норм з урахуванням технологічних змін в структурі виробництва електроенергії в майбутньому.

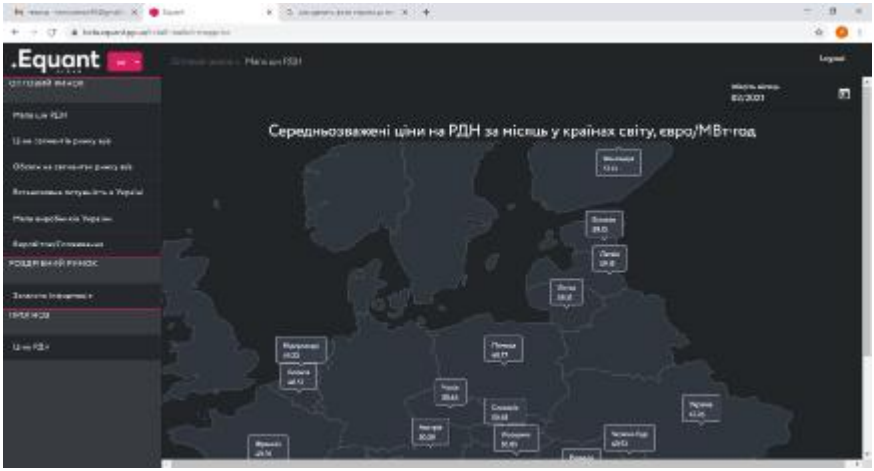

Рис.1. Меню комп'ютерної системи *Equant Cloud*.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Мохор В.В., Про створення мультиагентної імітаційної моделі процесів ціноутворення на ринку електроенергії / В.В. Мохор, В.А. Євдокімов // Електронне моделювання. – 2020. – Том 42, №6.- С. 3-17.*

2. *Національна комісія, що здійснює державне регулювання у сферах енергетики і комунальних послуг. Про затвердження Правил ринку. Постанова №307 від 14.03.2018 р. [Електронний ресурс] : [сайт] Режим доступу : https://zakon.rada.gov.ua/laws/show/v0307874-18/page#Text - (Дата звернення: 10.10.19).*

УДК 004.056:004.738.5(045)

І.А. Жуков, д.т.н.
М.М. Гузій, к.т.н.
Національний авіаційний університет, Київ

МОДЕЛІ ОПТИМАЛЬНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ КОНФЛІКТАМИ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Розвиток сучасних методів мережевих атак та засобів захисту інформаційних ресурсів в комп'ютерних системах обумовлює актуальність пошуку оптимальних рішень сторонами-учасниками інформаційного конфлікту.

Створення адаптивних систем захисту інформації потребує розробки моделей оптимального управління інформаційними конфліктами комп'ютерних систем, обґрунтування критеріїв оптимальності та обмежень в задачах оптимального управління динамікою інформаційних конфліктів.

Дана робота є логічним продовженням робіт [1-3] і спрямована на вибір критеріїв оптимальності, класифікації задач оптимального управління інформаційними конфліктами, побудову типових математичних моделей оптимального управління з урахуванням обмежень реального характеру.

Проведено аналіз узагальненої характеристики можливостей теорії марківських процесів для опису інформаційної взаємодії комп'ютерних систем. Динаміку взаємодії звичайно описано диференційними рівняннями А.М. Колмогорова у вигляді:

$$\frac{dP_i(t)}{dt} = -\sum_{j=1}^{m} P_{ij} f_i(t) + \sum_{j=1}^{m} P_{ij} f_j(t), \quad i = 1, m, \qquad (1)$$

де $P_i(t)$ – ймовірність перебування системи в i-му стані;

P_{ij} – умовна ймовірність переходу системи із i-го в j-ий стан;

$f_i(t)$ – щільність експоненціального розподілу часу перебування системи в і-му стані, $i,j=1,m$;

m – загальне число станів системи.

Із системи рівнянь (1) отримано рівняння для марківських і напівмарківських процесів і ланцюгів, а задачу Коші обчислено стандартним методом перетворень Лапласу.

Отримані рівняння є основою для побудови критеріїв оптимальності. Виберемо критерій оптимальності у вигляді, зручному для пошуку оптимальних рішень

$$F(l,h,m,q,a,b)=\frac{1}{T}\int_0^T \{q_0[P_0(t)-P_{00}]^2++q_a[P_a(t)-P_{aa}]^2+q_d[P_d(t)-P_{dd}]^2\}dt \quad (2)$$

де q_0, q_a, q_d – вагові коефіцієнти для врахування відхилення поточних значень ймовірності $P_0(t)$, $P_a(t)$ і $P_d(t)$ від заданих еталонних значень P_{00}, P_{aa}, P_{dd},

T – інтервал часу перехідного періоду, який враховується у пошуку оптимальних рішень.

У критерії оптимальності (2) використані метрики евклідового та гільбертового просторів, він дозволяє досить гнучко підходити до постановки і розв'язання завдань оптимального управління динамікою інформаційних конфліктів. Очевидними узагальненнями цього критерію можуть бути критерій середніх витрат. Критерій (2) дозволяє вирішувати також «мінімаксні» і «максимінні» ігрові задачі оптимального управління.

На основі запропонованих моделей розроблена графологічна модель інформаційних конфліктів, яка дозволяє аналізувати динаміку конфлікту, розробляти оптимальні стратегії управління конфліктом сторонами протиборства.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Игнатов В.А. Теория информации и передачи сигналов. Учебник для вузов, 2-е изд. – М.:"Радио и связь", 1990. – 280 с.*

2. *Игнатов В.А., Гузий Н.Н. Оптимальное адаптивное управление защитой информации в конфликтующих системах. Електроніка та системи управління:Збірник наукових праць.– Вип. 1(7). – К.: НАУ, 2006. – С. 137-143.*

3. *Ігнатов В.О., Гузій М.М. Моделювання балансу засобів нападу та захисту в конфліктуючих системах. Вісник Східноукраїнського національного університету ім. В. Даля №5 (111), 2007. – С.97-104.*

4. *Грищук Р.В. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних Інтернет-сервісах / Р.В.Грищук, К.В.Молодецька-Гринчук // Сучасний захист інформації. – №2(30), 2017. – С. 86-96.*

УДК 004.7 (043.2)

К.В. Заблоцький,
С.В. Малик,
Р.С. Одарченко, д.т.н.
Національний авіаційний університет, Київ

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ СИСТЕМИ МОНІТОРИНГУ NETWORK OLYMPUS ДЛЯ ПОТРЕБ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Невід'ємною частиною функціонування будь-якої компанії є постійний моніторинг компонентів даної мережі для підтримки їх працездатності та стабільної роботи. Для швидкого реагування та вирішення проблем безперервної роботи мережі існують програми моніторингу, такі як Network Olympus.

Перш за все, це служба з веб-інтерфейсом, що в свою чергу є і позитивним, оскільки надає більшу гнучкість, і негативним, оскільки там лише такий інтерфейс. Для автоматизації усунення виявлених проблем складних схем моніторингу в даній програмі існує конструктор сценаріїв, у основі якого є сенсори. [1]

Сенсори контролюють роботу пристроїв, а саме: збір інформації, її обробка та аналіз, оцінка параметрів та стану пристрою з можливістю повідомлення про проблему. Сценарій моніторингу також дозволяє запускати датчики, дії, процес сканування за розкладом. [2]

Прикладом сценарію може бути перевірка пристроїв в групі мережі, перевірка на віддаленому сервері значень в ключі реєстру, а також перевірка наявності самого серверу, тобто його доступності.

Для наочності роботи зі схемами моніторингу необхідна візуалізація інформації. Забезпеченням даної потреби є карта мережі, створення якої інтегроване у системі. Перш за все, у нас є можливість провести сканування із заданими діапазонами IP, що забезпечується віджетом стану Сканера. Коли ми вказуємо діапазони сканування і запускаємо цей процес, автоматично відбувається виявлення мережевих елементів. Результат сканування записується у віджеті журнал Сканера, а також усі знайдені елементи записуються у дерево мережі. Якщо необхідний пристрій уже записаний там, то інформація оновлюється.

Після процесу сканування ми можемо створити нашу мережу у карті мережі, або доповнити уже існуючий проект. Це дозволить студентам створити графічне представлення інфраструктури та керувати нею. На карту можна додавати вузли мережевих карт (ті пристрої, які появляються у дереві мережі після сканування), посилання та різні форми, а також використовувати її для контролю стану датчика.

Для ознайомлення з можливостями програми студенти також можуть створити локальну мережу з декількох комп'ютерів, після чого просканувати її та додати датчики. Наприклад якщо на кожен комп'ютер додати сенсор ping і вказати час, то воно почне автоматично перевіряти з'єднання між комп'ютерами. Також сюди можна додати певну дію або відправку звіту.

Недоліком багатьох систем моніторингу, включаючи Network Olympus, є те, що карта мережі створюється лише вручну, а не автоматично, що могло б полегшити процес навчання та розуміння будови мереж.

Висновок

Під час проведення дослідження системи моніторингу Network Olympus було визначено, що дана програма може використовуватися студентами для дослідження мереж, хоча має певні недоліки, особливо у створенні карти мережі. До недоліків Network Olympus також можна віднести те, що дана програма призначена лише для Windows і для створення великої мережі, наприклад підприємства, безкоштовної версії не вистачатиме, тому що там можна використовувати лише до 10 пристроїв.

ВИКОРИСТАНІ ДЖЕРЕЛА

[1]https://www.network-olympus.com/ru/
[2]https://www.network-olympus.com/files/Network-Olympus-docs-RU.pdf

УДК 027.7:004 (045)

О.В. Іванкевич, к.т.н.,
В.І. Мазур,
В.Ф. Сураєв, к.т.н.
Національний авіаційний університет, Київ

ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ КУЛЬТУРИ МАЙБУТНІХ СПЕЦІАЛІСТІВ – ПРІОРИТЕТНЕ ЗАВДАННЯ СУЧАСНОЇ ОСВІТНЬОЇ ДІЯЛЬНОСТІ НАУКОВО-ТЕХНІЧНОЇ БІБЛІОТЕКИ НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ

Розвиток інформаційних технологій на сьогодні набув широкого поширення майже в усіх галузях науки та техніки. Не є винятком і бібліотечні системи. Зростання різноманітних інформаційних ресурсів збільшило обсяг і рівень складності пошуку, збору, обробки та аналізу інформації, отже пошук і замовлення літератури стають все складнішими операціями як для читача, так і для бібліографа. На допомогу бібліотекам приходять електронні системи пошуку документів, системи електронних замовлень, віртуальні бібліографічні довідки та інші системи [1,3]. Розробка нових засобів створення швидких і оптимальних бібліотечних інформаційно-пошукових систем з високою доступністю даних, з одного боку, ще більше спростить пошук інформації [1,2], а з іншого, ще звузить коло читачів, що можуть користуватися такими системами. Тому на сучасному етапі розвитку є необхідність розвитку навиків та умінь звертання до інформації–інформаційна культура. Без формування інформаційної культури студентів, без надання студентам знань про можливості нових інтегрованих інформаційно-пошукових систем, без висвітлення переваг, що дають такі системи не буде досягнуто ні значної економії часу для користувачів, ні взагалі користі від придбання та використання таких систем.

Приклад взаємодії інформаційних модулів інформаційно-пошукової системи НТБ НАУ наведено на рис. 1. Сучасні читачі вимагають від електронного каталогу не звичайного пошуку за автором/назвою/темою документів, а інтеграції всіх доступних БД та електронних ресурсів бібліотеки в єдиному універсальному інтерфейсі.

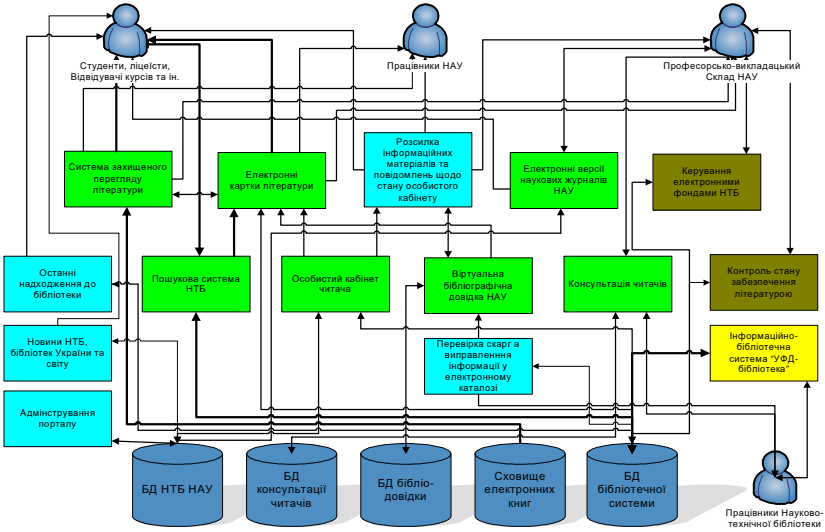

Рис.1 Взаємодія основних модулів інтегрованої інформаційно-пошукової системи Науково-технічної бібліотеки НАУ

Використання засобів автоматизації підбору літератури здатне забезпечити економію трудових і матеріальних витрат на роботу з документами і полегшити життя читача. Однак на сучасному етапі розвитку бібліотечної справи актуальними стають методи та засоби розвитку навиків та умінь звертання до інформації сучасних читачів бібліотек – формування інформаційної культури читача.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Іванкевич О.В. Концепція побудови інформаційно-пошукової системи науково-технічної бібліотеки НАУ / О.В. Іванкевич, В.Ю. Вахнован // Проблеми інформатизації та управління. - Вип. 2(24). - К. : НАУ, 2008. - С. 92-97.

2. Іванкевич О.В. Розвиток електронної бібліотеки Національного авіаційного університету / О.В. Іванкевич, В.Ю. Вахнован // Вісник Національного авіаційного університету.- К.: НАУ, 2011. - №4(49). - С. 74-79.

3. Іванкевич О.В. Створення проблемно-орієнтованої інформаційно-довідкової системи та бібліографічної бази даних "Бібліографічна довідка" наукових бібліотек ВНЗ / О.В. Іванкевич // Проблеми інформатизації та управління. - Вип. 1(29). - К.: НАУ, 2010. - С. 76-81.

УДК 004.03 (043.2)

А.В. Ільєнко, к.т.н.
С.С. Ільєнко, к.т.н.
О.О. Вертиполох
Національний авіаційний університет, Київ

ПІДХІД ЩОДО ВИКОРИСТАННЯ DOH ТА DOT ПРОТОКОЛІВ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

При проектуванні сучасних інформаційно-телекомунікаційних систем та мереж одним з найважливіших є завдання забезпечення захисту інформації з використанням новітніх методів та підходів. До найбільш ефективних методів рішення даного завдання варто віднести застосування підходу щодо захисту трафіку від втручання DPI систем, як забезпечення конфіденційності та цілісності інформаційних повідомлень.

Враховуючи аналіз останніх досліджень і публікацій, актуальним є питання захисту мережевого трафіку від втручання DPI систем, принцип дії якого ґрунтується на дослідженні вразливих місць стандартів, а саме DNS-запитів з врахуванням особливостей функціонування типових мережевих протоколів, з якими має справу переважна більшість користувачів мережі Інтернет.

Під поняттям DPI система будемо розуміти таку систему, яка виконує, так званий, глибокий аналіз мережевих пакетів на верхніх рівнях моделі OSI. Традиційний аналіз пакетів зазвичай перевіряє інформацію в заголовках пакетів мережевого та транспортного рівнів, DPI спрямований також на поведінковий аналіз трафіку прикладного рівня у режимі реального часу, тобто такий, що дозволяє розпізнавати користувацькі програми, для яких заздалегідь не визначено відомі заголовки протоколів та структури даних.

Використовуючи особливості мережевих протоколів можна виділити такі способи обходу DPI блокувань: додавання пробілів або інших символів табуляції між методом HTTP (GET, POST тощо) та URI; змішування літер регістру значення заголовка хоста; видалення пробілу між назвою заголовка та значенням у заголовку хосту; фрагментація на рівня TCP для першого пакету даних; фрагментація на рівні TCP для постійних сеансів HTTP; надсилання підроблених пакетів HTTP з низьким значенням часу

життя або неправильною контрольною сумою.

Сучасний веб та деякі інші мережеві протоколи захищені за допомогою TLS, але DNS-запити всю свою історію передають в незашифрованому вигляді. Компанії або держави використовують це в своїх інтересах, наприклад, для збору інформації про відвідувані сайти або фільтрації трафіку або навіть проводити атаки на DNS трафік, так званий спуфінг запитів з метою перенаправлення їх на власний сервер. Тому з метою вирішення проблеми шифрування DNS пропонуються такі протоколи: DNSCrypt; DNS-over-TLS (DoT); DNS-over-HTTPS (DoH); DNS-over-SSH (DoS); DNS-over-QUIC (DoQ).

Відповідно до проведеного аналізу авторами пропонується використання поєднаних методів DoT та DoH, які дозволяють одразу, без впровадження нових протоколів, із забезпеченням зворотної сумісності реалізувати захищену передачу трафіку. Перший метод більшого розповсюдження набуває на мобільних пристроях, наприклад, входить до реалізації Android 9. У той же час другий метод більшого поширення набув в системах, що вже реалізують використання HTTPS, наприклад, браузери.

Авторами реалізовано власний комплекс локального проксуючого серверу мовою програмування Python 3.8, та проведено його тестування на реальній системі. Цей комплекс дозволяє встановлювати захищене з’єднання з іншими довіреними серверами на базі використання протоколів DoH та DoT, та унеможливлює або значно ускладнює можливість використання DPI систем на межі звичайних місць їх встановлювання. Зважаючи на досягнення мети роботи практична цінність цих рішень є актуальною та необхідною для більшості користувачів та систем. Запропоноване рішення локального проксуючого серверу може бути розвинуто і далі. Наприклад, впроваджено реалізацію локального кешування або додано можливість створювати точніші правила для певних доменів та їх піддоменів, а реалізований тестовий DoH сервер може бути розгорнуто на довіреному виділеному сервері за межами можливих точок встановлення фільтруючого обладнання, що дасть змогу повністю контролювати власний трафік для резолвінгу доменних імен. Така реалізація дасть змогу повністю контролювати власний трафік для резолвінгу доменних імен.

УДК 004.03 (043.2)

А.В. Ільєнко, к.т.н.
С.С. Ільєнко, к.т.н.
Д.С. Сташевський
Національний авіаційний університет, Київ

МЕТОД ВІДСЛІДКОВУВАННЯ ПОМИЛОК У ВИСОКОНАВАНТАЖЕНИХ ВЕБ-ДОДАТКАХ МОВОЮ ПРОГРАМУВАННЯ JAVASCRIPT

На сьогодні відбувається стрімкий розвиток інформаційних технологій та інтенсивна розробка високонавантажених веб-додатків. Таким чином з великими об'ємами кодової бази постає потреба у відслідковуванні помилок у високонавантажених веб-додатках. Оскільки велика кількість веб-додатків написані мовою програмування Javascript, у цій мові програмування вже є деякі інструменти для відслідковування помилок. Проте, коли розміри веб-додатку починають збільшуватися, відслідковувати усі помилки та аналізувати їх дуже важко.

Під поняттям сучасний високонавантажений веб-додаток авторами надалі буде розумітися унікальна розробка, орієнтована на рішення значної кількості прикладних задач в інформаційних системах та мережах. Перевагою використання сучасних клієнт-серверних веб-додатків є те, що учасникам інформаційного обміну не потрібно додатково встановлювати спеціалізоване програмне забезпечення, оскільки для простоти реалізації всі дії відбуваються у браузері. До найпоширених помилок у високонавантажених веб-додатках можна віднести помилки при взаємодії користувача з веб-додатком, помилки з авторизацією та автентифікацією користувачів, помилки які виникають при високому навантаженні на додаток, помилки з кешуванням даних, що призводить до порушення конфіденційності та цілісності персональної інформації користувачів. Тому можна сказати, що механізм для вчасного та якісного відслідковування помилок, на сьогоднішній день – це необхідний компонент у будь-якому веб-додатку.

Авторами досліджено та визначено, що помилки, які виникають при розробці та використанні сучасних високонавантажених веб-додатків є дуже небезпечними, оскільки впливають на повноцінну життєдіяльність інформаційної системи в цілому та можуть

призводити до порушення конфіденційності та цілісності персональної інформації користувачів. На сьогодні існуючі рішення для відслідковування помилок у високонавантажених веб-додатках, а саме Sentry.io та Catch.js. Провівши їх дослідження та детальний аналіз можна дійти до висновку, що на сьогоднішній день існує рішення які більш-менш задовольняють потреби відслідковування помилок. Проте навіть, ці два рішення мають свої недоліки. Аналіз останніх досліджень і публікацій дозволив сформувати вимоги, яке висуваються до програмного модулю відслідковування помилок у високонавантажених веб-додатках. Враховуючи аналіз останніх досліджень і публікацій, актуальним питанням є розробка та впровадження удосконаленого авторського модуля відслідковування помилок у високонавантажених веб-додатках.

Результатом подальших досліджень стало створення авторського програмного модулю відслідковування помилок у висконавантажених веб-додатках для вирішення проблеми логування помилок, аналіз логів на повноту, обробку помилок та вирішення їх в майбутньому. Впровадження такого рішення дозволяє зменшити розмір програмного додатку для завантаження до 5 кілобайт та зберігати історію помилок. Розроблений програмний модуль відслідковування помилок у високонавантажених веб-додатках складається з двох частин клієнтської та серверної. Кожна частина є незалежним програмним модулем та може бути переконфігурована з мінімальними змінами конфігурації на будь-якому іншому ресурсі.

Така реалізація дає змогу повністю збирати метрики про кожен XMLHTTP запит, збирати інформацію про оточення користувача в якому сталася помилка, збирати інформація про те, чим саме була викликана помилка, визначати конкретне місце, де сталася помилка при виконанні програмного коду, за допомогою власноруч розробленого алгоритму, зберігати історії помилок у журналі Kibana.

Можливі подальші напрямки розвитку цієї роботи пов’язані із розширенням алгоритму відслідковування помилок у високонавантажених веб-додатках, для збору більшої кількості даних та удосконалення їх агрегації, на основі розширення метрик.

УДК: 004.056.55(003.26)

А.О. Капуста
Національний авіаційний університет, Київ

ЕВОЛЮЦІЯ АЛГОРИТМІВ ШИФРУВАННЯ RC

Алгоритми RC широко використовуються в багатьох мережевих додатках через їх сприятливі можливості швидкості та мінливої довжини ключів. В основному було розроблено шість алгоритмів RC, з яких використовують лише чотири. Незважаючи на подібність у своїх назвах, алгоритми здебільшого не пов'язані між собою.

RC1 так і не був опублікований, це був перший крок, який зробив Рівест для того, щоб продовжити з розробленням серії симетричних ключових алгоритмів, широко відомих як Rivest Cipher Algorithm. Основна ідея дослідження полягала в розробці алгоритму шифрування симетричного ключа, який би користувачі використовували для захисту своїх даних під час проходження через мережу.

RC2 - алгоритм блочного шифрування розроблений у 1987 році, розглядався як пропозиція щодо заміни DES. Шифрує дані блоками по 64 біта з використанням ключів змінного розміру: від 8 до 1024 бітів включно (рекомендованим розміром ключа є 64 біта). . Алгоритм розроблений для легкої реалізації 16-бітних мікропроцесорів. Якщо шифрування ключів було виконано заздалегідь, то цей алгоритм працює вдвічі швидше, ніж DES на IBM AT. Сам алгоритм включає 3 подальших алгоритми, а саме: розширення ключа, шифрування та розшифрування.

Алгоритм ***RC3*** не використовували, тому що він був пошкоджений під час його розробки для захисту RSA.

RC4 - це потоковий шифр з змінним розміром ключа, розроблений в 1987 році. Один і той же алгоритм використовується як для шифрування, так і для дешифрування. Потік даних виконує операцію XOR за допомогою серії згенерованих ключів. Змінна довжина ключа від 1 до 256 біт і використовується для ініціалізації 256-бітної таблиці стану. Він популярний завдяки своїй простоті. Шифр працює дуже швидко в програмному забезпеченні. Він вважався безпечним, поки він не став вразливим до BEAST атак.

RC5 розроблений в 1994 році як змінний на всіх фронтах. Розміри блоків можуть варіюватися від 32, 64 або 128 біт, а розміри ключів від 0-2040 біт і раундів від 0-255. Оригінальною пропозицією щодо параметрів був 64-бітний блок, 128-бітний ключ та 12 раундів. Він підходить для апаратного або програмного забезпечення. Це швидко, а також забезпечує безпеку, якщо обрані відповідні параметри.

RC6 був розроблений у 1997 році. Це блоковий шифр, який використовує 128-бітний розмір блоку і підтримує ключі розміром 128, 192 та 256 біт. Він був розроблений з метою задоволення вимог AES. Це вдосконалений алгоритм RC5. Забезпечує ще кращу безпеку від атак, які можуть бути можливими в алгоритмі RC5. Він використовує 4 регістри (кожен 32-х бітний) і є більш безпечним, ніж RC5. Він також захищений від різних інших можливих атак безпеки. Він використовує менше раундів і пропонує більш високу пропускну здатність.

Отже, запропоновано багато алгоритмів криптографії симетричного ключа. Алгоритми The Rivest Cipher - один із них. У цій роботі проведено огляд еволюції алгоритмів Rivest Cipher. Алгоритм RC6 хоч і не я є вразливим до будь-якої практичної атаки, але деякі теоретичні атаки все ще існують. У наш час, оскільки обчислювальна потужність зростає, RC6 може бути зламаним за кілька років. Таким чином, виникає потреба у більш сильному алгоритмі. Тому алгоритм повинен бути вдосконалений, щоб зробити його захищеним від атак.

ВИКОРИСТАНІ ДЖЕРЕЛА

1) https://en.wikipedia.org/wiki/RC_algorithm
2) https://www.globalsign.com/en/blog/glossary-of-cryptographic-algorithms
3) https://www.ripublication.com/irph/ijict_spl/ijictv4n17spl_13.pdf
4) http://crypto.pp.ua/2010/12/algoritm-rc2/
5) https://www.geeksforgeeks.org/rc4-encryption-algorithm/
6) http://solutionmes.wikidot.com/crypto-rc4

УДК 004.92 (043.2)

Н.В. Кірхар, к.т.н.,
Н.О. Рибасова
Національний авіаційний університет, Київ

СИСТЕМА ВІЗУАЛЬНОГО СКРИПТУ ЯК ЗАСІБ ПРОГРАМУВАННЯ

Програмувати на блупрінтах зовсім не складно, адже немає необхідності вчити складний синтаксис і писати код, а візуальна взаємодія дуже допомагає орієнтуватися в алгоритмі і «писати» програми швидше.

Blueprint (анл. план, креслення) – система візуального скриптинга, що представляє собою візуальний інтерфейс для створення елементів Геймплей, використовувана в ігровому движку Unreal Engine [1,2]. Вся логіка мови Blueprint будується з нодів (або блоків), які з'єднуються проводами. Яким би складними або простим він не здавався, він залишається досить таки потужним інструментом, на якому можна створити майже що завгодно, від простенького персонажа або відкриття дверцят до процедурної генерації рівня.

Два найбільш часто використовуваних типи блюпрінтів, блюпрінти-рівнів і блюпрінти-класи. Ноди – це візуальні уявлення подій, функцій і змінних [1]. Вони мають колірний код, що виражає їх призначення. Червоний нод – це нод події, що використовується для ініціювання виконання послідовності нодов. Сині Ноди – це функції для виконання певних операцій. Кольорові овальні Ноди, кожен з яких має тільки по одному контакту даних, представляють змінні.

Можна уявити процес візуального програмування як роботу електричного кола. Червоний нод події відправляє сигнал, що йде по проводах і запускає виконання будь-якого нода, через який цей сигнал проходить. Коли нод отримує сигнал, він отримує дані, які йому потрібні в контактах даних в лівій частині нода. Після чого нод виконує свою операцію, відправляє сигнал далі і повертає результати через контакти даних в правій частині нода.

Контакти даних мають колірний код, який базується на типі використовуваних ними даних. Контакти даних в лівій частині нода витягають дані, в той час як контакти даних в правій частині нода повертають дані [2].

Провода з'єднують Ноди. Колір кожного проводу відображає тип використовуваних їм даних. Подія (event) – це те, що відбувається в процесі гри, від натискання гравцем клавіші на клавіатурі або попадання аватара в якесь приміщення до зіткнення актора з іншим актором або початку гри. Події використовуються для ініціювання послідовності в блюпрінті. При запуску події з виведення exec-контакту надсилається сигнал, який проходить по дротах і обробляється всіма функціями, зустрінутими їм на шляху. Коли сигнал доходить до кінця послідовності нодів, він пропадає.

При запуску гри всі Blueprint коди переводяться на мову C ++. У самій грі використовується вже перекладений код на C ++. У професійного програміста різниця між скриптом на Blueprint і на C ++ може бути майже непомітна.

Самі Epic Games рекомендують використовувати блюпрінти, коли в проекті дуже багато посилань на контент, а його логіка працює в першу чергу на візуальну складову [2]. Також вони стануть в нагоді при створенні прототипів, прямолінійної або рідко використовуваної логіки, яка не є частиною основної архітектури. Все, що не отримає переваг в C ++ з точки зору продуктивності, масштабованості і стабільності, також може бути створено в Blueprints.

Блюпрінти виграють у C ++ на початкових етапах розробки, особливо якщо код гри пишеться з нуля. Вони не вимагають установки додаткової середовища, до того ж пропонують швидкі ітерації. А блоковий синтаксис блюпрінтів зрозумілий не тільки програмістам, але і тим, хто знайомий з аналогічними системами в програмах для створення контенту – наприклад, художникам.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Александр Буев. Основные приёмы blueprint-программирования — 2020. Режим доступу: https://it-cube48.ru/archives/18002

2. Арам Куксон, Райан Даулингсока, Клинтон Крамплер. Разработка игр на Unreal Engine 4 за 24 часа; [перевод с английского М. А. Райтмана]. — Москва : Эксмо, 2019. — 528 с.

УДК 519.872

О.В. Коба, д.ф.-м.н.,
Інститут кібернетики ім. В.М. Глушкова НАНУ, Київ
С.В. Серебрякова к.т.н.
Національний авіаційний університет, Київ

МОДЕЛІ ЛІНІЙ ОПТИЧНОЇ ЗАТРИМКИ КОМП'ЮТЕРНИХ МЕРЕЖ ЯК СИСТЕМИ ОБСЛУГОВУВАННЯ З ПОВЕРНЕННЯМ ЗАЯВОК

Лінії затримки забезпечують можливість управління тимчасовою затримкою сигналу. Лінії затримки – це важливі компоненти, які застосовуються в радіолокації, зв'язку та системах обробки сигналів. Загалом існує два типи ліній затримки: електричні та оптичні. Оскільки оптична лінія затримки має набагато ширшу смугу пропускання та вищу швидкість, вона найкраще застосоується у надширокосмугових системах, а тому останнім часом викликає значний інтерес серед дослідників [1]. Оптичні лінії затримки можуть застосовуватися, зокрема, в системах оптичного зв'язку та у фазованих решітках.

Перевагами оптичних ліній затримки є їх малі розміри і невелика вага. Ці пристрої базуються на концепції оптичної затримки, яку, в свою чергу, можна розуміти як властивість оптичного фільтра. Оптичні фільтри затримки використовуються для виконання різноманітних операцій обробки сигналів на надшвидкісних швидкостях передачі даних [2-3].

У сучасних магістральних комп'ютерних мережах як основний канал передавання інформації використовується оптичне волокно, однак, у той же час інші компоненти, такі як роутери, працюють із електричними сигналами. Оскільки електричні пристрої працюють набагато повільніше, аніж оптичні, без ліній затримки світлові імпульси постійно б накладалися один на одний, таким чином спричиняючи колізії. Таким чином, аби продовжити шлях оптичних сигналів його перенаправляють в оптичні лінії затримки, де сигнал проходить певні цикли у кільцях, таким чином формуючи буфер для світлових імпульсів.

Для моделювання ліній оптичної затримки можна скористатися системою обслуговування типу Лакатоша [4-5], оскільки оптичні сигнали не можуть наздогнати один одного, а завжди передаються за принципом «першим прийшов, першим обслужений» (FCFS).

Відмітимо також детермінованість часу перебування оптичного сигналу в лінії затримки: кожна лінія оптичної затримки має свою власну характеристику можливої тривалості затримки сигналу [6].

На рис.1 наведене схематичне зображення потоку оптичних сигналів, які проходять через оптичну лінію затримки.

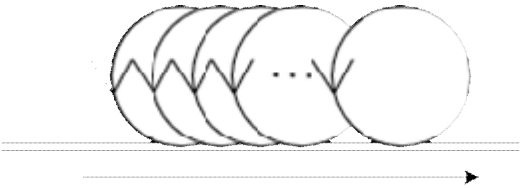

Рис.1. Потік заявок в оптичній лінії затримки.

Авторки розглядають оптичну лінію затримки як систему обслуговування типу Лакатоша із узагальними вхідним потоком (l) та потоком обслуговування (m), а також детермінованим часом перебування заявки на орбіті. Умова ергодичності системи:

$$\rho < \frac{e^{-\lambda T}(1 - e^{-\mu T})}{1 - e^{-\lambda T}}.$$

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Webster, J.G., Shahoei, H. and Yao, J. Delay Lines. Wiley: Encyclopedia of Electrical and Electronics Engineering, 2014.

2. Okamoto, K. Fundamentals of Optical Waveguides. Academic Press, 2005. 584pp.

3. W. Rogiest, K. Laevens, D. Fiems, and H. Bruneel, "A performance model for an asynchronous optical buffer," Performance Evaluation, Vol. 62, Nos. 1–4, 313–330 (2005).

4. Koba, O.V., Serebriakova, S.V. GI / G / 1 Lakatos-Type Queueing System with T-Retrials. Cybern. Syst. Anal., Vol. 57, No.2, (2021). https://doi.org/10.1007/s10559-021-00353-x

5. E. V. Koba and S. V. Pustova, "Lakatos queuing systems, their generalization and application," Cybern. Syst. Analysis, Vol. 48, No. 3, 387–396 (2012). https://doi.org/10.1007/s10559-012-9418-7.

6. URL: https://rfoptic.com/what-is-an-optical-delay-line-odl/

УДК 621.3

Л.П. Крючкова, д.т.н.,
М.О. Вовк
Державний університет телекомунікацій, Київ

МЕТОД РУЙНУВАННЯ ІНФОРМАТИВНИХ ПАРАМЕТРІВ СИГНАЛІВ РАДІОЗАКЛАДНИХ ПРИСТРОЇВ

В доповіді розглянуто проблему захисту акустичної інформації на об’єктах інформаційної діяльності від перехоплення радіозакладними пристроями.

Визначено параметри захисних сигналів для руйнування інформативних параметрів аналогових сигналів радіозакладних пристроїв та цифрового сигналу радіозакладного пристрою з широтно імпульсною модуляцією (рис. 1).

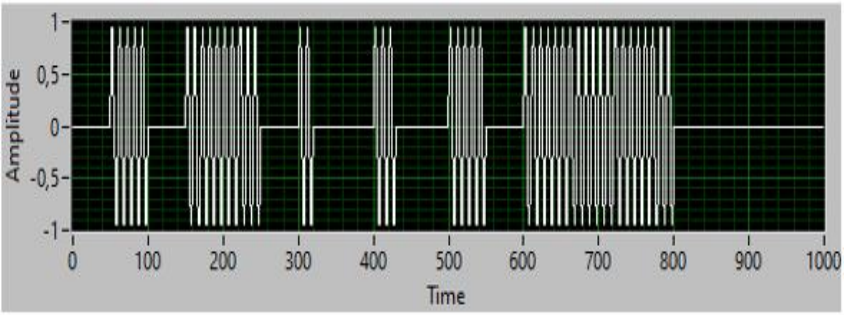

Рис.1. Зображення сигналу радіозакладного пристрою з широтно-імпульсною модуляцією

Сутність запропонованого методу полягає в застосуванні комбінованої активної завади (захисного сигналу), спрямованої на руйнування інформативних параметрів небезпечного сигналу радіозакладних пристроїв.

Засобами радіомоніторингу визначається несійна частота радіозакладного пристрою (небезпечний сигнал). Після виявлення несійної або несійних небезпечного сигналу, для активної протидії використання створеного зловмисником каналу витоку інформації формуються захисні сигнали з наступними параметрами:

- перший сигнал – несійний сигнал, з частотою, віддаленою на 10% від частоти небезпечного сигналу. В результаті впливу першого захисного сигналу на небезпечний сигнал з’являється ефект биття (рис. 2);

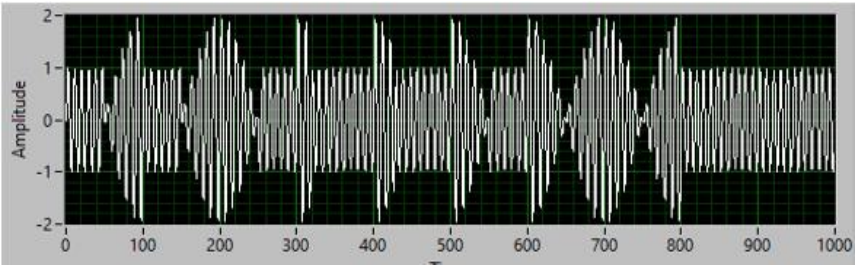

Рис.2. Зображення сигналу биття небезпечного та першого захисного сигналів

- другий сигнал – сигнал коливальної частоти в межах від 5% до 20% частоти небезпечного сигналу (рис. 3).

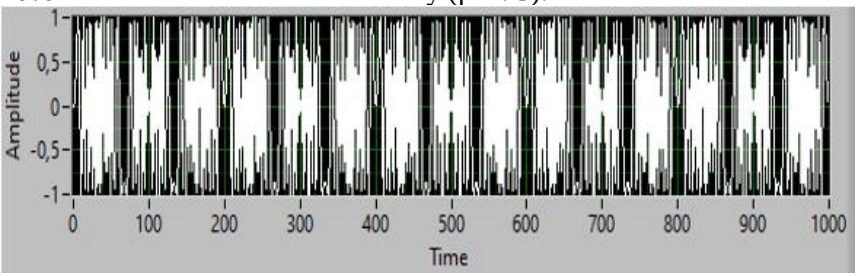

Рис.3. Зображення сигналу коливальної частоти

Такий комбінований вплив на небезпечний сигнал призводить до ефективної руйнації інформації, що передається радіозакладним пристроєм (рис. 4) та унеможливлює демодуляцію несійного сигналу.

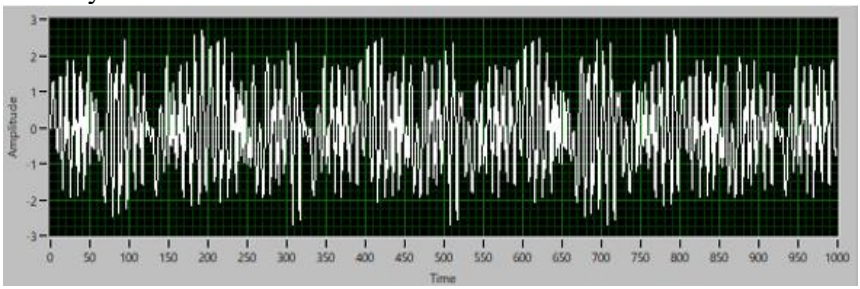

Рис.4. Зображення результуючого небезпечного сигналу

Захисні сигнали з вказаними параметрами забезпечують руйнування інформативних параметрів розглянутих сигналів радіозакладних пристроїв.

В перспективі планується проведення досліджень з метою визначення параметрів захисних сигналів, які забезпечують блокування інших цифрових сигналів радіозакладних пристроїв.

УДК 621.391

Л.П. Крючкова, д.т.н.,
Д.О. Тарасенко
Державний університет телекомунікацій, Київ

МЕТОДИКА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ В УМОВАХ ВПЛИВУ ЗОВНІШНІХ ЗАВАД

Одним з ключових напрямків розвитку сучасного суспільства є формування інтегрованого інформаційного простору на основі новітніх інформаційних технологій. Потреба підвищення пропускної спроможності та швидкодії інфокомунікаційних мереж постійно зростає. Управління інфокомунікаційними мережами, що функціонують в різних фізичних середовищах і зовнішніх умовах, є дуже важливою проблемою як з позицій розробки системи управління, так і з позицій реалізації управління в процесі функціонування інфокомунікаційної мережі.

Основна складність, що виникає при управлінні інфокомунікаційною мережею, – невизначеність і недостатність апріорної інформації про об’єкт управління, наявність невідомих факторів, що суттєво впливають на його поведінку, і, як наслідок, проблематичність побудови його адекватної аналітичної моделі. Додаткові складнощі виникають при управлінні інфокомунікаційними мережами в умовах впливу зовнішніх завад, створюваних спеціалізованими технічними засобами.

Створення систем, апріорно орієнтованих для роботи в умовах неповноти інформації, вимагає залучення нетрадиційних підходів до управління із застосуванням методів та технологій штучного інтелекту. Інтелектуальні системи управління фактично створюють новий клас, для якого принципи побудови, методи аналізу та синтезу повинні враховувати всі характерні особливості різнорідних інфокомунікаційних мереж.

Сучасні інфокомунікаційні мережі використовують різні сигнальні формати з різними енергетичними і спектральними параметрами. Застосування конкретного сигнального формату обумовлюється відповідністю цих параметрів умовам, в яких відбувається передача і приймання інформації.

Зростання ступеня інтеграції елементної бази електроніки, і, як наслідок, зниження електричної міцності окремих компонентів

апаратури призводить до підвищення уразливості сучасних електронних систем до впливу електромагнітних факторів різного походження.

Деструктивні впливи спрямовуються на руйнування інформаційних потоків, що циркулюють між елементами мережі; зниження швидкості інформаційного обміну між елементами системи управління, що суттєво збільшує тривалість циклу управління і, як наслідок, знижує ефективність управління мережею; забезпечення достатньо масованого і довготривалого виведення з ладу мережевих технічних засобів.

В доповіді зазначається відсутність комплексних технічних рішень, спрямованих на підвищення ефективності функціонування інфокомунікаційних мереж в умовах атак електромагнітного характеру. Огляд досліджень не дозволяє говорити про їх повне завершення та виявляє завдання, які чекають свого вирішення.

Актуальним завданням є розробка науково-обґрунтованих методів і технічних рішень для систем зв'язку, здатних забезпечити завадостійке приймання дискретної інформації в умовах інтенсивного впливу зовнішніх завад, та форм і способів упереджувальної протидії впливам різних дестабілізуючих і деструктивних чинників з боку навколишнього середовища як ненавмисного, так і навмисного характеру.

В доповіді розглядається метод ситуаційного управління інфокомунікаційною мережею, заснований на побудові адаптивної стратегії управління з прогнозуванням стану мережі і реалізацією керуючого впливу для забезпечення визначених показників якості функціонування мережі в умовах впливу зовнішніх завад.

Запропоновано модель прийняття рішення, засновану на урахуванні тенденцій змінювання вихідних параметрів, яка дозволяє забезпечити визначені показники якості функціонування мережі в умовах зовнішніх деструктивних впливів. Ситуаційна модель дозволяє автоматизувати пошук найкращих стратегій управління в системах, для яких важливим є принцип швидкого реагування.

Розглянуто метод побудови ефективного цифрового каналу для передачі керуючої інформації.

УДК 621.396

Л.П. Крючкова, д.т.н.,
Є.О. Українець
Державний університет телекомунікацій, Київ

ДОСЛІДЖЕННЯ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ USB ІНТЕРФЕЙСУ ТА ВІДЕОТРАКТУ ПК У БЛИЖНІЙ ЗОНІ

Останнім часом повідомлення про атаки на інформацію, про хакерів і комп'ютерні зломи заполонили всі засоби масової інформації. З масовим упровадженням комп'ютерів у всі сфери діяльності людини обсяг інформації, що зберігається в електронному вигляді, збільшився в тисячі разів.

Як показує практика, швидкий розвиток отримують методи перехоплення інформації каналами побічних електромагнітних випромінювань (ПЕМВ). Для виявлення ПЕМВ сучасної електронно-обчислювальної техніки доводиться використовувати спеціальні організаційні, алгоритмічні та методичні підходи, які враховують ці проблеми [1]. В роботі висвітлено деякі аспекти вимірювання та аналізу ПЕМВ, а також приділено увагу питанням захисту інформації, що циркулює в автоматизованих системах, носіями якої є електричні сигнали та електромагнітні поля.

Метою дослідження є розробка вдосконаленої методики виявлення побічних електромагнітних випромінювань USB інтерфейсу та відеотракту ПК у ближній зоні.

Структурна схема вимірювання експериментальної установки наведена на рис.1.

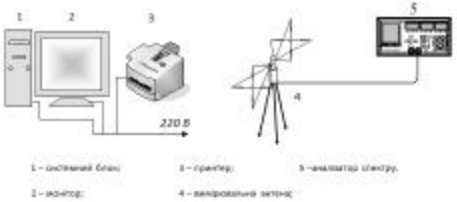

Рис.1. Структурна схема експериментальної установки

Перше дослідження проводились за допомогою аналізатора спектру ROHDE&SCHWARZ FSW 13 (Signal&SpectrumAnalyzer) з

використанням антени R&S ActiveDipoleAntenna HE527 та USB флеш накопичувача Transcend J32 2GB.

Зображення сигналів побічних електромагнітних випромінювань інтерфейсу USB 2.0 для різних частот з вимкненим та включеним тестовим сигналом подано на рис.2.

Рис.2. Фотографії спектрограм сигналів USB інтерфейсу при дослідженні побічних електромагнітних випромінювань

Друге дослідження проводились за допомогою аналізатора спектру ROHDE&SCHWARZ FSW 13 (Signal&SpectrumAnalyzer) з використанням точкової антени R&S MAGNETICNEAR-FIELDPROBEHZ-14 та монітору Samsung SyncMaster 940T.

Фрагменти спектрограм сигналів відеотракту ПЕОМ у ближній зоні наведено на рис.3.

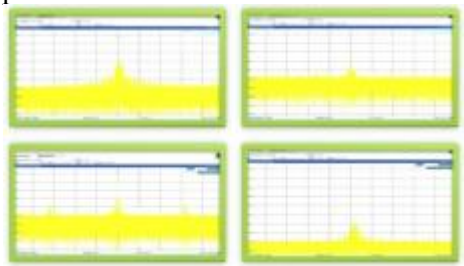

Рис.3. Фотографії спектрограм сигналів відеотракту ПЕОМ у ближній зоні при дослідженні побічних електромагнітних випромінювань

Запропонована нами удосконалена методика дослідження ПЕМВ конкретизує найбільш потенційно-небезпечний сигнал відеотракту та прискорює виявлення ПЕМВ порівняно з вимірюваннями, які проводяться при стандартних спеціальних дослідженнях ПЕМВ відеотракту ПК.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Голев Д.В., Кононович В.Г., Хомич С.В. Методики оцінки інформаційної захищеності телекомунікацій: навч. посіб. – Одеса, 2013. – 220 с.

УДК 621.3

Л.П. Крючкова, д.т.н.,
І.В. Цмоканич,
Державний університет телекомунікацій, Україна

УДОСКОНАЛЕНИЙ МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ

На об'єктах інформаційної діяльності циркулює інформація, яка має певний гриф секретності або може містити дані, які певним чином можуть впливати на безпеку держави та її громадян. Через це ця інформація може піддаватися спробам перехоплення. Внаслідок дії багатьох чинників можуть самочинно утворюватися або навмисно формуватись технічні канали витоку конфіденційної інформації. Враховуючи важливість інформації, застосовуються заходи та засоби, спрямовані на забезпечення захисту акустичної інформації та інформації, оброблюваної у інформаційних системах.

Одним з ефективних методів перехоплення конфіденційної інформації є методи високочастотного нав'язування [1]. В даний час застосовуються два способи перехоплення інформації каналами високочастотного нав'язування:

- за допомогою контактного або індукційного введення високочастотного сигналу в електричні кола, які мають функціональні або паразитні зв'язки з основним технічним засобом;
- шляхом опромінення високочастотним електромагнітним сигналом джерела інформації і прийняття відбитого модульованого сигналу.

Нами пропонується застосування активних методів захисту інформації від витоку каналами високочастотного нав'язування. Сутність методу полягає в реалізації системи захисту наступним чином [2]:

1. Методом радіомоніторингу на об'єкті інформаційної діяльності виявляється частота небезпечного сигналу.

2. У випадку виявлення вищезгаданим методом небезпечного сигналу, високочастотним генератором формується сигнал, спрямований на руйнування інформативних параметрів небезпечного сигналу, що унеможливлює перехоплення інформації.

Як відомо, перехоплення інформації може здійснюватись як на основній частоті, так і на гармоніках небезпечного сигналу. Удосконаленням і новизною методу є те, що забезпечується формування захисних сигналів не тільки на основній частоті, а й на гармоніках небезпечного сигналу. Отже, явище «биття» небезпечного і захисних сигналів буде прослідковуватись і на основній частоті, і на гармоніках.

Нами проведено розрахунки та експериментально визначено оптимальні значення захисного сигналу для забезпечення явища «биття». Визначено оптимальний діапазон, а саме: $0{,}005 \leq \Delta\omega \leq 0{,}3$, де $\Delta\omega$ – різниця частот небезпечного сигналу та сигналу, який формується генератором.

Рис. 1 – Демонстрація результуючого сигналу при умові $\Delta\omega$=0,01 кГц

Отримані спотворення небезпечного сигналу унеможливлюють відтворення перехопленої інформації, що дозволяє забезпечити захист інформації від витоку (рис.1).

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Крючкова Л.П., Провозін О.П. Перехоплення мовленнєвої інформації методами високочастотного "нав'язування" // Сучасний захист інформації – 2017. – №3(31), С.74-80.

2. Патент 95365 Україна, МПК (2011.01) H04K 3/00. Спосіб захисту інформації / Рибальський О.В., Хорошко В.О., Крючкова Л.П., Джужа О.М., Орлов Ю.Ю.; заявник і патентовласник Національна академія внутрішніх справ. - № a200913327; заявл. 22.12.2009; 55 опубл. 25.07.2011, Бюл. № 14.

UDC 004.65

Kudrenko S.A., Ph.D.
Pushkin Yu.A.
National Aviation University, Kyiv

MODEL AND SCHEME FOR ORGANIZING DATA WAREHOUSES

In traditional architecture, there are three general data warehouse models: virtual warehouse, data mart, and enterprise data warehouse:

A virtual datastore is a collection of separate databases that can be shared so that a user can efficiently access all of the data as if it were stored in a single datastore;

The data mart model is used for reporting and analyzing specific business lines. In this warehouse model, aggregated data from a number of source systems related to a specific business area, such as sales or finance;

The enterprise data warehouse model assumes storage of aggregated data that covers the entire organization. This model views the data warehouse as the heart of the enterprise information system with integrated data from all business units.

Star and snowflake schemas are two ways to structure your data warehouse.

A star schema has a centralized data store that is stored in a fact table. The schema splits the fact table into a series of denormalized dimension tables. The fact table contains the aggregated data that will be used for reporting, and the dimension table describes the stored data.

Denormalized projects are less complex because the data is grouped. The fact table uses only one link to attach to each dimension table. The simpler star schema design makes it much easier to write complex queries. A snowflake schema is different in that it uses normalized data. Normalization means organizing data efficiently so that all data dependencies are defined and each table contains a minimum of redundancy. In this way, the individual dimension tables are forked into separate dimension tables.

The snowflake scheme uses less disk space and better preserves data integrity. The main drawback is the complexity of the queries required to access the data – each query must go through multiple table joins to get the corresponding data.

There are two different ways to load data into the warehouse: ETL and ELT.

ETL (Extract, Transform, Load) first retrieves data from a pool of data sources. The data is stored in a temporary staging database. Transformation operations are then performed to structure and transform the data into an appropriate form for the target data warehouse system. The structured data is then loaded into the warehouse and ready for analysis.

In the case of ELT (Extract, Load, Transform), data is loaded immediately after being extracted from the original data pools. There is no staging database, which means that the data is immediately loaded into a single centralized repository.

The data is transformed in a data warehouse system for use with business intelligence and analytics tools. The structure of an organization's data warehouse also depends on its current situation and needs.

The basic structure allows end users of the warehouse to directly access, report, and analyze summary data from the source systems. This structure is useful for cases where data sources come from the same types of database systems.

Staging area storage is the next logical step in an organization with heterogeneous data sources with many different types and formats of data. The staging area converts the data into a generalized, structured format that is easier to query using analysis and reporting tools.

One type of middleware is adding data marts to a data warehouse. Data marts store summary data for a specific industry, making this data readily available for specific forms of analysis.

For example, adding data marts can enable financial analysts to more easily query detailed sales data and predict customer behavior. Data marts facilitate analysis by tailoring data specifically to meet the needs of the end user.

REFERENCES

1. Buyya R., Broberg J., Goscinski A., Cloud Computing. Principles and Paradigms, John Wiley & Sons, Inc., New Jersey. – 637 p.

2. Focus Group on Cloud Computing Technical Report, 2012, Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements, ver.1.0. – pp.62.

УДК 004.056

Т.В. Кузнєцова, доцент,
А.В. Чирков
Національний авіаційний університет, Київ

STATE AND PERSPECTIVES OF AIRCRAFT CYBERSECURITY

During the latest events in the aviation world, where experts in the field of cybersecurity (example) opened the possibility of gaining access to the aircraft's on-board systems, industry experts (and not only) thought about it. And we are doing quite a lot. There are many existing guides that contain recommendations and practices, for example: «Software Considerations in Airborne Systems and Equipment Certification» contains recommendations for evaluating security and assuring software quality. There is a separation of access, because all systems are somehow connected to each other through the on-board network (take at least maintenance to determine failures) – as a fig. 1:

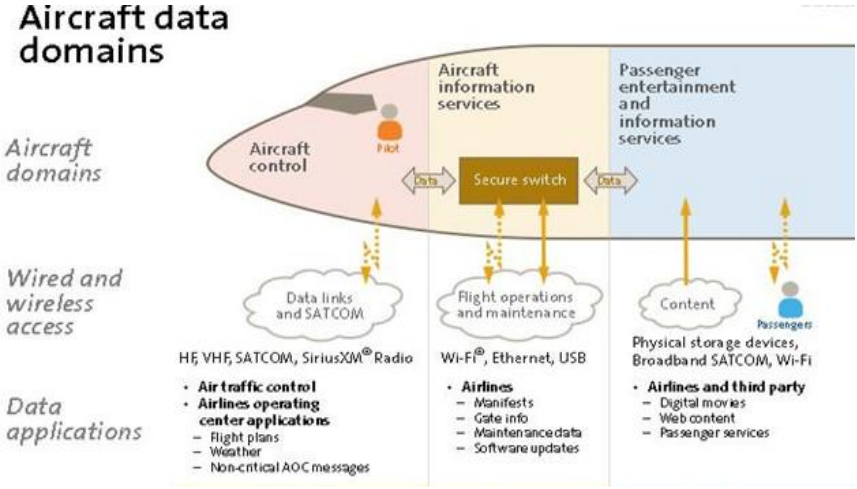

Fig. 1 Security and access restriction determined by aircraft domain [2]

• A high degree of integration of airborne equipment creates vulnerabilities in the security system;

• The FAA (US Federal Aviation Administration) did not properly implement the requirements for the Next Generation Air Transportation System (NextGen);

• An integrated information management network called SWIM based on satellite navigation of aircraft, tracking and digital transmission of voice and data creates significant and unresolved problems of cybersecurity;

• ADS-B technology, the introduction of which is planned to replace traditional radars, is inherently vulnerable to hacking due to its open architecture and the use of unencrypted signals.

GAO therefore highly recommended the FAA [1]:

• To fully apply the “Recommendations on information security throughout the life cycle of systems” developed by NIST (National Institute of Standards and Technology, also maintains a database of vulnerabilities);

• Make greater emphasis on guaranteeing the quality of airborne systems and consider safety and integrity issues in the airworthiness certification process.

The FAA continues to consider the aircraft guidelines acceptable for software certification, although they acknowledge that the guidelines do not fully cover all areas of software development and life cycle processes, and can sometimes be misinterpreted (Fig. 2).

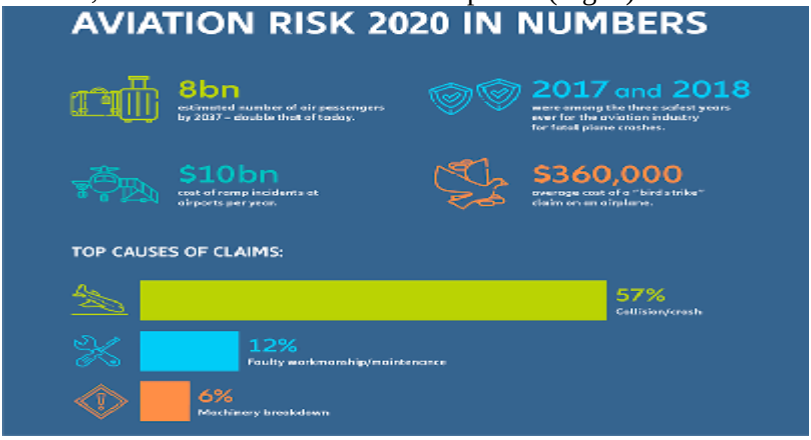

Fig. 2 Aviation Risk Forecast for 2020 [4]

Needless to say, the problem is finally recognized. She is, she exists. Some thought about it while watching the discovery movie «Inside A Plane Crash» – a Boeing crash test performed remotely. Some began to

breed panic and exposure. Nevertheless, at present, there is no single integrated approach to cybersecurity in the field of civil aviation. The American Institute of Aeronautics and Astronautics (AIAA) has published a general framework for aviation cybersecurity. The International Air Transport Association (IATA) has developed a set of cybersecurity tools. However, the FAA did not approve of them and set a goal to develop their own strategy that defines cybersecurity approaches to the entire aviation system. Actually, the work is being done in our aviation slowly, but with the deepest control and analysis of everything and everything, so that you can be calm and confident that you will fly in safety.

Although technology improves computer security, you should not forget about vigilance, for example, when receiving emails by e-mail. Hackers often hide behind messages from travel services, such as Airbnb, Booking.com, write on behalf of airlines, inform the user that they have paid for a plane ticket with their credit card, and offer a link to a phishing site where they allegedly can find out information about the upcoming flight [3].

In October 2019, it was the turn of cybercriminals who used the hype around the Ebola virus to send malicious emails. Again, WHO was indicated as the sender. In the text of the letters discovered by the experts, the attackers tried to convince the recipient that WHO had prepared a file with general information and precautions that would help protect the user and others from the deadly virus and other diseases.

In addition to exploiting topics that are relevant to society, spammers also send fake receipts from online stores invoicing a completed purchase, which can only be canceled on the phishing site [5].

REFERENCES

1. https://www.rbc.ua/ukr/tag/hakery
2. https://www.rbc.ua/ukr/tag/kiberataka
3. https://www.ukrinform.ru/tag-kiberataka
4. https://slovoidilo.ua/2020/04/13/kolonka/aleksandr-radchuk/bezopasnost/poligon-xakerskix-diversij-chto-zhdet-ukrainu-eru-kibervojn
5. https://forinsurer.com/news/20/04/10/37499

УДК 004 (043.2).

В.В. Кузнєцова
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ РЕТОПОЛОГІЇ У СУЧАСНІЙ ТРИВИМІРНІЙ ГРАФІЦІ

Тривимірна графіка на сьогодні є трендом в інформаційних технологіях. Вона стала настільки широким поняттям, що її використовують в архітектурі, для візуалізації концептів, друку 3D моделей або безпосередньо для створення та відображення об'єктів віртуальної реальності.

Окрім класичного підходу геометричного проектування, стає все більш вживана технологія скульптингу. Вона дозволяє безпосередньо ліпити фігуру, наче з глини, надаючи моделям плавного вигляду, якого складно досягти в геометричному проектуванні. Це особливо зручно коли моделюються живі істоти, наприклад, тварини. Скульптинг допомагає зберегти унікальні ознаки та надати життєподібного вигляду комп'ютерній моделі, якого б було складно добитись за допомогою класичного геометричного моделювання.

Зі збільшенням популяризації скульптингу в тривимірній графіці користувачі почали стикатись з проблемами продуктивності. Ця технологія зберігає усю інформацію про найменші виїмки і складки. Тож, хоча це виглядає детально і ефектно, такі моделі значно зменшують швидкість обробки кінцевого проекту, особливо на машинах нижчої обчислювальної потужності.

Очевидно, якщо просто відмовитись від технології загалом, то ми не зможемо отримувати моделі саме того органічного вигляду, що досягається тільки завдяки скульптингу. Тоді, треба знайти інший варіант, як обійти значне навантаження комп'ютера важкими файлами моделі.

Першим, та найбільш очевидним, з рішень проблеми може бути купівля обладнання з максимально високими експлуатаційними характеристиками. Однак це не є варіантом, що підходить для всіх проектувальників. До того ж, неможливо точно вгадати, чи зможе комп'ютер кінцевого користувача обробити модель з наявними в нього ресурсами.

Іншим способом є розділення проекту на менші частини для подальшого компонування в одному фінальному файлі. Цей варіант підійде для статичних картинок, але не для анімацій. До того ж, він все одно буде потребувати потужного комп'ютера для повної зборки усього проєкта на одному тлі.

Проблему вирішили несподівано просто: стали зменшувати кількість полігонів, вручну моделюючи їх сітку безпосередньо по поверхні, тим самим, перероблюючи стару топологію.

Ретопологія - це процес перетворення моделей з високою роздільною здатністю у щось набагато менше, що може бути використано для анімації. Це може бути складним процесом, але основна ідея полягає в тому, щоб створити ще одну сітку полігонів, яка спрощує оригінальну HD модель.

Крім того, якщо ви ретопологізуєте свої моделі, стає легше додавати текстури до виліплених моделей. Нова ретопологізована сітка не матиме спотворень та інших проблем, які часто є у автоматично сформованих 3D-сітках. [1] Але, через це, втрачається початкова деталізація моделі, тож була імплементована ще одна технологія. Тепер створюють додатковий файл, що містить інформацію про поверхневі особливості скульптованої моделі.

Карти нормалей та зміщення - це особливі види текстур зображення, які впливають на спосіб обчислення світла на поверхні. Вони створюють ілюзію глибини, змушуючи світло відбиватися від імітованих особливостей поверхні, хоча цих особливостей насправді там немає. [2]

Такі моделі можна відображати з різним рівнем деталізації на комп'ютерах як низької, так і високої обчислювальної потужності. І хоча використання такої технології займає час на створення спрощеної, ретопологізованої моделі, це значно полегшує подальшу роботу з анімацією та текстурами.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Petty J. What is Retopology? (A Complete Intro Guide For Beginners) [Електронний ресурс] / Josh Petty. – 2019. – Режим доступу до ресурсу: https://conceptartempire.com.

2. Lampel J. Normal vs. Displacement Mapping & Why Games Use Normals [Електронний ресурс] / Jonathan Lampel. – 2017. – Режим доступу до ресурсу: https://cgcookie.com.

УДК 004.056

С.В. Лазаренко, д.т.н.,
Т.Л. Щербак, к.т.н.,
Національний авіаційний університет, Київ
О.М. Фурсенко, к.т.н.,
Інститут державного управління у сфері цивільного захисту
Б.В. Ткач
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

РЕАГУВАННЯ НА СОЦІОТЕХНІЧНІ АТАКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Об'єкти критичної інфраструктури – підприємства та установи (незалежно від форми власності), що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення [1]. На таких об'єктах здійснюється обробка, зберігання, передача інформації з обмеженим доступом, несанкціоноване розповсюдження якої завдасть значної шкоди. У подальшому найбільшу загрозу інформаційній безпеці будуть представляти методи соціальної інженерії, що застосовуються для злому існуючих засобів захисту.

Основною причиною цього є те, що застосування соціальної інженерії не вимагає значних фінансових витрат і досконалого знання інформаційних технологій. Тому, актуальним є своєчасне реагування на соціотехнічні атаки та знешкоджня наслідків таких атак.

Соціальна інженерія – метод несанкціонованого доступу до інформації або до систем зберігання інформації без використання технічних засобів. Метод заснований на використанні слабкостей людського фактору. Дослідження показують, що людям притаманні деякі поведінкові схильності, які можливо використати для маніпулювання. Більшість зломів систем безпеки відбуваються завдяки використанню соціальної інженерії, а не технічному (електронному) злому [2, 3].

Атаки, засновані на методах соціотехніки, можливо розділити на п'ять основних напрямків: мережеві атаки; телефонні атаки; пошук інформації в смітті; персональні підходи; зворотна соціотехніка.

Оцінка ефективності реагування служб захисту інформації (адміністраторів безпеки, менеджерів з кібербезпеки тощо) на соціотехнічні атаки, повинна здійснюватись за рахунок застосування процедури вибору заходів і засобів реагування на соціотехнічні атаки, які функціонують в нечіткому середовищі [3, 4].

Існують базові методи реагування на атаки за допомогою методів соціальної інженерії, до яких відноситься: тестування системи захисту; поінформованість; активний захист.

Такі заходи дозволяють оцінити критичність впливу соціотехнічних атак на об'єкти критичної інфраструктури, а також забезпечити своєчасне реагування на соціотехнічні атаки і як наслідок, застосовувати ефективні засоби, що дозволяють захистити інформаційний простір від таких атак зі сторони зловмисника [3].

Таким чином:

1. Впровадження систем реагування на соціотехнічні атаки надасть можливість службам захисту інформації швидко та оперативно виявляти і здійснювати оцінку такої атаки.

2. За результатами оцінки виявленої атаки будуть вжиті ефективні заходи з локалізації такої атаки та знешкодження її наслідків.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Постанова Кабінету Міністрів України від 23.08.2016 № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».

2. Роуз М. Соціальна інженерія [Електронний ресурс] / Роуз Маргарет/ Режим доступу до ресурсу: http://searchsecurity.techtarget.com/definition/social-engineering

3. Рєзник Ю.М. Соціальна інженерія: В 2 ч. – Ч. 1. Теоретико-методологічні проблеми: Курс лекцій / Рєзник Ю.М., Щербина В.В. – М.: Союз, 1994. – 147 с.

4. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А. Г. – К.: МК-Пресс, 2006. – 320 с.

УДК 004.056.53

В.В. Липявка,
Г.В. Мартинюк, к.т.н.
Національний авіаційний університет, Київ

ПОБУДОВА СИСТЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Завдання забезпечення інформаційної безпеки в сучасному світі є особливо актуальним. Це пов'язано з широким впровадженням комп'ютерних систем та мереж на різноманітних об'єктах інформаційної діяльності. Вони здобули широке використання у всіх галузях промисловості, фінансових операціях, обліку тощо.

Організаційні вимоги до системи захисту передбачають реалізацію сукупності адміністративних і процедурних заходів. Вимоги щодо забезпечення схоронності мають виконуватися, насамперед, на адміністративному рівні. Організаційні заходи, проведені з метою підвищення ефективності захисту інформації, повинні передбачати такі процедури:

-обмеження несупроводжуваного доступу до обчислювальної системи;

-здійснення контролю за зміною в системі програмного забезпечення, виконання тестування і верифікації змін у системі програмного забезпечення і програмах захисту;

-організація і підтримання взаємного контролю за виконанням правил захисту даних;

-обмеження привілею персоналу, що обслуговує ІС;

-здійснення запису протоколу про доступ до системи;

-гарантія компетентності обслуговуючого персоналу;

-розробка послідовного підходу до забезпечення схоронності інформації для всієї організації.

Підсистема керування доступом має забезпечувати: ідентифікацію, аутентифікацію і контроль за доступом користувачів (процесів) до системи, терміналів, вузлів мережі, каналів зв'язку, зовнішніх пристроях, програм, каталогів, файлів, записів і т.д.; керування потоками інформації, очищення областей, що звільняються, оперативної пам'яті і зовнішніх накопичувачів.

У роботі представлено модель загроз для інформації з обмеженим доступом, що циркулює на об'єкті інформаційної діяльності. Згідно

з представленою моделлю можна описати технічні канали витоки інформації та шляхи недопускання цього.

Акустичний канал може бути створений: шляхом безпосереднього прослуховування розмов; шляхом перехоплення мовних сигналів за допомогою портативних технічних засобів акустичної розвідки (диктофонів та магнітофонів); шляхом застосування МНД та акустичних антен, що встановлюються в зоні прямої видимості. Для захисту мовної інформації від витоку можна застосовувати різноманітні проектно-архітектурні рішення, а саме: зашумлення, звукоізоляцію або ж кімнати для ведення переговорів розташовувати в місцях, де зняття інформації унеможливлене архітектурою будівлі.

Візуально-оптичний канал. За допомогою зорової системи людина отримує найбільший (до 90%) обсяг інформації із зовнішнього світу. Інфрачервоний і ультрафіолетовий спектри також несуть істотну інформацію про навколишні предмети. З метою захисту інформації від витоку рекомендується: робити просторові огородження; ввести енергетичні обмеження; використовувати засоби загародження або значного ослаблення відбитого світла; застосовувати засоби маскування, імітації та інші з метою захисту та введення в оману зловмисника.

Витік інформації по ланцюгам заземлення. Так як кола заземлення виходять за межі приміщення і будівлі, то сигнали, які поширюються по ним можуть бути зняті за допомогою технічних засобів. Небезпечний сигнал може бути «знятий» з кола заземлення індуктивним способом або з опору, включеного послідовно в цей ланцюг.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Кулаков Ю. А., Луцкий Г. М. Компьютерные сети. – К.: Юниор, 1998. – 380 с.*
2. *Бэрри Нанс. Компьютерные сети / Пер. с англ. – К.: Бином, 1995. – 214 с.*
3. *Торокин А.А. Основы инженерно-технической защиты информации /А.А. Торокин. – М.: Ось-89, 1998. – 336с.*
4. *Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа /Ю.Ф. Каторин и др. – СПб.: Полигон, 2000. – 896с.*

УДК 004.4

А.О. Мельник д.т.н.
Національний університет «Львівська політехніка», Україна

ВИСОКОРІВНЕВЕ ПРОЕКТУВАННЯ СПЕЦІАЛІЗОВАНИХ ПРОЦЕСОРІВ

Традиційно проектування комп'ютерних пристроїв виконується з використанням мов опису апаратних засобів VHDL та Verilog на архітектурному рівні подання цих пристроїв. Цей процес є досить складним та вимагає багато часу. Особливо проблематичним є проектування на основі цього підходу спеціалізованих процесорів, призначених для виконання складних алгоритмів з підвищеними вимогами до їх технічних характеристик, в першу чергу продуктивності та затрат обладнання. Постає завдання створення засобів автоматичного синтезу архітектурного опису спеціалізованих процесорів та розроблення технології їх проектування на основі цих засобів.

У роботі розглядається новий підхід до проектування спеціалізованих процесорів, який базується на системі автоматичного синтезу їх архітектурного опису та, на відміну від традиційного проектування на рівні міжрегістрових передач, передбачає опис виконуваного проектованим процесором алгоритму мовою високого рівня, окремий опис інтерфейсу процесора та його технічних характеристик, і генерування на основі цієї інформації за допомогою системи автоматичного синтезу спектру можливих варіантів процесора, їх синтез та дослідження і вибір найефективнішого за заданими критеріями.

Схема традиційного процесу проектування спеціалізованих процесорів на рівні міжрегістрових передач [1] містить такі етапи як розроблення, компілювання, відлагодження, завантаження, апаратне тестування (рис.1).

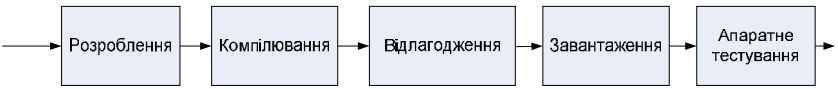

Рис. 1. Схема традиційного процесу проектування спеціалізованих процесорів

На етапі розроблення мовою опису апаратних засобів чи за допомогою графічного редактора функціональних схем створюють модель майбутнього пристрою. На етапі компілювання введені описи за допомогою засобів автоматизованого проектування перетворюють у конфігураційну біт-послідовність обраної моделі кристалу, на якому імплементують процесор. Симулювання буває двох типів: функціональне і часове. Функціональне симулювання дозволяє перевірити створений проект за допомогою стимуляції вхідних сигналів та аналізу часових діаграм вихідних сигналів. Часове симулювання перевіряє проект на відповідність заданим часовим вимогам. На етапі відлагодження завантажується створена на етапі компілювання конфігураційна біт-послідовність у конфігураційну пам'ять кристалу. Після цього етапу кристал вважається запрограмованим і готовим до тестування. Апаратне тестування – це перевірка роботи процесора на кристалі. На цьому етапі виявляють дефекти та недоліки, які будуть усунуті при поверненні до першого етапу схеми процесу проектування.

Створення програмних засобів для виконання автоматичного синтезу програмних моделей спеціалізованих процесорів із алгоритму, поданого мовою високого рівня, кардинально змінює підхід до проектування. Ці засоби дозволяють генерувати спеціалізовані процесори після подання до них алгоритму та технічних вимог до синтезованого процесора [2,3]. Подавши на вхід системи автоматичного синтезу вказані дані розробник отримує на її виході VHDL-описи процесора, які можуть бути імплементовані у кристалах різних моделей за допомогою САПР, наданих їх виробниками (Altera Quartus, Xilinx ISE і т. д.).

Найбільшими перевагами представленого підходу є максимальне скорочення та суттєве спрощення процесу проектування. В той час, як класична розробка спеціалізованих процесорів вимагає складної роботи з побудови цифрової схеми шляхом розроблення функціональних схем та написання коду мовами опису апаратних засобів, створення «тестових стендів» та тривалого і ретельного аналізу часових діаграм, система

автоматизованого синтезу генерує архітектурний опис процесора з мови С після вказівки його продуктивності та опису його інтерфейсу в конфігураційному файлі перед початком його синтезу, що дозволяє з максимальною гнучкістю підібрати потрібні параметри. При цьому алгоритм може бути написаний за допомогою будь-якого компілятора, на будь-якій операційній системі, з використанням будь-яких засобів відлагодження, які дозволяють детально та найбільш зручно відпрацювати алгоритм і відстежити коректність його роботи на всіх ключових етапах. Схема проектування спеціалізованих процесорів з використанням запропонованого підходу показана на рис.2.

Рис. 2. Схема процесу проектування спеціалізованих процесорів на основі системи автоматичного синтезу їх архітектурного опису

На універсальному комп’ютері мовою С описують алгоритм, який в результаті буде відображено в VHDL-файли апаратних засобів процесора. Разом з конфігураційним файлом, в якому налаштовують швидкодію генерованого процесора (обирають кількість паралельно працюючих АЛП), розроблений С код завантажують до системи автоматичного синтезу, яка, в свою чергу, генерує відповідно до вхідних даних файли VHDL-описів процесора. На основі цих описів створюють під конкретну модель кристалу в САПР, наданій виробником цього кристалу. На наступному етапі оцінюють характеристики процесора та, за потреби, проводять повторний синтез. Після цього проект проходить всі етапи підготовки до завантаження у кристал (компіляція, синтез, імплементація і т. д). В результаті отримують конфігураційну біт-послідовність, яку за допомогою САПР виробника завантажують до кристалу.

Тобто, використання система автоматизованого синтезу дозволяє у максимально-зручному режимі проектувати спеціалізовані процесори та вибрати серед синтезованих кращий за технічними характеристиками. При цьому розробка процесора є схожою до розробки програмних засобів, коли інженер максимально абстрагований від потреби працювати на рівні міжрегістрових передач та вирішувати питання синхронізації, конвеєризації, міжрегістрової взаємодії, тощо. Це дозволяє суттєво скоротити час проектування спеціалізованих процесорів залучати до розробки менш кваліфіковані кадри, що позитивно відобразиться на вартості проектування.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Мельник А. О., Мельник В. А. Персональні суперкомп'ютери: архітектура, проектування, застосування: монографія. – Львів: Видавництво Львівської політехніки, 2013. – 516 с.

2. Chameleon – the System-Level Design Solution. [Online]. Available: http://intron-innovations.com/?p=sld_chame.

3. Anatoliy Melnyk, Viktor Melnyk, Lyubomyr Tsyhylyk. Chameleon© C2HDL Design Tool In Self-Configurable Ultrascale Computer Systems Based On Partially Reconfigurable FPGAs // Proceedings of the Second International Workshop on Sustainable Ultrascale Computing Systems (NESUS 2015). Krakow, September 10-11, 2015. –P.135-142. https://e-archivo.uc3m.es/handle/10016/22006.

УДК 629.735.072.8.08.004(045)

В.І. Моржов, д.т.н.,
Л.І. Моржова,
Ю.О. Єрмачков,
Т.В. Німченко, к.т.н.
Національний авіаційний університет, Київ

ЗАХИСТ РОБОЧОГО МІСЦЯ ІНСТРУКТОРА АВІАЦІЙНОГО ТРЕНАЖЕРА ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Широке впровадження мультимедійних технологій та цифрової обчислювальної техніки в робоче місце інструктора (РМІ) - пілота сучасних авіаційних тренажерів (АТ) різного типу створило певні труднощі щодо захисту від несанкціонованого копіювання аеродинамічних характеристик повітряного судна та програмного забезпечення з масивами службової інформації, що розміщуються в комп'ютері РМІ.

До числа основних факторів, що обумовлюють необхідність розробки ефективних методів щодо захисту апаратно-програмних засобів АТ, відносяться: забезпечення недоступності інформації про характеристики повітряного судна (ПС) та його систем, яка є власністю організацій-розробників і не може передаватися нікому без їх відома; захист авторських прав розробників авіаційної техніки, яка моделюється в імітаторах АТ і розробників апаратних і програмних засобів тренажерної техніки.

Вся інформація про структуру побудови бортових систем та їх технічні характеристики, а також аеродинамічні і висотно-швидкісні характеристики ПС (цивільного або спеціального призначення) зберігається на технічних пристроях довгострокового зберігання інформації (жорсткі магнітні диски) комп'ютера тренажера. Суттєвим недоліком цих пристроїв є незахищеність від несанкціонованого копіювання інформації, яка зберігається на них. Це дозволяє досить просто здійснювати копіювання масивів інформації, що знаходяться на цих жорстких дисках.

Все це змушує розробляти спеціальні проектні рішення РМІ, які б забезпечували неможливість несанкціонованого доступу і копіювання масивів інформації та програмного забезпечення РМІ.

У зв'язку з цим, рішення цього завдання слід шукати при проектуванні РМІ, зокрема при розробці складу та структури

програмно-апаратних засобів РМІ. РМІ різного типу мають свої як апаратні, так і програмні особливості, які повинні враховуватися при розробці засобів захисту від несанкціонованого копіювання інформації.

Основною конструктивною особливістю є модульний принцип побудови програмного забезпечення РМІ, кожен модуль якого реалізує мультимедійну модель відповідної авіаційної системи

У зв'язку з цим, для такої модульної структури ПЗ доцільно здійснювати захист індивідуально по кожному мультимедійному модулю, тобто доступ до конкретної мультимедійної моделі РМІ буде здійснюватися тільки після підтвердження авторизації.

Цікавим є використання пристрою USB в якості міні HASP апаратного ключа (Hardware Against Software Piracy).

Доцільність такого використання пояснюється наступними факторами:

- незначна ціна таких апаратних ключів;
- тривалий термін використання ПЗ АТ;
- індивідуальний алгоритм захисту від несанкціонованого копіювання інформації.

У загальному випадку порядок організації захисту ПЗ від несанкціонованого копіювання необхідно здійснювати в наступній послідовності: 1) вибрати тип USB-пристрою, який буде використано в якості HASP апаратного ключа; 2) визначити серійні номери PID і VID USB-пристрою; 3) визначити точки входу в ПЗ тренажера через файл USB-ключа; 4) написати програму шифрування з використанням криптографічного алгоритму; 5) забезпечити автономність роботи РМІ (комп’ютер РМІ не повинен бути підключений до будь-якої комп'ютерної мережі).

Таким чином, особливості побудови ПЗ спеціалізованих АТ і їх апаратних засобів показують, що ефективний захист інформації може бути реалізовано на основі USB-пристроїв. Файл-ключ, записаний на зазначеному пристрої, відкриває доступ до певної програми цифрової моделі імітатора АТ.

Всі ці вимоги повинні бути викладені в тактико-технічному завданні на спеціалізований тренажер конкретного типу ПС.

УДК 658.336:656.7

В.І. Моржов, д.т.н.,
Л.І. Моржова,
Ю.О. Єрмачков
Національний авіаційний університет, Київ

СТРУКТУРА ТРЕНАЖЕРА ОПЕРАТОРА БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ (БПЛА)

У доповіді розглядаються питання побудови тренажера оператора (ТО) БПЛА на основі сучасних засобів обчислювальної техніки і програмного забезпечення, а також математичних моделей руху БПЛА у просторі.

Структура ТО БПЛА складається з апаратних засобів і програмного забезпечення (ПЗ), яке реалізує математичні моделі БПЛА і відображення на екранах дисплеїв інформації про його переміщення у просторі.

Апаратні засоби БПЛА уніфіковані та комплектуються зі стандартного обладнання персональної обчислювальної машини (ПОМ). Технічні характеристики цього обладнання визначаються на стадії ескізного проектування. Обладнання ТО є серійного виробництва та не потребує спеціальних доробок.

Важливою складовою частиною ТО БПЛА є ПЗ, яке розподіляється на системне і прикладне.

Розробка прикладного (спеціального) ПЗ становить основний об’єм робіт по створенню ТО БПЛА. ПЗ розроблюється за модульним принципом, що дозволяє:

- нарощувати кількість модулів систем конкретного БПЛА;
- модернізувати цифрові моделі в процесі експлуатації;
- використовувати готові цифрові моделі, що розроблені іншими організаціями;
- розширювати методичні можливості ТО БПЛА.

Спеціальне ПО включає математичні моделі імітатора руху БПЛА у просторі, математичні моделі приладів і органів управління, відеомоделі імітатора візуальної обстановки місцевості у межах якої знаходиться БПЛА в даний момент часу.

До системного ПЗ входять:

- базова операційна система ПОМ;
- програма управління обчислювальним процесом у реальному масштабі часу;
- програми введення/виведення інформації;
- програми діагностики апаратних засобів ТІП;
- програми мережевого обміну.

Передбачається, що БПЛА має двигуни, систему управління, камеру відеоспостереження і радіоканал, через який інформація у кожен момент часу передається оператору.

У модулі навчального класу передбачено два способи введення керуючих команд в бортову систему БПЛА, панель якого з органами управління і приладами, відображені на кольоровому екрані дисплея:

- за допомогою маніпулятора “Миша”;
- за допомогою сенсорного прозорого екрану, який розташований попереду кольорового дисплея, на якому відображена панель з відеомоделями органів управління і приладів. Торкаючись рукою конкретного органу управління системою, фахівець вводить керуючу команду в цифровий імітатор системи, яку вивчаємо, після чого починають змінюватися свідчення приладів, за якими спостерігає фахівець.

Реалізація тренажера оператора БПЛА з такою структурою забезпечить якісну підготовку операторів для дистанційного управління літальними апаратами (ЛА) на різних режимах руху (набір висоти, переміщення за заданими координатами місцевості, зниження, посадка на майданчику старту).

УДК 004.82.519.81;519.86

В.І. Надточій[1], к.т.н.,
Ю.П. Чаплінський[2], к.т.н.
[1]Національний авіаційний університет, Київ
[2]Інститут кібернетики ім. В.М.Глушкова НАН України, Київ

КОНТЕКСТНО-ОНТОЛОГІЧНИЙ ПІДХІД ДО ПРЕДСТАВЛЕННЯ ТА УПРАВЛІННЯ МЕРЕЖЕВИМИ МУЛЬТИМЕДІЙНИМИ РЕСУРСАМИ

Останнє десятиліття відзначається безпрецедентним розвитком технологій створення мультимедійного контенту та технологій доставки мультимедійних ресурсів, що дозволяє передачу, розповсюдження та надання мультимедійного контенту, як у професійному так і особистому середовищі. При цьому обсяг накопичуваних якісних мультимедійних даних настільки великий, що все більш актуальним стає розв'язання проблем їх зберігання, обробки, пошуку та архівації, а також забезпечення процесу обміну подібними даними через сучасні засоби комунікації в будь-який час і в будь-якому місці. Це визначає потребу в інформаційних засобах роботи з мультимедійними цифровими ресурсами: авторам, видавцям і споживачам потрібні ефективні засоби представлення, керування та навігації. Такий інструментарій надають системи управління цифровими ресурсами (Digital Asset Management, DAM), область застосування яких є від створення та поширення мультимедіа до ведення цифрових архівів. Сьогодні типова система DAM зазвичай базується на реляційних СУБД, що утруднює публікацію і обмін даними, оскільки фіксована інформаційна модель даних вимагає визначення явних зв'язків. Наприклад, сьогодні існує багато різних стандартів та форматів мультимедійних метаданих, таких як Exif, Dublin Core, VRA Core, DIG-35 та MPEG-7, які не є сумісними взаємно. Для семантичного представлення мультимедійного вмісту можуть використовуватися семантичні веб-технології, такі як XML, RDF та онтології.

Для людей, які створюють мультимедійний контент, та споживачів мультимедійних ресурсів сучасні онтологічні засоби забезпечують кращий доступ до мультимедійної інформації, яка визначена в онтології. Онтології дозволяють реалізувати знання орієнтовану підтримку мультимедійних ресурсів. Для цього всі знання, що описують прийняття рішень, розглядаються в розрізі

знань, що описують контекст, та знань, що описують контент.

Основою для представлення такої онтології є поняття та терміни як загальні, так і специфічні, і зв’язки між ними. Визначення термінів і понять, а також взаємозв'язок між ними повинні забезпечити кращу обробку програмними додатками. Для організації представлення мультимедійних ресурсів пропонується використовувати онтологію, що містить основні класи та поняття і терміни, що стосуються об’єктів мультимедійних ресурсів та засобів їх аналізу та обробки. Така онтологія може базуватися на W3C Ontology for Media Resource [1]. Вона використовує 18 форматів мультимедійних метаданих (Dublin Core, MPEG7, IPTC, Exif, OGG та ін.) та шість форматів мультимедійних контейнерів (3GP, FLV, QuickTime, MP4, OGG, WebM). Властивості такої онтології включають такі терміни, як ідентифікатор, заголовок, творець, дата, місцезнаходження, опис, ключове слово, рейтинг, авторські права, цільова аудиторія, формат тощо.

Під контекстом будемо розуміти будь-яку інформацію, яка може бути використана або характеризує відповідну складову процесу створення та використання мультимедійних ресурсів. На загальному рівні контекст описується наступними контекстними областями: мета/результат, актор, процес/дія, об'єкт, середовище, можливості, засоби, представлення, розташування та час.

Такі онтології розробляються для того, щоб служити для виконання кількох із наступних завдань: анотація - позначення або позначення мультимедійного вмісту; аналіз - семантичний аналіз мультимедійного вмісту, що управляється онтологією; отримання - отримання мультимедійного контенту на основі контексту; персоналізація - рекомендація та фільтрація мультимедійного вмісту на основі уподобань користувача; керування алгоритмами та процесами - моделювання мультимедійних процедур та процесів; міркування - персоналізація та пошук для створення автономних програм вмісту.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Lee W., Bailer W., Burger T. Ontology for Media Resources 1.0 // Recommendation // w3C [Електронний ресурс] - *February 2012.* – Режим доступу: *http://www.w3.org/TR /mediaont-10/*

УДК 629.735.33.07:51-37

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

ПРО ЗАСТОСУВАННЯ КОМП'ЮТЕРНОЇ АНІМАЦІЇ В ЗАДАЧАХ ДИНАМІКИ ПОЛЬОТУ

У прийнятому на 38-ій сесії Асамблеї Міжнародної організації цивільної авіації Глобальному плані забезпечення безпеки польотів підкреслюється: «Постійне підвищення рівня безпеки польотів у глобальному масштабі має засадниче значення для забезпечення того, щоб повітряний транспорт і надалі відігравав важливу роль одного з рушіїв сталого економічного та соціального розвитку у всьому світі...Забезпечення безпеки польотів має бути найпершим та першочерговим завданням» [1].

Рівень безпеки польотів визначається багатьма чинниками, вплив яких досліджується в реальних умовах експлуатації або шляхом комп'ютерного моделювання динаміки польоту повітряних суден (ПС), особливо на етапах злету, заходу на посадку та посадки, на які припадає значна кількість аварій та катастроф [2].

Це пов'язано з великою кількістю завдань, що одночасно вирішуються екіпажем на цих етапах, близькими до критичних значеннями параметрів польоту та їх значною зміною, а також дефіцитом часу на прийняття екіпажем управлінських рішень та їх виконання, особливо в складних метеоумовах при значному психологічному тиску на екіпаж чинника близькості землі.

З погляду на наведені обставини, комп'ютерне моделювання динаміки польоту ПС дозволяє здійснювати дослідження в лабораторних умовах практично на будь-яких етапах та режимах польоту без загрози для його безпеки, причому, з високою точністю як в реальному, прискореному або уповільненому часі.

Валідність отриманих результатів поставленим завданням дослідження визначається застосуванням обґрунтованих методів математичного моделювання, а також забезпеченням подібності динамічних та статичних характеристик розробленої математичної моделі та реального об'єкту.

Методами комп'ютерної анімації забезпечується високий ступінь наочності та візуальної ілюзії руху повітряного судна в

просторі під час проведення досліджень та аналізу їх результатів, що особливо важливо не тільки в навчальному процесі, але й при розслідуванні важких авіаційних інцидентів.

Комп'ютерна анімація за способом формування графічних зображень використовує растрову, векторну та фрактальну графіку, а за способом просторового представлення зображень – 2D та 3D графіку, кожна з яких має свої особливості, переваги та недоліки і використовується в залежності від поставленого завдання [3].

Зокрема, якщо при дослідженні заходу літака та посадку передбачається розглядати його рух у бічній площині (вид зверху) з анімацією бічного відхилення від площини посадкового курсу, відстані до злітно-посадкової смуги (ЗПС) і курсу, або рух у повздовжній площині (вид збоку) з імітацією висоти, відстані до ЗПС і тангажу, то доцільно використовувати 2D метод анімації, який потребує менших комп'ютерних ресурсів, ніж 3D метод.

Якщо ж передбачається анімація зміни всіх параметрів руху літака в просторі та (або) роботи його механізації крила та відхилення органів управління, причому, з видом на літак з різних ракурсів, то доцільно використовувати 3D метод анімації.

У даній роботі досліджується захід на посадку літака в режимі автоматичного управління в умовах як спокійної, так і турбулентної атмосфери різної інтенсивності з 2D та 3D анімацією руху літака. Дослідження здійснюються з використанням розробленої програмної математичної моделі, яка дозволяє дослідити процеси виходу літака в площину посадкового курсу та стабілізації його на ній, стабілізації літака на заданій висоті кола, «захвату» глісади та стабілізації його на ній до висоти 15-20 м.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Глобальный план обеспечения безопасности полетов. ИКАО: 2013. 76 с. URL: https://www.icao.int/Meetings/a38/Documents/GASP_ru.pdf (дата звернення: 07.03.2021).

2. Statistics. Causesof Fatal Accidents. Fatalities by Phaseof Flight. URL: http://www.planecrashinfo.com/cause.htm (Last accessed: 11.03.2021).

3. Полухін А.В. Про 2D та 3D методи комп'ютерної анімації при моделюванні динаміки польоту літака. Зб.: Сучасні тенденції розвитку системного програмування: тези доповідей науково-практичної конференції, 26-27 листопада 2019 р. – К.: НАУ. – 44 с.

УДК 004.337

С. Ю. Пунда
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ

ДОСЛІДЖЕННЯ ВПЛИВУ КОМПРЕСІЇ ДАНИХ НА ПРОДУКТИВНІСТЬ СИСТЕМИ ЗБЕРЕЖЕННЯ ДАНИХ

Поява алгоритмів компресії зумовлена постійним ростом кількості даних у світі. Щодня генеруються петабайти структурованих даних і одна із першочергових задач бізнес користувача полягає у здатності до їх зберігання

В якості апаратного рішення, яке здатне керувати такою кількістю даних використовуються системи зберігання (далі СЗД). На відміну від сервера, першочерговою задачею якого є обчислення і обробка даних, СЗД використовуються для їх зберігання, вони здатні вміщувати сотні дисків, які можна віртуалізувати за допомогою вбудованого програмного забезпечення.

Однією із важливих характеристик СЗД є можливість компресії даних, оскільки вона дозволяє помістити більшу кількість інформації на накопичувач. Тим самим бізнес користувач може заощадити свої кошти.

Існує декілька видів компресії:

- апаратна компресія;
- програмна компресія.

Як правило використання програмної компресії приводить до значного зниження продуктивності системи, це пов’язано з тим, що СЗД виділяє частину своїх обчислювальних ресурсів на роботу з алгоритмами скорочення даних.

Існують системи зберігання в яких компресія реалізована, як додатковий апаратний прискорювач. В такому випадку зниження продуктивності СЗД буде не значним, але варто відзначити, що такий функціонал, як правило необхідно оплачувати додатково.

У цій роботі було проведено дослідження впливу компресії даних на продуктивність системи збереження даних. На рис.1 наведені графіки залежності продуктивності вводу виводу (далі IOPS) від часу обслуговування однієї команди для SSD накопичувачів з використанням апаратної та програмної компресії

даних. Дана інформація була отримана внаслідок моделювання роботи СЗД IBM Strowize v5030 та Storwize 5100

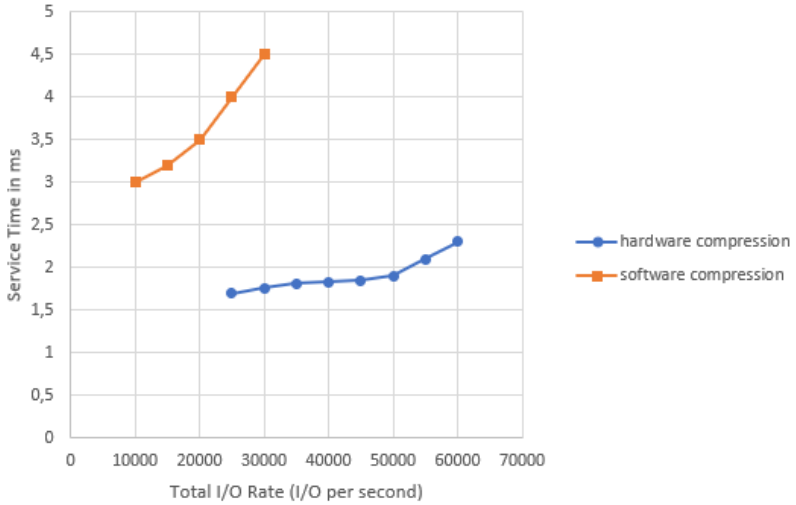

Рис.1. Графік залежності кількості IOPS від часу обслуговування для SSD накопичувачів з використанням апаратної та програмної компресії даних

Порівнюючи графіки між собою, можна підсумувати, що використовувати програмну компресію варто лише для задач, які не потребують великої продуктивності IOPS, адже час обслуговування одного запиту на 10000 операцій вводу виводу займає близько трьох мілісекунд, водночас для бази даних Oracle розробники рекомендують, щоб час обслуговування був менше однієї мілісекунди. Апаратна компресія є доцільним рішенням навіть при роботі з базами даних. Однак необхідно розраховувати на системи вищого рівня, наприклад IBM FlashSystem 7200. Дана система має два 8 ядерних процесори на контролер, це означає, що пікове завантаження процесора при включеній компресії відбудетеся приблизно на позначці в 200 тисяч IOPS.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *IOPS [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/IOPS.*

УДК 004.451.44

O.V.Rusanova, assistant professor
A.V.Korochkin, assistant professor
O.P.Shevelo, assistant

NTUU "Igor Sicorsky Kyiv Politechnical Institute", Kyiv

SCHEDULING PROBLEMS FOR MOBILE CLOUD COMPUTING

Nowadays the popularity of mobile devices is rapidly increased. New facilities of them (Wi-Fi, GPS, high speed processors etc.) allows to improve mobile applications in commerce, learning, gaming, health monitoring, sports etc. But really there are several reasons that limit mobile computing: limited storage capacity, limited battery life and limited processing power of mobile devices.

This paper is dedicated to Mobile cloud computing (MCC). We consider MCC as combination of mobile and cloud computing where both data storage and data processing are performed outside the mobile device but inside the cloud [1].

We analyze the following main components and their features of MCC, such as:

Mobile network

Internet service

Cloud service

Scheduling is one of the important factors in progress MCC. Scheduling methods can be divided into three categories: workflow, task and resource scheduling. In this paper we discuss all these categories and focus on task scheduling. Then we consider taxonomy of task scheduling for mobile cloud computing. We classify all methods by following characteristics:

Dynamic, static or hybrid dynamic + static;

Independent of dependent tasks;

Homogeneous or heterogeneous mobile nodes;

Heuristics types: cluster, genetic, list and duplication

We consider advantages of dynamic+static methods for heterogeneous mobile cloud computing with list scheduling heuristics. We discuss the main optimization criterions for MCC scheduling methods, such as minimization of execution time; maximization of

resources effectiveness; minimization of energy with given limits to completion time. In this paper we will focus on scheduling with last optimization criterion. Firstly, we analyze a directed acyclic graph (DAG) that uses as task graph for mobile applications. DAG includes set of task nodes and edges set that defines dependencies between tasks. Each of nodes has set of weights that correspond to execution times and set of energy consumption for different mobile resources. Each of edges also has set of weights that correspond to communication cost for mobile resources. Then we analyze one of the most effective scheduling approach for MCC [2], that combines dynamic and static technique.

We propose the development of this approach based on the static algorithm improvement. The progress of static approach for MCC is in following:

using of list scheduling;

prioritization for DAG nodes is based on b-level with average values of computational and communication costs, such as in paper [3];

allocation procedure use performance of cores, data transfer time and energy consumption.

All results of this paper can be used for MCC scheduling methods improvement.

REFERENCES

C Arun, K.Prabu.Overview on Mobile Cloud Computing // International Journal of Advanced Research in Computer Science and Software Engineering – 2017. Vol.7.- P.396-398.

Yibin L. Energy Optimization With Dynamic Task Scheduling Mobile Cloud Computing / L.Yibin, D.Wenyun, Q.Meikang.//IEEE Systems Journal.-2017.- №11.- P.96-105.

Русанова О. В., Ярох Ю.А. Планирование вычислений в гетерогенных кластерных системах. // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: Зб. наук. пр. – К.: Век+, -2011. –No 54. –С. 155-163.

УДК 004.75

І.В. Телешко, к.т.н.,
Національний авіаційний університет, Київ

МЕТОД БАЛАНСУВАННЯ НАВАНТАЖЕННЯ У ВІРТУАЛЬНИХ МЕРЕЖАХ

Проблема балансування навантаження з метою підвищення ефективності використання віртуальних ресурсів актуалізувалася у зв'язку з масовим використанням хмарних обчислювальних систем на віртуальних платформах. Одним із аспектів проблеми є ефективне планування та розподіл завдань між віртуальними системами з метою оптимізації використання ресурсів та скорочення часу обчислень. Тобто часто виникає ситуація, при якій частина обчислювальних ресурсів простоює, в той час, як друга частина ресурсів перевантажена і, ймовірно, наявна велика кількість завдань на очікуванні свого виконання.

Необхідність балансування навантаження розподіленої системи виникає з наступних причин:

- неоднорідність структури обчислювального комплексу (наприклад, кластера), тобто різні вузли мають різну продуктивність;
- неоднорідність структури міжвузлової взаємодії, тобто лінії зв'язку які з'єднують вузли, можуть мати різні характеристики пропускної здатності.

Рішення задачі виявилося настільки актуальним що було запропоновано багато алгоритмів балансування навантаження. Всі ці алгоритми працюють або на підставі поточного стану системи, або на підставі статусу ініціатора алгоритму. Алгоритми які працюють на підставі статусу поділяються на статичні та динамічні, а ті, які працюють на підставі статусу можуть бути ініційовані відправником, отримувачем або бути комбінованої ініціації.

При цьому слід зазначити що властивості віртуальних середовищ суттєво залежать від того яке наповнення мають віртуальні машини які це середовище утворюють. Відповідно до цього можна стверджувати те, що ефективність будь-якого алгоритму балансування навантаження може суттєво залежати від конкретного середовища, де цей алгоритм застосовується. В даному випадку розглядається середовище SDN-NFV мереж.

Результати чисельних досліджень, проведені за останнє десятиліття свідчать про те, що трафік у комп'ютерних мережах має самоподібні властивості. Такий трафік відзначається значними затримками та втратою пакетів навіть у випадку, коли навантаження далеке від максимального. В звя'зку з цім почали активно розроблятися методи та алгоритми управління трафіком з урахуванням його самоподібних та мультифракторальних характеристик [1].

Система балансування навантаження будується на основі підсистеми регулювання та підсистеми керування і моніторингу. Підсистема регулювання реалізує алгоритм балансування, на підставі інформації щодо поточного стану системи, міри її завантаженості та стану динамічного розподілу трафіку. В підсистемі керування та моніторингу здійснюється збір та аналіз статистики щодо стану системи, визначення самоподібних та мультифракторальних властивостей вхідного трафіку, розрахунок розподілу потоків по вузлам мережі з урахуванням класифікації трафіку, завантаженості серверів та каналів.

Основним критерієм завантаженості розподіленої системи вважається сумарне значення дисбалансу компонентів системи. Запропонований метод балансування навантаження передбачає використання як внутрішнього так і зовнішнього моніторингу. Метод базується на застосуванні стратегії найкоротшої черги (*англ. Shortest Queue strategy*). При використанні цієї стратегії диспетчер балансування надсилає завдання на сервер із найменшою кількістю завдань у черзі. Якщо є кілька серверів із найменшою довжиною черги диспетчер випадково вибирає сервер із цього списку. Використання такої стратегії дозволяє вирівняти поточну кількість завдань на кожному сервері.

В роботі виконано дослідження запропонованого методу і загалом доведена його коректність у порівнянні з існуючими рішеннями.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Л.О.Кириченко, И.Н,Иванисенко, Т.А. Радивилова. Анализ дисбаланса распределенной системы при самоподобной нагрузке.//Інформаційні технології. Вісник ХНТУ – 2016 – Вип.3(58) – С.224-231.

УДК 004.7:004.738.5(043.2)

О.В. Толстікова[1], к.т.н.,
О.В. Пономаренко[2], к.т.н.,
С.В. Водоп'янов[1], к.т.н.
[1]Національний авіаційний університет, Київ
[2]Фаховий коледж інженерії та управління, Київ

ПИТАННЯ ЗАБЕЗПЕЧЕННЯ НАСКРІЗНОЇ QoS З ЕКОНОМІЄЮ АПАРАТНИХ ТА ПРОГРАМНИХ РЕСУРСІВ

Для підтримки різних видів трафіку широко використовуються безпроводові мережі нових поколінь. У цих мережах обмін даними між абонентами може бути покращений завдяки високій якості зображень та відео, а доступ до інформації та послуг – за рахунок підвищення швидкості передачі даних, якості сервісу (QoS) та зменшення рівня бітових помилок, заходів безпеки, урахування локації абонента, енергоефективності та новим гнучкими комунікаційним можливостям.

При цьому необхідно пред'являти надзвичайно високі вимоги стосовно швидкості розв'язання завдань оптимального розподілу ресурсів з прийнятною якістю. Задовольнити цим вимогам за умов незалежної адаптації на окремих рівнях моделі *OSI*, звичайно, можна, але тут неминуче виникає відома проблема: вартість такої системи є неприйнятною. Тому треба застосовувати альтернативні підходи.

Основним принципом міжрівневої оптимізації є комплексне рішення задачі ефективного використання обмеженого числа радіоресурсів, що враховує ряд першорядних чинників: підвищення пропускної спроможності; забезпечення рівнодоступності - справедливого (*fair*) поділу ресурсів між користувачами; досягнення необхідної або, принаймні, найкращої можливої якості обслуговування. Переваги міжрівневого підходу безпосередньо пов'язані з принципами функціонування безпроводової мережі.

Надання гарантій якості є важливою метою розробки безпроводових мереж. Різні методи можуть мати дуже різноманітні вимоги до якості щодо термінів передачі даних, міжкінцевої затримки та ймовірностей порушення, пов'язаних із затримкою. Для підтримки гарантій QoS запропоновано два загальні підходи.

Перший підхід – мереже-орієнтований. За таким підходом маршрутизатори, комутатори та центри збору даних у мережі повинні забезпечувати підтримку QoS для задоволення вимог щодо швидкості передачі даних, обмеженої затримки та втрати пакетів, що вимагаються програмними застосунками.

Другий підхід базується виключно на *End-to-End* системі і не пред'являє жодних вимог до мережі. Зокрема, в *End-to-End* системах використовуються методи управління для досягнення максимальної якості на рівні застосунків без підтримки QoS на транспортному рівні. Розглядається проблема забезпечення QoS з мережної точки зору.

Найбільш перспективним підходом до розв’язання проблеми пошуку оптимального маршруту в мережі з багатьма вузлами є використання методів теоретичного аналізу та оптимізації наскрізної якості сервісу. Задачі пошуку оптимального маршруту в мережі з N вузлами є задачами цілочисельного програмування, тісно пов’язаними з проблемами комбінаторної та дискретної математики. Вони відносяться до класичної задачі про потоки в мережах як різновид квадратичних задач розміщення. Квадратична задача про розміщення (Quadratic Assignment Problem, QAP) - це відома задача дискретної оптимізації, яка є однією з найбільш важких завдань в цій області.

Використання наближених методів і алгоритмів є на даний момент фактично єдиним способом вирішення проблеми.

Для розв'язання задачі комбінаторної оптимізації, зокрема, квадратичних задач розміщення (або квадратичних задач призначення) приходиться застосовувати наближені методи, зокрема, евристичні та метаевристичні методи. Одним з них е метод табу-пошуку. Метод досить легко алгоритмізується та програмується.

Алгоритми табу-пошуку при своїй відносній простоті є досить ефективними для вирішення завдань маршрутизації. Модифікації алгоритму з урахуванням специфіки предметної області дозволяють підвищити ефективність пошуку точок розміщення мережних вузлів шляхом згладжування цільової функції та "обходу" локальних екстремумів.

УДК 004.056.55

Д.Н.М. Томнюк
Національний авіаційний університет, Київ

ПРОГРАМНИЙ МОДУЛЬ ШИФРУВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ

Актуальність теми. Постійно зростаючі вимоги створення нових криптостійких до різних типів атак потокових шифрів. Врахування ними особливостей сучасної елементної бази, створення нових видів атак обумовлює потребу в розробці та дослідженні нових підходів до побудови блокових шифрів.

ІНФОРМАЦІЙНИЙ РЕСУРС, КРИПТОГРАФІЧНИЙ ЗАХИСТ ДАНИХ, БЛОКОВИЙ СИМЕТРИЧНИЙ ШИФР, ІНФРАСТРУКТУРА РОЗПОДІЛУ КЛЮЧІВ, КІБЕРПРОСТІР.

Об’єкт дослідження – кіберпростір, блоковий алгоритм шифрування.

Предмет дослідження - метод блокового алгоритму шифрування.

Мета роботи – розробка системи захисту інформації на базі блокового алгоритму.

Блокові алгоритми шифрування - це основа, на якій реалізовано майже всі криптосистеми. Техніка створення ланцюгів із зашифрованих блоковими алгоритмами байт дозволяє їм шифрувати пакети інформації необмеженої довжини. Така властивість блокових шифрів, як швидкість роботи, використовуються асиметричними криптографічними алгоритмами, які повільні за своєю природою. Відсутня статистична кореляція між бітами вихідного потоку блокового шифрування використовується для обчислення контрольних сум пакетів даних та в хешуванні паролів.

Криптоалгоритм називається ідеально стійким, якщо існує можливість читати зашифрований блок даних лише переглянувши всі можливі клавіші, поки повідомлення не буде значущим. Оскільки теоретично потрібний ключ буде знайдений з імовірністю 1/2 після перебору половини всіх ключів, то для злому ідеально стійкого криптоалгоритму з ключем довжиною N потрібно в середньому

$2^{(N-1)}$ перевірки. Таким чином, у загальному випадку стійкість блокового шифру залежить лише від довжини ключа і зростає експоненціально у міру зростання. Навіть якщо припустити, що пошук ключів здійснюється за спеціально розробленою багатопроцесорною системою, в якій, завдяки діагональному паралелізму, на перевірку 1 клавіші йде лише 1 година, то для того, щоб зламати 128-бітний ключ, потрібно, як мінімум 10^{21} рік. Звичайно, все вищесказане стосується лише ідеально стійких шифрів.

Блокові алгоритми шифрування на сьогодні являються основним засобом криптографічного захисту інформації.

Основними перевагами блокових алгоритмів шифрування є:

- висока швидкість шифрування/розшифрування;
- висока гарантована стійкість, яка до того ж може бути доведена математично;
- можливість ефективної програмної реалізації.

Встановлено, що застосування блокових алгоритмів при застосуванні з іншими методами захисту інформації значно підвищує рівень кібербезпеки.

Результати, отримані в ході дослідження дипломної роботи, рекомендовано використовувати для захисту інформаційних ресурсів у кібернетичному просторі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Криптографические методы защиты информации : учебник / А.В. Бабаш, Е.К. Баранова. — Москва : КНОРУС, 2018. — 190 с. — (Бакалавриат и магистратура)

2. ГОСТ 34.310-95 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

3. ГОСТ 34.311-95 Информационная технология. Криптографическая защита информации. Функция хеширования.

4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си — М.: Триумф, 2002. — 816 с.

5. Шнайер, Брюс. Прикладная криптография (Applied Cryptography), 2-е издание.

УДК 004.92

Д.В. Ходаков, к.т.н.,
В.В. Горіна,
Національний авіаційний університет, Київ

ФОРМАЛЬНО-ЛОГІЧНА, АБСТРАКТНА ТЕОРІЯ АЛГОРИТМІВ

Зокрема, абстрактна теорія алгоритмів встановлює відсутність алгоритмів для вирішення ряду масових проблем.

Інтуїтивне розуміння поняття алгоритму складалося в практиці, в науці і, перш за все, в математиці з найдавніших часів. Алгоритм в такому розумінні є якась чітка система інструкцій, яка будучи послідовно застосована до початкового набору будь-яких конструктивних об'єктів в результаті за кінцеве число кроків приводить до створення якогось результуючого конструктивного об'єкта. При такому інтуїтивному розумінні поняття алгоритму можна говорити про алгоритми в найрізноманітніших галузях людської діяльності.

У 1930-і роки і перші післявоєнні роки було розроблено кілька абстрактних понять алгоритму або, як кажуть, формалізацій інтуїтивного розуміння алгоритму [2]. Це машини Тюрінга і обчислювані з їх допомогою функції, рекурсивні функції як функції обчислювані за допомогою деякого алгоритму, нормальні алгоритми А.А. Маркова і обчислювані з їх допомогою функції. Абстрактна теорія алгоритмів встановлює еквівалентність цих абстрактних понять. Найважливішою проблемою тут є також проблема існування таких алгоритмів для вирішення тієї чи іншої масової проблеми.

Поняття задачі «в загальному вигляді» отримує своє уточнення за допомогою поняття «масова проблема» або «масова алгоритмічна проблема». Така проблема задається нескінченною серією окремих однотипних одиничних задач і полягає у вимозі знайти єдиний алгоритм їх вирішення. Численні довідники з різноманітних наукових дисциплін значною мірою заповнені алгоритмами вирішення різноманітних масових проблем, що виникають у відповідній галузі науки [1]. Алгоритми утворюють свого роду «золотий запас» кожної наукової дисципліни. Їх значення для науки можна охарактеризувати наступними положеннями:

1) алгоритми є формою викладу наукових результатів;

2) вони є керівництвом до дії при вирішенні вже вивчених проблем і як наслідок:

3) засобом, що дозволяє економити розумові зусилля і розумову працю;

4) вони служать необхідним етапом при автоматизації вирішення завдань;

5) алгоритми є засобом (інструментом), що використовуються при дослідженні та вирішенні нових проблем;

6) алгоритми надають мову для опису різноманітних складних процесів.

Тут слід зазначити, що, хоча алгоритми складають важливу частину кожної науки, вони звичайно ж не вичерпують повністю її змісту. Не менш важливі в науці поняття і їх визначення, що входять в дану науку, встановлені нею факти (в математиці - це доведені теореми), вироблений наукою підхід до досліджуваних об'єктів і явищ.

Природним є прагнення багатьох математиків і дослідників створювати все більш і більш потужні алгоритми, які вирішують по можливості все більш і більш великі класи завдань (завдання вельми широкого і загального типу). Виникає загальна проблема: побудувати такий алгоритм, який дозволить вирішувати будь-яку математичну задачу. Ще великий німецький математик і філософ Лейбніц мріяв про створення загального методу, що дозволяє ефективно вирішувати будь-яку задачу. Надалі сама проблема отримала певне уточнення у вигляді однієї з найважливіших проблем математичної логіки, а саме: проблеми розпізнавання виводимості результатів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Айзерман, М. А. Логика, автоматы, алгоритмы / М. А. Айзерман, Л. А. Гусев, Л. И. Розеноэр. – М. : Физмат, 1963. – 615 с.

2. Игошин В.И. Курс математической логики в системе среднего профессионального образования // Профессиональное образование в современном мире. 2017. Т. 7, №2. С. 1018–1022. DOI: 10.153/ PEMW20 170211.

Наукове видання

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
XIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2021)

15–17 квітня 2021 року

Тези доповідей надруковані в авторській редакції однією із трьох робочих мов конференції: українською, англійською, російською