МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

Національний авіаційний університет

Навчально-науковий інститут комп'ютерних інформаційних технологій

CSNT 2018

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

XI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖНІ ТЕХНОЛОГІЇ

19-21 квітня 2018 року

Київ 2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
Національний авіаційний університет
Навчально-науковий інститут
комп'ютерних інформаційних технологій

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
XI МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2018)

19–21 квітня 2018 року

Київ 2018

УДК 004.7(043.2)

Збірник тез доповідей XI Міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2018), м. Київ, 19–21 квітня 2018р., Національний авіаційний університет. – К.: НАУ, 2018. – 82 с.

Збірник тез доповідей укладено за матеріалами XI міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2018). 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 друку вченою радою Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету (протокол № 3 від 26 березня 2018 р.).

ЗМІСТ

УДК 004.75 (043.2)

С. В. Балакин, аспирант,
Национальный авиационный Университет, Киев

ОПТИМИЗАЦИЯ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ ПРИ ИДЕНТИФИКАЦИИ НЕСАНКЦИОНИРОВАННЫХ СЕТЕВЫХ ВОЗДЕЙСТВИЙ

Задача оптимизации искусственных иммунных систем требует использования современных и эффективных инструментов, которые способны значительно повысить быстродействие и минимизировать затраты системных ресурсов на решение поставленных задач. Процесс оптимизации позволит избежать ошибок при обучении иммунных сетей и позволит своевременно реагировать и предотвращать несанкционированные действия в компьютерной сети [1]. Средства оптимизации искусственных иммунных систем при идентификации атак представляют собой новые технологии с потенциалом развития [2].

Многочисленные задачи по оптимизации являются одними из ключевых сфер для применения эвристических алгоритмов, основанных на разных процессах моделирования и отражения несанкционированных действий в сетях. Современное состояние искусственных иммунных систем (ИИС) дает возможность применять их во многих сферах жизни человека.

Рассмотрены основные преимущества и недостатки ИИС, новые способы и методы их применения. Сделан обзор наработок в области искусственных иммунных систем, иммунного ответа, соматической гипермутации, теории опасности и процессов отбора.

Предложена и рассмотрена реальная модель оптимизации искусственных иммунных систем, которая дает возможность использовать ее при идентификации атак и несанкционированных действий в компьютерной сети и значительно повысить скорость их обучения.

Предложенная модель оптимизации подходит для реализации программного продукта и приложений для ускорения процесса обучения искусственных иммунных систем. Выделены основные направления развития ИИС при идентификации вторжений в компьютерных сетях.

Решение данной задачи заключается в использовании только тех возможностей ИИС, которые могут быть задействованы при работе

с атаками и вторжениями. Это позволяет конкретизировать описание основных операторов и их результаты. Такого рода оптимизация даст возможность сконцентрировать вычислительные ресурсы на решении поставленной задачи без побочных операций, которые характерны при работе ИИС. Оптимизация позволит существенно снизить потребляемые системные ресурсы и ускорить обучение ИИС при выявлении вторжений в компьютерной сети.

Создание ИИС тесно связано с развитием медицины и иммунологии, потому что ее алгоритмы применяются при построении математических моделей и создании некоторых видов иммунных систем в сферах компьютерной инженерии. Методы ИИС, которые могут решать задачи оптимизации, зачастую основаны на принципах работы иммунной системы организма человека. Клетки иммунной системы проходят многочисленные модификации, для создания антител, обеспечивающих максимальную защиту организма. ИИС так же как и искусственный интеллект способны обучаться и принимать решения.

Перспективы ИИС открыли возможность для расширения сфер применения этих систем и были созданы мультипопуляционные ИИС (MOM-aiNet) с двойной кластеризацией. Эта сеть базируется на принципах работы аминокислот, а с помощью кластеризации легко перенесена в ИИС.

Концепция искусственных иммунных компьютерных сетей открывает перспективу расширения набора решаемых функциональных задач, а также является средством для применения данных методов для реализации более совершенных систем и программных комплексов.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Романюхин А. А. Искусственные иммунные системы и их применение / А. А. Романюхин. – М.: ФИЗМАТЛИТ, 2009. – 320 с.

2. Балакін С.В. Застосування штучних імунних систем при виявленні шкідливих программ в комп’ютерній мережі / С.В. Балакін – К.: НАУ Проблеми інформатизації та управління: зб. наук. праць, 2017. – № 1-2(57-58). – С.61–68.

УДК 004.021(043.2)

К. И. Бекала,
Национальный авиационный университет, Киев

АЛГОРИТМ ЗАЩИТЫ СЕТЕЙ IP-ТЕЛЕФОНИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

VoIP давно стала объектом атак, поскольку с каждым днем ее популярность увеличивается. IP-телефония вызывает большой интерес у кибер-преступников - имеет доступ к почтовому серверу и банковского онлайн-счета. Такая заинтересованность обычно приводит к совершению атак на сеть. Последствия атак могут быть: кража вызовов, сбой в работе серверов, а также кража персональных данных и дальнейшие действия с ними.

Уровень сложности и количество атак на VoIP-серверы в дальнейшем увеличиваются. Автоматическое сканирование портов и зондирования безопасности используется много раз в день. Каждая новая попытка атаки осуществляется с другого IP, а также потенциальные хакеры используют botnet. С помощью этого усложняется их блокировки брандмауэром. Другая сложность к блокированию атак заключается в том, что исходная адрес намеренно подделывается. Такие действия затрудняют выявление настоящей адреса отправителя, которое замаскированное «шумом» случайно-сгенерированных адресов.

Предложена универсальная методика выявления достоверности IP-адреса пользователя при входе в сети и фильтрации адресов с блоком недостоверных или подозрительных действий при попытке доступа достоверных адресов. Данный алгоритм позволяет избежать атак, пытаются быть невыявленными. Применение такого варианта защиты возможно во всех закрытых IP-сетях. Решение задачи защиты сетей таким образом возможно за счет регистрации при входе в IP-сети адреса для дальнейшей ее авторизации. Алгоритм способен снизить частоту попыток ошибочной аутентификации.

Первая часть метода это фильтрация IP-адресов. Поскольку IP-телефония представляет собой закрытую сеть, существуют конкретный список пользователей, имеющих доступ к системе.

Вторая часть метода заключается в том, что программа сканирует файлы журнала логирования и запрещает IP-адреса, которые проявляют признаки вредоносной аактивности. Такими

признаками являются большое количество сбоев паролей, поиск ьбь эксплойтов. Второй этапу позволяет предотвратить намеренной изменении адреса и втрученню в сеть через любое доступа к компьютеру.

В совокупности двух этапов метод дает мощный отпор атакам, особенно атакам типа «отказ в обслуживании и взлома пароля методом полного перебора. Метод работает независимо от других протоколов Asterisk, поэтому его работа не может повредить собственно работе связи.

Данный метод защиты также включает в себя такие составляющие системы защиты IP-сетей: политика сложные пароли, отключение ответы о неправильном пароль и блокировки доступа после неудачных попыток регистрации. Кроме того такой подход прекрасно дополняет другие составляющие. Такие как применение межсетевых экранов, шифрования телефонных разговоров и собственно использования VPN.

Созданный алгоритм имеет ряд преимуществ от существующих аналогов. Во-первых, не требует установки дополнительных программных средств или приложений. Во-вторых, он может работать без участия брандмауэра. В-третьих, метод может применяться как политика безопасности входа в сеть, может влиять на слабую аутентификацию. В-четвертых, в методе не предполагается постоянный контроль за системой.

Таким образом, в работе предложен метод может потенциально повысить защищенность сетей IP-телефонии и снизить возможность вмешательства посторонних лиц в сеть и похищения персональной информации, а также использования ее.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Джим Ван Меггелен, Лиф Мадсен, Джаред Смит “Asterisk: The Future of Telephony”, 656, 2015.

2. https://habrahabr.ru/post/188440/

3. L. Madsen, J. V. Meggelen, R. Bryant, "Asterisk: The Definitive Guide", 736, 2011.

4. N. Simionovich, "Asterisk Gateway Interface 1.4 and 1.6 Programming", 220, 2009.

УДК 004.056.32 (043.2)

О. В. Борисенко,
Б. Я. Корнієнко, д.т.н.,
Національний авіаційний університет, Київ

АНАЛІЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Політика безпеки – основа системи безпеки будь-якого підприємства. В більшості випадків якісна система безпеки будується на моделі безпеці. Модель безпеки визначає метод впровадження політики та технологій, які вона використовує. Мета цієї моделі – відображення суті вимог до безпеки даної системи. Вона визначає потоки інформації, що дозволені в системі, і правила управління доступом до інформації. Модель дозволяє провести аналіз властивостей системи, але не накладає обмеження на реалізацію тих чи інших механізмів захисту. Коли модель створюється, вона називається неформальною моделлю безпеки. Коли модель математично перевіряється, вона стає формальною. Одними з найпоширеніших і перевірених часом моделей безпеки є моделі безпеки Bell-LaPadula, Biba та Clark-Wilson.

Модель Bell-LaPadula, або BLP – це модель, що базується на забезпеченні конфіденційності інформації. Це абстрактна модель, яка набула значного поширення, наприклад, вона використовується Міністерством оборони США (DoD). Модель визначає поняття безпечного стану з визначеною функцією переходу, яка переміщує систему з одного стану безпеки в інший. Кожному суб'єкту надається рівень доступу, що відповідний рівню конфіденційності, а об'єктам надається рівень таємності. Модель визначає основний режим доступу для читання та запису даних, а також те, як суб’єкти отримують доступ до об'єктів.

Модель BLP визначає доступ до об'єкта на основі рівня очищення, пов'язаного як з об'єктом, так і з об'єктом, і лише потім – на рівнях тільки читання, читання-запису чи тільки запису. Модель надає доступ до трьох основних властивостей. Проста властивість безпеки (англ. ss-property) відповідає за те, що суб’єкт, що має конкретний рівень доступу, може читати інформацію тільки з того об’єкта, рівень доступу якого не є вищим за його власний. Ця властивість також відома під назвою «Немає читання зверху» (англ. no read up, NRU). Друга властивість називається властивістю

* (англ. *-property) і стосується доступу до запису. Суб'єкт може записувати інформацію лише в об’єкт, рівень доступу якого не нижчий за його власний. Ця властивість також відома під назвою «Немає запису вниз» (англ. no write down, NWD). Таким чином можна запобігти копіюванню суб’єктом інформації з поточного рівня класифікації на нижчі. Третя властивість називається сильною властивістю * (англ. strong *-property) і є альтернативою другої властивості. Її відмінність від властивості * полягає в тому, що суб’єкт може записувати інформацію лише в об’єкт, рівень доступу якого рівний його власному.[1]

Головним недоліком моделі Bell-LaPadula є те, що неможливо змінити рівень доступу об’єкта під час роботи системи.

Модель BLP є дискреційною моделлю безпеки, оскільки суб’єкт визначає, який конкретний режим доступу необхідний для даного об'єкта.

Модель Biba – перша спроба реалізації моделі безпеки, що базується на забезпеченні цілісності інформації. Ця модель політики безпеки визначається фразою «Немає читання знизу, немає запису вгору» на противагу моделі BLP, яку можна описати фразою «Немає читання зверху, немає запису вниз». Тобто, модель Biba можна розглядати як інверсію моделі Bell-LaPadula. Модель Biba розглядає лише одне з завдань цілісності інформації – захист системи від доступу неавторизованих користувачів, доступність та конфіденційність взагалі не розглядаються. Також передбачено зосередження тільки на зовнішніх загрозах, внутрішні не аналізуються.

Логіка побудови моделі Biba є схожою на логіку побудови моделі BLP. Як читання об’єкта нижчого рівня таємності може призвести до втрати конфіденційності інформації на вищому рівні, так і читання об’єкта нижчого рівня цілісності може призвести до зниження цілісності інформації на вищому рівні.

Три головні властивості моделі Biba також схожі на властивості моделі BLP: проста властивість цілісності (англ. ss-property), властивість * (англ. *-property) і властивість запиту. Проста властивість цілісності визначає, що суб’єкт не може отримати дозвіл на доступ чи читання об’єкта меншого рівня цілісності, властивість * визначає, що суб’єкт не може модифікувати об’єкт з більшим рівнем цілісності, властивість виклику стверджує, що

суб’єкт не може надсилати повідомлення (тобто логічні запити для сервісу) до об'єкта з більшим рівнем цілісності.[2]

На відміну від моделі Biba, модель Clark-Wilson відповідає всім завданням забезпечення цілісності інформації, оскільки вона запобігає внесенню змін неавторизованими користувачами, спрямована на внутрішню і на зовнішню узгодженості, а також запобігає неправильним модифікаціям інформації авторизованими користувачами. Внутрішня узгодженість означає, що програма працює точно так, як очікується, кожного разу, коли вона виконується; зовнішня – що дані програми узгоджуються з реальними даними.

Модель Clark-Wilson базується на так званих правильно сформованих транзакціях. Це транзакції, які достатньо структуровані та деталізовані, щоб відповідати вимогам і внутрішньої, і зовнішньої узгодженості, для цієї мети також є необхідною імплементація принципу розподілення обов’язків. Для цього операція ділиться на складові частини, за кожну складову відповідає окремий користувач чи процес. Це робить можливим гарантування того, що введені дані узгоджуються з інформацією, яка доступна поза межами системи. Це також запобігає внесенню користувачами несанкціонованих змін [2].

Всі моделі політики безпеки, розглянуті вище, мають багато переваг, але в разі їх використання не можна забувати про те, що жодна з них не є універсальною. Вони вирішують тільки пріоритетні питання, що поставлені перед ними, вони не враховують не тільки унікальні характеристики реальних систем, щодо яких вони застосовуються, а і зовнішні чинники, які важко спрогнозувати заздалегідь.

Необхідно пам’ятати, що ці моделі є лише основою побудови політики безпеки, всі наступні кроки залежать від наданої системи, що підлягає захисту.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. John McLean. Security Models – NJ: Wiley, 1994.
2. Matt Bishop. Mathematical Models of Computer Security - Boston: Addison Wesley, 2015.

УДК 004.056 (043.2)

І. В. Вантух, студент,
Національний авіаційний університет, Київ

АВТЕНТИФІКАЦІЯ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ЗА ДОПОМОГОЮ ТОКЕНІВ

Поява глобальних телекомунікаційних комп'ютерних мереж спростили отримання доступу до інформаційних ресурсів як для окремих користувачів, так і для цілих організацій. Проте одночасно з цим виникла проблема — загроза мережевих атак, в тому числі несанкціонованого доступу до даних користувачів і їх несанкціонованої зміни.

Одним з перспективних рішень проблеми є ідентифікатори доступу — токени. Токени (tokens) — це невеликі електронні пристрої, що базуються на захищеному мікроконтролері. Вони являють собою аналоги смарт-карт, але не вимагають додаткового обладнання для зчитування і підключаються до порту USB, який є в будь-якому сучасному комп'ютері.

Токен призначений для автентифікації користувачів при доступі до секретної інформації, безпечного зберігання паролів, ключів шифрування, цифрових сертифікатів, даних користувачів. Так, в комплексі з іншими програмними і апаратними засобами, токен здатний вирішувати проблеми авторизації і розділення доступу в мережах, контролювати доступ до захищених інформаційних ресурсів, забезпечувати необхідний рівень безпеки при роботі з електронною поштою.

Токени можуть містити чіпи з різними функціями від дуже простих, до дуже складних, у тому числі й кілька методів автентифікації. Найпростішим токенам безпеки не потрібні ніякі підключення до комп'ютера. Токени мають фізичний дисплей; Користувач просто вводить відображене число для входу. Інші токени підключаються до комп'ютерів, використовуючи бездротові технології, такі як Bluetooth. Ці токени передають ключову послідовність локальному клієнтові або найближчої точки доступу в мережі. Крім того, інша форма токену, який був широко доступний багато років, є мобільний пристрій, який взаємодіє з використанням «позасмугового» каналу (наприклад, SMS або

USSD). Тим не менше, інші токени підключаються до комп'ютера, і може знадобитися PIN-код. Залежно від типу токену, операційна система комп'ютера або прочитає ключ від токену та виконає криптографічні операції на ньому, або попросить, щоб програмне обладнання токену виконало ці операції самостійно. Таким додатком є апаратний ключ (електронний ключ), необхідний для деяких комп'ютерних програм, щоб довести право власності на програмне забезпечення. Найкращим видом зберігання токену є використання смарт-карт.

На смарт карті, зберігається закритий ключ клієнта, що підтверджує токен. Фактично він представляє собою засіб автентифікації користувача, якому замість запам'ятовування безлічі паролів доступу досить мати смарт-карту і пам'ятати PIN-код до нього (так звана двофакторна автентифікація). Процес ідентифікації клієнта в мережі зображено на рис.1.

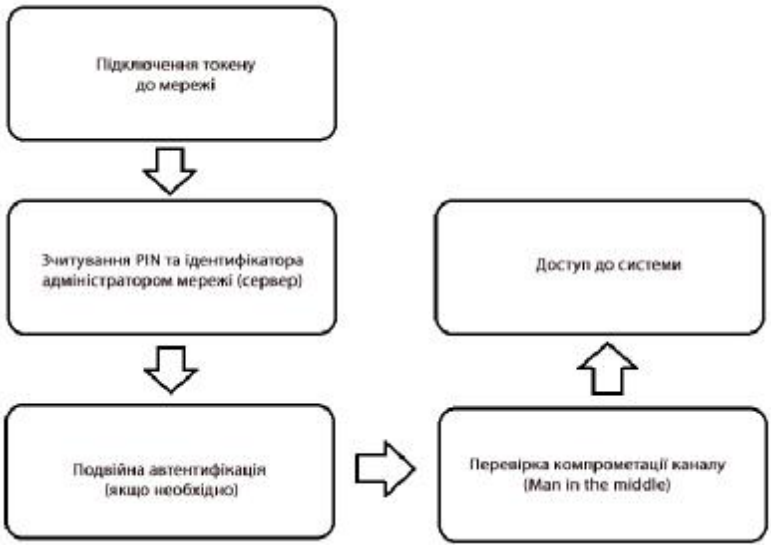


Рис. 1. Ініціалізація в мережі з використанням токену

З описаного вище, стає зрозумілим перспектива використання токенів для автентифікації не тільки в комп’ютерних мережах, а й у інших сферах (банки, державні установи і т. д.). Використання токенів дозволяє максимізувати безпеку користувача в мережі за рахунок двофакторної автентифікації та використання смарт-карт.

УДК 004.42(043.2)

В. В. Горіна, асистент
Національний авіаційний університет, Київ

ІНТЕГРАЦІЯ СИСТЕМ ПРИ ПРОЕКТУВАННІ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Реальний процес проектування інформаційної системи (ІС) відображається в технологічній мережі проектування [1, 3].

Технологічна мережа проектування (ТМП) – взаємопов'язана за входом і виходом послідовність технологічної операції (ТО) проектування, виконання яких має забезпечити створення проекту ІС.

Складанню ТМП передує ознайомлення з предметною областю, сформулювати основні цілі та задачі проектування, визначити перелік основних комплексів робіт, у тому числі ТО.

Проектування ІС – складний процес роботи багатьох виконавців, що включає багато різноманітних робіт і потребує суворої впорядкованості, певної послідовності та планомірності їх виконання.

Найпоширенішим методом планування й управління розробкою і впровадженням проекту є система планування мереж та управління (СПУ PERT), за допомогою якої можна отримати уявлення про всю ТМП, що забезпечує найраціональнішу послідовність проектних робіт [1].

Порядок виконання робіт зі створення ІС подається у вигляді графа мережі, який включає детальний опис проектування і містить багато операцій (робіт).

Розширений граф мережі за стадіями й етапами проектування дає змогу простежити розвиток системи від початку робіт з її створення до введення в експлуатацію. Його параметри обчислюють на ЕОМ із застосуванням спеціального ППП.

Застосування графіків мереж для організації управління процесом проектування ІС дає змогу визначити його загальну трудомісткість і на основі існуючих нормативів з'ясувати потрібну кількість ресурсів на виконання проектних робіт [2]. Календаризація графіка мережі здійснюється на основі наявності трудових і технічних ресурсів. Для цього розробляють календарний

графік для виконавців з урахуванням застосовуваних ними технічних засобів у процесі проектних робіт.

Визначення критичного шляху і резервів за ТО дає змогу контролювати виконання проектних робіт, оперативно керувати процесом проектування, перерозподіляючи роботи між виконавцями-розробниками системи або навпаки (виконавців між роботами) з метою створення проекту ІС у суворо встановлені терміни.

Отже, СПУ для організації процесу проектування ІС вказує на те, що під час роботи з ТМП може бути використаний математичний апарат.

Якщо в ТМП у жодній ТО не застосовуються засоби проектування, тобто всі подані в ній операції виконуються вручну, то таку мережу називають канонічною ТМП, яка відображає процес створення ІС для конкретного ОУ. У ній цей процес подається на найнижчому рівні декомпозиції і є базою для обґрунтування застосування та розроблення різних засобів проектування (ТПР, ППП тощо).

Загальний вигляд отриманого сценарія показаний на рис. 1, з якого видно, яким чином база даних дозволяє інтегрувати системи CAD, CAE і CAM, що і являється кінцевою метою системи інтеграції.

Рис. 1. Інтеграція CAD, CAM і CAE через базу даних

Наведений сценарій демонструє використання систем CAD/CAM/CAE в рамках усього життєвого циклу продукту для досягнення згаданих цілей: підвищення якості (Q), зниження вартості (C) и прискорення відвантаження (D). Цей сценарій може показатися дещо спрощеним на фоні сучасних передових комп'ютерних технологій, однак він ілюструє напрям розвитку техніки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Шалумов А.С. Введение в CALS-технологии: Учебное пособие / А.С. Шалумов, С.И. Никишкин, В.Н. Носков. Ковров: КГТА, 2002. – 137 с.

2. Красильникова М.В. Проектирование информационных систем: Учебное пособие / М.В. Красильникова – М.: МИСиС, 2004. – 106 с.

3. Орлов С.А. Технологии разработки программного обеспечения. Разработка сложных программных систем / С.А. Орлов. – СПб.: Питер, 2002. – 464 с.

УДК 004 (043.2)

М. О. Гриб,
А. Т. Дехтяренко,
Національний авіаційний університет, Київ

ТЕХНОЛОГІЯ FLASH У ВЕБ-РЕСУРСАХ

З розвитком інформаційних технологій та суттєвого збільшення інформації в ресурсах, особливої уваги потребують технології, які дозволяють зменшувати обсяги даних. Серед них, провідної ролі набувають flash-технології, які окрім унаочнення, передбачають динамічну візуалізацію та залучення аудіо-контенту. Такі технології наразі активно залучаються до створення більш інформативних веб-ресурсів.

Flash – мультимедійна платформа, призначена для створення векторної анімації та інтерактивних додатків (в тому числі й ігор), а також інтеграції відеороликів на web-сторінках. Сайт постійно розвивається привертаючи увагу Інтернет користувачів. Значною перевагою flash є можливість отримання анімованих динамічних інтерактивних сторінок невеликого розміру, що є доцільним для їх застосування в Інтернеті. Це забезпечується використанням векторної графіки і потужних алгоритмів стиснення інформації. Також технологія flash дозволяє використовувати форми для створення запитів до сервера, а, отже, і потенційну можливість підключення до бази даних.

Інтерактивна веб-анімація або технологія Flash, розроблена за підтримки компанії Macromedia, з появою в 1996 році, стала невід'ємною частиною більшості сучасних веб-ресурсів. На відміну від звичайної gif-анімації, проектування Flash-елементів інтегрує мультимедійні технології і скриптову мову ActionScript, яка базується на ECMAScript — стандарті скриптових мов. Орієнтація на векторну графіку, як на основний інструмент розробки Flash-програм, дозволила реалізувати всі базові елементи мультимедіа: рух, звук та інтерактивність об'єктів. Однією з переваг даної технології є можливість створення динамічних веб-сторінок в основі яких лежить так званий векторний морфінг, що дозволяє задавати лише кілька ключових кадрів для створення складних мультиплікаційних сцен, тоді як для gif-анімації необхідно окремо задавати ключові кадри, навіть для найдрібніших змін. Flash-файли мають розширення .swf і для перегляду вимагають

наявності програми Adobe Flash Player, що може бути встановлений як плагін для браузера. Також до особливостей flash-сторінок можна віднести кросплатформність та інтерактивність.

Потрібно зазначити, що на відміну від інших технологій анімації веб-сторінок, при використанні Flash-технологій, відсутня проблема невідповідності розмірів екрану і сторінки, яка вирішується відсотковим відношенням розміру флеш-об'єкта до розміру екрану.

Також до основних переваг Flash-технологій можна віднести: невеликий розмір файлів, що пов'язано з використанням векторної графіки і потужних алгоритмів стискання інформації, усунення проблем сумісності між браузерами, наявність вмонтованої мови опису сценаріїв, наявність засобів експортування зображень в найбільш розповсюджені графічні формати.

Головний недолік Flash-об'єктів— надмірна вимогливість до ресурсів процесора. Використання Flash для розміщення текстової інформації перешкоджає її індексуванню пошуковими системами.

Все частіше технологія Flash застосовується для створення складних інтерактивних веб-ресурсів і в останні роки перетворилася на промисловий стандарт для роботи з інтерактивним контентом. Один з головних принципів Flash, - «Build once, deliver anywhere» («Розробив один раз, поширюй скрізь»). Програми, створені на базі Flash, працюють на різних платформах Windows, Macintosh, UNIX, PDA і навіть в мобільних телефонах. Продукт Macromedia Flash Player фактично став стандартом і сьогодні встановлений на комп'ютерах 97,6% користувачів Інтернету.

Отже, з підвищенням вимог до мультимедійності та інтерактивності веб-ресурсів, Flash-технологія може забезпечити нові можливості і скласти високу конкуренцію іншим технологіям.

Проаналізувавши основні поняття flash-технології та їх історію розвитку можна зробити висновок, що flash-технології стрімко розвиваються і мають широке застосування в розробці веб-ресурсів. Вони також дозволяють розробляти інтерактивні мультимедійні додатки, цікаві flash-презентаці та істотно розширюють можливості flash-дизайну.

УДК 681.3.06 (043.2)

В. В. Демчик, студент,
О. В. Корочкін, к.т.н., **О. В. Русанова,** к.т.н.,
Національний технічний університет України "КПІ ім. І. Сікорського", Київ

КОМБІНОВАНИЙ ПАРАЛЕЛІЗМ ЯК ЗАСІБ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ

В роботі наводяться результати експериментальних досліджень застосування в багатоядерних системах комбінованого паралелізму, запропонованого в роботі [1]. Підхід базується на одночасному застосуванні (комбінації) паралелізму різної гранулярності. Дослідження ефективності в порівнянні з іншими типами паралелізму здійснювалось шляхом тестування розробленого пакету паралельних програм для матричних операцій в комп'ютерній системі, оснащеній шестиядерним процесором AMD Phenom II. В табл. 1 наведені отримані результати тестування паралельних програм для операції множення матриць для різних значень N (розмірність матриць), реалізованих різними засобами (бібліотека OpenMP, мови C# та Java) та з різною зернистістю паралелізму, на рисунках 1-3 – графіки зміни коефіцієнтів прискорення (Кп),

Таблиця 1. Результати тестування

N	Час виконання (сек.)								
	Середня зернистість			Дрібна зернистість			Змішана зернистість		
	OpenMP	Java	C#	OpenMP	Java	C#	OpenMP	Java	C#
516	1,7	0,2	1,2	1,6	0,2	1,1	1,5	0,2	1,1
1032	13,3	3,3	9,8	12,8	2,9	9,8	12,4	3,1	9,5
1548	46,7	14,0	35,6	45,9	12,1	34,1	44,9	13,0	33,8
2064	111,7	38,5	79,8	110,8	33,5	78,1	108,1	35,5	74,8

Виходячи з отриманих результатів тестування, можна стверджувати, що запропонований в роботі підхід, який ґрунтується на комбінованому паралелізму, показав свою ефективність і дозволів збільшити Кп при використанні в мові C# та бібліотеці OpenMP. При цьому спостерігається зростання Кп при збільшенні обсягу оброблюваних даних, що є одним з найважливіших аргументів доцільності застосування даного підходу.

Можна припустити, що ефективність використання змішаного паралелізму буде збільшуватися при зростанні кількості ядер в системі, де: з'являться додаткові процесорні ресурси для його реалізації, можна зменшити розмір дрібної зернистості,можна знайти оптимальне співвідношення між кількістю потоків і підпотоків.

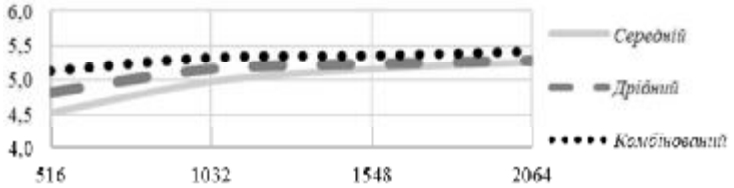


Рис.1. Графік залежності Кп від N. Бібліотека OpenMP

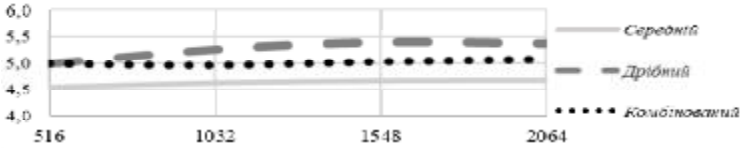


Рис.2. Графік залежності Кп від N. Мова Java

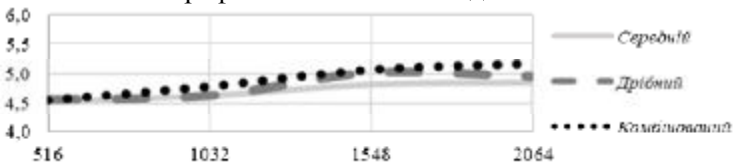


Рис.3. Графік залежності Кп від N. Мова C#

Таким чином, можна стверджувати що застосування комбінованого паралелізму в більшості випадків є ефективним підходом до реалізації об'ємних паралельних обчислень в багатоядерних комп'ютерних системах.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Демчик В.В. Дослідження ефективності використання дрібнозернистого паралелізму в багатоядерних комп'ютерних системах / В. В. Демчик. О. В. Корочкін О. В. Русанова - Тези X Міжнародної науково-технічної конференції "Комп'ютерні системи і мережні технології". − К.: НАУ, 2017, С. 34-34.

УДК 004 (043.2)

В. И. Дрововозов, к.т.н.,
С. В. Водопьянов, аспирант,
Н. В. Журавель,
Национальный авиационный университет, Киев

КОМПЬЮТЕРНАЯ СЕТЬ ЦЕНТРА ВЫСОКОПРОИЗВОДИТЕЛЬНОЙ ОБРОБОТКИ ДАННЫХ

Центр высокопроизводительной обработки данных (ЦВОД) должен обеспечить поддержку и ускорение высокопроизводительных расчетов при решении различных фундаментальных задач в областях науки и техники, вопросы организации высокоскоростного доступа к вычислительным и информационным ресурсам, мониторинга и управления, надежности и защищенности. Для решения таких задач требуются большие скорости вычислений, технологии распараллеливания расчетов, визуализации, ввода и хранения колоссальных объемов данных.

Применение современных технологий организации таких сетей должны обеспечивать объединение удаленных высокопроизводительных компьютеров в вычислительную сеть ЦВОД и доступ компьютеров к банкам данных.

Основными функциями сети вычислительного центра остаются:

- скоростная связь между узлами сети;
- скоростной доступ для удаленных пользователей;
- связь Центра с партнерами.

Составляющие: комплекс услуг сети Интернет (web-сервис, почта, news-сервис), сервис телеконференций, сервис доступа к ресурсам (NSF, FTP, SSH, …), службы управления (NIS и Active Directory для пользователей, управление доступом, пользователями, управление устройствами и доступом), мониторинг и отчетность;

Основными причинами, требующими модернизации локальной вычислительной сети центра являются:

- расширение вычислительных мощностей и информационных ресурсов центра и достигнутый в настоящее время предел производительности сети;

– возросшие требования надежности и наличие уязвимых с точки зрения надежности мест в существующей конфигурации сети;

– увеличение объема и сложности решаемых задач и появление принципиально новых сетевых приложений требующих контроля качества обслуживания.

Направления развития сетевой инфраструктуры центра.

Направления развития сетевой инфраструктуры напрямую вытекают из целей стоящих перед информационной системой ЦВОД.

В связи с увеличением объема и сложности решаемых задач и с появлением принципиально новых приложений, активно использующих аудио и видео информацию, необходимо повышать производительность сети и внедрять систему контроля качества обслуживания на уровне приложений.

С другой стороны увеличения количества приложений предъявляет повышенные требования к надежности сети.

Повышенные требования к надежности неизбежно влекут повышения внимания к защите сети от несанкционированного доступа.

Кроме того, мощнейшим инструментом для решения проблем производительности, качества обслуживания, надежности и защиты является эффективная система управления сетью.

Таким образом, основными приоритетами при развитии сети ЦВОД становятся:

– повышение производительности и масштабируемости сети;
– внедрение интеллектуальных сервисов для приложений;
– повышение надежности сетевой инфраструктуры;
– усиление защиты сети;
– внедрение эффективной системы управления сетью.

Возможные решения

Повышение производительности сети может быть обеспечено как расширением общей пропускной способности сети, так и расширением полосы пропускания отдельных сегментов.

Анализ информационных потоков в локальной сети центра показывает, что основные информационные потоки – это потоки между серверным и пользовательским сегментами. Обычно, в корпоративной сети можно снизить информационные потоки,

распределив сервера между рабочими группами. Но в локальной сети вычислительного центра это трудно выполнить, так как все сервера, имеют общее «вычислительное» назначение. Для повышения производительности сети необходимо увеличить пропускную способность каналов, соединяющих коммутаторы уровня доступа и уровня распределения, увеличить производительность коммутаторов уровня распределения.

Кроме того, для обеспечения межсегментной маршрутизации на уровне распределения целесообразно использовать коммутаторы третьего уровня.

Поскольку одним из главных требований к модернизируемой сети является требование поддержки управления качеством обслуживания на уровне приложений. Для обеспечения требуемого качества сервиса (QoS), необходимого для передачи критичных к задержке приложений маршрутизаторы и маршрутизирующие коммутаторы должны поддерживать эффективные алгоритмы построения очередей с учетом приоритетов, а также возможность резервирования полосы пропускания. Кроме того, маршрутизаторы (и маршрутизирующие коммутаторы) должны поддерживать необходимые для передачи видео и аудиотрафика протоколы Protocol Independent Multicast (PIM) и протокол резервирования ресурсов Resource Reservation Protocol (RSVP).

Эффективное групповое управление позволяет снизить объем непроизводительного трафика, уменьшает нагрузку на коммутаторы и оптимизирует использование полосы пропускания. Таким образом, сеть используется более эффективно, а, следовательно, повышается ее производительность (в широком смысле).

Повышение надежности сети может быть достигнуто за счет обеспечения отказоустойчивости работы ключевых сетевых элементов и узлов сети. Для этого наиболее ответственное активное оборудование и каналы могут дублироваться или резервироваться. Кроме того, может использоваться перенаправление трафика по альтернативным путям.

В локальной сети ЦВОД дублирование наружных маршрутизаторов и коммутаторов ядра сети представляется совершенно оправданным. Естественно, коммутаторы уровня доступа должны подключаться двумя каналами к разным

коммутаторам. Сервера также должны присоединяться к сети как минимум двумя каналами.

Возможно, оправданным является и резервирование коммутаторов уровня доступа, хотя подключение каждого рабочего места к двум коммутаторам вряд ли экономически целесообразно.

Защита сети центра может быть усовершенствована за счет установки отказоустойчивой системы защитных экранов, обеспечивающих бесперебойный доступ к внешним ресурсам из сети ЦВОД и контролируемый доступ к ресурсам ЦВОД извне.

Кроме того, защищенный удаленный доступ в сеть ЦВОД может быть расширен за счет установки сервера удаленного доступа.

Эффективные средства управления сетью способны помочь решению проблем повышения производительности, надежности и защиты сети. Система управления сетью должна решать следующие задачи:

- управление конфигурацией сети;
- управление ошибками;
- управление производительностью;
- управление безопасностью;
- учет работы сетевых устройств.

Система управления сетью должна иметь возможность интеграции с используемой в центре системой управления информационными ресурсами и технологиями предприятия [1-4].

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Julia H. Allen. The CERT® Guide to System and Network Security Practices, Addison-Wesley, USA, 2001.

2. Earl Carter. Cisco Secure Intrusion Detection System. Cisco Press, USA, 2001.

3. Thomas A. Limoncelli and Christine Hogan. The Practice of System and Network Administration. Addison-Wesley, USA, 2002.

4. Дрововозов В.І. Розвиток корпоративної мережі центру високопродуктивної обробки даних // В.І. Дрововозов, М.М. Дидар. Проблеми інформатизації та управління: зб. наук. праць. – К.: НАУ, 2014. – Вип.1 (45). – С. 42–46.

УДК 004.075

O. O. Drozd, MCE,
V. I. Nadtochii, PhD
National Aviation University, Kyiv

BLOCKCHAIN BASED MODEL OF DATA STORAGE SYSTEM

Recently Blockchain-technology is becoming increasingly popular. Although most Blockchains currently handle financial transactions, in general, the transaction can be considered simply as atomic changes in the state of a particular system. For example, Blockchain can be used to register documents and protect them from changes.

All transactions in the Blockchain are stored in a single registry. In the special field of each block, the hash of the entire block, adjacent blocks and each transaction of the block is stored. In addition, a certain condition is imposed on the hash block, for example, it should start with ten zeros. Thereby, in order to substitute some information in a separate transaction, it is necessary to list all hashes in this block and blocks that follow it.

Since the transactions are fully arranged by time, the current state of the system (a set of balances of users in case of financial Blockchain) is determined solely by this transaction register. Storing the entire history of system state changes has its advantages, for example, the ability to determine the state of the system at any given time simply by re-executing the corresponding transactions.

The purpose of the work is to create a module using Blockchain technology to save data. Electronic voting system was chosen as an example of data storage system. It will combine all the advantages of electronic voting systems with the highest possible protection of data from alteration or substitution.

In recent years, electronic voting has become very popular and is the latest hot topic of research. Electronic in the sense of counting ballots has been there for some time, but attention is now more focused on the issue of how to count electronic bulletins.

Electronic voting already exists in various forms, including the counting of votes on a computer using electronic equipment, polling stations and voting via the Internet from your own computer or mobile device. There are several types of modern electronic voting systems: optical scan system, a system of electronic urns, end-to-end system of voting, Internet voting systems that have their own nuances, strengths

and weaknesses.

The objectives of enabling a voter to vote from their home computer are: raise of convenience; reduction of paper usage; increasing the availability of voting for voters with disabilities; and much more.

Like all information systems, electronic voting systems are vulnerable to computer attacks. Though Internet voting can improve some electoral factors, there are concerns that this counter potential security threats neglected.

As a result of the work, the algorithm and the architecture of the module were designed to save the results of voting using the technology Blockchain.

The method of study is investigation and analyzing Blockchain technology, modern data storage system and their usage. Selection of data storage system type and modeling Blockchain solution. Creation a secure algorithm for transmission storage based on the Blockchain technology.

Over the past few years the Blockchain technology has become very popular because of the opportunities it opens up when is used: the creation of decentralized systems to save any changes of data in a form that these changes impossible to replace. This is confirmed by both mathematically and in a practice (e.g., cryptocurrency Bitcoin).

The results of this study can be used to create a reliable and safe system of electronic voting. In addition, information storage module can be used in other fields, such as finance and business.

The work has practical value. Further developments are possible in the direction of implementation the history of a file changes.

The created module allows to store in Blockchain not only financial transactions, but also any changes to the status of some object, such as a file. Thus, the scope of applicability developed module is very large, from the financial sector to public or commercial sector.

The results of this study can be used to create a reliable and safe system of electronic voting. In addition, information storage module can be used in other fields, such as finance and business.

The work has practical value. Further developments are possible in the direction of implementation the history of a file changes in a Blockchain.

УДК 004.75 (043.2)

О. О. Жолдаков,
А. О. Жолдаков,
Національний авіаційний університет, Київ

ІНТЕЛЕКТУАЛЬНИЙ АГЕНТ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ПОВІТРЯНИХ СУДЕН

На цей час провідні авіакомпанії світу впроваджують елементи і цілі системи штучного інтелекту для досягнення більшої якості, надійності і економічної ефективності технічного обслуговування і ремонту повітряних суден (ТОіР ПС).

Суттєвими є витрати авіакомпаній з причин затримки і навіть відміни рейсів у разі виявлення непридатних для польотів компонентів ПС.

Особливо трудомісткими є роботи щодо обслуговування авіаційних двигунів, для досконалої перевірки яких треба знімати ці агрегати з літаків, що надовго виводить ПС з графіку польотів. Фірми-розробники авіадвигунів – *General Electric, Rolls-Royce, Pratt & Whitney* – почали створювати маленьких роботів – пристрої штучного інтелекту які могли б проводити діагностику (і навіть налаштування) компонентів двигунів без розбори і знімання з планеру.

Все більш проглядає необхідність впровадження цілісних систем штучного інтелекту не тільки для виконання окремих видів робіт з ТОіР, але також для автоматизованого управління ТОіР.

Ключовим елементом штучного інтелекту АС ТОіР є так званий агент, що включає в себе датчики технічного стану компонентів ПС, виконавчі механізми (в т.ч. – роботи) та інформаційно-програмне забезпечення ведення баз даних і знань для їх накопичення та пошуку і прийнять рішень з управління АС ТОіР.

Першим етапом проектування інтелектуального агента ТОіР ПС повинно бути визначення його проблемного середовища.

Проблемним середовищем технічного обслуговування повітряних суден є саме ПС з усім оточуючим його середовищем, як то умови експлуатації, перевірки технічного стану і ремонту та жорстко регламентовані обмеження за технологією і часом виконання ТО ПС, а також – людино-машинна система виконання ТО ПС, разом з АС керування цією системою.

Опис проблемного середовища потребує максимальної повноти, що починається із її класифікації. Проблемне середовище ТОіР ПС може бути визначене наступними характеристиками:

– таке, що підлягає частковому спостереженню (особливо у фазах оперативного ТО);

– стохастичне, тому що не повністю визначається поточним станом і діями агента з причин непередбачуваних умов;

– епізодичне у сенсі того, що агент повинен формувати рішення щодо дефектності і ремонту деталі незалежно від рішень відносно перевірок інших компонентів;

– динамічне, тому що середовище може змінитися у ході того, коли агент приймає поточне рішення;

– дискретне, як пов'язане із дискретною множиною виявлених сенсорами-датчиками показників стану компонентів ПС, а також необхідних дій діагностики і ремонту.

Програму простого рефлексивного агента виконання ТОіР, що діє згідно правилу (*rule*) відповідно до поточного стану (*state*) перевірки компоненту ПС, можна зобразити наступним псевдокодом:

function *Simple-Reflex-Agent* (відчуття *percept*) ***returns*** дія *action*

static: *rules,* множина правил умова-дія

state ← *Rule-Match* (*state, rules*)

action ← *Rule-Action* [*rule*]

return *action.*

Але така програма агента може бути застосована у простих випадках, коли рішення може бути прийняте на основі виключно сприйняття поточного стану компонента ПС.

На сучасному етапі провідні авіакомпанії починають впроваджувати предикативні системи технічного обслуговування літаків, що дозволяє прогнозувати можливий вихід стану компонента ПС із діапазону льотної придатності, що потребує накопичення і ведення великих баз даних і знань щодо стану компонентів ПС впродовж всього експлуатаційного етапу їх життєвого циклу.

Тоді агент штучного інтелекту повинен мати компонент, що вміє навчатися, використовуючи досвід виявлення попередніх станів компонентів ПС і реакцій-дій щодо усунення виявлених порушень.

УДК 004.7 (043.2)

І. А. Жуков, д.т.н.,
М. К. Печурін, д.т.н.
Національний авіаційний університет, Київ,
Л. П. Кондратова, к.т.н.
Інститут прикладного системного аналізу КПІ ім. Ігоря Сікорського, Київ,
С. М. Печурін, к.т.н.

ПРО ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ INTERNET OF THINGS

Проблемою організаційного (кадрового) забезпечення новітніх типів комп'ютерних мереж, систем та їх компонентів, зокрема транспортної (авіаційної) сфери, обіймаються ряд навчально-наукових організацій в Києві, Харкові, Львові. Останнього часу об'єктом уваги цих організацій стає кадрове забезпечення Internet of Things (т. зв. Інтернету речей),

Досвід роботи спецради НАУ із спеціальності «комп'ютерні системи та компоненти», кафедри комп'ютерних систем та мереж Навчально-наукового інституту комп'ютерних інформаційних технологій та задачі реформування системи наскрізної підготовки кадрів, що вони витікають з прийнятого у 2014 році Закону України «Про вищу освіту», спонукають авторів поділитися міркуваннями щодо організації підготовки кадрів вищої кваліфікації для Інтернету речей.

Структура наскрізної (трирівневої) системи підготовки, у тому числі фахівців для інтернету речей, відслідковується в ОПП, ОКХ, ОНП відповідних спеціальностей сучасної галузі знань ІТ.
Атомарними складовими згаданих документів є модулі навчально-наукових дисциплін навчальних та навчально-наукових планів.

Припустивши, що проблематика Інтернету речей породжує окрему спеціальність у галузі знань ІТ, формуємо відповідну модульну конструкцію (систему навчально-наукових дисциплін) третього рівня підготовки. При цьому використовуємо розподіл функцій [1] згідно з Еталонною моделлю взаємодії відкритих систем: незважаючи на перманентні на неї напади, вона залишається достатньо конструктивною.

Існуюча (останній рік) система атестації наукових кадрів у вигляді спецрад по захисту дисертаційних робіт класифікована за науковими спеціальностями з атомарними складовими, сукупність яких утворюють Паспорти спеціальностей.

Встановивши (метод АНР з використанням експертних оцінок) ступені наближення модулів навчально-наукових дисциплін до атомарних складових паспортів спеціальностей, висхідну задачу можна звести до узагальненої задачі вибору (про призначення) [2].

Оціночні результати розв'язання сформульованої задачі про призначення виокремили такі наукові спеціальності з переліку існуючих вітчизняних, що є найбільш наближеними до проблематики інтернету речей: комп'ютерні системи та компоненти, системи та засоби штучного інтелекту, телекомунікаційні системи та мережі, антени та пристрої мікрохвилевої техніки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Печурін С.М., Кондратова Л.П., Печурін С.М. Применение инструментария формальных грамматик для переклассификации функций эталонной модели взаимодействия открытых систем в беспроводной компьютерной сети // Проблеми інформатизації та управління: зб. наук. праць.–2012.–Вип.1 (37).– С.89-94.

2. Жуков И.А., Печурин Н.К., Кондратова Л.П., Печурин С.Н. Декомпозиционный алгоритм распределения вычислительных ресурсов в беспроводной компьютерной сети // Проблеми інформатизації та управління: зб. наук. праць.–2015.– Вип.3 (51).– С. 40-44.

УДК 004:629.7 (043.2)

М. В. Зірка,
Центральний науково-дослідний інститут озброєння та військової техніки ЗС України, Київ
Н. П. Кадет,
Національний авіаційний університет, Київ

СИСТЕМА УПРАВЛІННЯ РИЗИКАМИ ПРОЕКТІВ СТВОРЕННЯ ПЕРСПЕКТИВНИХ ЗРАЗКІВ АВІАЦІЙНОЇ ТЕХНІКИ З ВИКОРИСТАННЯМ ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

На сьогодні реалізація високих (заданих) тактико-технічних вимог до нових зразків авіаційної техніки (АТ), у більшості випадків, вже не забезпечується шляхом еволюційного розвитку складових елементів літака, його систем та агрегатів, озброєння, бортового обладнання, окремих виробів у межах одного покоління. Тому розробниками все частіше запроваджуються нові більш складні технічні рішення, компоновки, схеми, алгоритми, програми тощо. Відбувається суттєва зміна їх поколінь за рахунок впровадження новітніх інформаційних технологій.

У той же час, впровадження нових технічних рішень, компоновок, схем, алгоритмів, програм, як показує закордонний досвід (F-22, A-400M, F-35, T-50, Су-100), призводить до ускладнення проектів, появи багатьох факторів невизначеності, які не можуть бути завчасно враховані, що створює певні ризики щодо виконання проекту в задані терміни, призводить до перегляду бюджету та вимог технічного завдання.

Отримана статистика, в результаті проведеного аналізу, виявляє тенденцію щодо значного перевищення бюджетів та планових термінів виконання таких проектів, як F-22, F-35, T-50, Ан-70, A-400, A-380, Boeing 787 “DreamLiner”. А загалом і підвищення ступеня ризику виконання проектів.

В таких умовах актуальним постає питання впровадження сучасної дієвої системи управління ризиками інноваційних проектів.

Одним з дієвих інструментів мінімізації ризиків при реалізації проектів, у тому числі з розробки та створення АТ, безумовно, є система підтримки прийняття рішень (СППР). Для практичної реалізації такої системи застосовуються сучасні програмні

продукти (ПП) (ERP системи, такі як SAP, J.D. Edwards, Baan та ін.).

Значний внесок у розвиток теоретичної бази управління ризиками та ризик-менеджменту зробили такі відомі закордонні вчені, як Адам Сміт, Томас Л.Бартон, М. Маккартні, Йоганн Ніколаус Тетенс, І.Т. Балабанов, Д.А. Фролов, Є.Ю. Хрустальов та інші.

Треба зазначити, на теперішній час в Україні також відбуваються процеси, спрямовані на впровадження західних методів управління компаніями, у тому числі щодо ризик-менеджементу. Це стосується таких українських провідних компаній, як Metinvest, ДТЭК та ін.

Як показує світова практика, компанії в галузі ризик-менеджменту розробляють ряд стандартів підприємства на основі процедури ідентифікації, оцінки та обліку ризиків. Розроблені групи стандартів розрізняються по об'єктах управління та кваліфікації виконавців. Показовим прикладом та практичною реалізацією в авіаційній промисловості можна вважати впровадження деяких ОКБ, зокрема стандарту СТП 07509416.00.254.

Наведено приклад реалізації методики оцінки ризиків інноваційних проектів створення зразків АТ на основі математичної обробки значень показників з використанням інформаційних технологій на базі теорії нечітких множин, що дозволяє отримувати значення показників прогнозованих процесів в умовах невизначеності.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Олійник І.І., Жданов С.В., Сорока М.В. Актуальні питання оцінки ризиків при реалізації нових проектів створення авіаційної техніки // Зб. наук. праць ЦНДІ ОВТ Збройних Сил України, 2014. Вип.3(50). - С.122-140.

2. Power D.J. A Brief History of Decision Support Systems. DSSResources. COM, World Wide Web, http://DSSResources.COM/history/dsshistory.html, version 2.8, May 31, 2003.

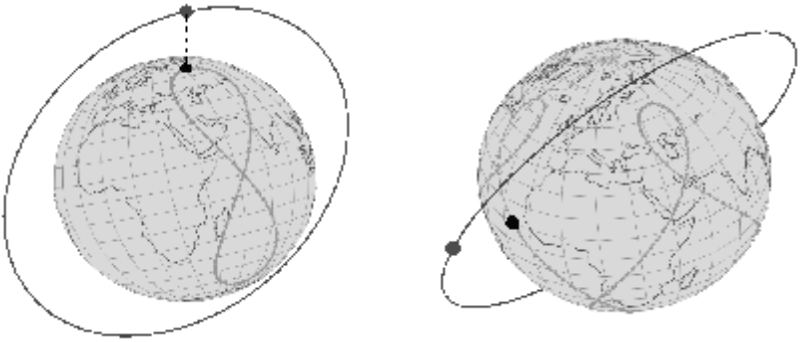
УДК 004.942:52-87(043.2)

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

КОМП'ЮТЕРНА 3D МОДЕЛЬ РУХУ ШТУЧНИХ СУПУТНИКІВ ЗЕМЛІ

В рамках дослідження, описаних у роботі [1] було розроблено і протестовано комп'ютерну 3D модель руху штучних супутників Землі, яка дозволяє візуалізовати траєкторію руху космічного апарату, а також побудувати центральну проекцію його положення на поверхню Землі. Також розроблена модель дозволяє відображати максимальну зону покриття (зону видимості) супутника, що є корисним інструментом при проектуванні телекомунікаційних і навігаційних систем, які містять космічний сегмент [2]. У моделі можливо задавати різноманітні параметри орбіти (ефемериди), зокрема радіус орбіти (або параметри еліптичної орбіти в більш складному варіанті), нахил площини орбіти до екваторіальної площини, орієнтацію орбіти по відношенню до нульового меридіану, а також початкове положення і напрямок руху супутника на орбіті. Можливо також додатково задавати параметри прецесії і нутації орбіти. Період обертання супутника розраховується за третім законом Кеплера.

На рис.1а наведено приклад розрахунку "трека" супутника на геосинхронній орбіті (так звана аналема), а на рис.1б - на орбіті з періодом обертання, що дорівнює 4/5 зоряної доби.



а) б)

Рис.1.

Рівняння для кругової орбіти супутника задається параметрично; для симуляції обертання використовуються відповідні матриці повороту. Трек (проекція) супутника на поверхню Землі являє собою просторову криву Клелії.

Модель реалізовано у двох системах відліку: у нерухомій системі (пов'язаній із космосом) - у ній орбіта стала, а Земля обертається, та у системі відліку, пов'язаною із Землею - у ній площина орбіти обертається, а Земля нерухома. Було реалізовано комп'ютерну симуляцію у вигляді 3D анімації, що містить синхронізовані моделі в обох цих системах відліку (рис.2). Перегляд анімаційної моделі можна здійснювати з різних ракурсів.

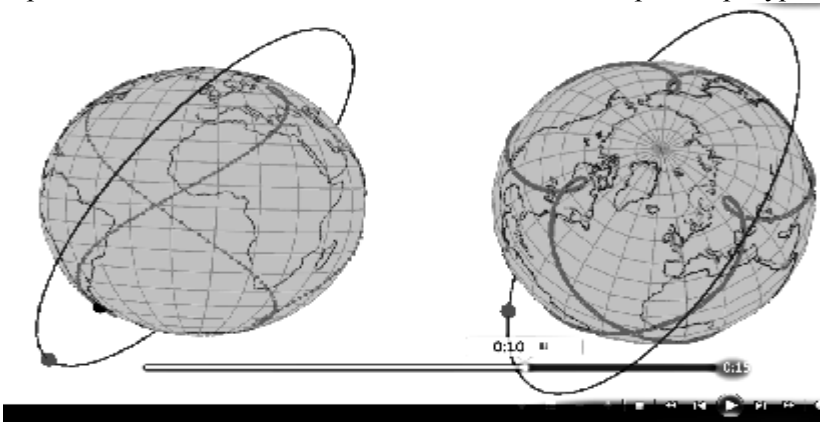


Рис.2.

Зона покриття (видимості) для кожного супутника розраховувалась за методикою, описаною у роботі [1].

Розроблена система може бути корисною у навчальному процесі і при проектуванні телекомунікаційних і навігаційних супутникових систем.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Муригін С.Ю., Зудов О.М., Горіна В.В. Комп’ютерне моделювання глобальних навігаційних супутникових систем // Проблеми інформатизації та управління.–2015.– №4(52).– С.99-105.

2. Генике А.А., Побединский Г.Г. Глобальные спутниковые системы определения местоположения и их применение в геодезии. Изд. 2-е.— М.: Картгеоцентр, 2004. – 355 с.

УДК 004.942 (043.2)

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

ПЕРЕТВОРЕННЯ ХААРА ДЛЯ СТИСКАННЯ ГРАФІКИ

Для стискання графічних зображень методами із втратами найбільш розповсюдженим форматом є jpeg. В ньому застосовується редукція спектру, отриманого за допомогою дискретного косинусного перетворення (ДКП). Відомі недоліки цього алгоритму, яких можна позбутися або суттєво зменшити, застосувавши інші ортогональні перетворення. Такі альтернативні підходи іноді застосовуються, але вони досі не дістали широкого розповсюдження (таких як jpeg2000), або в досить екзотичних випадках (наприклад кодування стандарту ICER, яке використовує NASA для стискання зображень знімків з космічних апаратів [1]).

Для дослідження ефективності компресії необхідно оцінити втрати якості зображення для декількох методів з однаковим ступенем стиснення. Але поняття якості зображення є комплексним і часто суб'єктивним. Тому було поставлено задачу розробити об'єктивні критерії для такої оцінки. У якості прикладу здійснювалось порівняння стискання на основі традиційного алгоритму jpeg і вейвлет-перетворення Хаара: $S = H \times I \times H^T$, де S – отриманий вейвлет-мпектр, що підлягає надалі редукції; I – матриця растрового зображення-оригіналу розміром 2^nx2^n; H і H^T – нормалізована матриця Хаара і її транспонування.

а) б) в)

Рис. 1. а – оригінальне зображення; б –перетворення Хаара; в) jpeg формат (ДКП)

На рис.1 показані результати компресії зображення із фактором стискання 1:60. Візуально якість зображення для вейвлет-перетворення виглядає кращою, але для кількісної характеристики якості методикою, запропонованою у [1], були розраховані співвідношення сигнал/шум. Результати порівняння алгоритмів jpeg і перетворення Хаара демонструють перевагу останнього, але на декілька децибел (в залежності від сюжету зображення, коефіцієнта стискання тощо). Натомість суб'єктивні оцінки вказують на більш суттєві відмінності якості. Саме з цієї причини нами було запропоновано інший підхід. Його ідея полягає у застосуванні алгоритмів оптичного розпізнавання образів (OCR), зокрема, розпізнавання тексту. Для реалізації даного підходу були взяті зображення з текстовою інформацією і піддані перетворенням з великим фактором стискання, після чого до декодованих зображень були застосовані алгоритми розпізнавання із подальшим підрахунком кількості помилок.

а) б) в)

Рис. 2. Приклади компресії зображень з текстом

У якості таких алгоритмів розпізнавання були використані різні рушії, зокрема ABBY FineReader і Tesseract. На рис.2 показані приклади компресії зображення із текстовою інформацією (а) для двох методів компресії: вейвлет-перетворення Хаара (б) і ДКП (в).

Результати досліджень однозначно свідчать про перевагу вейвлет-перетворення у порівнянням з ДКП. Так, наприклад, для перетворення Хаара кількість помилок становить на 30-40% менше (в залежності від контрасту зображень) в порівнянні з jpeg форматом при однаковому коефіцієнті стискання 1:50. Застосування альтернативних перетворення для стискання графіки, зокрема перетворення Хаара, має великі перспективи.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Kiely A.; Klimesh M. The ICER progressive wavelet image compressor // The interplanetary network progress report. – 2003. – vol. 42-155. – P. 1-46.

УДК 004 (043.2)

Н. П. Кадет,
Д. О. Озімай,
Національний авіаційний університет, Київ

МЕТОДИ ІНТЕГРАЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Кількість користувачів програмного забезпечення стрімко збільшується, розмір програм та їх складність також невпинно зростає. Це призводить до збільшення кількості людей, задіяних у процесі розроблення програмного забезпечення, та їх впливу на роботу один одного. Разом з цим збільшується складність управління системою загалом, а також ускладнюються процеси, пов'язані з розгортанням окремого сервісу, перевірки його роботи відносно інших сервісів, виконання інтеграційного тестування та можливості незалежної інтеграції виправлень у сховище коду.

Останнім часом стає актуальним обговорення комп'ютерним суспільством питання інтеграції програм. Загальні цілі інтеграції програм можна сформулювати наступним чином: зменшення вартості експлуатації сукупності програм підприємства, збільшення швидкості виконання типових завдань або гарантувати його термін виконання, підвищення якості виконання завдань за рахунок формалізації процесів та мінімізації людського фактору, як основного джерела помилок. Майже не існує інформаційних систем, які самостійно мали змогу задовольнити потреби сучасних підприємств. Середні і великі організації зазвичай експлуатують не менше десятка багатокористувацьких систем, а іноді і тисячі. У цих системах доволі часто обробляються однакові данні – починаючи із довідників та класифікаторів. Для взаємодії програм звичайно використовуються такі методи, як обмін файлами, загальна база даних (БД), віддалений виклик і асинхронний обмін повідомленнями. В цьому переліку немає прямого обміну даними між БД програм: цей метод більш наближений до переміщення даних, ніж інтеграції програм.

Обмін файлами найбільш поширений підхід до організації взаємодії. Це зв'язано з відносною легкістю реалізації, а також існуванням стандартних форматів обміну. Наприклад, більша частина корпоративних інформаційних систем дозволяє завантажувати файли, наприклад у форматі *CSV(Comma Separated Values* – «поля, розділені комами»). Недоліком даного підходу є те,

що якщо необхідно оперувати складними структурами, то прості формати обміну вже не актуальні.

Загальна БД. Даний підхід концептуально дуже простий – декілька інформаційних систем або програм використовують одну БД. Головний його недолік – зв'язок між інтегрованими програмами настільки тісний, що іноді неможливо помітити різницю між ними. Прикладом такого підходу може служити більшість *ERP*-систем, де різні модулі системи використовують одну базу.

Стандарти на віддалений виклик процедур виникли доволі давно, дозволяючи програмному коду, який виконується на одному комп'ютері, викликати код на іншому. Перевагою віддаленого виклику процедур є його синхронність, завдяки цьому виклик виконується негайно. Якщо б виклик був асинхронний, то він би повторювався поки процедура віддаленої програми не була успішно викликана. Основний недолік віддаленого виклику – вимога працездатності усіх задіяних програм в момент взаємодії.

Асинхронний обмін повідомленнями – це, скоріше, єдиний із перерахованих підходів, який відтворювався спеціально для інтеграції інформаційних систем. Ідея концептуально проста і нагадує роботу електронної пошти. Повідомлення гарантовано дійде завдяки механізму черг повідомлень, які звільняють з взаємодіючих систем турботу про надійність мережі передачі даних, працездатності взаємодіючих систем в певний час тощо.Недоліком цього підходу є висока ціна. Система гарантованої доставки на основі черг повідомлень зазвичай сама по собі не дешева. Але, є і вільно поширювані безкоштовні (наприклад, *ActiveMQ*), які потрібно розвернути, навчити фахівців, підтримувати, написати адаптери між системою доставки і програмою тощо.

Проаналізувавши основні методи інтеграції програмного забезпечення можна зробити висновок, що всі методи мають позитивні і негативні сторони. При постанові завдання вибору між цими методами потрібно дивитись на тип програм, як вони розташовані і на скільки складну інформацію потрібно буде передавати між програмами.

УДК 004.42 (043.2)

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

ТЕХНОЛОГІЧНИЙ ПРОЦЕС ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

На весь життєвий цикл (ЖЦ) системи поширюється технологія проектування інформаційної системи (ІС).

Технологія проектування ІС – створення або модернізація її проекту на основі використання методів і засобів проектування [1].

Основою технології проектування ІС є технологічний процес. Пов'язана з розробленням її проекту діяльність колективу спеціалістів, яка має задовольняти потрібні споживчі властивості й умови ефективності при використанні відповідних засобів проектування та виділених ресурсів.

На кожній стадії проектування (передпроектне обстеження, створення технічного і робочого проектів, упровадження, модернізація та супровід) існує своя технологія його проведення з відповідними технологічними процесами, що відображають особливості виконання проектних робіт саме на цій стадії [1, 2].

Через те, що у процесі проектування ІС застосовуються різні засоби, технологія проектування має бути формалізована. Доцільно для кожного засобу створювати технологію його використання при проектуванні ІС, побудовану за формалізованим каноном. Таким чином, розробник ІС може користуватися будь-якими засобами проектування. Основою для формалізації є технологічна операція (ТО) проектування – відносно самостійний фрагмент технологічного процесу, в якому визначено вхід (X), вихід (Y), перетворювач (C), ресурси (R) і засоби (S).

Графічна інтерпретація ТО може бути подана так (рис.1).

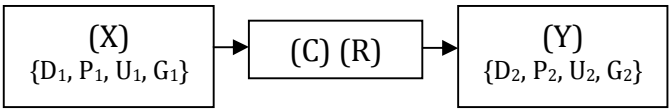


Рис.1 – Технологічна операція

Перетворювач (С) – методика, формалізований або машинний алгоритм перетворення входу ТО на її вихід.

Ресурси (R) – нормовані значення трудових, матеріальних, технічних (машинних) ресурсів, необхідні для виконання перетворювача за допомогою відповідних засобів проектування (S).

Засоби проектування (S) – ТПР, ППП, типові проекти ІС, інструментальні засоби проектування.

Документи (D) – фіксують факти, умови, вимоги, кількісні та якісні параметри.

Параметри (P) – це характеристика, умови або певні обмеження проектної системи. Наприклад, обсяг фінансування, виділений на проектування системи, календарна доба проектування, площа, виділена під обчислювальний центр та ін.

Універсум (U) – повний перелік можливих значень певного компонента технічного забезпечення або обсяг знань про нього. Універсум може містити перелік та опис СУБД, перелік та характеристики ТПР тощо.

Програма (G) – програмні рішення з реалізації заданої функції управління або з оброблення даних.

Усю сукупність перетворювачів, що визначають зміст відповідних ТО для створення ІС, можна поділити на кілька великих класів: пошук і вибірка інформації, створення універсальних універсумів, управління метаданими, вибір загальносистемних проектних рішень, використання інструментальних засобів проектування, параметризація компонентів ІС, перетворення алгоритмів і програм, проведення контролю, формалізація розрахунку показників [3].

Процес проектування ІС можна формально описати, якщо відомо повний набір ТО, потрібних для створення відповідного проекту, то існує також формалізований алгоритм побудови ІС.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Соммервил Иан. Инженерия программного обеспечения, 6-е издание /Иан Соммервил. – М.: Вильямс, 2002. – 624 с.

2. Орлов С.А. Технологии разработки программного обеспечения. Разработка сложных программных систем / С.А. Орлов – СПб.: Питер, 2002. – 464 с.

3. Кірхар Н.В. Аналіз технологій проектування інформаційних систем. Проблеми інформатизації та управління: зб. наук. праць - Київ – 2015. – №4 (52). – С.45–49.

УДК 004.047 (043.2)

Н. А. Ковалев, к.т.н.
Национальный авиационный университет, Украина

АППАРАТНАЯ РЕАЛИЗАЦИЯ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ

Использование булевых функций (БФ) позволяет повышать стойкость современных шифров к методам криптоанализа [1]. Значительный рост сложности логических задач делает целесообразным исследования нетрадиционных представлений и исчислений БФ. Одно из таких направлений представляет позиционная алгебра логики (ПАЛ) [2].

В отличие от булевой алгебры в ПАЛ БФ представляются и исчисляются с полиномиальной сложностью на основе принципов позиционности, используя аппарат позиционных операторов и эквивалентных преобразований. Это позволяет арифметизировать и распараллеливать логические вычисления.

Предложен способ построения комбинационных схем (КС) для реализации значительного числа БФ с помощью произвольного l - преобразования и простого позиционного *S*-оператора:

$$z = l_k^{r,w} S_j^n (X_n).$$

На рис.1 в обозначениях САПР Altera Quartus II приведена структура таких КС, на входы которых подаются: *n*-разрядный

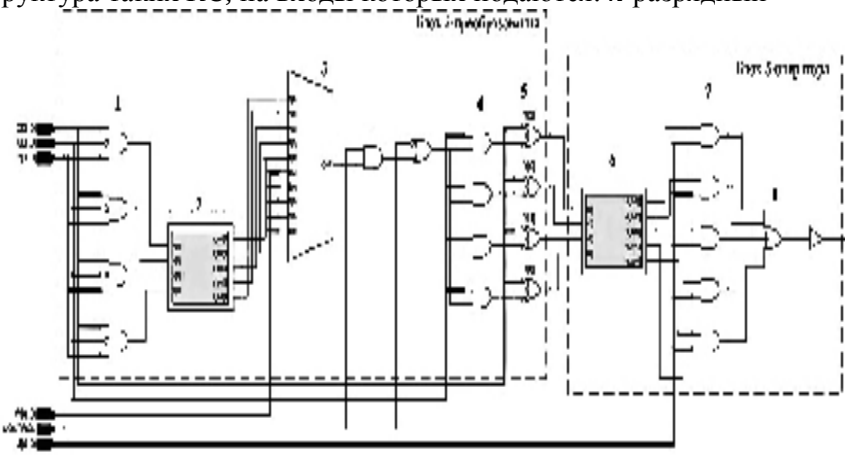


Рис. 1. КС для реализации БФ

входной набор аргументов X_n; (n+1)-разрядный вектор j позиционного S-оператора; n-разрядные параметры k, r и (n+1)-разрядный параметр ω l-преобразования; сигнал управления типом l-преобразования. КС состоит из блоков l-преобразования и S-оператора, включая: логические вентили «И» 1, 4, 7; исключающего «ИЛИ» 5; «ИЛИ» 8; компаратор 3; КС определения числа единиц входных наборов 2 и 6.

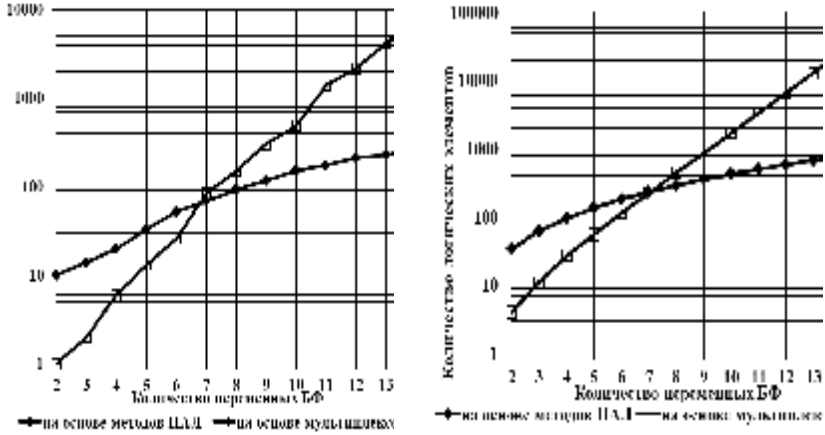


Рис. 2. Сложность по Квайну и ресурсоемкость сравниваемых КС при их реализации на базе FPGA

Аппаратная сложность по Квайну и ресурсоемкость интегральной реализации на базе FPGA (рис. 2) разработанной КС в сравнении с традиционным применением для реализации БФ мультиплексора при n>8 уменьшается в разы, затем – на порядки.

Таким образом, реализации БФ от большого числа переменных с применением аппарата ПАЛ могут успешно конкурировать с известными способами реализации БФ и эффективно применяться в криптопроцессорах на основе ПЛИС.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Нелинейные булевы функции: бент-функции и их обобщения / Токарева Н Н. – Saarbrucken, Germany: Издательство LAP LAMBERT Academic Publishing, 2011. – 180 с.

2. Тельпиз М.И. Принцип позиционности для счисления и исчисления функций / М.И. Тельпиз – М.: ИКИ РАН, 2001. – 457 с.

УДК 519.81(075.8)

И. А. Коваленко (ДНТБ Украина)
О. Г. Коврижкин, д.т.н.,
Национальный авиационный университет, Киев

СИСТЕМА ПРОТИВОДЕЙСТВИЯ СРЕДСТВАМ ПЕРХВАТА УПРАВЛЕНИЯ БПЛА

Проблема соревновательного противодействия двух антагонистических технических систем, чаще известная как «броня-снаряд», в полной мере присутствует и в интенсивно развивающейся области использования беспилотных летательных аппаратов (БПЛА). После периода использования БПЛА в информационно-вспомогательных целях (фото-видео разведка, ретрансляторы и т.п.), явственно это проявилось при появлении, так называемых «ударных» БПЛА способных нести оружие и наносить существенный ущерб противнику.

Основными методами борьбы с БПЛА противника остаются непосредственное применение средств ПВО и средств радиоэлектронной борьбы (РЭБ). Разрабатываемая авторами система предназначена для противодействия средствам РЭБ.

При использовании РЭБ применяются такие основные методы:

- «ослепление» систем навигации и управления БПЛА с применением мощного шумового подавления сигналов;
- искажение навигационных сигналов (прежде всего, имитация сигналов систем спутниковой навигации большей мощности);
- расшифровка системы команд от операторов управления и их «перехват на себя».

В свою очередь, системы управления БПЛА, в основном, используют три метода (чаще их взаимное комплексирование):

- навигация по сигналам от внешних источников (радиомаяки, спутники, ретрансляторы и т.п.);
- автономная навигация с использованием бортовых средств, как правило, бесплатформенных инерциальных систем (БИНС);
- непосредственное использование управляющих сигналов от оператора (с базовой станции или от промежуточных пунктов управления).

Основная проблема автономных защищенных режимов навигации от БИНС, «дальше летим – больше ошибка». Поэтому и

используют независимые от времени полета «внешние» источники, к сожалению, подвергаемые риску искажения.

Существуют способы шифрования «своих» сигналов управления и, соответственно, способы «взлома» этой защиты. Рассматриваемой авторами проблемой защиты от средств РЭБ – является распознавание факта подавления (простейший случай), искажения или перехвата сигналов навигации/управления. Автономное (на борту) распознавание факта появления ложных сигналов позволяет системе игнорировать несанкционированные сигналы и осуществить переход на защищенный режим работы навигационной системы (от БИНС). Что позволит выполнить маневр - «возврат на исходный/заданный конечный пункт маршрута» или даже завершить задание в автономном режиме.

В [1,2] предложены методы создания подсистемы искусственного интеллекта, основанные на использовании нечеткого структурного графа. При работе используется эксперты. На борту анализ ситуации якобы выполняет «опытный оператор».

В [3] предложен поход к построению защищенных систем управления БПЛА, рассмотрены методы навигации с использованием БИНС.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Коврижкін О. Г. Формирование компромиссных правил нечеткого вывода // Техн. кібернетика. − 1992. - № 5. - С. 50-55.

2. Коврижкін О. Г. Аксиоматика имитационной модели принятия решений // Материалы международной конференции: Интеллектуальные системы принятия решений и проблемы вычислительного интеллекта (isdmcI”2009). – 2009 г., Евпатория, Украина, том 1. с.181.

3. Коврижкін О.Г., Коваленко І. А. Создание программного обеспечения интегрированных БИНС для беспилотных ЛА // Матеріали конференції: Сучасний стан і перспективи розробки, застосування БПЛА в Україні, НЦВПСУ. − Київ, 2004. − с.42.

UDC 004.75

S. A. Kudrenko,
National Aviation University, Kyiv

APPLICATION JPPF TO COMPLEX COMPUTATIONAL PROBLEMS

Nowadays, the range of tasks that require for their solution the use of powerful computing resources, is constantly expanding. This is due to the fact that there have been fundamental changes in the organization of scientific research. As a result of the widespread introduction of computer technology, has significantly increased area of numerical simulation and numerical experiment.

Java Parallel Processing Framework is a grid tool that makes it easy to run applications in parallel. A brief feature list of JPPF includes: API support for delegation of parallelized tasks to local and remote nodes, user interface tools for task administration and monitoring functions, Java Swing-based user interface, real-time adaptive load balancing, scalable to an arbitrary number of nodes, fail-over and recovery support. limited code intrusiveness, runs on Linux and several Windows variants.

There are many clustering methods available, and each of them may give a different grouping of a dataset. The choice of a particular method will depend on the type of output desired, The known performance of method with particular types of data, the hardware and software facilities available and the size of the dataset. In general , clustering methods may be divided into two categories based on the cluster structure which they produce. The non-hierarchical methods divide a dataset of N objects into M clusters, with or without overlap.

These methods are sometimes divided into partitioning methods, in which the classes are mutually exclusive, and the less common clumping method, in which overlap is allowed. Each object is a member of the cluster with which it is most similar, however the threshold of similarity has to be defined. The hierarchical methods produce a set of nested clusters in which each pair of objects or clusters is progressively nested in a larger cluster until only one cluster remains. The hierarchical methods can be further divided into agglomerative or divisive methods. In agglomerative methods, the hierarchy is build up in a series of N-1 agglomerations, or Fusion, of pairs of objects, beginning with the un-clustered dataset. The less common divisive methods begin with all

objects in a single cluster and at each of N-1 steps divide some clusters into two smaller clusters, until each object resides in its own cluster.

The partitioning methods generally result in a set of M clusters, each object belonging to one cluster. Each cluster may be represented by a centroid or a cluster representative; this is some sort of summary description of all the objects contained in a cluster. The precise form of this description will depend on the type of the object which is being clustered. If the number of the clusters is large, the centroids can be further clustered to produces hierarchy within a dataset.

- Single Pass: A very simple partition method, the single pass method creates a partitioned dataset as follows:
- Make the first object the centroid for the first cluster.
- For the next object, calculate the similarity, S, with each existing cluster centroid, using some similarity coefficient.
- If the highest calculated S is greater than some specified threshold value, add the object to the corresponding cluster and re determine the centroid; otherwise, use the object to initiate a new cluster. If any objects remain to be clustered, return to step 2.

As its name implies, this method requires only one pass through the dataset; the time requirements are typically of order O(NlogN) for order O(logN) clusters. This makes it a very efficient clustering method for a serial processor. A disadvantage is that the resulting clusters are not independent of the order in which the documents are processed, with the first clusters formed usually being larger than those created later in the clustering run.

Clustering lies at the heart of data analysis and data mining applications. The ability to discover highly correlated regions of objects when their number becomes very large is highly desirable, as data sets grow and their properties and data interrelationships change.

REFERENCES

1. Cluster Computing [Web resource]. – Access mode - link.springer.com/journal/10586

2. Boden, N.J. Cluster Computing and Applications / Boden N.J. – M: ДМК, 2010. – p. 454.

УДК 004.272.3

О. С. Маковець,
Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського», Київ

МЕТОД ВИЯВЛЕННЯ ПРОГРАМ-ВИМАГАЧІВ ЗА ОЦІНКОЮ СКЛАДНОСТІ БІНАРНОГО КОДУ

На сьогоднішній день проблема виявлення програм-вимагачів стає однією з найсерйозніших задач кібербезпеки: атаки стають складнішими, цілеспрямованішими, збитки зростають і зашифровані дані рідко можна відновити.

Статистичні дані показують, що ransomware-програми є серйозною проблемою для інформаційної безпеки:

- 60% завантажень зловмисного програмного забезпечення в першому кварталі 2017 року були програми-вимагачі [1].
- атаки програм-вимагачів зростають на 350% щорічно [2], за період з 2015 року по 2016 рік кількість атак збільшилась з 1000 атак на день до 4000 [3].

На сьогодні немає єдиного засобу захисту та запобігання атакам програм-вимагачів. Подібний тип атак легше передбачити, ніж усувати наслідки.

У 2017 році найчастіше проходило зараження наступними програмами-вимагачами: WannaCry, Locky, CryptoLocker, Jaff, CryptoWall [4].

Використовуються різноманітні техніки впровадження ransomware до системи, найчастіше використовуються вразливості ОС Windows. Зазвичай дані шифруються алгоритмом RSA, в більш високорівневих атаках шифрування відбувається за алгоритмом AES; при своїй роботі код відкриває, прочитує і закриває файл, потім записує зашифрований файл з видозміненим ім'ям і видаляє первинний(нешифрований). Шифруванню підлягають заздалегідь розглянуті розширення файлів, тож код спочатку порівнює і шукає файли необхідних розширень. Шифруються не тільки жорсткі диски, а також зйомні, RAM диски та мережні. Застосовуються різні техніки обфускації та схеми приховування коду. Найчастіше неможливо розшифрувати файли, як вручну, так і після сплати.

Для виявлення зловмисних програм використовуються наступні види аналізу коду: сигнатурний, динамічний та статистичний. Для ransomware-програм сигнатурний аналіз не підходить так, як для

подібних атак сигнатур ще немає, або код обфусковано, що унеможливлює виявлення сигнатур. Динамічний аналіз також є проблематичним, так, як при запуску зловмисний код розпочне шифрування даних і заблокує станцію, або код може визначити запуск в пісочниці. Також вразливості в деяких віртуальних машинах дозволяють зловмисному коду вийти за межі віртуальної середи. В роботі розглянутий статичний аналіз коду, адже він не потребує запуску. Складність коду програм-вимагачів має бути вища від звичайних програм, так, як використовується шифрування, зазвичай обфускація ускладнює код і кількісно структура програми є складнішою від звичайного ПЗ.

Для статичного аналізу використовуються наступні метрики складності бінарного коду, враховуючи особливості ransomware-програм: інформаційна складність модуля щодо структури даних (метрика складності потоку даних програми), метрика Холстеда (кількісна метрика) та метрика Харрисона і Мейджела (метрика складності потоку керування програми). Розглянуті метрики враховують, як кількісну складність програми, враховуючи її логіку, так і достатньо оглядають внутрішню структуру, враховуючи вкладеність і звернення до структури даних.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Cybercrime Tactics and Techniques Q1 2017 [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.malwarebytes.com/pdf/labs/Cybercrime-Tactics-and-Techniques-Q1-2017.pdf.

2. Ransomware Lessons for the Financial Services Industry [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://blogs.cisco.com/financialservices/ransomware-lessons-for-the-financial-services-industry.

3. How to Protect your networks from Ransomware [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.justice.gov/criminal-ccips/file/872771/download.

4. Number of ransomware attacks worldwide from 2014 to 2016 (in millions) [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/.

УДК 004.77

М. М. Орлова, к.т.н.,
Г. В. Щербакова,
Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського», Київ

ПОРІВНЯННЯ ТА АНАЛІЗ АЛГОРИТМІВ УЩІЛЬНЕННЯ ВЕЛИКИХ ОБСЯГІВ ДАНИХ

Характерною особливістю більшості типів даних є їх надлишковість. При передачі та збереженні великих обсягів інформації надмірність відіграє негативну роль, оскільки вона не тільки призводить до збільшення часу передачі та її зберігання, а й до зростання сукупної вартості. В зв'язку з цим на сьогоднішній день для забезпечення ефективності передачі великих обсягів інформації широко використовуються алгоритми ущільнення.

Метою роботи є дослідження та аналітичне порівняння алгоритмів ущільнення великих обсягів інформації та розробка модифікованої версії алгоритму на основі отриманих результатів.

На поточний час алгоритми ущільнення без втрат, умовно можна розділити на дві великі групи.

1. Потокові та словникові алгоритми. До цієї групи належать алгоритми сімейств RLE (Run-Length Encoding), LZ (Lempel-Ziv). Особливістю всіх алгоритмів цієї групи є те, що при кодуванні використовується інформація про послідовності, що зустрічалися раніше [1].
2. Алгоритми статистичного (ентропійного) ущільнення. Ця група алгоритмів стискає інформацію, використовуючи нерівномірність частот, з якими різні символи зустрічаються в повідомленні. До алгоритмів цієї групи відносяться алгоритми Шеннона-Фанно та Хаффмана [1].

У цій роботі представлено аналітичне порівняння чотирьох алгоритмів: RLE, LZ, Шеннона-Фанно та Хаффмана. Для порівняння використовуються наступні критерії: коефіцієнт ущільнення та коефіцієнт збереження.

У таблиці 1 наведено порівняння алгоритмів.

Таблиця 1

Порівняння алгоритмів ущільнення інформації

	RLE	LZ	Алгоритм Хаффмана	Алгоритм Шеннона-Фано
Розмір оригінальних даних (байт)	188 223	188 223	188 223	188 223
Коефіцієнт ущільнення (%)	100.45	49.61	62.62	63.76
Коефіцієнт збереження (%)	0.45	50.39	42.24	40.51

Відповідно до отриманих результатів алгоритми Хаффмана и Шеннона-Фано показали найкращі результати.

На основі отриманих результатів розроблено модифікований алгоритм Хаффмана, який працює наступним чином.

1. Дані стискаються за допомогою динамічного методу зменшення біт.
2. Виявлення унікальних слів.
3. Використання кодування Хаффмана для отримання кінцевого результату.

Дослідження показали, що в середньому запрпонована версія дозволяє збільшити коефіцієнт збереження на 11%.

Таким чином проведено дослідження та порівняння чотирьох алгоритмів ущільнення даних. Алгоритм Хаффмана показав себе як найбільш ефективний. На основі проведеного аналітичного порівняння запропоновано модифіковану версію алгоритму, яка дозволяє отримати покращені результати порівняно з існуючими алгоритмами в середньому на 11%.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Ватолин Д.С. Алгоритмы сжатия изображений. Методическое пособие / Д.С. Ватолин. – М.: Издательство МГУ, 1999. – 200 с.

УДК 004.415.2 (043.2)

М. С. Панасенко,
І. О. Тюрменко,
В. М. Боровик, к.т.н.
Національний авіаційний університет, Київ

СИСТЕМА ОБЛІКУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ДЛЯ СТУДЕНТІВ STUDFUTURE

В наші дні інформаційні джерела розвиваються дуже швидко, об'єм інформації, який ми використовуємо, також стрімголов росте. Новини, статті, замітки, навчальні матеріали, розважальні ресурси – сучасна людина потопає в шаленому потоці інформації. Що ж говорити про студентів, які як ніхто усвомлюють проблему фільтрації та централізації інформації. У великих установах та на підприємствах існують централізовані інформаційні системи, які допомагають бути в курсі всіх подій, швидко знаходити актуальну інформацію та підтримувати контакт із колегами. Швидкість передачі інформації та її доступність в таких системах грають не далеко не останню роль.

Часто-густо контроль та відслідковування потоку інформації перетворюється в проблему, особливо, якщо вона має різні джерела і призначена для різних сфер застосування. В таких умовах студентам надзвичайно складно бути в курсі всіх подій, новин і корисної інформації, яка пов'язана з університетом та студенським життям взагалі. Для пошуку потрібних данних доводиться мандрувати із сайту на сайт, з однієї спільноти в соціальній мережі до іншої, що в результаті призводить до такого явища як “Bad UX” (англ. Bad User Experience), дослівно з англійської «поганий досвід користувача» Вирішенням даної задачі буде створення централізованої системи обліку інформаційних ресурсів для студентів StudFuture.

Дана ідея реалізується у вигляді веб-системи, що забезпечить швидкий та зручний доступ до актуальних для студента інформаційних ресурсів та сервісів в режимі онлайн. Система включатиме в себе принципово нові для таких систем модулі, посилання на вже існуючі ресурси та оновленні рішення інформаційних проблем. Тобто основна мета системи – це централізувати вже існуючі інформаційні ресурси, додати нові рішення та оновити вже існуючі.

Структурно система включатиме в себе такі модулі:

- Посилання на корисні інформаційні ресурси;
- Посилання на детальну карту НАУ;
- Інформація про гуртки, клуби, спортивні секції, студентську раду, творче об'єднання студентів тощо;
- Студентські проекти та стартапи;
- Вакансії для судентів;
- Календар студентських подій;
- Знижки для студентів;
- Онлайн-здача лабораторних та домашніх завдань;
- Методичні рекомендації, лекції, навчальна література, інтерактивні навчальні ресурси;
- Актуальний розклад пар, модульних контрольних, екзаменів, консультацій;
- Віртуальна екскурсія по університету;
- Промо-лекції викладачів.

Дана система забезпечить тісний взаємозв'язок між користувачами заради створення найкращих умов для розвитку студентів. Після реалізації цього проекту студентам буде набагато простіше й легше орієнтуватися в подіях університету і не тільки, користувачі будуть оперативно отримувати актуальні новини, зможуть в будь-який момент дізнатися інформацію про спільноти та проекти, які їм цікаві. Система зблизить викладачів, студентів, організаторів подій, роботодавців та абітурієнтів, допоможе зав'язати нові знайомства. В перспективі дана система буде працювати не тільки для студентів НАУ, а також і для студентів інших університетів по всій Україні.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Ergonomics of human-system interaction -- Part 420: Selection of physical input devices [Електронний ресурс] // International Organization for Standardization. – 2011 https://www.iso.org/standard/52938.html.

УДК 004.4:001.102:006.35(100)ISO (043.2)

Н. В. Пащенко,
О. В. Самойліченко, к.т.н.
Національний авіаційний університет, Київ

РИЗИК-ОРІЄНТОВАНА ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ ПРОЦЕСАМИ ЛАБОРАТОРІЇ

З появою нової редакції стандарту ДСТУ ISO 9001:2015 в сфері систем управління якістю почала впроваджуватись концепція управління ризиками та можливостями. Вона знайшла відображення і у новій версії ДСТУ ISO/IEC 17025:2017 [1] та ДСТУ EN ISO 15189:2015 «Медичні лабораторії. Вимоги до якості та компетентності».

Стандарт [1] вимагає від випробувальних лабораторій планування та реалізації заходів з управління ризиками і можливостями. Такі заходи створюють основу для підвищення ефективності системи управління, поліпшення результатів та запобігання негативних наслідків та потенційних збоїв у своїй діяльності. Крім того, даний стандарт містить вимоги до системи управління інформацією лабораторії, такі як захищеність від несанкціонованого доступу, забезпечення цілісності даних та інформації, реєстрація помилок системи та відповідних негайних та коригувальних дій.

Серія стандартів ISO 31000 містить принципи та загальні вказівки з ефективного виявлення та керування ризиками, розробки, постійного покращення та інтеграції процесу керування ризиками в загальну систему упарвління. Тому для розробки ризик-орієнтованої інформаційної системи управління процесами лабораторії необхідно врахувати і даний стандарт.

В цілому процедура управління ризиками складається з наступних етапів: визначення області застосування (які процеси будуть піддані аналізу); ідентифікація небезпек та подій, які призводять до реалізації небезпеки; оцінка небезпек за кількома параметрами; визначення прийнятності оцінених ризиків; розробка плану із зменшення ризиків; проведення risk/benefit аналізу (якщо зниження ризику з певних причин недоцільно або неможливо); виконання плану із зменшення ризиків; виявлення ризиків, які виникли в результаті реалізації плану зі зниження ризиків; оцінка загального остаточного ризику; моніторинг.

Для визначення переліку ризиків в лабораторії можна використовувати доступну інформацію про типові ризики, потім побудувати діаграму Ісікава («рибна кістка») і карту процесів лабораторії, які будуть доповнюватися при проведенні внутрішніх аудитів. Необхідно оцінити, як мінімум, п'ять компонентів процесу тестування для потенційних збоїв та помилок: зразок, систему тестування, реагенти, навколишнє середовище, тестування персоналу. Також можливі організаційні та фінансові ризики.

Використання інформаційної системи управління процесами лабораторії дозволяє автоматизувати процес прийому замовлень, складання завдання на проведення випробувань, розрахунок результатів вимірювань, невизначеностей та інших значень, формування протоколів випробувань, а також ряду фінансових документів, необхідних для виконання замовлення.

Щоб відповідати вимогам до управління та технічним вимогам стандартів [1] та ДСТУ EN ISO 15189:2015, інформаційна система має містити модуль управління ризиками та можливостями, що передбачає внесення індикаторів якості, обчислення оцінок ризиків та розгляд запобіжних дій.

Як показав досвід впровадження стандартів з компетентності медичних [2] та випробувальних (калібрувальних) лабораторій [3], існуючі інформаційні системи не забезпечують виконання вимог до управління ризиками та можливостями. Тому створення такої інформаційної системи є актуальним питанням.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. ДСТУ ISO/IEC 17025:2017 Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій. – ISO, 2017. – 30 с.

2. Мокійчук В.М., Рамазанова-Стьопкіна О.А. Впровадження стандарту ДСТУ EN ISO 15189:2015 у практику медичних лабораторій. Метрологічні аспекти // Практика управління медичним закладом №3, ТОВ «Пресс Альянс», 2016. – С.84-87.

3. Рубан Я.І., Мокійчук В.М. Досвід впровадження стандарту ДСТУ ISO/IEC 17025:2006. Technical Using of Measurement: 2016 тези доповідей Всеукраїнської науково-технічної конференції молодих вчених у царині метрології.

УДК 629.735.33.073 (043.2)

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

ПРО ВПЛИВ НА БЕЗПЕКУ ПОЛЬОТІВ ЗСУВУ ВІТРУ НА МАЛИХ ВИСОТАХ

Світова статистика свідчить, що близько 36% усіх катастроф на авіаційному транспорті відбувається на етапах заходу на посадку та посадки. Якщо ж врахувати, що їх тривалість у середньому не перевищує (3-4)% загального часу польоту середньомагістрального літака, то рівень безпеки польоту на цих етапах є нижчим у десятки разів, ніж рівень безпеки протягом усього польоту [4].

До багатьох чинників, які негативно впливають на рівень безпеки польотів, відносяться технічні, організаційні, людські чинники, а також різноманітні атмосферні явища: тумани, грози, опади, хмари, вітер, зокрема, його зсув на малих висотах тощо.

Зсув вітру визначається як векторна різність швидкостей вітру в двох точках повітряного простору, віднесена до відстані між ними. У залежності від просторової орієнтації цих двох точок він поділяється на вертикальний та горизонтальний. Причому, зсув вітру може бути як додатним, так і від'ємним [3].

Проблема безпеки польотів в умовах зсуву вітру є багатогранною, тому її вирішення здійснюється за різними напрямками. Одним з них є розроблення та удосконалення рекомендацій екіпажу щодо дій при попаданні в зону цього небезпечного атмосферного явища за результатами математичного моделювання динаміки польоту літаків різних класів.

Дослідження заходу на посадку середньомагістрального літака за сигналами глісадного радіомаяка в режимах автоматичного та штурвального управління в умовах вертикального зсуву вітру різної інтенсивності показують, що на завершальній фазі етапу заходу на посадку, коли літак у посадковій конфігурації знижується по глісаді, маючи критичні запаси швидкості та висоти, найбільш небезпечним для безпеки польоту є додатний зсув вітру, який викликає зменшення повітряної швидкості літака по мірі зменшення висоти [1].

Зазначимо, що на можливість успішного завершення заходу на посадку та здійснення посадки літака впливає не лише

інтенсивність зсуву вітру, але й часове запізнення втручання пілота в управління літаком після початку дії цього атмосферного явища.

Несвоєчасне виявлення моменту попадання літака в зону зсуву вітру та запізнення втручання пілота в управління роблять безпечну посадку літака проблематичною через його значну «просадку» відносно глісади і він повинен уходити на друге коло.

Відповідно до вимог нормативних документів ІСАО, ухід на друге коло повинен починатися для літаків усіх класів не нижче висоти прийняття рішення в схемах точного заходу на посадку або в указаній точці схем неточного заходу на посадку не нижче мінімальної висоти зниження. При уході на друге коло набір висоти повинен здійснюватися, як правило, по прямій із запасом висоти над перешкодами не менше 50 м [2].

Так звані мінімуми ІСАО при заході на посадку визначаються за спеціальними методиками, які враховують швидкість руху літака, висоту перешкод у зоні посадки, відповідність наземних та бортових систем встановленим вимогам та кваліфікацію пілота.

Тобто нормативні документи ІСАО щодо висоти прийняття рішення та уходу на друге коло в умовах зсуву вітру не враховують прийомистість двигунів, масово-інерційні, аеродинамічні, пілотажні характеристики літака, зокрема, вертикальну швидкість зниження під час його руху по глісаді, а також інтенсивність зсуву вітру та своєчасність виявлення попадання літака в зону його дії. Тому ці нормативні документи потребують уточнення та доповнення для літаків різних класів з урахуванням викладеного.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Бабич Я.О. Особливості заходу на посадку літака в режимах автоматичного та штурвального управління в умовах вертикального зсуву вітру / Я.О. Бабич, А.О. Бочелюк, А.В. Полухін // Проблеми інформатизації та управління. Зб. наук. праць. – К.: НАУ, 2017. – Вип. 4 (60). – С. 5-11.

2. Производство полетов воздушных судов // Издание пятое (с поправками). Doc 8168 OPS/611/ Том 1. Правила производства полетов. ИКАО: 2006. – 386 с.

3. Руководство по сдвигу ветра на малых высотах // Издание первое (с поправками). Doc 9817 AN/449. ИКАО: 2005. – 264 с.

4. Statistics. Causesof Fatal Accidents. Fatalities by Phaseof Flight.– URL: http://www.planecrashinfo.com/cause.htm.

УДК 004.94:004.422 (043.2)

Н. О. Рибасова,
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ПРОЕКТУВАНЯ З SPARX ENTERPRISE ARCHITECT

Розглядаються особливості проектування і конструювання програмного забезпечення за допомогою сучасного CASE-інструменту Sparx Enterprise Architect (EA). EA є багатофункціональним додатком, що повністю підтримує специфікацію UML2.0.

Основними ключовими функціями EA є:

- створення елементів UML;
- розміщення цих елементів на діаграмах та в пакетах;
- створення коннекторів між елементами;
- документування створених елементів;
- генерація коду сконструйованої моделі;
- реверс-інжиніринг з готового коду.

Форвард та реверс-інжиніринг можна виконати на ActionScript, C++, C#, Delphi, Java, Python, PHP, VB.NET і Visual Basic.

Також є можливість моделювати бізнес-процеси, веб-сайти, користувацькі інтерфейси, сіті, конфігурації апаратного забезпечення, оцінювати розмір трудовитрат проектних робіт в годинах, фіксувати вимоги, ресурси, тест-плани, дефекти і запити на зміни.

Особливістю EA є високопродуктивний репозитарій моделей, що дозволяє команді незалежно один від одного працювати над проектом. EA здійснює з'єднання через власний драйвер БД з проектним репозитарієм, що організований у вигляді бази даних. В якості БД по умовчанню використовується Microsoft Jet. Також, як сервер БД можуть використовуються SQL Server, MySQL, Oracle 9i і 10g, PostgreSQL, Adaptive Server Anywhere, MSDE Server, Progress OpenEdge.

В проектному репозитарії зберігаються наступні елементи моделювання: об'єкти моделі, такі як UML-елементи та пакети, коннектори, що зв'язують взаємодіючі об'єкти, діаграми, що відображають об'єкти та коннектори і посилання на інші діаграми.

Також в репозитарії зберігається додаткова і службова інформація: додаткові довідники, довідники в яких зазначені типи

стереотипів, шаблони звітів, шаблони проектування, такі як UML паттерни і UML профілі, що дозволяють швидко відтворити типові рішення, змодельовані раніше, моментальні знімки пакетів в XML форматі. Для обміну інформацією між репозитаріями використовується експорт/імпорт файлів XML формату.

Ще однією особливістю EA є симуляція бізнес-процесів, що дозволяє в динаміці перевірити правильність процесів та краще зрозуміти роботу всієї бізнес-системи.

Особлива увага в EA приділяється управлінню вимогами:

- вимоги можна фіксувати в системі;
- задавати користувацький атрибут вимогі у відповідності з потребами;
- групувати, трасувати, встановлювати зв'язки між різними вимогами, групами вимог;
- вести роботи по дефектам, змінам, тестам;
- використовувати вимоги для планування задач;
- працювати з варіантами використання та їх моделями.

EA має потужні інструменти для генерації документації і звітів з повним редактором шаблонів WYSIWYG, це дає можливість згенерувати детальні звіти на основі необхідної інформації та в потрібному форматі.

В EA вбудований Automation Interface, що забезпечує доступ до внутрішніх процесів моделей. Ось деякі задачі які можна виконати з його допомогою:

- автоматично згенерувати і опублікувати щоденні звіти HTML в інтернеті;
- записати задачі що повторюються;
- згенерувати код із кінцевої діаграми;
- створити користувацькі звіти .

Отже, Enterprise Architect це потужний сучасний інструмент котрий підтримує всі аспекти циклу розробки, забезпечуючи повне трасування від початку проектування до розміщення та підтримки продукту. Також цей CASE засіб придатний для використання в навчальному процесі, має зрозумілий інтерфейс, який можна налаштувати під власні потреби та є досить популярним додатком в іноземних навчальних закладах.

УДК 004.451.44

О. В. Русанова, к.т.н.,
О. В. Корочкін, к.т.н.,
Л. В. Любарська
Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського», Київ

СПОСІБ ПЛАНУВАННЯ ОБЧИСЛЕНЬ ДЛЯ ГЕТЕРОГЕННИХ МУЛЬТИЯДЕРНИХ КОМП'ЮТЕРНИХ СИСТЕМ

Згідно з останньою 50-ї редакцією списку *TOP-500* найпотужніших комп'ютерних систем, найефективніші з них мають кластерну архітектуру, в яких використовуються багатоядерні процесори, причому кількість ядер постійно збільшується. Так, у найпотужнішій системі у світі *Sunway TaihuLight* використовуються багатоядерні 64-бітові RISC процесори, загальна кількість процесорів у системі - 40 960, кожен процесор містить 4 керуючих ядра загального призначення і 256 обчислювальних RISC-ядер, що в сукупності дає 10 649 600 ядер. Така система не є повнозв'язаною топологією. Швидкість обчислень системи більш ніж в 2,5 рази вище в порівнянні з попереднім світовим рекордсменом *Tianhe-2*. Крім того, з кожним роком збільшується кількість сопроцесорів у системах (у 50-й редакції *TOP-500* збільшилась кількість таких систем на 19%), що впливає на їх гетерогенність. Відомо, що реальна продуктивність систем пов'язана з ефективним плануванням обчислень. Сьогодні підвищення ефективності планування в першу чергу залежить від якості врахування основних характеристик, таких як топологія, багатоядерність процесорів та гетерогенність комп'ютерних систем.

У даній роботі аналізуються відомі алгоритми планування, які можуть бути використані для таких систем. Розглядаються три найвідоміші підходи, а саме: гібридний генетичний алгоритм *HGAHS*; списковий алгоритм планування *SHTS (HCPPEFT)* з використанням дублювання та алгоритм планування для мультиядерних систем *SAMCS*.

Перший алгоритм спочатку генерує список підзадач, згідно з їх пріорітетами. Далі, відбувається призначення на процесори за допомогою генетичного алгоритму. Алгоритм *HGAHS* підходить

для гетерогенних систем, але він не розрахований на мультиядерну архітектуру. Другий алгоритм також спочатку формує список підзадач, згідно з пріорітетами, далі відбувається призначення на процесори з використанням дублювання обчислень. Даний алгоритм підтримує тільки повнозв'язну топологію системи. Третій алгоритм спочатку розподіляє підзачі по кластерам, а далі по ядрам. Відбувається розбиття на групи для мінімізації пересилок,в групи об'єднуються найбільше зв'язані підзадачі. Недоліком цього алгоритму є також орієнтованість на повнозв'язні кластерні системи. Таким чином, ні один із алгоритмів не враховує усі характеристики – топологію, багатоядерність та гетерогенність.

У даній роботі пропонується кластерно-списковий ***HTMS*** (Heterogeneous Multicore Task Scheduling) спосіб статичного планування обчислень для підвищення реальної продуктивності гетерогенних мультиядерних кластерних систем, таких як ***Sunway TaihuLight***. Даний алгоритм підходить для систем з будь якою топологією. У роботі розглядаються основні три етапи алгоритму ***HMTS*** такі, як: визначення пріоритетів підзадач згідно з критичним шляхом, кластеризація підзадач, розподіл підзадач по кластерах та ядрах, згідно з мінімальнім часом пересилки (визначається за допомогою моделювання). Кожна підзадача призначається на процесор згідно з її типом (обчислювальна або спеціалізована для сопроцесора).

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Yanyan Dai. A Synthesized Heuristic Task Scheduling Algorithm // Institute of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China, 2014. – 67 p.

2. Xiaozhong Geng, Gaochao Xu, Xiaodong Fu, Yuan Zhang, «A Task Scheduling Algorithm For Multi-Core-Cluster Systems», Journal of Computers, vol.7, n.11, P. 2797-2804, November 2012.

3. Kamaljit Kaur. Heuristics Based Genetic Algorithm for Scheduling Static Tasks in Homogeneous Parallel System // Department of Computer Science & Engineering, Guru Nanak Dev University, Amritsar- 143001, Punjab, India, IJCSS, vol.4, P. 183-198, 2010.

УДК 004.056.53 (043.2)

Є. О. Сидоров,
Л. П. Галата
Національний авіаційний університет, Київ

МЕТОД АНАЛІЗУ ТА КЛАСИФІКАЦІЇ SIEM СИСТЕМ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Сьогодення характеризується досить актуальною проблема виявлення інцидентів порушення безпеки інформації та політик безпеки інформаціх на основі аналізу логів (журналів реєстрації подій) в інформаційних системах. Кількість журналів реєстрації в сучасних системах обчислюється сотнями, а кількість подій – десятками чи сотнями тисяч на добу, що обумовлює необхідність застосування автоматизованих систем – так званих SIEM-систем(Security information and event management systems). Враховуючи те, що на сьогодні на ринку систем захисту присутні багато різноманітних SIEM-систем від різних виробників, актуальною є задача якісного та оптимального (за певними ознаками) вибору SIEM-системи для бізнесу, а також створення комплексного підходу для оцінки якості, що буде враховувати весь перелік критеріїв закладених у систему. Розглянуто вирішення такої задачі та її застосування до лідерів ринку SIEM-систем: системи McAfee Enterprise Security Manager від McAfee, QRadar від IBM та ArcSight від HP.

Як правило, такі питання вимагають інвестування певної суми коштів, а також розкриття деякої внутрішньої інформації бізнесу. І якщо раніше організації більш за все не використовували SIEM-системи, то зараз це є необхідністю для підвищення рівня безпеки інформації. У результаті захищеність даних та інфраструктури таких організацій підвищується. Тому сьогодні для виконання цього завдання можна і потрібно використовувати системи виявлення та реагування на інциденти безпеки інформації.

Перш за все слід розглянути один з основних етапів роботи SIEM системи – передобробка лог-файлі. Слід зазначити, що у рішенні QRadar, при відправленні журнала подій в систему, розпізнавання джерела та нормалізація проводиться автоматично, а у ArcSight(з коробки) адаптація нових джерел відбувається вручну. IBM QRadar SIEM реалізує аналіз лог-файлів в спрощенному

вигляді, на відміну від рішення HP ArcSight SIEM, що зберігає їх у сховище, а потім обробляє. На відміну від конкурентів McAfee Enterprise Security Manager використовує готові шаблони дії, що забезпечує більшу гнучкість. Розглянувши ці три підходи з точки зору надійності, можна зазначити, що в першому випадку маємо більшу ймовірність помилки 2го роду, тобто вищу ймовірність пропустити подію, що загрожує безпеці бізнес процесу.

Ще однією відмінністю є те, що QRadar та McAfee Enterprise Security Manager мають більше встановлених конекторів, але при цьому більш легка розробка та інтегрування конекторів до системи у рішенні ArcSight. Слід звернути увагу і на те, що в QRadar та McAfee Enterprise Security Manager обробка подій здійснюється до 7 рівня моделі взаємозв'язку відкритих систем, а в ArcSight – тільки до 5 рівня. Отже, вже на прикладі розгляду способів попередньої обробки лог-файлів SIEM-системами бачимо, що неможливим є порівняння систем тільки за однією ознакою. Звідси маємо задачу багатокритеріальної оптимізації, а рішенням є не одне рішення, а парето- множина рішень.

Не менш важливим етапом роботи SIEM-системи вважається процес кореляції подій важливих з точки зору безпеки. Розглянемо цей процес докладніше, на прикладі двох SIEM-систем. Після отримання інформації від джерел, система починає аналізувати цю інформацію. Рішення QRadar є комплексом «з коробки», тому в ньому вже є вбудований набір правил кореляції. Рішення HP ArcSight теж має стандартний набір правил кореляції, але в меншій кількості, оскільки орієнтований на ручне налаштування системи під потреби організації. Дані правила в обох випадках складаються з визначених наборів умов і сценаріїв дій. Правила кореляції розбиті на категорії. Кожне правило окремо можна включити або відключити.Всі спрацьовування різних правил кореляції логічно пов'язаних між собою відносяться до одного інциденту і автоматично так званий «Offense». Якщо правила кореляції продовжують спрацьовувати, нова інформація додається в цей Offense, а не генеруються нові. У HP ArcSight спочатку це різні зкорельовані події. Пов'язування між собою відбувається вручну. дбання ліцензій для програмно-апаратних засобів. Слід зазначити, що така система потребує від аналітиків інформаційних загроз відповідної кваліфікації .

Зібравши та обробивши події, що надійшли від обраних джерел, SIEM-система за допомогою методів прийняття рішень, відносить ту чи іншу подію до класу інцидентів інформаційної безпеки. Оскільки в QRadar обробка подій здійснюється до 7 рівня, то система надає більш точний та компактний набір зкорельованих подій, аніж ArcSight. QRadar та ArcSight використовують декілька методів прийняття рішень. В роботі розглянуто методи, що використовують для прийняття рішень, одними з яких є поведінкові методи , що в процесі своєї роботи порівнюють параметри спостережуваної поведінки з інформацією про нормальну поведінку системи, і випадок значних відхилень розглядається як свідчення наявності атаки. Недоліком даного методу є хибні спрацьовування, які пояснюються в першу чергу складністю точного і повного опису безлічі легітимних дій користувачів. Окрім цього, в SIEM-системах для прийняття рішень використовують методи на основі знань. У статті описано дані методи, як такі, що в контексті заданих фактів, правил виводу і зіставлень, що відображають ознаки заданих атак, виробляють дії по виявленню атак на основі закладеного механізму пошуку. Ці методи працюють з базою знань, в якій включено опис вже відомих атак. Зважаючи на те, що кожен з цих методів не ідеальний, виробники QRadar та ArcSight використовують поєднання цих методів, задля компенсування їх недоліків.

У даній роботі було проведено комплексний аналіз характеристик систем управління подіями інформаційної безпеки (SIEM), на прикладі рішень IBM QRadar, HP ArcSight, та McAfee Enterprise Security Manager що полегшує підбір SIEM-системи під вимоги організації. Рекомендовано для великих організацій, холдингових структур, в якості платформи для побудови центру захисту інформації використовувати рішення від компанії HP, зважаючи на його гнучкість, багатий функціонал та стійкість до великих навантажень. Організаціям меншого масштабу рекомендовано розглянути рішення від компаній IBM та McAfee .

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Ч. 1 // Труды СПИИРАН.–2016.– Вып. 47. С. 5-27.

УДК 004.056.53 (043.2)

Ю. І. Сінько, к.пед.н.
Національний авіаційний університет, Київ

СТІЙКІСТЬ WINDOWS 10 ДО ШКІДЛИВОГО ПРОГРАМНО-МАТЕМАТИЧНОГО ВПЛИВУ

Програмно-математичний вплив – це вплив на інформацію, що захищається, за допомогою шкідливих програм. Шкідлива програма – програма, яка призначена для здійснення несанкціонованого доступу до інформації та (або) впливу на інформацію або ресурси інформаційної системи. Іншими словами шкідливою програмою називають деякий самостійний набір інструкцій, який здатний виконувати наступне:

1) приховувати свою присутність у комп'ютері;

2) мати здатність до самознищення, маскуванням під легальні програми та копіювання себе в інші області оперативної або зовнішньої пам'яті;

3) змінювати (руйнувати, спотворювати) код інших програм;

4) самостійно виконувати деструктивні функції – копіювання, модифікацію, знищення, блокування і т. ін.;

5) спотворювати, блокувати або підмінювати виведену до зовнішнього каналу зв'язку або на зовнішній носій інформацію.

Основними шляхами проникнення шкідливих програм, зокрема, на комп'ютер, є мережева взаємодія і знімні носії інформації (флешки, диски і т.ін.). Під час цього впровадження в систему може носити випадковий характер.

У реальному світі більшість загроз безпеки взагалі не припускають участі людини. Програмне забезпечення (ПЗ) автоматизувало багато аспектів нашого життя, а шкідливе ПЗ автоматизувало атаки на наші ПК. Ці атаки нещадні. Шкідливе ПЗ безперервно змінюється, і розпізнати його і видалити із зараженого ПК може бути дуже складно. Слід зазначити, що сучасні сертифіковані операційні системи мають вбудовані засобами захисту, які дозволяють вирішувати багато проблем, що виникають. Профілактика – найкращий захист, і Windows 10 забезпечує надійний захист від шкідливого ПЗ, тому що використовує надійне апаратне забезпечення, яке гарантуватиме безпечний запуск і захищає базову архітектуру ОС.

Далі перераховуються конкретні загрози, що пов'язані з шкідливим ПЗ, і засоби захисту, які реалізовані в Windows 10.

Загроза: Комплекти завантаження вбудованого ПЗ (bootkit – буткіти) замінюють його шкідливим ПЗ.

Рішення Windows 10: Всі сертифіковані ПК оснащені UEFI з технологією безпечного завантаження, яка вимагає використання підписаного вбудованого ПЗ для поновлення UEFI і Option ROM (додатковий ПЗП).

Загроза: Буткіти запускають шкідливе ПЗ до запуску Windows.

Рішення Windows 10: Безпечне завантаження UEFI перевіряє цілісність завантажувача ОС Windows, щоб переконатися, що ніяка шкідлива ОС не запущена до запуску Windows.

Загроза: Системні руткіти (rootkit – набір для отримання необмеженого доступу) або драйверні руткіти запускають шкідливе ПЗ на рівні ядра під час запуску Windows, до запуску Захисника Windows і рішень, що захищають від шкідливого ПЗ.

Рішення Windows 10: Система надійного завантаження Windows перевіряє завантажувальні компоненти Windows; драйвери Майкрософт і драйвер захисту від шкідливого ПЗ ELAM, який перевіряє сторонні драйвери.

Паралельно надійному завантаженню виконується вимірюване завантаження, яке надає віддаленому серверу інформацію про стан завантаження пристрою і гарантує успішну перевірку системи модулем надійного завантаження та іншими завантажувальними компонентами.

Загроза: Шкідливе ПЗ рівня користувача використовує уразливість в системі або додатку і вступає у володіння пристроєм.

Рішення Windows 10: Удосконалення в області технологій ASLR, DEP і алгоритмів управління пам'яттю знижують ймовірність успішного захоплення системи з використанням вразливостей. Технологія захищених процесів ізолює недовірені процеси один від одного і від важливих компонентів ОС.

VBS на основі Microsoft Hyper-V захищає секретні процеси Windows від ОС Windows, ізолюючи їх від процесів, які виконуються в режимі користувача, і ядра Windows.

Налаштовувана цілісність коду забезпечує реалізацію політики адміністрування, що вказує, які саме додатки можуть виконуватися в режимі користувача. Запускати інші додатки заборонено.

Загроза: Користувачі скачують небезпечне ПЗ (наприклад, додаток, який здається нормальним, але містить вбудований троянський вірус) і запускають його, не усвідомлюючи ризики.

Рішення Windows 10: Функція репутації додатків за даними SmartScreen є частиною базової ОС; Microsoft Edge і Internet Explorer можуть скористатися цією функцією, щоб попередити користувачів або заблокувати скачування і запуск потенційно шкідливого ПЗ.

Загроза: Шкідливе ПЗ використовує уразливість у надбудові браузера.

Рішення Windows 10: Microsoft Edge – це універсальний додаток, який не запускає старі двійкові розширення, в тому числі Microsoft Active X і допоміжні об'єкти браузера, які часто використовуються на панелях інструментів. Тим самим зазначені ризики виключаються.

Загроза: Веб-сайт з шкідливим кодом використовує вразливість в Microsoft Edge і Internet Explorer для запуску шкідливого ПЗ на клієнтському ПК.

Рішення Windows 10: У Microsoft Edge і Internet Explorer реалізований розширений захищений режим, який використовує AppContainer для захисту системи від вразливостей, які можуть виявлятися в розширеннях, що запускаються в браузері (наприклад, Adobe Flash, Java) або самому браузері.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Електронний ресурс. Режим доступу: https://www.microsoft.com/uk-ua/ - офіційна сторінка Microsoft.

УДК 004 (043.2)

О. В. Толстікова, к.т.н.,
К. С. Ушаков, аспірант,
А. О. Нестеренко
Національний авіаційний університет, Київ

АГЕНТНИЙ ПІДХІД ДО МОДЕЛЮВАННЯ СКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

З розвитком інформаційних технологій все частіше з’являються складні системи, які можуть бути охарактеризовані взаємодією безлічі автономних суб'єктів, поведінка яких визначає розвиток всієї системи.

Концепція комп'ютерного моделювання передбачає використання моделі для дослідження поведінки складних систем, які передбачають здатність приймати власні рішення.

Для складних систем, де час і динаміка важливі, імітаційне моделювання являє собою дуже потужний засіб аналізу.

Набувають популярності розподілені системи, в яких знання і ресурси розподіляються між досить самостійними агентами, але зберігається загальний орган командного управління, який приймає рішення в критичних або конфліктних ситуаціях. Подальшим кроком в цьому напрямку стала парадигма повністю децентралізованих систем, в яких управління відбувається тільки за рахунок локальних взаємодій між агентами. При цьому вузька функціональна орієнтація агента на рішення якоїсь однієї окремої частини загального завдання поступово стала поступатися місцем автономності. В основі такого підходу лежить поняття мобільного програмного агента, який реалізований і функціонує як самостійна спеціалізована комп'ютерна програма або елемент штучного інтелекту.

При вирішенні проблеми моделювання складних інформаційних систем має важливе значення застосування мультиагентних систем.

Сутність мультиагентних технологій полягає в принципово новому методі вирішення завдань. На відміну від класичного способу, коли проводиться пошук деякого чітко визначеного алгоритму, що дозволяє знайти найкраще вирішення проблеми, в мультиагентних технологіях рішення виходить автоматично в результаті взаємодії безлічі самостійних цілеспрямованих програмних модулів - програмних агентів.

Мультиагентні системи складаються з безлічі штучних агентів, які спільно працюють. Агентне моделювання є універсальним підходом, адже воно дозволяє врахувати будь-які складні структури і поведінку системи. Для побудови агентної моделі і визначення її глобальної поведінки, потрібно визначати індивідуальну логіку поведінки учасників процесу.

Автономність агентів полягає у здатності функціонувати без людського втручання і можливості певною мірою контролювати свій стан. Взаємодія між даними сутностями відбувається за допомогою певної мови. Важливою властивістю агентів є можливість відчувати навколишнє середовище, в якій він розташовується і відповідно реагує на її зміни. Про його інтелектуальну поведінку свідчить здатність до навчання, пошуку оптимальних способів поведінки та здатність діяти за власною ініціативою для досягнення внутрішньої мети.

Побудова агентних моделей вимагає визначення безлічі агентів і основ їхньої поведінки, визначення взаємовідносин між агентами і теоретичних основ цих відносин, вибору платформи для агентного моделювання. Визначення агентів з точним завданням їх поведінки і взаємодії з іншими агентами - це основа для розробки адекватних агентних моделей. Даний напрямок, націлений на отримання результатів, адже агентно-орієнтований підхід до моделювання може бути ефективно використаний для вивчення, пояснення і прогнозування поведінки складних систем [1,2].

Для імітаційного моделювання складних динамічних систем пропонуємий агентний підхід, при якому агенти розглядаються як активні елементи, які взаємодіють між собою та здатні виявляти індивідуальні властивості, можна вважати ефективним підходом.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Городецький В.І., Грушинський М.С., Хабаля А.В. Багатоагентні системи // Новини штучного інтелекту. – 1997. – № 1. – С. 15-30.

2. Зеленцов В.А., Ковальов О.П. Аналіз існуючих підходів до прогнозування показників довговічності стартового комплексу як складної системи // Подвійні технології. – 2000. – № 1. – С. 20-22.

УДК 004.05

О. І. Трембовецька,
КПІ ім. Ігоря Сікорського, Київ

МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ SOC

Інфраструктура організацій та установ (банків, великих приватних компаній, тощо) з часом серйозно ускладнюється. Це пов’язано як з ростом власне компаній, так і, більшою мірою, з розвитком технологій та збільшенням кількості пристроїв різного призначення. Традиційний підхід до контролю інфраструктури таким чином стає занадто трудомістким та заплутаним, внаслідок чого неефективним. Як вирішення цієї проблеми часто приймається рішення створити центр моніторингу і реагування на інциденти інформаційної безпеки - SOC.

Створення власного SOC - це дорогий та тривалий процес, що вимагає значних ресурсів: людських та матеріальних. При цьому процес є тривалим у часі і не має завершення. Велика кількість організацій (включаючи деякі великі організації) вирішують відмовитися від власного центру. Замість цього вони обирають інші варіанти контролю безпеки, такі як залучення постачальника послуг керованої безпеки – зовнішнього SOC.

Security Operations Center (SOC) може бути визначений як об'єкт, призначений та організований для попередження, виявлення, оцінки та реагування на загрози та інциденти, пов'язані з кібербезпекою, а також для забезпечення відповідності певним вимогам(compliance) та перевірки цієї відповідності.

Суть SOC складають три елементи: команда, технології, процес. При цьому базовою технологією зазвичай слугує самописна або вже готова система моніторингу та реагування на інциденти інформаційної безпеки (SIEM).

Завдяки використанню журналів різного роду, аналітики можуть відразу ж переходити від використання системи моніторингу як детективного інструменту до її використання як інструменту розслідування, переглядаючи підозрілі заходи, що складають даний інцидент, і навіть як інструменту управління реакцією на інцидент або порушення. Більша ефективність SOC, тобто отримання більшої продуктивності з меншими витратами, може бути досягнута через мінімізацію операційних витрат на контролі –

правила, що складають суть функціонування SIEM.

Без наявності формалізації та стандартизації процесу створення контролів виникає ряд проблем та складнощів. Процес проектування та власне реалізації не формалізований. Адміністрування ускладнене, масштабування може потребувати великої кількості операцій. Важко вести облік контролів, що в свою чергу може призводити до надлишковості, або навпаки недостатності.

Формалізація може застосовуватися вже на етапах аналізу та проектування. При цьому ефект від роботи кожного окремого контролю не зміниться, а отже ефективність зросте.

Умови спрацювання задаються у вигляді логічних виразів, відповідно для формалізації процесу проектування доречно буде використовувати апарат математичної логіки, зокрема логіку висловлень. Вимоги до контролю формуються у вигляді речень природної мови. Для подальшої роботи необхідно подати їх у вигляді формул висловлення.

Загалом контроль зазвичай складається з загальних умов та специфічних умов окремої організації. Таким чином, якщо правило розбивати на окремі атоми, то можна буде виділити групу загальних. Винесення таких частин з усіх контролів дає можливість зменшення кількості операцій для подальшого адміністрування та масштабування.

В загальному вигляді контроль записується як комбінація атомів (напр. А - події з пристроїв під управлінням ОС Windows, Б – додавання облікового запису до групи, В – група є привілейованою, Г – додавання користувача дозволено, Д – подія належить певному клієнту) та логічних зв’язок (кон’юнкції, диз’юнкції, заперечення). А, Б і В при цьому – атоми, що відображають загальні умови, а Г і Д – специфічні.

Додатково винесення окремих атомів дає змогу визначити від яких типів подій залежить кожен окремий контроль. Порівняльний аналіз подій що надходять до системи та тих, що впливають на контролі (таблиця 1) надає параметри, за якими можна обмежити надходження «зайвих» подій. Адже велика кількість таких подій призводить як до зростання часу реагування, так і до фінансових втрат, якщо, наприклад, ліцензування відбувається за величиною вхідного потоку чи загальним обсягом подій.

Таблиця 1. Події з Windows-джерел за event log ID

Event ID	Кількість, од.	Доля в загальному потоці, %	Застосовність в контролях
5158	2523558	30.96%	Ні
5156	1744098	21.40%	Ні
5154	1427449	17.51%	Ні
4624	804310	9.87%	Так
4634	794624	9.75%	Ні
5152	274753	3.37%	Ні
4672	214430	2.63%	Так
4688	164546	2.02%	Ні
5157	122338	1.50%	Ні
4648	81363	1.00%	Так
		Кількість незастосовних	86.50%

В процесі роботи було розглянуто групу контролів, та виділено загальні їх частини. При винесенні цих частин у окремі ресурси можна побачити певне зменшення витрат – операцій та, відповідно, часу – на масштабування та адміністрування контролів. Для адміністрування – якщо до винесення кількість необхідних операцій для редагування (оновлення) кожної умови контролю вимагала кількості операцій рівній кількості організацій, до яких контроль застосовний, то після – лише одну. Для масштабування ефект схожий – оскільки при копіюванні ресурсів внутрішні посилання контролю зберігаються, то для масштабування в загальному випадку потрібна кількість операцій, що відповідає кількості атомів, при чому операція визначення кожного атому може складатися з великої кількості дій. Відповідно масштабування спрощується у стільки разів, скільки спільних атомів вдалося виділити.

В проведеному досліді при виділенні топ-10 за кількістю унікальних типів подій Windows було встановлено, що повністю зберігаючи працездатність контролів можна зменшити кількість вхідних подій на 86,5%, при цьому при виділенні топ-30 типів ця кількість зростає незначно, до 86,81%.

УДК 004.075:004.7 (043.2)

І. І. Феденко, аспірант
Національний авіаційний університет, Київ

ПІДХОДИ ДО ГЛОБАЛЬНОГО БАЛАНСУВАННЯ ТРАФІКУ

Технологією MPLS сьогодні стали де-факто стандартом побудови мереж операторів зв'язку. В міру того як стандарт обростав м'язами, ставало зрозуміло, що застосування декількох міток, названих згодом стеком, дозволяє поглянути на MPLS як на технологію з уніфікованими методами надання та забезпечення сервісів. Так, мітки в стеці умовно поділили на сервісні та транспортні. Для великих мереж цього виявилося недостатньо і незабаром з'явилася власна ієрархія транспортних міток. Транзитні маршрутизатори не зобов'язані розуміти який саме сервіс вони передають, їх завдання обмежується роботою з верхньої міткою своєї ієрархії. Такий підхід дозволяє транзитним маршрутизаторам передавати трафік сотень тисяч і навіть мільйонів потоків різних сервісів.

Здавалося б, чого ще бажати, але ось ефективно розділяти якраз не дуже то виходило, в тому сенсі, що трафік хочеться балансувати якомога рівномірніше в рамках обмеженої кількості каналів зв'язку силами некваплівих, з точки зору змін, апаратних рішень.

LDP, на перший погляд, разом з парадигмою Hop-by-Hop destination based routing успадковує ECMP можливості IGP, однак разом з тим успадковуються і деякі особливості балансування, властиві IP світу. IP маршрутизатори очікують побачити всередині пакету те, що їм добре знайоме, - потенційно високо ентропійних заголовки мережевого і транспортного рівнів. Їх легко розібрати і, при великій кількості потоків, розподіл виглядає цілком рівномірним. Складність застосування цього правила в MPLS світі полягає в тому, що транзитний LSR, заглянувши всередину стека, не завжди знаходить там IP пакет, часто під транспортної міткою знаходиться сервісна, наприклад VPNv4, Labeled Unicast, VPWS, VPLS або EVPN, часто з більш низькою ентропією, тому така ідея, як інспекція транзитними маршрутизаторами всього стека міток і навіть упакованого в стек пакета / фрейма, стала вимушеною необхідністю. Складнощі, пов'язані з необхідністю інспекцією всього стека, можна вирішити іншим способом. Для цього в точці надання сервісу в стек додаються мітки підвищують ентропійність.

Стандарти Flow Aware Transport і Entropy Label якраз про це, але начебто за законом збереження енергії, знизивши вимоги до транзитних маршрутизаторів, стандарти підвищують вимог до прикордонних. В стек за один прохід крім транспортних і сервісних міток потрібно помістити від одного до двох ентропійних, це виходить не у всіх чіпів і не у всіх випадках, тому ефективність балансування MPLS трафіку в LDP домені залежить від апаратної реалізації комутаційних чіпів, довжині стека і величини його ентропійності.

Distributed RSVP-TE вирішує завдання балансування зовсім іншим методом. Рівномірність розподілу тут залежить не стільки від можливостей транзитних маршрутизаторів, скільки від якості рішення оптимізаційної задачі граничними маршрутизаторами, кожен з яких розраховує шляху до сусідів з урахуванням поточного рівня утилізації каналів і характеристик трафіку. Маршрутизатор може впливати на вже встановлені шляхи тільки за допомогою setup і hold пріоритетів, призначення пріоритетів не є тривіальним завданням і є кілька підходів до її вирішення (пріоритет по смузі, пріоритет по типу трафіку і т.д.). Так як кожен з підходів має вузькі цілі, а кошти автоматизації цього процесу відсутні, класичний RSVP-TE складно назвати простою технологією із загальним застосуванням. Якщо вузлів в мережі не багато, а смуга деяких шляхів близька до канальної ємності, легко отримати мережу з фрагментованою утилізацією. Тому на практиці зазвичай уникають надмірного роздуття шляхів за рахунок розрахунку

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Гольдштейн А.Б. Технология и протоколы MPLS / Гольдштейн А.Б., Гольдштейн Б.С. - СПб.: БХВ — Санкт-Петербург, 2005. — 304 с.

УДК 004.42 (043.2)

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

ПОСЛІДОВНІСТЬ ПРОЕКТУВАННЯ СПЕЦІАЛІЗОВАНИХ СИСТЕМ НА КРИСТАЛІ

Спеціалізована комп'ютерна система (СКС) побудована на основі системи на кристалі (СНК), в більшості проектів має наступну структуру (рис.1).

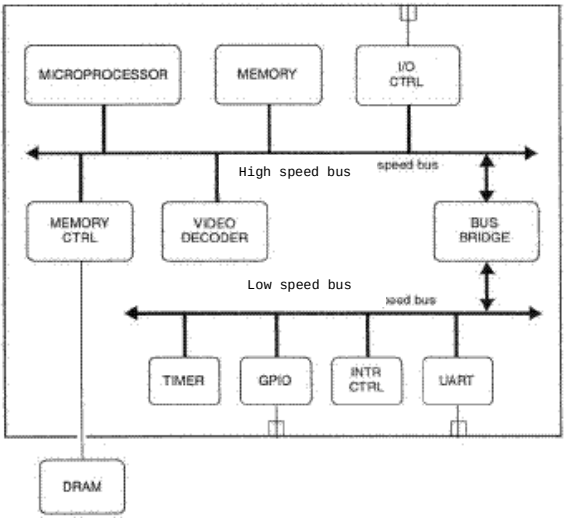


Рис. 1. Канонічна система на кристалі

Реальні системи типово складаються з декількох ядер (IP Cores), декількох типів шин та інтерфейсів. Крім того сучасні СНК містять декілька мікропроцесорів та комбінації мікропроцесорів та процесорів обробки сигналів [1]. Аналогічно, системи пам'яті є значної складності та різних типів, в багатьох випадках використовується багатопортова пам'ять, наприклад.

- Мікропроцесором системи може бути будь-який мікропроцесор від 8-ми бітногот 8051 до 64-х бітного RISC.
- Система внутрішньої пам'яті може бути одно чи багаторівневою, та може включати SRAM чи DRAM.
- Зовнішня пам'ять може бути DRAM, SRAM, Flash.

- Відеодекодерами можуть бути пристрої кодування MPEG, ASF, AVI.

- Контролер інтерфейсів GPIO можуть містити буферні підсилювачі вихідних портів різного типу.

Процес проектування потребує специфікації СНК з метою подальшої розробки та тестування складових компонентів [1, 3].

З метою забезпечення вимог до СНК, сучасні послідовності проектування проходять еволюцію в двох напрямках:

- з водоспадної послідовності в спіральну;
- з низхідної послідовності у комбіновану низхідну та висхідну послідовності проектування.

Традиційно при проектуванні СНК використовується водоспадна послідовність проектування. При даній послідовності проектування розробка проекту виконується згідно заданої послідовності кроків з системного до фізичного рівня без повернення розробки з одного кроку в інший. При цьому, враховуючи велику складність проекту, на кожному кроці проектування збирається інша команда розробників.

Дана послідовність проектування є ефективною при складності розробки до 100 тис. вентилів [2]. Дана послідовність проектування наштовхується на проблему сумісної роботи команд розробників. При зростанні складності проекту водоспадна технологія проектування втрачає ефективність, оскільки програмна частина проекту є суттєвою і розробка ПЗ після завершення розробки прототипу збільшує час проектування.

Вимоги ринку по скороченню термінів проектування, наявність сучасних засобів проектування, наявність широкої гами розроблених компонентів ставить нові вимоги до послідовності проектування. Низхідна послідовність не відповідає даним вимогам та не дозволяє ефективно використати можливості сучасних засобів [3].

Тому, в сучасних розробках використовується комбінована низхідно-визхідна послідовність проектування. При даній послідовності, при плануванні системи використовують результати розробки (апаратні та програмні компоненти) розроблені розробниками.

Оскільки складність СНК постійно зростає за геометричною прогресією, а сучасний ринок вимагає скорочення часу проектування СНК, то розробники використовують послідовності

проектування відмінні від водоспадної. Особливу ефективність надає розробникам новітня спіральна послідовність проектування. При спіральній послідовності проектування максимально задіяно всі групи розробників різних рівнів проектування.

Прикладом ефективної послідовності проектування є послідовність проектування, розроблена спеціалістами Sun Microsystems при розробці мікропроцесора UltraSPARC. В даній послідовності використано комбіновану низхідно-визхідну спіральну послідовність.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Шалумов А.С. Введение в CALS-технологии: Учебное пособие / А.С. Шалумов, С.И. Никишкин, В.Н. Носков. Ковров: КГТА, 2002. – 137 с.

2. Красильникова М.В. Проектирование информационных систем: Учебное пособие / М.В. Красильникова. – М.: МИСиС, 2004. – 106 с.

3. Орлов С.А. Технологии разработки программного обеспечения. Разработка сложных программных систем / С.А. Орлов. – СПб.: Питер, 2002. – 464 с.

УДК 004.056.53:004.056.055 (043.2)

І. Ю. Юрчук,
Л. П. Галата,
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ ПРОТОКОЛУ SSL ЯК ЗАХИСТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Безпека даних у відкритих інформаційних мережах, а саме Інтернет, завжди буде джерелом будь-яких атак. Тому вкрай важливо створити безпечне середовище для передачі та обробки інформації. Найчастіше передані дані мають різні вимоги щодо захисту даних, серед яких: конфіденційність, достовірність і цілісність. Цим критеріям відповідає криптографічний мережевий протокол – SSL.

Протокол SSL (Secure Socket Layer) використовує асиметричне шифрування, відоме також як шифрування з відкритим ключем. У шифруванні з відкритим ключем створюються два ключа, один публічний, інший секретний. Дані, які були зашифровані секретним ключем сервера, можуть бути розшифровані тільки за допомогою публічного ключа цього ж сервера, даючи впевненість в тому, що дані прийшли від нього.

Протокол SSL розроблений Netscape Communications і RSA Data Security, він забезпечує встановлення безпечного з'єднання між клієнтом і сервером. SSL забезпечує безпеку, аутентифікацію на базі сертифікатів і узгодження безпеки за встановленим мережним з'єднанням.

Через те, що з'явилися атаки на протоколи - стає актуальною проблема розробки методики тестування конфігураційних параметрів протоколу, реалізації методики для клієнтських і серверних веб-додатків, які використовують протокол, формування і застосування рекомендацій щодо захисту.

Для запобігання перехоплення секретних відомостей рекомендовано використовувати протокол SSL. Він призначений для того, щоб допомогти користувачам упевнитися, що вони взаємодіють саме з тим сайтом, який їм потрібен, і що вся інформація, що передається залишається приватною і захищеною.

Використання SSL-сертифіката гарантує відвідувачеві сайту:

1. Справжність даних. SSL підтверджує, що користувач отримує дані з домену, на якому розміщений сайт компанії.

2. Конфіденційність. SSL-шифрування захищає дані від перехоплення в момент передачі.

3. Цілісність інформації. SSL-з'єднання допомагає уникнути спотворення даних при передачі.

Для отримання сертифіката необхідно підготувати дані для перевірки: підтверджений домен при отриманні Domain Validation SSL, свідоцтво про внесення до Єдиного державного реєстру юридичних осіб і будь-який документ, що підтверджує реальне існування компанії.

Слід згенерувати CSR (Certificate Signing Request) або запит на підписання сертифіката - це блок закодованого тексту, який генерується на тому сервері, де буде використовуватися сертифікат. Він містить в собі інформацію, яка буде включена в ваш сертифікат: назва організації, доменне ім'я, юридичну адресу та країну. Також в CSR міститься відкритий ключ, який буде включений у сертифікат.

Необхідно відіслати замовлення на отримання сертифіката і сплатити отриманий рахунок. Далі встановити отриманий сертифікат і слідкувати за строком його дії.

У даній статті була аргументована важливість надання захищеного сеансу зв'язку і наскільки необхідним це є для забезпечення конфіденційності інформаційного потоку даних. Кількість викрадених персональних даних зростає з кожним днем, тому потрібно прийняті захисні заходи. Протокол SSL – це криптографічний протокол, який вирішить проблему з викраденням, модифікацією або знищенням цінної інформації.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. «SSL-сертифікати» https://tucha.ua/blog/ssl-certifikaty-chto-eto-dlya-chego-nuzhno-i-kak-sgenerirovat-zapros-na-podpisanie-sertifikata/

2. «HTTPS і SSL: переваги, недоліки, проблеми та рішення» https://seosreda.com.ua/https-ssl-dlya-seo/

3. «Переваги та недоліки протоколу HTTPS для інтернет магазину» https://ain.ua/2015/03/05/preimushhestva-i-nedostatki-protokola-https-dlya-internet-magazina

Наукове видання

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
XI МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2018)

19–21 квітня 2018 року

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

Підп. до друку 12.04.18. Формат 60х84/16. Папір офс.
Офс. друк. Ум. друк. арк. . Обл.-вид. арк. 6
Тираж 60 пр. Замовлення № 111-1

Видавець і виготівник
Національний авіаційний університет
03680. Київ-68, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002