МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ 23-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ»

16 – 18 квітня 2019 р.

Том 5

КОНФЕРЕНЦІЯ «ВІРТУАЛЬНИЙ ТА ФІЗИЧНИЙ КОМП'ЮТІНГ»

Харків 2019

23-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. матеріалів форуму. Т. 5. – Харків: ХНУРЕ. 2019. –191с.

В збірник включені матеріали 23-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті».

Видання підготовлено факультетом комп'ютерної інженерії та управління Харківського національного університету радіоелектроніки

61166 Україна, Харків, просп. Науки, 14
тел./факс: (057) 7021397

E-mail: mref21@nure.ua

ФІЗИЧНИЙ КОМП’ЮТІНГ

ФУНКЦИОНАЛЬНАЯ ВЕРИФИКАЦИЯ ПЕРЕХОДОВ КОНЕЧНЫХ АВТОМАТОВ ПРИ ПОМОЩИ ЯЗЫКА SYSTEMVERILOG

Пшеничный К.Ю.
Научный руководитель – к.т.н., доц. Хаханова А.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. АПВТ, тел. (057) 702-13-26)
e-mail: anna.hahanova@nure.ua, факс (057) 702-13-26

The given work is devoted to finite state machines transition path coverage using functional verification capabilities of SystemVerilog hardware description language. Cover directives method for transition path coverage has been proposed in this paper.

Современные методы верификации цифровых систем, спроектированных при помощи языков описания аппаратуры (HDL), включают в себя генерацию случайных ограниченных тестовых наборов и использование средств анализа полноты покрытий для оценки результатов тестирования. Конечный цифровой автомат (FSM) имеет дискретное число состояний, определенное число условий, которые возбуждают переходы между состояниями, и функции выходов. Несколько условий могут возбуждать один и тот же переход. Покрытие перехода между двумя состояниями при помощи определенного тестового набора показывает, что данный тест учел лишь определенный переход между состояниями, но не учел условие перехода. Покрытие путей предоставляет комплексный анализ, который учитывает условия переходов между состояниями во время верификации. Путь – переход между двумя состояниями под определенным условием. Между двумя состояниями может быть множество путей. Цель исследования – повышение качества тестирования конечных цифровых автоматов за счет использования методов функциональной верификации для анализа полноты покрытий переходов автомата. Задача – разработка функциональной модели анализа полноты покрытий переходов при помощи средств языка SystemVerilog.

Использование конструкции свойств (property) языка SystemVerilog позволяет выразить возможные пути между двумя состояниями для последующей верификации их полноты во время моделирования.

```
property STANDBY_SLEEP_CMD5 ;
   @(posedge clk)
   ((state == STANDBY) |=> ((state == SLEEP) && (cmd == 5) ) ) ;
endproperty
```

Рисунок1.1 – Свойство, описывающее путь из состояния STANDBY в состояние SLEEP

Путь можно выразить вектором <q_0, q_1, r>, где q_0 – начальное состояние пути, q_1 –конечное состояние пути, r – условие перехода. На рис.1.1 представлено свойство, описывающее путь из состояния STANDBY в состояние SLEEP, который активируется, когда сигнал cmd принимает значение 5.

Данное свойство использует оператор импликации (|=>). Предшествующее(antecedent) выражение (слева от оператора) является простым нетемпоральным выражением, проверяющее текущее состояние автомата. Последующее (consequent) выражение (справа от оператора) описывает целевое состояние пути и его условие. Поскольку одно свойство описывает один путь между смежным состояниями, количество свойств, необходимых для описания всех путей, равно количеству путей между смежными состояниями.

Количество свойств будет иметь линейную зависимость, если между смежными состояниями существует всегда один путь, или экспоненциальную, если таковых путей более одного.

Далее необходимо определить верификационный метод для проверки данного свойства. Язык SystemVerilog имеет следующие верификационные директивы: assert, assume и cover[2-3]. Так как целью данного метода является покрытие, то используется директива cover.

```
ARC1: cover property (STANDBY_SLEEP_CMD5);
```

Рисунок 1.2 – Верификация свойства при помощи директивы cover

Научная новизна определяется новым методом тестирования конечных автоматов при помощи мониторинга полноты покрытий путей средствами функциональной верификации языка описания аппаратуры SystemVerilog. Использование данного метода в совокупности с тестирование при помощи случайных тестовых наборов (Constrained Random Testing) позволяет дать процентную оценку покрытия переходов во время верификации.

Список источников:

1. Janick Bergeron. Writing Testbenches: Functional verification of HDL models, 2nd edition. Springer. 2003. С. 80-120.

2. Foster D, Harry D. Assertion-Based Design, 2nd Edition. Springer. 2005. С. 90 – 150.

3. Ben Cohen, SystemVerilog Assertions Handbook, 2nd Edition. Springer. 2010. С.50 – 70.

3D МОДЕЛЮВАННЯ МІСЦЕВОСТІ З ВКИОРИСТАННЯМ ДРОНІВ

Прядка Д.О.
Науковий керівник – ст. викл. Морозова А.І.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Системотехніки,
тел. (057) 702-13-06)
e-mail: daria.priadka@nure.ua, телефон (099) 739-62-04

The given work presents description of process of using 3D reconstruction technique based on 2D pictures of a building taken by a quadcopter . The latter is an unmanned aerial vehicle (UAV) being used to survey buildings of various heights without interfering with public transport. Moreover, the quadcopter can reach any position required to take the necessary angle for a favourable photos that should be connected together in 3D model. 3D technology is often used in different spheres of life because creating 3D model of real object allow to research and analyze information about real object easily with help of software.

Сучасні дрони активно використовуються у багатьох галузях людської діяльності. Основні галузі застосування БПЛА - логістика, будівництво, сільське господарство, дика природа, розвідка. Вони дозволяють отримати точні фото і відеоматеріали, які після обробки в спеціалізованому програмному забезпеченні дозволяють одночасно обробляти і об’єднувати тисячі фотографій, знятих з різних ракурсів, і автоматично створювати 3D моделі місцевості.

Перевагою БПЛА є те, що зйомка може проводитися з невеликої висоти з великою деталізацією, недоступною для великої авіації і супутників. Завдяки тому, що дрони використовують камери з оптикою високого дозволу (до 4К), можна отримати дуже високу точність моделей

Етапи розробки 3D моделі умовно можна поділити на такі групи: підготовка (планування польотів, вибір точок для зйомки, вибір та налаштування обладнання), збір даних (отримання зображень об’єкту) та безпосередньо моделювання (обробка зображень, аналіз точності отриманих результатів).

Зазвичай для подальшого моделювання охоплюється площа близько 300 на 300 метрів. Рекомендована висота – 50 м (це дозволить зробити більш якісні фото), за виключенням зйомки високих об’єктів. Бажано, щоб дрон підіймався не більше, ніж на 20 метрів над верхньою точкою будівлі. Технічно дрон може підійматися на більшу відстань та охоплювати більшу площу, але в такому разі погіршуються характеристики зображень.

Для передачі зображень використовується спеціальне програмне забезпечення, наприклад: PolarPro, Drone Harmony тощо. Завдяки цьому

під час польоту можна регулювати деякі параметри зйомки (позиція, швидкість) та бачити стан пристрою.

В процесі бажано отримати якнайбільше зображень з різних ракурсів під різними кутами зйомки, адже від цього залежить точність майбутньої 3D моделі. Після зйомки фото обробляються у декілька етапів.

Перший етап - попереднє створення карти. Початковий аналіз знімків здійснюється для виявлення кореляції між ними.

Другий етап - виведення функцій на знімках за допомогою оператору SIFT (scale-invariant feature transform). Алгоритм SIFT включає чотири етапи: екстремальне виявлення масштабного простору, локалізація ключових точок, призначення орієнтації, створення дескриптора ключових точок.

Третій етап - визначення відповідних ознак для пари зображень. Відповідні функції можна знайти при порівнянні характеристик опису, отриманих на попередньому етапі.

Четвертий етап - інтеграція зображень. Коли всі відповідності між зображеннями ідентифіковані, можна об'єднати всі зображення разом. Послідовність зображень ділиться на n-2 групи по три зображення і визначаються відповідності між ними. Потім координати зображення наступної групи порівнюються з координатами попередньої.

П’ятий етап – уточнення координат зображення. Узгоджені точки координати зображення, отримані за допомогою SIFT-дескриптора, не зовсім точні. Тому для усунення цієї проблеми використовується алгоритм найменших квадратів.

Шостий етап - створення 3D-моделі. Координати зображення для всіх відповідних точок є результатом застосованого методу. Вони використовуються для орієнтування зображення і створення геометрії розглянутого об'єкта.

Створене графічне представлення об'єктів у вигляді 3D-моделей підносить інформацію в найбільш зручному і природному для людини вигляді, що позитивним чином позначається на якості і оперативності прийняття рішень. Розробка 3D моделей реальних об’єктів є важливою задачею у різних галузях, де має місце застосування БПЛА, зокрема в архітектурі та будівництві.

Список джерел:

1. T.T. Bertrama , T.T. Bockb , A.G.Bulgakovc, A.A.Evgenovd Generation the 3D Model Building by Using the Quadcopter 2014.

2. Lumion. Drone-to-3D Workflow for Architectural Visualizations 2018.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА АНАЛИЗА СООТВЕТСТВИЯ НАУЧНО-ПЕДАГОГИЧЕСКОГО ПЕРСОНАЛА ВУЗОВ КАДРОВЫМ ТРЕБОВАНИЯМ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Кондрюков С.Э.
Научный руководитель – к.т.н, доц. Кулак Э.Н.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. АПВТ, тел. (057) 702-13-26)
e-mail: staskond@gmail.com

Metric appraisals of processes and phenomena for an adequate distribution of moral and material resources are the moral basis of fair social relations in the company, organization and country. An economically efficient system can provide decent wages. However, the democracy of the passive majority is not in a position to adopt a constructive metric for assessing the activities of the team. Therefore, unpopular tight regulatory influences from management, which is characterized by the cyberculture of system management by the company, organization, country, is necessary.

В текущее время имеется большое количество структурных подразделений университета, которые задействованы в процессе мониторинга деятельности кафедр: сами кафедры, отделы мониторинга, службы обработки и валидации данных. Отделы мониторинга не создают продукцию. Они слабо помогают кафедрам уменьшить временные затраты на составление электронных отчетов.

Вместо бумажных отчетов от кафедр и передачи итоговых бумажных документов в службу обработки данных предлагается: 1) Создание облачных электронных форм для заполнения кафедральных отчетов руководителями кафедр с цифровой подписью. 2) Электронный кабинет кафедры, который всегда доступен для постоянного внесения актуальных метрических данных на протяжении года. 3) Все метрические достижения кафедр и университета в целом видно руководителям университета и структурных подразделений.

Для оценивания научно-образовательной деятельности предлагается взвешенный в интервале (0-1) критерий качества Q интегральной деятельности структурного подразделения за текущий год, с учетом средней активности коллектива за последний p лет, который имеет n штатных сотрудников, по m параметрам Pi, где каждый из них приведен до максимального или эталонного подразделения Pi(max) в структуре университета и имеет при каждом параметре экспертный коэффициент научно-образовательной и социальной значимости, который утверждается на раде экспертов-ученых.

Этот критерий качества может быть также использован в виде интегральной метрики оценивания результативности научно-

образовательной деятельности ученого профессора по лучшим достижениям по каждому виду творчества.

Фактически метрика оценивает усредненную, нормированную в интервале (0,1) по m показателям результативности ученого в масштабе кафедры, факультета или университета. Критерий Q, который равен единице, свидетельствует о метриках лучшего (идеального) ученого по всем показателям, принятым в университете. При этом в числители суммы фигурируют личностные достижения, а в знаменателе - лучшие по подразделению или университету численные значения достижений ученых в каждой из n номинаций. Нулевые показатели в предложенной метрике не производят негативного влияния на оценку деятельности ученого или подразделения. Наличие нулевых оценок по определенным видам активности компенсируется высокими значениями параметров в других областях научно-образовательной деятельности. Более того, суперпозиция непересекающихся компетентностей (глубоких специализаций) ученых и кафедр дает возможность получать более высокие абсолютные показатели по основным видам деятельности университета. Кроме того, критерии учитывают совокупную деятельность ученого (сотрудника) за последний m лет, который формирует интегральную матрицу компетентности или достижений на протяжении всего жизненного и творческого цикла сотрудника. Учет истории особенно важен для немолодых сотрудников, которые должны получать достойное материальное награждение за свою продуктивную работу в прошедшие года.

Если важные для университета показатели остались без внимания ученых и кафедр, то мониторинг-сервис должен вернуть к ним внимание сотрудников и руководителей путем повышения значимости соответственных экспертный коэффициентов. Придерживаясь показателей активности каждого ученого, уже не руководитель, а облачный сервис управления ресурсами назначает премии и надбавки в пределах университета или кафедры. Существенно, чтобы такая информация была доступна всем сотрудником, для исключения распространения слухов о несправедливом или тайном распределении вознаграждений.

Список источников:

1. Gaol F. L., Hutagalung F. D. Social Interactions and Networking in Cyber Society. – Springer International Publishing, 2017.

2. Barnaghi P., Sheth A., Singh V., Hauswirth M. Physical-Cyber-Social Computing: Looking Back, Looking Forward // IEEE Internet Computing. – 2015. –Vol. 19, no. 3.

3. Koch F., Koster A., Tiago P. Social Computing in Digital Education. – Springer International Publishing, 2016.

МОБІЛЬНА СИСТЕМА ПЕРЕВІРКИ СТАНУ ЗДОРОВ'Я

Давидов Д.А
Науковий керівник – к.т.н, доц. Філіппенко І.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. АПОТ, тел. (057) 702-13- 06)
e-mail: dmytro.davydov@nure.ua

Given work describes how to put health management system on mobile devices, what components it must have and how to create such system. Mobile devices are used in order to gather data either via communication with a user or with a help of various sensors. Further data can be consumed by a server or processed directly on mobile devices in order to keep fast and stable workflow of system. This work shows what features such type of system can contain, how to put all components together and how to create a typical workflow for such system. Also work specifies merits of doing the workflow on mobile phone.

Система перевірки стану здоров’я використовується для того, щоб своєчасно повідомляти людину про можливі проблеми зі здоров'ям або показувати статистику, зібрану під час користування. Зазвичай система містить такі головні компоненти як мобільний пристрій та сервер. Мобільний пристрій відповідає за збір даних за допомогою сенсорів або мануального вводу даних від користувача, а сервер за обробку цих даних і прийняття рішення. Але комунікація між цими двома компонентами вимагає використовування інтернету, або іншого способу зв'язку, що може вплинути на надійність системи. А для системи, яка відповідає за здоров'я, – надійність один з найголовніших факторів. Отже, якщо виконати сбір і обробку зібраної інформації на пристрої, то це підвищить стабільність роботи. Мета дослідження – надати спосіб слідкування за здоров'ям за допомогою мобільного пристрою не використовуючи серверу, як способу обробки інформації. Задача – показувати людини дані, які були зібрані під час роботи та при необхідності інформувати її про можливі хвороби, наслідки або автономно виконати роботу.

Процес прийняття рішення та аналізу це досить не тривіальна річ, так як є дуже багато факторів, які необхідно враховувати. Для вирішення такої задачі можуть ідеально підійти нейронні мережі. Навчанна на реальних даних нейронна мережа, може аналізувати дані і робити висновки. Для того щоб мати змогу запускати нейрону мережу на мобільному пристрої, Google створила “ML Kit” (Machine Learning Kit), – бібліотека, за допомогою якої можливо запускати нейронні мережі на самих пристроях дуже швидко та ефективно. Якщо даних не багато і вони не потребують глибокого аналізу, то система може сама мати вбудовану логіку класифікації проблеми. Незважаючи на спосіб класифікування проблеми, системі необхідно отримувати вхідні дані для того щоб їх опрацьовувати. Дані збираються за допомогою вбудованих сенсорів в смартфон. За

допомогою сенсора “Акселерометр” девайс збирає інформацію про те, скільки людина рухається, і як результат, мобільний пристрій видає кількість кроків, зроблених людиною. Мобільний пристрій робить це непомітно для користувача і потім видає статистику на екрані у вигляді кількості кроків, яка людина зробила. За допомогою сенсору “Серцебиття” смартфон може отримувати інформацію про кількість ударів серця в хвилину. Але якщо “Акселерометр” може робити свою роботу непомітно, то для використання сенсору “Серцебиття” людині необхідно прикласти палець до камери телефону і система отримує необхідну інформацію. Після цього система визначає, чи в нормі ритм серця, і за необхідності може виконати певну дію, наприклад, відправити SMS або зателефонувати на визначений номер. За допомогою цього система може допомогти родичам користувача швидше дізнатися про проблему або інформувати медичний заклад про можливі проблеми людини. Якщо стався серцевий напад, то в більшості випадків людина не в змозі сама покликати на допомогу і своєчасна медична допомога може врятувати життя. Ці дані також збираються системою і показуються користувачу у вигляді статистики перевірок, за допомогою якої він може слідкувати за станом свого здоров'я. Типовий робочий процес такої системи виглядає так: 1) Збір інформації, 2) Аналіз інформації, 3) Можливе прийняття рішення, 4) Можлива дія, 5) Додавання даних до статистики.

Практична значимість цієї роботи визначається використанням смартфону, як мобільного пристрою для моніторингу стану здоров’я і прийняття можливого рішення на самому телефоні без використання Інтернету, що підвищує надійність такої системи. Така система дозволяє людині в будь якому місці мати доступ до перевірки стану свого здоров’я, та перегляду статистики. А за допомогою автономного прийняття рішення, може допомогти в деяких ситуаціях.

Список джерел:

1. Machine learning for mobile developers [Электронный ресурс] / developers.google.com – Режим доступу: https://developers.google.com/ml-kit/ – 01.11.2018 р. – Загл. с экрана.

2. Errol Ozdalga. The Smartphone in Medicine: A Review of Current and Potential Use Among Physicians and Students [Текст] / Errol Ozdalga, Ark Ozdalga, Neera Ahuja // Journal of Medical Internet Research. – 2012. – Т. 28, №12. – С. 1858–1866.

3. Sensors [Электронный ресурс] / developers.google.com – Режим доступу: https://developers.google.com/guide/topics/sensors/ – 17.04.2018 р. – Загл. с экрана.

РОЗРОБКА ШАБЛОНУ ОПИСУ КІНЦЕВИХ АВТОМАТІВ З ВИКОРИСТАННЯМ ТЕМПОРАЛЬНИХ ГРАФІВ

Кучеренко І.О.
Науковий керівник – доц. Кулак Е.М.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. АПОТ, тел. (057) 702-13- 26)
e-mail:iryna.kucherenko@nure.ua

The paper considers ways to implement digital devices, such as automatic and software hardware implementation, and the main features of automated programming. The problem of the existence of two measurements of time in digital devices is considered, it is proposed to use temporal graphs in developing a template describing the algorithms of the operation of finite automata, which takes into account the real-time delay for each of the states of automata. This graph resolves a conflict between two dimensions, which will help when creating a pattern description algorithms functioning.

Будь-який цифровий пристрій, котрий реалізує алгоритм обробки інформації та її управління може бути реалізовано апаратним або програмно-апаратним способом. При програмно-апаратному способі алгоритм реалізується на апаратно-орієнтованій мові програмування. Найпопулярніша мова для цього – С зі спеціальними бібліотеками. Апаратна сторона реалізується, як правило, на різноманітних мікроконтролерах. При апаратному способі алгоритм описується на мові описання апаратури HDL, синтезується інструментальними засобами систем автоматизованого проектування (САПР) та імплементується у ПЛІС або ASIC. При написанні алгоритму функціонування цифрових пристроїв використовуються автоматні програми, у яких розділяється написання логіки програми та описання семантики. Автоматні програми мають тільки три вида функцій: функції переходів, функції виходів та функції реалізації затримок і переходів у новий стан. Вони мають шаблон та використовують оператори вибору, умовні оператори та функції таймеру або фронта.

Об’ект дослідження: шаблони описання кінцевих керуючих автоматів на мовах програмування та описання апаратури. Предмет дослідження: використання темпоральних графів при розробці шаблонів описання кінцевих керуючих автоматів на мовах програмування та описання апаратури Ціль дослідження: підвищення ефективності процесу розробці кінцевих керуючих автоматів с часовим (не мікропрограмним) керуванням на мовах програмування та описання апаратури. Задача – використати темпоральний граф при розробці єдиного шаблону описання автоматних пристроїв у стилі автоматного програмування.

Пристрої логічного управління, побудовані на основі кінцевих автоматів, функціонують одразу у двух вимірах: в автоматному часі та у

реальному часі. Автоматний час вимірюється в автоматних тактах. Автоматний такт – дискретних відрізок часу за який автомат переходить з одного стану в інший. Тривалість такого такту визначається частотою синхросигналу Clk. Реальний час визначається часовими параметрами алгоритму функціонування пристрою. Для усунення протиріччя пропонується використання темпорального графа переходів, який описується розширеною функцією переходів.

$$Z(t+1) = f(X(t), Z(t), T)$$

У такому графі кожному стану становиться у відповідність затримка Ti, яка визначається числом автоматних тактів, протягом яких автомат знаходиться у даному стані. При цьому темпоральний граф переходів є не тільки візуальним відображенням алгоритму функціонування кінцевого керуючого автомата, а й його повною математичною моделлю. Затримка в кожній вершині темпорального графа переходів реалізується через петлю, умовами для якої є підрахунок числа тактів Clk, що схемно реалізується лічильником в ПЛІС або таймером з перериванням в МК. Це означає, що темпоральний граф ідеально підходить для розробки шаблону опису алгоритмів функціонування кінцевих автоматів у стилі автоматного програмування.

Наукова новизна даного досліду – ефективність при використанні темпоральних графів для розробки шаблонів опису кінцевих автоматів та використанні стилю автоматного програмування при написанні програмного коду на мові програмування С та мові опису апаратури VHDL. Шаблони опису алгоритмів функціонування кінцевих автоматів в системах логічного управління на мовах VHDL і С можуть бути використані новачками проектувальниками цифрових систем логічного управління.

Список джерел:

1. Гамма Э., Хелм Р., Джонсон Р., Влассидес Дж. Приемы объектно-ориентированного проектирования. Паттерны проектирования. СПб.: Питер, 2001. – 368 с.

2. Шалыто А. А. Автоматное программирование / Н.И. Поликарпова, А.А. Шалыто. – Спб.: Питер, 2008. – 168 с.

3. 4.Haskell R. Digital Design Using Digilent FPGA Boards - VHDL / Active-HDL Edition / Richard E. Haskell, Darrin M. Hanna. – LBE Books Rochester Hills, MI, 2009.– 381 p.

4. Shkil A.S. Design automation of easy-tested digital finite state machines / M.A. Miroschnyk, Y.V. Pakhomov, A.S. Shkil, E.N. Kulak, D.Y. Kucherenko // Radio Electronics, Computer Science, Control. – 2018. – №2. – P. 117-124.

ІНТЕЛЕКТУАЛЬНА СИСТЕМА УПРАВЛІННЯ ОЦІНЮВАННЯ СТУДЕНТІВ НАВЧАЛЬНОГО ЗАКЛАДУ

Мамішев Р.І.
Науковий курівник – к.т.н., доц. Кулак Е.М.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. АПОТ, тел. (057) 702-13-06)
e-mail: rauf.mamishev@nure.ua, тел. (066) 704-97-02

The relevance of the review of the assessment process is determined by the modern strategic goals of education, the need to improve the level of education, taking into account international standards and modern requirements for the quality of education, the need to develop uniform assessment requirements. learning outcomes and graduate competitiveness.

The evaluation of the system in the education system is unique because it is the most obvious integration into the educational space and contains the basic principles underlying the educational process as a whole.

An electronic journal is a set of software tools for recording student progress and monitoring student attendance.

Сучасному студентові необхідна віртуальна система, що дасть змогу слідкувати за навчальним процесом у режимі реального часу[1]; електронний журнал, який надаватиме можливість контролювати якість навчального процесу університету; прозора система контролю результатів оцінювання.

Науково-практична задача дослідження – створення електронного журналу університету, з відображенням контенту у браузері Chrome, з авторизацією під різними статусами користувачів, та наданням доступу до функціональності системи в залежності від статусу.

Ринкова привабливість дослідження полягає в істотному зменшенні часових та матеріальних витрат, що на даний момент потребуються для управління оцінюванням студентів. Дистанційний доступ до матеріалів викладання, журналу оцінювання та учбового плану навчального процесу.

Мета дослідження – істотне підвищення продуктивності викладання та вивчення предметної області[2]. Впровадження прозорого оцінювання, надання можливості доступу до журналу дистанційно та полегшення обробки даних для підсумування успішності студентів з курсу.

Наукова новизна – зміна процесу оцінювання студентів з традиційного на технологічний. Універсальна система контролю якості освіти для начальний закладів. Прозоре оцінювання студентів, доступ до журналу дистанційно у будь-який момент часу[2].

Вимоги до взаємодії з системою:

– авторизація. Для того щоб мати доступ до функціональних можливостей системи потрібно пройти авторизацію. Доступ до даного функціоналу надається в залежності від статусу користувача:

а) викладач. Має можливість формувати сторінки журналу. Додавати дані до БД та переглядати сторінки журналу груп та предметів, які викладає.

б) студент. Має можливість переглядати сторінки журналу своєї групи.

в) завідуючий кафедри. Має можливості подібну попереднім статусам, а також видаляти та змінювати існуючі дані з БД.

– взаємодія с базою даних. Система має підтримувати CRUD операції.

– інтерфейс підготовки електронного журналу. Кожний семестр починається з підготовки робочого процесу. Викладачеві надається доступ до створення сторінки предмету в електронному журналі групи. Для цього потрібно пройти декілька етапів:

а) знайти себе серед списку викладачів. Список групується в залежності від факультету та кафедри;

б) обрати групу зі списку. Список формується в залежності від факультету, напряму підготовки та дати формування;

в) обрати предмет зі списку. Список формується на основі семестрового плану;

г) обрати види занять;

д) обрати кількість білів за заняття;

Електронний журнал успішності дає дистанційний доступ до оцінок студентів. При введенні логіна та пароля кожен має змогу контролювати свої оцінки, заборгованості та індивідуальний рейтинг серед студентів групи[3]. Електронний журнал містить теми усіх занять, що дає змогу підготувати пропущені заняття. Батьки мають змогу слідкувати за відвідуванням занять своїх дітей[3]. Електронний журнал робить навчання прозорим. Дана система обробляє та записує дані до бази даних, що дає змогу маніпулювати даними для отримання рейтингів та карти якості освіти у студентів різних років, що забезпечить підтримку підготовки кадрів на належному рівні. Оцінки студентів будуть зберігатися у системі на протязі багатьох років. Забезпечить захист оцінкам студентів від будь-яких вад.

Список джерел:

1. Gaol F. L., Hutagalung F. D. Social Interactions and Networking in Cyber Society. – Springer International Publishing, 2017.

2. Meiselwitz G. Social Computing and Social Media. – Springer International Publishing, 2016.

3. Koch F., Koster A., Tiago P. Social Computing in Digital Education. – Springer International Publishing, 2016.

ПЕРСОНАЛІЗАЦІЯ МОБІЛЬНОГО ДОДАТКУ

Лебедєв В.О., Кіян С.О.
Научный руководитель – проф. Аксак Н.Г.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. ЭВМ, т. 7021354)
e-mail: lebedevvalen@gmail.com, (063)-145-17-36,
svetulyakiyan@gmail.com, 050-8014306

The existing methods of personalization of resources were analyzed and their drawbacks were revealed. Issues related to personalization with Big Data were considered, as well as examples of networks that introduced the technology of personalization using Big Data. A mobile application with built-in personalization on the backend was developed

Раніше аналітика трафіку була дуже дорогим задоволенням. Тільки найбільші компанії були здатні це собі дозволити. З часом софт для тестування та аналітичні інструменти “демократизувались” й тим самим сприяли збільшенню кількості аналітиків, здатних використовувати їх потрібним чином. Саме через це сьогодні для веб-сайтів абсолютно неможливо не думати про якість трафіку - звідки він, куди і яким чином він конвертується. Персоналізація, або можливість оптимізувати послання для певних клієнтів, - один із найбільш популярних трендів нашого часу. Все через те, що вона дає брендам можливість запропонувати клієнтам саме те, що вони хочуть. Однак персоналізація значно еволюціонувала з того часу, коли під нею розумілося використання імені отримувача в повідомленнях. Сьогодні все йде до того, щоб пропонувати винятковий досвід кожному користувачу.

В [1-4] докладно розглянуто те, який вплив персоналізація має на сприйняття користувачами програмного забезпечення, проблеми із якими стикаються розробники під час впровадження персоналізації на сайти або в додатки, питання стосовно персоналізації за допомогою Big Data, а також приклади мереж, у роботу яких впроваджена технологія персоналізації за допомогою Big Data.

У багатьох випадках логіка програми найкраще контролюється на сервері, щоб уникнути втручання на стороні клієнта. Cloud Functions повністю ізольовані від клієнта, тому розробник може бути впевненим, що його функції є приватними та безпечними та не можуть бути спроектовані у зворотному порядку.

Для персоналізації запитів з серверу слід розглянути декілька алгоритмів пошуку відстані редагування та провести тести. В роботі розглянуто відстань Хеммінга, відстань Левенштейна та відстань Дамерау-Левенштейна. Через те, що персоналізація ресурсу має відбуватись за списком інтересів користувача (їх він обирає в мобільному додатку), обраний алгоритм має обов’язково враховувати такі зміни, як

перестановки всередині слів, а також перестановки слів між собою. В таблиці наведено результати тестів.

Таблиця – Результати тестів

Очікуваний рядок	Meet Teen Die	
Тестові рядки	Meat Team Lie	Mete Tene Dei
Відстань Хеммінга	4	5
Відстань Левенштейна	4	5
Відстань Дамерау-Левенштейна	4	3
Тестові рядки	Die Teen Meet	Teen Die Meet
Відстань Хеммінга	11	9
Відстань Левенштейна	6	8
Відстань Дамерау-Левенштейна	6	8

Результати отримані після проведення тестів свідчать про те, що відстань Хеммінга відповідає поставленим умовам, але вона ніяк не враховує наявність слова в тексті. Також можна помітити, що відстань Дамерау-Левенштейна, на відміну від відстані Левенштейна не враховує перестановки в середині слів. Таким чином, в нашому випадку найбільше підходить відстань Левенштейна.

Персоналізація за допомогою Big Data ефективно працює якщо в системі є велика кількість користувачів, а кількість зібраної інформації дійсно величезна. Інакше така персоналізація приносить мало користі. А ось її альтернатива (прогресивна персоналізація) є ефективною навіть у випадках коли даних не дуже багато.

Список джерел:

1. Big Data, Personalization and the No-Search of Tomorrow - https://www.searchtechnologies.com/blog/big-data-search-personalization.

2. The Difference Between Customization and Personalization - https://uxplanet.org/the-difference-between-customization-and-personalization-624ddd70b163.

3. Big data, personalization and market manipulation - https://docplayer.net/11243271-Big-data-personalization-and-market-manipulation.html.

ОПЫТ ПРАКТИЧЕСКОГО ВНЕДРЕНИЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Степанова К.А.
Научный руководитель – проф. каф. АПВТ, д.т.н. Кривуля Г.Ф.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. АПВТ, тел. (057) 702-13-26)
e-mail: kristina.stepanova@nure.ua

Wireless Sensor Networks and the main features and difficulties in implementation have been considered. Some solutions of problems of introducing WSN using MeshLogic technologies have been offered.

В последние годы активное развитие получили технологии беспроводных сенсорных сетей – многоячейковых сетей с низкой скоростью передачи данных и сверхнизким энергопотреблением узлов, основной сферой применения которых является сбор по радиочастотным каналам связи показаний от множества датчиков в следующих прикладных областях: автоматизация зданий, промышленная автоматика, безопасность и оборона, здравоохранение и сельское хозяйство. Цель исследования – рассмотреть основные особенности и сложности, которые возникают на практике при внедрении беспроводных сенсорных сетей и систем телеметрии. Задача – описать некоторые варианты решения проблем внедрения БСС с помощью технологий MeshLogic.

В БСС используются маломощные радиоканалы, отличающиеся значительными колебаниями и асимметрией качества связи (вероятность успешного приема пакета), причинами которых являются неравномерность затухания сигнала в сложных условиях распространения радиоволн, случайные отклонения параметров приемопередатчиков от номинальных значений и изменения локальной помеховой обстановки. При этом надежность беспроводных соединений между узлами сети оказывает непосредственное влияние на пропускную способность и энергопотребление узлов, так как низкое качество радиоканала приводит к возрастанию числа потерь пакетов и повторных передач, а также повышается вероятность перевыбора маршрута доставки данных, вызванного отказом одного из каналов на пути следования пакета. Поэтому наличие актуальной информации о параметрах беспроводных соединений является необходимым условием для получения высоких показателей качества обслуживания БСС.

В общем случае оценка качества радиоканала выполнятся в два этапа: мониторинг параметров канала и вычисление метрики качества на основе накопленных значений. В сетевом стеке MeshLogic используется пассивный мониторинг канала, то есть в фоновом режиме анализируется только существующий в сети трафик без передачи тестовых пакетов специально для целей оценки качества радиоканалов. По сравнению с

активным мониторингом (периодически передаются специальные сигнальные сообщения) данный подход минимизирует энергозатраты узлов, но при этом снижается скорость реакции на изменения в топологии сети, поэтому этот вариант применим в сетях со стационарной топологией, в которых все или большинство узлов не перемещаются, а параметры окружающего пространства изменяются медленно.

В БСС информация от многих сенсорных узлов поступает по радиоканалу в одну точку сбора, поэтому надежность всей системы телеметрии зависит от степени доступности шлюза. Для снижения этой зависимости рекомендуется использовать в системе несколько шлюзов, при этом в зависимости от требований прикладной задачи узлы могут передавать пакеты только ближайшему шлюзу или всем шлюзам для резервирования данных. Кроме того, установка в сети нескольких шлюзов позволяет более равномерно распределить сетевой трафик между узлами, чтобы их элементы питания разряжались примерно с одинаковой скоростью.

Существуют ситуации, когда часть узлов сети большую часть времени не имеют возможности передать телеметрическую информацию из-за отсутствия связи с каким-либо другим узлом, а при этом требуется, чтобы узлы постоянно с заданным периодом выполняли измерения независимо от доступности радиоканала. Для этого в беспроводных узлах можно использовать встроенный кольцевой буфер для хранения результатов измерений, содержимое которого асинхронно передается по радиоканалу при появлении возможности.

Научная новизна определяется использованием БСС для решения задач, в которых использование традиционных проводных каналов связи ограничено или невозможно по техническим, экономическим или организационным причинам. Несмотря на то, что опыт практического использования подобных систем мал, можно смело заявить, что беспроводные системы телеметрии на основе БСС являются эффективным средством мониторинга в различных областях применения.

Список источников:

1. Аристова Н.И. Беспроводная связь в промышленной автоматизации: современные стандарты и области применения // Автоматизация в промышленности. 2013. № 1.

2. Баскаков С.С. Беспроводные сенсорные сети: вопросы и ответы // Автоматизация в промышленности. 2008. № 4. С. 34-35.

РАЗВЕРТЫВАНИЕ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Срибная М.А.
Научный руководитель – проф. каф. АПВТ, д.т.н., Кривуля Г.Ф.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. АПВТ, тел. (057) 702-13-26)
e-mail: mariia.sribna@nure.ua

The work is devoted to Wireless Sensor Networks (WSNs), which are widely used for various civilian and military applications, and thus have attracted significant interest in recent years. The present work represents a research of the important problem of optimal deployment of WSNs in terms of energy consumption and coverage, what provides the biggest possible measurement coverage and maximum service life of a WSN after the situation where a number of nodes have failed. This work presents a self-relocation algorithm for optimizing of a distributed coverage using the average relative position between pairs of sensors.

Беспроводные сенсорные сети (WSN) широко используются для различных гражданских и военных задач и, таким образом, вызвали значительный интерес в последние годы. Цель исследования – анализ существующих решений проблемы оптимального развертывания WSN с точки зрения энергопотребления и покрытия. Задача – нахождение алгоритма развертывания с максимальным диапазоном измерения и минимальным энергопотреблением, что обеспечит оптимальный охват измерения и максимальный срок службы, а также с возможностью самовосстановления работы WSN после того, как ряд узлов вышел из строя.

В данной работе представлен алгоритм самоперемещения для оптимизации распределенного покрытия с использованием среднего относительного положения между парами датчиков. При выполнении оптимизации используются как относительное расстояние, так и направление. Поэтому для применения этого алгоритма требуются системы локализации. Для того, чтобы минимизировать затраты энергии на зондирование, используются датчики с регулируемым диапазоном.

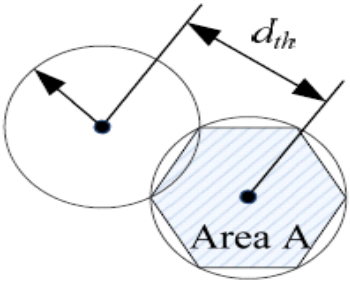


Рисунок 1 – Оценка порога расстояния

Алгоритм использует идеальную модель покрытия для расчета порога повторного использования датчиков. Несмотря на то, что порог покрытия можно рассчитать по уравнению, для датчиков с регулируемым диапазоном это не применимо. В данном алгоритме используется средняя площадь, которая должна быть покрыта каждым датчиком для оценки радиуса восприятия.

Цель данного алгоритма – переместить случайно развернутые датчики и выполнить настройку диапазона измерений, чтобы достичь оптимального покрытия с минимальным потреблением энергии. Алгоритм состоит из трёх этапов: первый выполняет принятие решения, второй перемещает датчики в новое место, третий выполняет настройку диапазона чувствительности. На первом этапе каждый датчик обнаруживает себя и передает информацию о своем местоположении другим в пределах своего диапазона связи. Датчики, которые могут общаться друг с другом, называются соседями, у каждого есть своя коммуникационная окрестность. Соседство зависит от дальности связи, её радиуса и расположения поля (то есть препятствий). Датчики получают информацию о местоположении других в процессе широковещательной передачи, и затем решают, перемещаться или нет в соответствии с собранной информацией о местоположении. На втором этапе они перемещаются только если критерии движения соблюдены. После перемещения датчиков они снова транслируют свои местоположения, и алгоритм запускается с начальной фазы.

Алгоритм подходит для мобильных беспроводных сенсорных сетей со случайным начальным развертыванием и направлен на изменение относительного расстояния датчиков в разных направлениях. Он использует только часть относительных расстояний для расчета для оптимизации. Этот алгоритм надежен даже когда доступна лишь неточная информация о географическом местоположении.

В этой работе был проведён анализ оптимизации покрытия для мобильных беспроводных сенсорных сетей. Также было обращено внимание на проблему неточной локализации систем. Научная новизна состоит в нахождении нового алгоритма оптимизации со свойствами самовосстановления. Алгоритм также является самовосстанавливающимся, поэтому его можно использовать и в суровых условиях.

Список источников:

1. J. Huanxiang, W. Yong and T. Xiaoling, "Localization algorithm for mobile anchor node based on genetic algorithm in wireless sensor network, "International Conference on Intelligent Computing and Integrated Systems", Guilin, China, October 22-24, 2010, pp. 40–44.

ПРОЕКТИРОВАНИЕ СИСТЕМ ЛОГИЧЕСКОГО УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ ТЕМПОРАЛЬНОГО АВТОМАТА

Малахов Н.В.
Научный руководитель – д.т.н., доц. Шкиль А.С.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. АПВТ, тел. (057) 702-13-26)
e-mail: malakhov.mykyta@nure.ua, тел. 380508242402

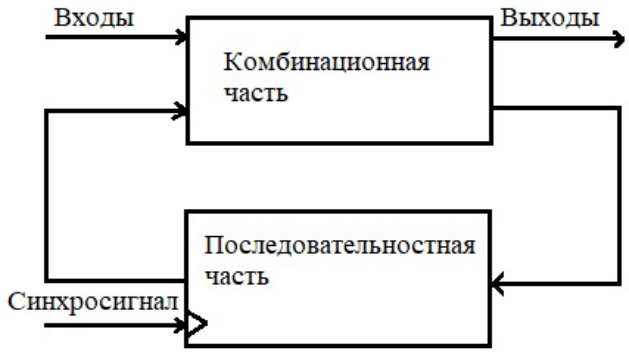
Approaches to the design of logical control systems are discussed in the given work. Particular attention is paid to the benefits of the implementation of the device on a programmable logic integrated circuit. The concepts of finite state automata and timed automata are analyzed in the work. A Moore finite state automata model construction method for a given digital control system is proposed. The method involves using of a counter to implement clock constraints.

При реализации алгоритма функционирования систем логического управления активно применяются микроконтроллеры [3,4]. Альтернативой программно-аппаратному способу описания алгоритма функционирования системы является аппаратный, когда описание алгоритма формируется на языке описания аппаратуры, после чего синтезируется в программируемую логическую интегральную схему. Цель исследования — существенное увеличение быстродействия и гибкости разрабатываемых систем логического управления за счет аппаратного способа реализации алгоритма функционирования устройства, что дает возможность снизить затраты на производство данных систем. Задача — разработка метода построения конечного автомата для устройств логического управления, функционирующих в реальном времени, который может быть синтезирован в программируемую логическую интегральную схему.

Для описания систем логического управления предлагается использовать модель темпорального автомата. Темпоральный автомат определяется кортежем: 1) множество состояний управления; 2) множество действий; 3) множество таймеров; 4) отображение, связывающее состояния управления и временные инварианты; 5) множество переходов; 6) начальное состояние [1]. Распространенным подходом к реализации систем, функционирующих в реальном времени, является реализация устройства на микроконтроллере. Для синтеза описания устройства в программируемую логическую интегральную схему, необходимо модель темпорального автомата преобразовать в синтезируемую модель.

Дискретный конечный автомат - это модель, которая может быть сформирована с помощью языка описания аппаратуры. Данный автомат представляется кортежем: 1) множество входных символов; 2) множество выходных символов; 3) множество состояний; 4) функция переходов; 5)

функция выходов; 6) инициальное состояние. Структурная модель конечного автомата состоит из последовательностной части, которая представляет синхронные триггеры, предназначенные для хранения состояния автомата, и комбинационной части, которая представляет схемы формирования функций выходов и функций переходов [2].



Утверждается возможность построения конечного автомата Мура на основе заданного темпорального автомата. Необходимо, чтобы каждому состоянию темпорального автомата с заданным временным инвариантом соответствовало состояние автомата Мура, от которого существовал переход в это же состояние, при этом данный переход должен осуществляться при соответствующем значении, которое хранится в триггерах счетчика. Временные инварианты темпорального автомата реализуются с помощью счетчика.

Определен метод построения дискретного автомата для устройств логического управления, функционирующих в реальном времени, для данного подхода характерно проектирование устройства на ПЛИС, что позволяет повысить производительность разрабатываемых устройств за счет увеличения затрат времени на разработку интерфейса ввода-вывода. Практическая ценность исследований заключается в возможности аппаратной реализации систем логического управления на основе модели структурного автомата, что дает возможность увеличить гибкость и быстродействие разрабатываемых систем.

Список источников:

1. Alur R. A theory of timed automata / R. Alur, D. L. Dill. A // Theoretical Computer Science.– 1994. – V.126/ – N 2. – P. 183-235.

2. Haskell R. Digital Design Using Digilent FPGA Boards - VHDL / Active-HDL Edition / Richard E. Haskell, Darrin M. Hanna. – LBE Books Rochester Hills, MI, 2009. – 381 p.

3. Шалыто А.А. Автоматное программирование / Н.И. Поликарпова, А.А. Шалыто. – Спб.: Питер, 2011.– 167 с.

4. Шалыто А.А. Использование граф-схем и графов переходов при программной реализации алгоритмов логического управления / А.А. Шалыто // «Автоматика и телемеханика», 1996. N6, с. 148-158; N7, с. 144-169.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ КОНТРОЛЕРА ARDUINO ТА АДРЕСНОЇ СВІТЛОДІОДНОЇ СТРІЧКИ ДЛЯ РОЗРОБКИ ПРИСТРОЮ ПО ОБРОБЦІ ЗВУКУ З УТВОРЕННЯМ КОЛЬОРОВИХ ОБРАЗІВ

Несчотний В.В
Науковий керівник – проф. Немченко В.П.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. АПОТ, тел. (057) 702-13-26
e-mail: vladyslav.neschotnyi@nure.ua, тел (095) 349-17-15

This paper describes the features of the use of the Arduino controller and the dedicated LED tape for the development of a device for processing sound to produce color images.

На сьогодні ринок має багато пристроїв по обробці звуку та утворенні ними кольорових образів. Більшість з них використовують контролер, як засіб керування. У ньому міститься програма за якою він працює. Контролер може мати кнопки керування на своєму корпусі або керуватись за допомогою пульту дистанційного керування. Також він повинен мати вхід для аудіосигналу. Кольорові пучки світла з’являються на екранах, прожекторах з різнокольоровими фільтрами, на світлових смужка які складаються з великої кількості світлодіодів. *Мета дослідження* – розібратись в особливостях використання світлодіодної стрічки та платформи Arduino, для обробки звукового сигналу та створення світломузики. Задача – проаналізувати особливості та переваги плат Arduino і світлодіодної стрічки, а також їх використання для пристрою обробки звукового сигналу та створення світломузики, який на відміну від аналогів буде більш дешевий.

Arduino – це відкрита програмована апаратна платформа для роботи з різними фізичними об'єктами, інакше – контролер, який реагує на зміну одних параметрів зміною інших. Вона являє собою просту плату ввід-вивід з мікроконтролером, а також спеціальне середовище розробки для написання програмного забезпечення мікроконтролера.

Існує багато видів контролерів Arduino де, їх вибір впливає на: параметри (швидкість ЦП і швидкість передачі даних), що використовуються при компіляції і завантаженні скетчів і на налаштування запису завантажувача мікроконтролера.

Для виконання поставленої задачі краще використовувати контролер Arduino Nano v3.0 він входить в трійку найпопулярніших плат Arduino. Плата має багато плюсів серед аналогів такі як:

- не висока ціна на ринку (близько 90 грн.);
- компактний розмір, який дозволяє вбудовувати плату в невеликий корпус;
- використовує той же мікроконтролер що й Arduino Uno;

- прошивається через Micro-USB вбудованим Bootloader-ом.

Буде використовуватися світлодіодна конструкція – стрічка в якості джерела світла. Вона являє собою стрічку з адресних діодів, один такий світлодіод складається з RGB світлодіоду і контролера. Так, всередині кожного світлодіода вже знаходиться контролер з трьома транзисторними виходами. Завдяки такій начинці у нас є можливість управляти кольором будь-якого світлодіода в стрічці і створювати приголомшливі ефекти. Адресна стрічка може мати 3-4 контакти для підключення, два з них завжди живлення (5V або 12V і GND), а інші (один або два) – логічні, для управління. Для управління стрічкою використовуються готові контролери.

Якщо використовувати контролер Arduino, то стрічку потрібно правильно підключити. Команди в стрічці передаються від діода до діода, почерзі. У стрічки є початок і кінець, напрямок рух команд на деяких моделях зазначено стрілкою. У стрічки є три контакту. Два на живлення, а третій на початку стрічки називається DI (digital input), а в кінці – DO (digital output). Стрічка приймає команди в контакт DI. Контакт DO потрібен для підключення додаткових частин стрічки або з'єднання матриць. Цифровий вхід стрічки йде безпосередньо на вхід контролера всередині діода, тому між стрічкою і керуючим виводом Arduino потрібен струмообмежуючий резистор з номіналом 200 – 500 Ом, він обмежує струм, і керуючий вивід Arduino не перевантажується (тобто резистор – захист виводу Arduino по струму). Миготіння стрічки створює імпульсні перешкоди на лінію живлення, а якщо стрічка і контролер живляться від одного джерела – перешкоди йдуть на мікроконтролер і можуть стати причиною нестабільної роботи. Для згладжування таких перешкод рекомендується ставити конденсатор на живлення стрічки та Arduino.

Компактні розміри, велика гама кольорів і мале споживання електроенергії визначили широке застосування адресної світлодіодної стрічки.

Існує велика кількість світломузичних пристроїв, але вони багато коштують. Використовуючи контролер Arduino а також адресну світлодіодну стрічку можна самостійно зібрати схожий пристрій, з таким же функціоналом, але ціною до 25$. Найближчий за функціоналом аналог на ринку коштує щонайменше 150$, що зробить розроблений пристрій дуже перспективною розробкою на ринку аудіоелектроніки.

Список джерел:

1. Blum J. Exploring Arduino / J. Blum. – Wiley, 2013. – 384 с.
2. Купкин, И. В. Обзор светодиодных лент типа RGB наиболее распространенных производителей / И. В. Купкин, А. А. Горбунов // Научные труды SWorld. – 2014. – Т. 5, №.3. – С. 80–82.

ОЦЕНКА ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ПЛИС И DSP ДЛЯ ЗАДАЧ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

Громова С.А.
Научный руководитель – Филиппенко И.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. АПВТ, тел. (057) 702-13-26),
e-mail: yokocha477@gmail.com, тел. (057) 702-13-26

The main advantages and disadvantages of using FPGAs and DSP processors as applied to the task of digital signal processing are considered. A comparison of the computational capabilities of modern representatives of FPGA chips and DSP processors is given on the example of the implementation of the integer Fourier transform.

В современных системах при решении задач цифровой обработки сигналов во главу угла всегда ставится выбор технических средств. Осуществление сложных алгоритмов ЦОС в реальном масштабе времени требует применения эффективных базовых алгоритмов, таких как фильтрация, спектральный анализ. Для реализации задач ЦОС могут быть использованы как цифровые сигнальные процессоры (DSP), современные микроконтроллеры, а также ПЛИС. Использование DSP процессоров, несмотря на их широкое распространение, сопровождается проблемами, связанными с отсутствием какой-либо стандартизации языков программирования. При переходе на новую элементную базу необходимо разрабатывать проект заново.

Все чаще предпочтение отдается FPGA с гибкой архитектурой, высоким уровнем параллелизма работы и достаточно высокой производительностью, особенно при разработке систем, выпускаемых малыми или средними сериями. Однако, FPGA не могут выполнять операции с плавающей запятой, если ключевое требование задачи – точность. В тоже время часто необходимо решение задач для большого числа БПФ, обычно выполняемых с плавающей запятой, поскольку операции с фиксированной запятой ограничивают динамический диапазон получаемого решения, т.е. при создании этих устройств следует применять DSP. Кроме того, операцию обращения (или деления) матрицы также лучше выполнять с помощью DSP.

Необходимо также учитывать и другие важные различия между DSP и FPGA. Так, быстродействие DSP велико, но такой процессор может одновременно выполнять лишь несколько операций, тогда как FPGA способны выполнять одновременно практически неограниченное число операций, обеспечивая высокий параллелизм работы.

Самые простые методы сравнения микроконтроллеров, ПЛИС и цифровых сигнальных процессоров заключаются в сравнении тактовых частот, объемов памяти и максимальном числе преобразований. В более

сложных методах анализируется число определенных операций, таких как умножение и сложение, выполняемых в единицу времени. Самые сложные методы сравнения основываются на сравнении скорости выполнения алгоритмов, таких как быстрое преобразование Фурье, КИХ- и БИХ-фильтрация, свертка и т. д.

Процессор ADSP-BF533 является представителем семейства процессоров Blackfin с расширенными возможностями, которые обладают значительно большей производительностью и меньшей потребляемой мощностью. Архитектура ядра процессора Blackfin является архитектурой с единым набором команд, включающей ядро обработки сигналов со сдвоенным блоком умножения-накопления, имеющей ортогональный набор команд, характерный для RISC-микропроцессоров, обладающей гибкостью команд типа SIMD и мультимедийными возможностями.

Одними из основных операций ЦОС являются операции умножения, умножения с накоплением (MAC), сложения, а также операции пересылки между памятью и вычислительными модулями. ADSP-BF533 поддерживает эти операции аппаратно. Также для реализации ЦОС-алгоритмов очень часто используются внутренние циклы. Такие циклы содержат относительно небольшое количество команд, которые чаще являются командами ветвления.

Применение ПЛИС выгодно при построении систем, в которых требуется многоканальная обработка данных или многоступенчатая фильтрация. ПЛИС позволяют эффективно реализовать сложные параллельные алгоритмы даже на микросхемах относительно недорогих семейств. При этом процессоры DSP имеют преимущество при выполнении последовательных или насыщенных циклами алгоритмов, а также при реализации сложных алгоритмов, требующих вычислений с плавающей точкой. Процессоры лучше подходят для реализации малобюджетных проектов, проектов, не требующих большой вычислительной мощности, а также для создания устройств с низким энергопотреблением

Список источников:

1. Cortex-M3 Technical Reference Manual. ARM Limited.

2. Куприянов М. С., Матюшкин Б. Д., Цифровая обработка сигналов: процессоры, алгоритмы, средства проектирования. - СПб.: Политехника, 1999.– 215 с.

ВИКОРИСТАННЯ R-ФУНКЦІЙ У 3D МОДЕЛЯХ

Гайдар М.І.
Науковий керівник – Асистент кафедри системотехніки Морозова А.І
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Системотехніки,
тел. (057) 702-13-06)
e-mail: maksym.haidar@nure.ua

The given work is devoted to the study of the work of Rvachev functions in 3D models.

The development of modern technology is impossible without the availability of reliable and efficient methods for numerical analysis of the strength and durability of complex engineering structures. The use of a computer for analyzing the constructive properties of designed structures is based on the methods of computational mathematics, based on the idea of transition from an extended task to a discrete one, when the continuous object under study is replaced by some final model.

R-функция (функция Рвачёва) – числовая функция действительных переменных, знак которой вполне определяется знаками её аргументов при соответствующем разбиении числовой оси на интервалы $(-\infty; 0)$ и $[0; +\infty)$. Впервые R-функции были введены в работах В. Л. Рвачёва.

Процедурное моделирование с полей расстояний, начинающихся с Риччи (Ricci, 1973); R-функции (Рвачев, 1963) впервые были применены для моделирования формы более 20 лет спустя (см. (Shapiro, 1994) и (A. Pasko et al., 1995)).

Задача формализации исходного описания геометрических объектов и их представления в памяти компьютера является достаточно сложной. Для этих целей применяются различные геометрические модели: каркасные, поверхностные, твердотельные, объектно-ориентированные и т.д.

Но на практике чаще всего используют именно твердотельные геометрические модели, в которых в явной форме содержатся сведения о принадлежности элементов конструкции внутреннему или внешнему по отношению к ней пространству (модель объекта с замкнутым объемом).

Существует несколько основных подходов к описанию геометрических объектов: построение геометрических моделей в виде некоторой комбинации базовых примитивов, объединенных набором Эйлеровых операций, реконструкция трехмерной геометрической модели объекта по имеющимся техническим чертежам его проекций, параметрическое (функциональное) описание границы объекта.

Наиболее универсальным и эффективным является именно функциональный подход, т.к. с его помощью можно сравнительно легко и однозначно построить модель геометрического объекта произвольной формы. Теория R-функций позволяет с помощью элементарных

математических соотношений в неявном виде формально описать произвольный геометрический объект.

В основе теории R-функций лежит идея алгебры предикатов, представленных выражениями вида $f(x_1, \ldots, x_n) = m$ (1), где m – некоторое численное значение, качественно характеризующее предикат по шкале значений. При этом m = 0 условно принимается за поверхность геометрического объекта, а отрицательные и положительные области разделяют внешнюю и внутреннюю его части, соответственно.

Под геометрическими формами в трехмерном декартовом пространстве понимаются такие геометрические области, которые поддаются единому аналитическому описанию вида (1), а также параметрическому представлению, выраженному через шаг или угол поворота. Таким образом, такие элементарные геометрические фигуры, как квадрат, куб или призма, не подходят под это определение по первому признаку. Они образуются пересечением прямых линий или плоскостей, которые теперь представлены простыми геометрическими формами. Окружность, сфера, тор и другие фигуры вращения, образуемые кривыми или поверхностями второго и выше порядков, попадают под это определение, поскольку могут быть представлены одним или несколькими функциями вида (1), и поддаются параметрическому описанию.

Применение аппарата аналитических функций В.Л. Рвачева дает возможность иметь в системе геометрического моделирования пустое множество объектов-примитивов или предикатов в предположении, что пользователь определит их сам либо в символьном виде с помощью формул, либо посредством вычислительных процедур.

На основании вышесказанного можно сделать вывод о том, что применение математического аппарата R-функций позволяет существенно упростить процесс описания топологических моделей геометрических областей практически любой сложности. При этом такой подход лишен большинства недостатков вышеописанных стандартных методов геометрического моделирования.

Список источников:

1. Ollivier-Gooch C.F. Guaranteed-quality simplicial mesh generation with cell size and grading control / C.F. Ollivier-Gooch, Ch. Boivin // Engineering with Computers, 17(3):269–286, 2001.

2. Красковский Д.Г. AutoCAD 2000 для всех (русская и английская версии) / Д.Г. Красковский, А.В. Виноградов. – 2-е изд.– М.: КомпьютерПресс, 1999. – 272 с.: ил.

3. Рвачев В.Л. Теория R-функций и некоторые ее приложения / В.Л. Рвачев. – К.: Наукова думка, 1982. – 552 с.

ОБЗОР СУЩЕСТВУЮЩИХ ПОДХОДОВ И РЕШЕНИЙ В ОБЛАСТИ ПРОЕКТИРОВАНИЯ МНОГОПОТОЧНОЙ АРХИТЕКТУРЫ МИКРОКОНТРОЛЛЕРНЫХ СИСТЕМ

Корниенко В.Р.
Научный руководитель – к.т.н., доц. Филиппенко И.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. Автоматизации и проектирования вычислительной техники, тел (057)70-21-326)
e-mail:valentyn.korniienko1@nure.ua

One of the microcontroller`s world problem now – problem of choice the concept of middleware software with simple bare-metal interaction. Modern embedded systems usually based on ARM microchips, that provide all possibilities for multithreaded architecture of application. This article is brief overview of concepts and modern techniques for microsystem designs.

Тенденция увеличения производительности микроконтроллерной системы за счет усовершенствования архитектуры и периферийных возможностей существенно влияет на подходы к архитектуре встраиваемого программного обеспечения. На текущий момент традиционные известные подходы не являются подходящими для организации архитектуры достаточно сложной системы. Известными на сегодня типовыми решениями являются: State-based программирование - типичная модель конечного автомата, примененная в рамках системы управления устройством. Данный подход к архитектуре позволяет проектировать решение в кратчайшие сроки, вводя в проектируемое приложение проблему связности архитектурных компонентов. Тесная связность компонентов ограничивает возможности тестирования приложения и возможности создания кроссплатформенного решения. Также в многопоточной среде модель состояния вводит в систему проблемы, связанные с обеспечением уникального доступа к периферийным ресурсам и данным, что ведет за собой ограничения, как по максимальной производительности решения, так и по надежности системы в целом, т.к. реализация уникального доступа к ресурсам является нетривиальной задачей в встраиваемых решениях. Следующим подходом, позволяющим решить архитектурные проблемы в приложении на МК, является построение архитектуры на базе операционной системы реального времени (ОСРВ), что позволяет добавить в приложение архитектурную модель диспетчера задач - множества задач. Данная модель позволяет проектировать систему как множество отдельных задач, не имеющих зависимостей между собой.

ОСРВ для встраиваемых систем в большинстве своем поддерживают режим вытесняющей многозадачности, предоставляют гибкий менеджмент памяти и ресурсов внутри системы. Некоторые ОСРВ поддерживают

тесное взаимодействие с графическими библиотеками для встраиваемых систем, одной из таких графических библиотек является свободно-распространяемая TouchGFX. На данный момент есть множество операционных систем, которые можно подразделить на три группы: универсальные, которые обеспечивают максимальную переносимость, специализированные, заточенные под конкретное семейство микроконтроллеров и сертифицированные, отвечающие определенным отраслевым требованиям и стрндартам.

Наиболее применимой ОСРВ для подобных решений является FreeRTOS с дополнительным C++ APIв виде CMSIS-OS. Недостатком данного подхода является привязка к конкретному APIвыбранной операционной системы. На данный момент набирает популярность построение систем на основе модели Акторов – концепции распределенных вычислений, позволяющей строить отказоустойчивые приложения с возможностью самовосстановления состояния Актора. Актор представляет собой примитивную единицу, получающую сообщения из диспетчера сообщений и выполняющую действия на основе полученных сообщений. Данная модель является синтезом модели многозадачной системы и системы на базе автоматных состояний. Каждый из акторов получает сообщения асинхронно, но обрабатывает по-очереди. Данная модель позволяет создавать систему из простых взаимодействующих компонентов с возможностью независимого тестирования каждого из акторов и обеспечивает масштабируемость, достаточную для переноса приложения на другую архитектуру или семейство процессоров.

Таким образом, из приведенных в статье подходов к проектированию архитектуры микроконтроллерного приложения необходимо отметить набирающую популярность модель акторов как основу приложения и проектирование архитектуры приложения на базе операционной системы реального времени. Данные подходы обеспечивают необходимую гибкость и масштабируемость приложения, достаточную для портирования и тестирования.

Список источников:

1. Сорокин С. Как много ОСРВ хороших. Современные технологии автоматизации. 1997. No 2.

2. Борисов-Смирнов А. Операционные системы реального времени для микроконтроллеров. Chip news. 2008. No 5.

3. Сорокин С. Системы реального времени. Современные технологии автоматизации. 1997. No 2.

4. Татарчевский В. Применение SWITCH- технологии при разработке прикладного программного обеспечения для микроконтроллеров. Компоненты и технологии. 2006. No 11.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ЯЗЫКОВ ОПИСАНИЯ АППАРАТУРЫ VHDL И VERILOG

Садковая М.В.
Научный руководитель – Филиппенко И.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. АПВТ, тел. (050)861-15-14)
e-mail: mariia.sadkova@nure.ua

VHDL and Verilog are hardware descriptive languages. These languages are designed for simulate electronic circuits at the level of valve, register transmissions, microcircuit cases. Therefore, they can be called languages of through fвпunctional and logical design. However, they have a number of differences, which we will consider in this article.

Языки VHDL и Verilog относятся к языкам описания аппаратуры. Эти языки предназначены для моделирования электронных схем на уровнях вентилей, регистровых передач, корпусов микросхем. Поэтому их можно назвать языками сквозного функционально-логического проектирования. Однако они имеют ряд отличий, которые необходимо учитывать при проектировании различных цифровых устройств.

VHDL (Very high speed integrated circuits Hardware Description Language) – данный язык предназначен для описания проектируемых систем на схемотехническом уровне проектирования и замены классического подхода к схемотехническому проектированию на уровне отдельных элементов. Язык позволяет описывать цифровые системы на алгоритмическом уровне. При помощи специального программного обеспечения описание на языке VHDL преобразовывается в схему на уровне простейших элементов цифровой электроники.

Verilog – это язык описания аппаратуры, используемый для разработки и моделирования электронных систем. Этот язык (также известный как Verilog HDL) позволяет осуществить проектирование, верификацию и реализацию (например, в виде СБИС) аналоговых, цифровых и смешанных электронных систем на различных уровнях абстракции.

По сравнению с Verilog, VHDL более богатый и строго типизованный и строго детерминистический язык, более детализированный. В результате проекты, написанные на VHDL, считаются самодокументированными. Синтаксис сильно отличается от стиля языка С, и инженеры, работающие в VHDL, постоянно сталкиваются с необходимостью явного преобразования из одного типа данных в другой. VHDL часто сразу показывает ошибки, которые пропускает Verilog, а так же имеет подчеркнуто однозначно недвусмысленную семантику, и поэтому легче переносится между разными системами разработки (в том смысле, что перенос точнее переносит все тонкости работы исходного проекта).

Verilog выглядит более гармонично и удобочитаемо. Что достигается отсутствием длинных названий типов данных и строк объявления сигналов и регистров. Так же проще и аккуратнее реализована запись векторов.

Алфавит моделирования в VHDL включает в себя 9 значений: {‘U’, ‘X’, ‘0’, ‘1’, ‘Z’, ‘W’, ‘L’, ‘H’, ‘-’}. Verilog же имеет всего 4 значения: {‘0’, ‘1’, ‘X’, ‘Z’}.

Verilog слабо проверяет типы, и более краток, с эффективной нотацией. Он также детерминистический. Все типы данных заранее определены в Verilog, и каждый из них имеет битовое представление, по сравнению с VHDL, в котором пользователь имеет возможность вводить свои типы данных. Синтаксис похож на C. Из-за своей структуры VDHL отлавливает больше ошибок уже на ранних стадиях процесса разработки. С другой стороны Verilog позволяет инженерам быстро описывать модели.

Так же в VHDL, для расширения языка, позволяется использовать внешние пакеты и библиотеки, в то время как, Verilog не имеет подобной возможности. Из-за своей структуры VDHL отлавливает больше ошибок уже на ранних стадиях процесса разработки. С другой стороны Verilog позволяет инженерам быстро описывать модели.

Таким образом, VHDL является более академичным, многословным и сложным языком. Требуется написание большего объема кода, но строгость означает, что он с большей вероятностью будет работать. Verilog проще для типичного цифрового дизайна, но, соответственно, упрощает создание сложных ошибок. Выбор одного или другого зависит от используемых инструментов. Например, некоторые из популярных инструментов FPGA лучше работают с VHDL, когда популярные инструменты ASIC улучшают работу с Verilog

Список источников:

1. microsin URL: http://microsin.net/programming/xilinx/difference-between-vhdl-verilog-systemverilog.html
2. VHDL с нуля. // easyelectronics URL: http://we.easyelectronics.ru/plis/vhdl-s-nulya.html
3. Исследование комбинационных устройств: // URL: http://we.easyelectronics.ru/plis/vhdl-s-nulya.html
4. Особенности языков описания архитектуры // parallel URL: https://parallel.ru/fpga/hdl.html
5. habr URL: https://habr.com/ru/post/191606/

КРИТЕРИИ ВЫБОРА МИКРОКОНТРОЛЛЕРА

Адамович В.Р.
Научный руководитель – к.т.н, доц. Филипенко И.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. АПВТ, тел. (057) 702-13-26)
e-mail: vladyslav.adamovych@nure.ua

In this work were examined the basic families of modern microcontrollers, such as 8051-compatible microcontrollers, STM32. Some aspects of their history, architecture and physical characteristic. Also were inspected their fundamental differences, distinctive features and scope between each other.

Выбор микроконтроллера является одним из самых важных решений, от которых зависит успех или провал задуманного проекта. При выборе микроконтроллера необходимо учесть и оценить большое количество факторов.

Основная цель выбрать наименее дорогой микроконтроллер (чтобы снизить общую стоимость системы), но в то же время удовлетворяющий спецификации системы, т.е. требованиям по производительности, надежности, условиям применения и т.д. Оценка общей стоимости системы включает следующие этапы: инженерные исследования и разработку, производство (комплектующие и оплата труда), гарантийный ремонт, дальнейшее усовершенствование, обслуживание, совместимость, простоту в обращении и т.д.

Приступая к выбору, разработчик должен четко определить требования к системе и, следовательно, характеристики микроконтроллера.

Проведение поиска микроконтроллеров, которые удовлетворяют всем системным требованиям, включает анализ технической документации, для анализа характеристик микроконтроллера. В настоящее время стала вполне доступной информация о предлагаемых как традиционных, являющихся промышленным стандартом микроконтроллерах, так и новейших микроконтроллерах. На данный момент на рынке есть два конкурирующих между собой классов микроконтроллеров 8-ми и 32-х разрядные, типичным представителями которых являются MCS-51 и STM32.

В настоящее время среди всех 8-битных микроконтроллеров - семейство MCS-51 является бесспорным лидером по количеству разновидностей и количеству компаний, выпускающих его модификации. Все микроконтроллеры семейства MCS-51 имеют общую командную систему. Наличие дополнительной периферии влияет только на количество регистров специального назначения. Микроконтроллер семейства 8051 имеют следующие аппаратные особенности: внутреннее ОЗУ объемом 128 байт; четыре двунаправленных побитно настраиваемых восьмиразрядных порта ввода-вывода; два 16-разрядных таймера-счетчика; встроенный

тактовый генератор; адресация 64 Кбайт памяти программ и 64 Кбайт памяти данных; две линии запросов на прерывание от внешних устройств; интерфейс для последовательного обмена информацией с другими микроконтроллерами или персональными компьютерами. Микроконтроллер 8751 снабжен УФ ПЗУ объемом 4 Кбайт.

STM32 – семейство 32-битных микроконтроллеров производства STMicroelectronics. Чипы STM32 группируются в серии, в рамках каждой из которых используется один и тот же 32-битное ядро ARM. Каждый Микроконтроллер состоит из ядра процессора, статической RAM-памяти, флэш-памяти, наладочного и различных периферийных интерфейсов.

МК ARM – один из быстро развивающихся сегментов рынка МК. Особенностью архитектуры ARM является вычислительное ядро процессора. Большим преимуществом МК, построенных на ядре CortexM, является их программная совместимость, что теоретически позволяет использовать программный код на языке высокого уровня в моделях разных производителей. Благодаря оптимизированной архитектуре стоимость МК на основе ядра CortexM в некоторых случаях даже ниже, чем у многих 8-разрядных микроконтроллеров.

Окончательный выбор микроконтроллера при разработке проекта очень важное решение. С каждым годом они становятся более сложными, за счёт добавления дополнительных внутрисхемных ресурсов. И с тех пор, как процесс развития микроконтроллеров движется в сторону все большей внутрисхемной интеграции внешних ресурсов для понижения стоимости системы, решение становится все более сложным.

Список источников:

1. Atmel [Электронный ресурс] Режим доступа:
https://www.microchip.com/mymicrochip/NotificationDetails.aspx?id=9922&pcn=%27LIAL-22MHLM308%27.
2. STMicroelectronics [Электронный ресурс] Режим доступа:
https://www.st.com/content/st_com/en/about/st_company_information/who-we-are.html.
3. Habr [Электронный ресурс] Режим доступа: https://habr.com/ru/company/microsoftlumia/blog/136629/.

МАТЕМАТИЧНІ МОДЕЛІ ПРИСТРОЇВ ДЛЯ ОБЧИСЛЕННЯ ДРОБОВО-РАЦІОНАЛЬНИХ ФУНКЦІЙ

Селезньова Є.О.
Научный руководитель – к.т.н, доц. Ларченко Л.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. АПВТ, тел. (057) 702-13-26)
e-mail: lina.larchenko@nure.ua, факс (057) 702-13-26

The project analyzes and uses the method of gradual approximation of function reproduction. This model can be used to create a device that can be used in automatic control systems, modeling and control, information measuring systems as functional converters of various physical quantities derived from information sensors.

Метою дослідження є розробка математичної моделі пристрою для обчислення дробово-раціональної функції. Даний пристрій може бути застосований в автоматичних системах управління, моделювання і контролю, інформаційно-вимірювальних системах в якості функціональних перетворювачів різніх фізичних величин, отриманих з датчиків інформації.

Для розв'язання поставленого завдання використано: теорію математичного моделювання, теорія методу ступінчатої апроксимації, теорія структурно-функціональних моделей.

Досліджуваний пристрій для обчислення раціональних функцій, має обчислювати функцію:

$$y = \left[\frac{\sum_{i=1}^{2} a_i x^i}{m} + 0{,}5 \right]$$

де x – аргумент функції, що представляє собою числоімпульсний (унітарний) код;

0,5 – граничне значення абсолютної похибки ділення полінома $ax_i^2 + bx + c$ на константу m.

Вхідним інформаційним сигналом обчислювача є числова імпульсна послідовність x, що подається на вхід пристрою. На виході пристрою формується числоімпульсна послідовність y, яка відтворює безперервну задану функцію з похибкою, що не перевищує половини одиниці молодшого розряду.

Математична модель обчислювача, отримана з використанням методу ступінчатої апроксимації функцій в якому значення x_y можуть бути знайдені шляхом послідовної підстановки y=1,2,3, ... в нерівність:

$$\Psi(y - |\delta_m|) \le_a x_{y\,x} < \Psi(y - |\delta_m|) +_a 1,$$

де $|\delta_{max}|$ - абсолютна похибка обчислення безперервної функції;

$\Psi(y - |\delta_{m\ a}|)$ - функція, зворотна $f(x)$.

Математична модель обчислювача, представлена системою нерівностей:

$$2\sum_{i=1}^{2} a_i x_1^i \geq m$$

$$2(\sum_{i=1}^{2} a_i x_2^i - \sum_{i=1}^{2} a_i x_1^i) + \Delta_1 \geq 2m$$

$$2(\sum_{i=1}^{2} a_i x_3^i - \sum_{i=1}^{2} a_i x_2^i) + \Delta_2 \geq 2m$$

. . . . . .

$$2(\sum_{i=1}^{2} a_i x_y^i - \sum_{i=1}^{2} a_i x_{y-1}^i) + \Delta_{y-1} \geq 2m,$$

де $\Delta_{y-1} = 2(\sum_{i=1}^{2} a_i x_y^i - \sum_{i=1}^{2} a_i x_{y-1}^i) + \Delta_{y-2} - 2m$.

В цьому випадку визначення x_y може бути зведено до обчислення приростів гратчастої функції $2\sum_{i=1}^{2} a_i x^i$ змінної x на кожному з інтервалів $(x_{y-1}; x_y]$ і їх порівнянні з приростами функції m(2y - 1) з урахуванням їх різниці Δ_{y-1}, отриманої на попередньому кроці інтервалу $(x_{y-2}; x_{y-1}]$ в точці x_{y-1}.

Прирости функції правої частини нерівностей дорівнюють константі 2m яка утворюється в ряду різниць першого порядку при підстановці y=1, 2, 3,… в праву частину нерівності $2\ x_y \geq m(2y-1)$.

Наукова новизна дослідження в створенні математичної моделі спеціалізованого пристрою для обчислення дробово-раціональної функції з заданою абсолютною похибкою обчислень з використанням методу ступінчастої апроксимації відтворення функцій. Спроектований пристрій може бути використаний при відтворенні траєкторій рухомих об'єктів в двомірному і тривимірному просторі, при проведенні математичної обробки первинної вимірювальної інформації в інформаційно-вимірювальних системах та при побудові аналого-цифрових і цифро-аналогових перетворювачів форм представлення інформації.

Список джерел:

1. Ларченко Л.В. Метод формирования приращений при функциональной обработке единичных кодов. Радиоэлектроника и информатика. - 2001. №3. - С. 61-63

2. Ларченко Л.В., Хаханова А.В. Специализированный вычислитель для извлечения корня квадратного из суммы квадратов. // Радиоэлектроника и информатика. 2010. № 1(48) – с.71 – 74.

3. Джексон Р.Г. Новейшие датчики. М.: Техносфера, 2008–400с.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ДОПОЛНЕНОЙ РЕАЛЬНОСТИ В СФЕРЕ ПРОЕКТИРОВАНИЯ

Чернов А.Ю.
Научный руководитель – к.т.н., доц. Немченко В.П.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. АПВТ, тел. (057) 702-13-26)
e-mail: oleksii.chernov@nure.ua, тел. 380976266548

In this paper, we propose to consider the use of a stack of technologies of augmented reality and object recognition in the subject area of design, engineering and planning.

О дополненной реальности, как и о виртуальной, говорят уже далеко не первый год, но основные шаги в этом направлении еще предстоит сделать. Отчасти это обусловлено тем, что практическое применение технологий дополненной реальности (Augmented reality - AR) было возможно только в узкоспециализированных областях, но основная причина в недоступности необходимого оборудования для большинства пользователей. За последние годы ситуация изменилась. Распространение высокопроизводительных смартфонов с GPS-модулями, датчиками движения и камерами означает, что потребители привыкли к возможности наложения информации (в любой её форме) на представление реального мира с помощью камеры устройства. Цель исследования – провести обзор рынка устройств, которые поддерживают возможность AR, провести обзор рынка инструментов для создания AR-приложений, выявить основные аппаратные и программные критерии и требования для создания нового инструмента для создания собственной AR-технологии. Задача - разработать AR-приложение, которое было бы доступно для большинства пользователей, при этом имело высокую производительность. В приложении реализовать возможность отслеживания ровных поверхностей для размещения 3D моделей, возможность размещать несколько моделей на разных плоскостях, предусмотреть возможность перемещения моделей.

За последние несколько лет технологии и устройства AR/VR настолько сильно выросли, что теперь они могут встречаться повсюду. Однако, есть определенные проблемы с используемым к ним подходу. Отсутствует «AR мышление». Есть проблемы, требующие решения, и эти проблемы имеют ограничения, которые могут быть преодолены путем пространственного мышления. Первый шаг в определении того, является

ли дополненная реальность подходящим средством – определение пользователей и их потребностей. Эти проблемы включают в себя погружение пользователей в реальном времени, помощь им в пространстве или их физическое вовлечение? Существуют ли физические ограничения, которые в настоящее время не позволяют им быть успешными? Если это так, то высока вероятность, что дополненная реальность может повысить ценность решения.

Дополненная реальность – это цифровое расширение продуктового дизайна. Применяются те же принципы мышления лишь с некоторыми изменениями. Вместо того, чтобы иметь физические ограничения, пользователь теперь имеет технологические ограничения и возможности. Это означает, что мир больше не связывает пользователя, однако он все еще скован материальными ограничениями, определяемыми технологией. Отличным примером является iPhone старшего поколения без датчиков движения и глубины по сравнению с более новой моделью, имеющей эту технологию. Аппаратное обеспечение, как правило, легче оценить и прогнозировать, чем поведение пользователей. Для дизайнеров крайне важно выходить за рамки существующих технологических ограничений, чтобы они могли помочь продвигать технологию вперед.

Научная новизна данного исследования состоит в отображении состояния нового рынка устройств и технологий, исследования сильных и слабых сторон технологии дополненной реальности и аппаратных требований для реализации данной технологии. Актуальность применения рассматриваемых технологий в сфере проектирования связана с тем, что они позволяют повысить эффективность процесса проектирования, при этом обеспечив удобство и доступность практически для каждого участника данного процесса.

Список источников:

1. Steve Aukstakalnis – Practical augmented reality, 2016.
2. Dieter Schmalstieg, Tobias Höllerer – Augmented reality, 2015.

РЕАЛІЗАЦІЯ АЛГОРИТМУ LDPC КОДУВАННЯ ЗА ДОПОМОГОЮ ПЛІС

Сергієнко В.І.
Науковий керівник – к.т.н, доц. Філіппенко І.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: serhiienko.w@gmail.com

This work is devoted to usage of error-prof low density parity check codes and how algorithm of coding information can be optimized and implemented using FPGA. Because FPGA gives opportunity to parallelize computations and optimize algorithms, it can produce codding much more faster instead of using CPU. Also generator matrix for low density parity check codes can be generated so that can be stored in shift registers. It allows not to store full generator matrix but store only parts of it. To restore the rest of the matrix, it is only necessary to perform a cyclic shift operation.

В даний час існує великий об’єм інформації, який необхідно постійно передавати чи звідкилясь отримувати. Зазвичай ця інформація передається через канали зв’язку, що не є ідеальними або близькими до ідеальних. В цих каналах постійно виникають перешкоди, що псують якість зв’язку і призводять до втрати корисної інформації. Основним методом боротьби з цією проблемою є використання завадостійкого кодування. За допомогою додавання надлишкової інформацію до корисної в деяких випадках на стороні прийому даних можна дізнатися, чи були пошкоджені дані, а в деяких випадках можна навіть відновити первісну інформацію.

Одним з видів завадостійкого кодування є використання кодів з низькою плотністю перевірок на парність. Ці коди дозволяють знаходити і виправляти помилки у прийнятій інформації. Даний вид кодування відноситься до блокових кодів, а через це корисна інформація ділиться на інфораційні слова та до них додається блок перевірочної інформації, за допомогою ж якої і відбувається відтворення первинної інформації. В результаті отримуємо кодові слова, що й передаються через канали зв’язку.

Найчастіше розмір інформаційного слова у кодах з низькою плотністю перевірок на парність починається з декількох тисяч. Через це виникає проблема швидкості кодування інформації. Оскільки для обчислення блока перевірочної інформації необхідно провести операцію множення інформаційного слова на породжуючу матрицю, а розміри слів і матриць починаються з декількох тисяч, складність такого кодування може бути занадто велика, що призведе до неможливості передачі даних без затримки. Це може бути критичним для систем управління літальними засобами та іншою технікою, де швидкість реагування повинна бути до 0,1 секунди.

Якщо проводити кодування за допомогою процесорних ресурсів, то може виникнути ситуація, коли швидкість даних буде перевищувати швидкість кодування, наприклад в системах передачі відеоданих з надвисокою якістю. Через це необхідні методи кодування, які будуть обходити цю проблему. Одним з таких методів є використання ПЛІС, оскільки засобами ПЛІС можна дуже сильно розпаралелити обчислення.

Для кодування інформації в кодах з низькою плотністю перевірок на парність використовують спеціально згенеровані породжуючі матриці, що мають певні закономірності та структуру. Це дозволяє оптимізувати процес множення інформаційного слова на цю матрицю.

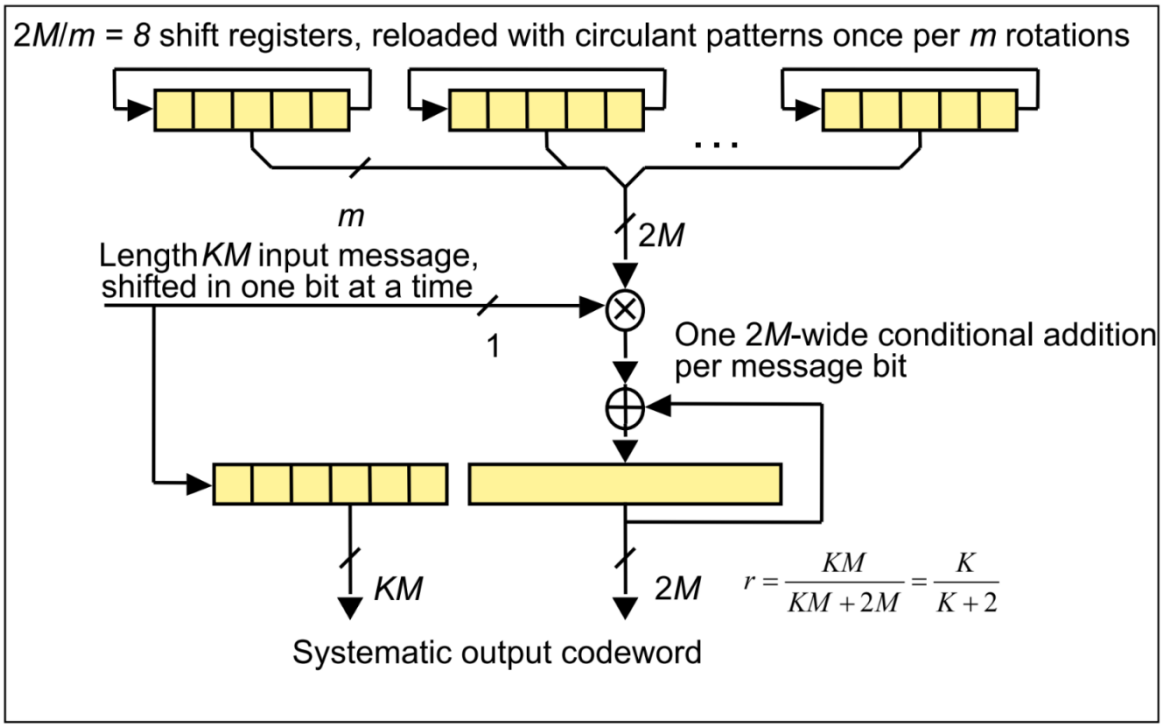


Рисунок 1 – Алгоритм кодування даних

На рисунку 1 наведено алгоритм кодування інформації запропонований в [1]. Засобами ПЛІС породжуючу матрицю можна зберігати в зсувних регістрах, що будуть змінювати своє значення за один такт. Також за один такт буде проводитись множення біта інформаційного слова на вектор породжуючої матриці і додавання його до вже накопичених векторів. В результаті кодування одного біта буде займати один такт, що дозволяє передавати закодовану інформацію без затримки.

Список джерел:

1. Low density parity check codes for use in near-Earth and deep space applications. Experemental specification CCSDS 131.1-O-2 [Текст] / The Consultative Committee for Space Data Systems. – 2007. С. 3-8 – 3-11.

РОЗРОБКА СИСТЕМИ БЕЗПЕКИ ЗА ДОПОМОГОЮ БЕЗДРОТОВОЇ ТЕХНОЛОГІЇ ZIGBEE

Ковальчук А.Є.
Науковий керівник – к.т.н., проф. Немченко В.П.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. науки,14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: artem.kovalchuk@nure.ua

ZigBee technology makes it possible to build a smart house with minimal costs and maximum convenience and efficiency.

Вступ. Сучасні бездротові технології дозволяють створювати принципово нові пристрої і системи, а при заміні існуючих дротових технологій – підвищувати гнучкість і знижувати вартість життєвого циклу виробів. Область застосування бездротових технологій досить велика.

Мета дослідження – розробка системи раннього виявлення надзвичайних ситуацій на прикладі однієї з аудиторій університету, для раннього попередження надзвичайних ситуацій на основі бездротових сенсорних мереж.

Задачі дослідження. Важливою задачею є вибір найбільш актуальної для розробки технології, яка б поєднала у собі простоту у використанні, мале енергоспоживання і високу функціональність. Слід також брати до уваги специфіку роботи систем безпеки та їх використання.

Зміст дослідження. Технологія ZigBee дозволяє створювати бездротові мережі, що самоорганізуються і самовідновлюються та мають найбільший потенціал зниження енергоспоживання, з автоматичною ретрансляцією повідомлень. Мережі ZigBee при відносно невеликих швидкостях передачі даних забезпечують гарантовану доставку пакетів і захист інформації, що передається. Відстані між вузлами мережі складають десятки метрів при роботі усередині приміщення і сотні метрів на відкритому просторі. За рахунок ретрансляцій зона покриття мережі може значно збільшуватися. На основі приладів ZigBee сенсорна мережа будується таким чином: мережевим вузлом є трансивер стандарту 802.15.4 з керованим маршрутизацією стеком ZigBee і програмним профілем. Якщо до трансивера підключається сенсор, вузол отримує профіль сенсорного. Цей профіль пропонує збирати дані і відправляти вузлу, який є центром збору даних. На сьогоднішній день найбільш оптимальним є комплексний підхід до будівництва систем моніторингу і сповіщення, що базуються на бездротових сенсорних мережах. Інновацією проекту є алгоритм, на якому базується технологія автоматизованого збору і передачі даних за допомогою бездротової сенсорної мережі. Початкові дані для обробки збираються за допомогою сенсорних мереж, що самоорганізуються. Кожен вузол цієї БСМ (бездротова сенсорна мережа) забезпечений автономним джерелом живлення, що дозволяє встановлювати їх у важкодоступних

місцях для зняття необхідних свідчень з мінімальними трудовитратами. Зв'язок між пристроями відбувається по радіоканалу в різних стандартах – у тому числі по протоколу Zigbee, в діапазоні частот, що не ліцензується, або по мобільній цифровій радіомережі.

Висновки. Технологія ZigBee є актуальною у наш час. Вона поєднує у собі майже всі переваги бездротових мереж та виключає більшість недоліків, які мають інші мережі. На практичній побудові системи безпеки ми наочно побачимо як технологія виділяється серед інших та її користь у багатьох сферах життя від автоматизації управління безпекою на підприємствах до “розумних” будинків.

Список джерел:

1. Варгаузин В.А. Сетевая технология ZigBee // ТелеМультиМедиа. 2015. № 6. – С. 29-32.

2. Кривченко Т.И. Zigbee- модемы ETRX компании Telegesis // Беспроводные технологии. 2014. № 2. – С. 28-30.

3. Соколов М.А. Программно- аппаратное обеспечение беспроводных сетей на основе технологии ZIGBEE/802.15.4 // Электронные компоненты. 2014. № 12. С. 80-87.

4. Waltenegus Dargie, Christian Poelabauer «Fundamentals of Wireless Sensor Networks Theory and Practice» - Wiley Series on Wireless Communications and Mobile Computing, 311c, 2010 John Wiley & Sons Ltd.

5. Методи маршрутизації, [Електронний ресурс] // URL: http://sgainformatika.ru/1006012/232-102-routing-methods/

6. Carlos de Morais Cordeiro. Ad hoc & Sensor Networks, Theory and Applications / Carlos de Morais Cordeiro, Dharma Prakash Agrawal. – Singapore: World Scientific Publishing Co, 2006. – 642 p.А. Д. Яманов, Д.А. Алевский, А.Е. Плеханов. Технология развертывания локальных беспроводных радиосетей ZigBee в системах промышленной автоматизации и диспетчеризации // «ИСУП», 2011.

РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Жугель Е.Ю.
Научный руководитель – к.т.н., доц. Филиппенко И.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Автоматизации проектирования вычислительной техники, тел. (057) 702-13-26)
e-mail: yevhen.zhuhel@nure.ua, тел. (057) 702-13-26)

The article presents a description of distributed database management systems, as an option to store and manage data more economically and efficiently.

У любой компьютерной системы есть две основные задачи – хранение данных и их обработка. Сегодня, существует огромное количество способов и методов решения таких задач. Задачу хранения информации берут на себя базы данных(БД). Помимо хранения, существует необходимость в удобном инструментарии для работы с данными. Для этого существуют системы управления базами данных(СУБД). Цель и задача любой СУБД – обеспечить пользователю доступ к созданию и использованию БД.

Так как операция обращения к базам данным потребляет большую часть ресурсов вычислительной системы, существует необходимость в создании наиболее оптимального варианта относительно стоимости ЭВМ, кол-ва потребляемых СУБД ресурсов, производительности и надёжности. Распределенные СУБД являются одним из самых перспективных способов решения данной задачи.

Распределенная база данных (distributeddatabase (DDB)) представляет из себя набор многочисленных, логически связанных между собой баз данных распространённых на всю область компьютерной сети.

Распределенная система управления базами данных (distributeddatabasemanagementsystem (D–DBMS)) – это узкоспециализированное ПО, которое управляет базами данных и предоставляет механизм доступа к ним, что в свою очередь является соединяющем звеном между базами данных и пользователями.

В данной системе (Рис. 1) вся информация храниться на одном сайте, и все обращения к базе данных проходит через Site 2. Является классическим примером хранения данных.

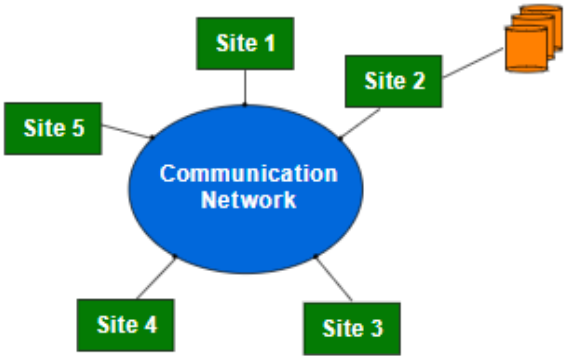


Рисунок – 1 Централизованная система управления базами данных

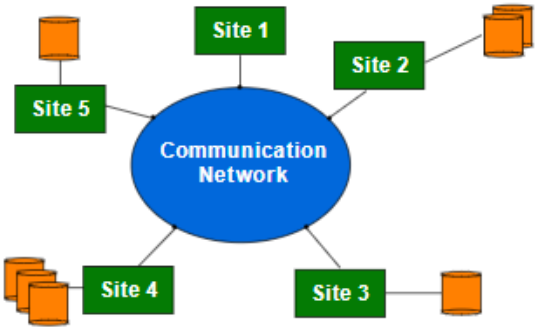


Рисунок 2 – Распределенная система управления базами данных

Для решения этой проблемы была предложена модель распределенной системы управления базами данных (Рис. 2), в которой информация распределена между всеми участниками коммуникационной сети.

В данной системе:

1 Информация храниться на сайтах, каждый из которых логически функционирует в однопроцессорной среде.

2 Процессоры функционируют между собой посредством компьютерной сети, образуя единую многопроцессорную систему.

3 Распределенная база банных представляет из себя набор полноценных баз данных, а не набор файлов с информацией.

4 Р-СУБД является полномасштабной СУБД.

Преимущества разработанной системы:

1 Открытый доступ к распределению, разделениюи распространению информации.

2 Улучшенная защита/доступ через распределение транзакций.

3 Сравнительно быстрая производительность.

4 Аппаратная и финансовая дешевизна.

Недостатки:

1 Более сложные модели БД.

2 Необходима повышенная система защиты отдельных элементов.

3 Отсутствие должного опыта работы с распределенными системами.

4 Необходимо наличие дополнительного ПО.

Список источников:

1 https://cs.uwaterloo.ca/~tozsu/courses/cs856/F02/lecture-1-ho.pdf

2 https://www.geeksforgeeks.org/dbms-advantages-of-distributed-database/

СИСТЕМА СБОРА И ПОДСЧЁТА ГОЛОСОВ В СРЕДЕ ИНТЕРНЕТ-ГОЛОСОВАНИЯ

Жугель Е.Ю.
Научный руководитель – к.т.н., доц. Филиппенко И.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Автоматизации проектирования вычислительной техники, тел. (057) 702-13-26)
e-mail: yevhen.zhuhel@nure.ua, тел. (057) 702-13-26)

Nowadays, the creation of clear, accurate, autonomous and secure voting system is very urgent problem. It's very important in any election to find the most impartial and secure way to collect and count votes. In this work I've described a modern solution and presented my own way how to deal with that problem.

Современные системы сбора и подсчёта голосов избирателей в большинстве стран производятся с помощью группы людей, а это способствует развитию недоверия и итоговый результат подвергается всеобщему спору. Для возможного решения данных проблем была разработана современная система Электронного голосования. Основным различием от обычных способов, сборка и подсчёт голосов происходит электронно-техническим путём, а не напрямую людьми.

Технологии электронного голосования могут включать в себя перфокарты, системы оптического сканирования и специализированные терминалы для голосования. Они также могут включать передачу избирательных бюллетеней и голосов по телефону, частным компьютерным сетям или через Интернет.

Технология электронного голосования позволяет ускорить процесс подсчёта голосов, а также упростить голосование людям с ограниченными возможностями. Но данная система имеет свои трудности реализации.

Основными разновидностями технологий Электронного голосования могут быть: бумажно-электронная система голосования, система голосования с прямой записью, системы голосования, использующие публичные сети, системы интерактивного голосования

Каждая система должна состоять из трёх независимых аппаратно-программных частей:

– устройства подсчёта голосов или система оптического сканирования бюллетеней;

– устройства заполнения, например сенсорный экран, либо сканер штрих-кода;

– устройства отображения итогового результата.

Наиболее перспективно развивающаяся система – использующая публичные сети, а именно система Интернет-выборов. Интернет-выборы – один из способов электронного голосования, представляющий собой

проведение части или полностью голосования на выборах и референдуме с использованием сети Интернет. Наиболее ярким примером является эстонская система i-votingсервиса e-government.

Архитектура данной системы обязана строиться с помощью очень сложных механизмов, обеспечивающих высокую защиту информации и бесперебойную работу. Вся система должна работать в среде распределенных вычислений для должной регуляции нагрузки на основной сервер подсчёта и сбора голосов. Была предложена программно-аппаратная модель системы сбора и подсчета голосов. Она включает в себя следующие модули:

1 Организация регистрации избирателя с сохранением анонимности следующая: пользователь регистрирует свой документ в системе для идентификации.

2 При получении положительного ответа о праве голосования, пользователь получает сгенерированную системой ссылку (которая сокрыта от всех остальных участников), при переходе на которую избиратель переходит на страничку-бюллетень, где указывает нужного кандидата и дважды подтверждает выбранный пункт.

3 Система передаёт бюллетень в базу в виде пары – id сессии и кодированный результат выбора. На этом этапе данные о пользователе теряются, а любые способы получения данных об избирателе невозможны в виду отсутствия данного механизма в системе.

4 Сервис обработки бюллетеней работает локально без доступа в глобальные сети, тем самым, ограничивая возможного влияния на подсчёт голосов извне.

5 Результат итогового подсчёта каждого локального сервиса отправляется на главный сервер, который производит итоговый подсчёт всех голосов.

6 Текущий результат можно отслеживать на специально выделенном сервере, задача которого – отображение текущего положения выборов (имя кандидата и % голосов).

Главные преимущества предложенной системы: высокая скорость подсчёта голосов, высокая защита информации.

Необходимые аппаратные ресурсы для реализации данной системы: сервера оснащённые процессорами семейства IntelXeonE3(и выше), объём ОЗУ свыше 8Гб. Связь со всеми сервисами/серверами производиться с помощью высококачественных сетей, пропускной способностью не менее 100Мбит/с.

Программные ресурсы: клиент-серверное ПО, организованная среда распределенных вычислений.

Список источников:

1 https://ru.wikipedia.org/wiki/Электронное_голосование.

2 https://e-estonia.com/solutions/e-governance/government-cloud/

АРХІТЕКТУРНИЙ ПАТЕРН ENTITY COMPONENT SYSTEM

Пасічко В. В.
Науковий керівник – проф. Хаханова И.В.
Харківський національний університет радіоелектроніки (61166, Харків, пр. Науки,14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: volodymyr.pasichko@nure.ua

Entity–component–system (ECS) is an architectural pattern that is mostly used in game development.

Для впровадження нових механік в гру, зазвичай, потрібно змінювати код у багатьох місцях, редагувати ієрархію класів, проводити оптимізацію та тестування із-за зміненої логіки. Звичайно, архітектуру можна продумати з самого початку, але в практиці це недосяжна ціль в програмуванні ігор, тому що дизайн-документ досить часто змінюється, якісь частини викидаються, додаються абсолютно нові частини, які ніяк не пов'язані зі старою логікою поведінки. ECS – це рішення цієї проблеми, тому що придає додатку велику гнучкість, сильно спрощує впровадження редагувань та подальше розширення додатків новим функціоналом без кардинальних змін у поточному коді. Мета дослідження - підвищення швидкості роботи з оперативною пам’яттю, прискорення розробки ігор, легкий перенос коду між абсолютно різними іграми, можливість створення тестів, великий рівень абстракції, можливість легко та швидко впроваджувати нові механіки. Задачі дослідження - розробка фреймворку для середовища Unity 3D, яке дає можливість використовувати паттерн ECS. Фреймворк вміщує інтерфейси для основних частин ECS, генератор коду та бібліотеку на написання тестів.

Entity -Component-System – це шаблон проектування, який забезпечує велику гнучкість в проектуванні загальної архітектури програмного забезпечення. Такі великі компанії, як Unity, Epic або Crytek використовують цей шаблон в своїх фреймворках, щоб надати розробникам дуже багатий можливостями інструмент, за допомогою якого вони розробляють власне ПО.

Основна ціль ECS – розподіл різних проблем і завдань між сутностями (Entities), компонентами (Components) і системами (Systems). Це три основні поняття цього шаблону. Сутність це контейнер для компонентів. Компонент – це невеликий об’єкт, який не володіє ніякою логікою. Зазвичай компонент містить одне чи два поля. В ідеалі це об'єкти з простою структурою даних. Кожен тип компонента можна прикріпити до сутності, щоб дати їй щось на зразок властивості. Наприклад, до сутності можна прикріпити «Health-Component», що дозволить зробити її смертною, давши їй здоров'я, яке є звичайним цілочисельним або дробовим значенням в пам'яті. Системи містять в собі логіку, наприклад,

переміщення чи запуск анімації. Системи працюють с сутностями, які мають потрібний для неї набір компонентів.

Компонент є найпростішою частиною у ECS. Це просте представлення даних. Він може бути порожнім, мати одне або багато властивостей або бути позначеним як унікальний.

Сутність - це лише контейнер для компонентів. Сутність завжди повинна бути частиною контексту. Контекст - це керуюча структура даних, яка контролює життєвий цикл об'єктів.

Існує декілька видів систем. Update System - це система, яка повинна виконуватися кожен кадр. В цих системах зазвичай описується логіка, яка повинна відбуватися під час усієї ігрової сесії, наприклад рух чи програвання анімації. Start system - цей вид систем спрацьовує лише один раз на початку ігрового циклу. Ці системи зазвичай використовуються для створення ігрових об’єктів. End System - це система, яка спрацьовує в кінці ігрового циклу, використовуються, зазвичай, для знищення ігрових об’єктів.

ECS має багато переваг на звичайною системою компонентів в Unity. Поділ логіки і даних. Можливість змінювати логіку (міняти системи, видаляти / додавати компоненти), не ламаючи дані. Тобто можна будь-який момент відключити групу систем, що відповідають за певну функціональність, і все інше продовжить працювати(крім відключеного функціоналу) і це не торкнеться поточних даних. Ефективне використання пам'яті. Можна перевикористати створені об'єкти сутностей і компоненти, використовуючи пули; можна використовувати типи-значення для даних і зберігати їх в пам'яті поруч (Data locality).

Результатом дослідження є фреймворк, який дозволяє використовувати архітектурний патерн ECS у середовищі Unity 3D. Його практична значимість полягає у тому, що він є кращим рішенням для розробки ігор, оскільки має великий рівень абстракції та логіку дуже легко редагувати чи доповнювати.

Список джерел:

1. Understanding Component-Entity-Systems [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.gamedev.net/articles /programming/general-and-gameplay-programming/understanding-component-entity-systems-r3013.

2. Nystrom R. Game programming patterns / Robert Nystrom., 2012. – 50 с.

СПЕЦИАЛИЗИРОВАННЫЙ МОДУЛЬ ДЛЯ ВОСПРОИЗВЕДЕНИЯ СТЕПЕННЫХ ФУНКЦИЙ

Шапа Л.С.
Научный руководитель – к.т.н, доц. Ларченко Л.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. АПВТ, тел. (057) 702-13-26)
e-mail: liudmyla.shapa@nure.ua , факс (057) 702-13-26

The project analyzes and uses the method of gradual approximation of function reproduction. This model can be used to create a device that can be used in automatic control systems, information measuring systems.

Специализированные модули для воспроизведения степенных функций имеют широкое применение. При проведении математической обработки первичной измерительной информации в информационно-измерительных системах наряду с арифметическими, алгебраическими и другими операциями часто требуется выполнение различных нелинейных функциональных преобразований частоты импульсных последовательностей. Решать такие задачи приходится при линеаризации функций преобразования частотных сенсоров, при выработке нелинейных поправок в результате измерения на влияние внешних неизмеряемых параметров, при решении задач косвенного измерения, при получении корректирующих сигналов в системах управления, при получении нелинейных математических зависимостей исходных сигналов.

В данной работе целью исследования является разработка специализированных устройств для вычисления степенных функций с дробными показателями с унитарным кодированием Абсолютная погрешность вычисления степенных функций не превышает половины единицы младшего разряда аргумента. Основными задачами являются: анализ известного интерполяционного метода ступенчатой аппроксимации воспроизведения непрерывных функций; разработка математических моделей устройств для вычисления степенных функций, синтез структуры вычислителя, в котором процедуры возведения в степень и извлечения корня совмещены во времени, содержащего модули для вычисления полиномов и устройств для извлечения корня.

Определение общего члена числовой последовательности x_y, соответствующего узлам аппроксимации степенной функций, могут быть найдены с помощью неравенства:

$$\Psi(y-|\delta_{\max}|) \le x_y < \Psi(y-|\delta_{\max}|)+1, \qquad (1)$$

где $|\delta_{\max}|$ - абсолютная погрешность вычисения непрерывной функции;
$\Psi(y-|\delta_{\max}|)$ - функция, обратная $f(x)$.

Устройство для вычисления степенных функций воспроизводит фунцию $y=[x^{\frac{m}{n}}+0{,}5]$ с заданной абсолютной погрешностью вычисления, не превышающую 0,5 единицы младшего разряда аргумента x. На основе формулы общего члена получено неравенство для определения общего члена числовой последовательности x_y, соответствующего узлам аппроксимации степенной функций:

$$(2y-1)^n < x_y^m 2^n < (2y-1)^n + 1. \qquad (2)$$

Рассматриваемый метод формирования степенных ступенчатых функций обеспечивает процесс одновременного формирования параллельных кодов приращений функций x^m и y^n, в темпе поступления входной последовательности x, непрерывном сопоставлении их текущих значений и формировании выходных импульсов устройства в момент их равенства.

Разрабатываемый модуль вычисляет функцию $y=[x^{\frac{2}{3}}+0{,}5]$. При этом, неравенство (2) трансформируется в неравенство:

$$(2y-1)^3 < x_y^2 2^3 < (2y-1)^3 + 1 \quad , \qquad (3)$$

анализ которого и позволяет перейти к структурно-функциональной модели устройства.

Научная новизна состоит в разработке математических моделей устройства для вычисления степенных функций. Метод ступенчатой аппроксимации обеспечивает минимально возможное время воспроизведения при минимально возможной погрешности вычислений,. По сравнению с известными предложенные разработки обеспечивают более высокую точность воспроизведения функций в реальном масштабе времени при более простой технической реализации. Основным вычислительным узлом представленных разработок является накапливающий сумматор результата, который используется в качестве схемы сравнения параллельных кодов. Практическая значимость рассмотренного технического решения состоит в улучшении временных характеристик управляющих и информационно-измерительных систем, в которых может использоваться данный модуль.

Список источников:

1. Джексон Р.Г. Новейшие датчики. М.: Техносфера, 2008–400с.

2. Ларченко Л.В., Хаханова А.В. Специализированный вычислитель для извлечения корня квадратного из суммы квадратов. // Радиоэлектроника и информатика. 2010. № 1(48) – с.71 – 74.

3. Олег Матвійків, Сергій Ткаченко, Володимир Хаханов. Інженерне проектування складних об’єктів і систем. Навчальний посібник. Національний університет «Львівська політехніка», 2016 – 261с.

ОСОБЕННОСТИ КОНТРОЛЯ И ОТЛАДКИ МПС НА РАЗЛИЧНЫХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА

Комаровский В.Э.
Научный руководитель – к.т.н, доц. Филипенко И.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. АПВТ, тел. (057) 702-13-26)
e-mail: volodymyr.komarovskyi@nure.ua

The feature of control and debugging of microprocessor are examined on three stages of life cycle, such as design manufacturing and exploitation. The specific of every stage is taken into account. On every stage, microprocessor can have some defect and specialist analyzes and eliminates it by using special tool. This article is a brief overview of concepts for microprocessor debugging.

Процедура проверки правильности функционирования микропроцессорной системы (МПС), называется контролем или тестированием. В результате чего определяется, удовлетворяет ли разработанная система техническому заданию. В противном случае возникает задача диагностирования (поиск неисправностей). После происходит процесс устранения найденных неисправностей (отладка). Тестовые входные воздействия и ответные реакции определяются, исходя из спецификаций устройства. Полное тестирование практически осуществимо только для простых компонентов, для достаточно сложных реальных систем полное тестирование неосуществимо. При эксплуатации могут проявляется остаточные дефекты как ошибки проектирования, следовательно, на любой стадии жизненного цикла достаточно сложных систем нельзя утверждать об отсутствии неисправностей.

Существенно отличаются по сложности поиска и характеру неисправностей процедуры отладки МПС на различных этапах ее существования. Можно выделить три типа процедур отладки МПС: отладка опытного образца (макета); отладка в процессе серийного производства; отладка в процессе эксплуатации.

В процессе отладки опытного образца выявляются и устраняются следующие типы ошибок: ошибки разработчика (в том числе ошибки документации); ошибки соединений (дефекты печатных плат, ошибки монтажа); ошибки программного (микропрограммного) обеспечения, в том числе ошибки тестовых процедур. Отсутствие отлаженных непосредственно на этой МПС тестовых процедур создает неопределенность при поиске источника ошибок. Ошибка может быть, как программная, так и аппаратная. Отладка опытного образца ведется при помощи сложной, разнообразной и дорогостоящей аппаратуры (запоминающие многолучевые высокочастотные осциллографы,

логические анализаторы и др.) персоналом высокой квалификации - чаще всего самими разработчиками.

На этапе отладки серийного изделия предполагается, что ошибки разработчика (в аппаратуре и программах) устранены. Производственный контроль осуществляется путем функциональных испытаний МПС-плат на мощных установках промышленного контроля, снабженных хорошо разработанной системой тестов. Реакция проверяемой платы сравнивается с эталоном (физическим, вычисляемым или хранимым в памяти). По результатам сравнений выдается сообщение "Годен" - "Не годен"; локализация неисправностей осуществляется только до уровня ТЭЗа или не проводится вовсе. Для осуществления такого контроля можно привлекать персонал невысокой квалификации. Неисправные изделия возвращаются на участки, где их отладка проводится на специализированных стендах квалифицированными регулировщиками.

Поиск неисправностей в МПС на этапе эксплуатации осуществляется в основном средствами самодиагностики или специальной, но достаточно простой аппаратурой (например, сигнатурными анализаторами).

Контроль в процессе эксплуатации, как правило, проще, чем на предыдущих этапах, по следующим причинам: вероятность появления двух и более неисправностей одновременно весьма мала; обычно требуется контроль правильности работы только при решении конкретных задач, при этом тесты поставляются вместе с самим изделием.

Однако требования к инструментальным средствам, предназначенным для эксплуатационного обслуживания МПС, весьма противоречивы. С одной стороны, это требование компактности, а часто даже портативности этих средств, с другой - требования универсальности и автоматизации процесса контроля, чтобы иметь возможность использовать персонал невысокой квалификации.

Тестирование и отладка МПС на различных этапах его жизненного цикла позволяет избежать множества ошибок функционирования изделия. На текущий момент существует большое количество разнообразных способов обнаружить и устранить неисправности устройства. Благодаря этому обеспечивается качество и надёжность МПС.

Список источников:

1. Хелпикс.Орг[Электронный ресурс]// Режим доступа: https://helpiks.org/9-59607.html.
2. StudFiles [Электронный ресурс]// Режим доступа: https://studfiles.net/preview/1047152/page:9/.
3. Электроника для всех[Электронный ресурс] // Режим доступа: https://emkelektron.webnode.com/news/montazh-i-naladka-mikroprotsjessornykh-sistjem-/.
4. PPTonline[Электронный ресурс] // Режим доступа: https://en.ppt-online.org/317805.

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ОПЕРАЦИОННЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

Примеров М.В., Солодухина Е.Е.
Научный руководитель – к.т.н, доц. Филиппенко И.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. АПВТ, тел. (057) 702-13-26)
primerovmax@gmail.com, catherinesolodoukhina@gmail.com

A real-time system is a system that must respond to events in the external environment or affect the environment with in the required time constraints.

В докладе обсуждаются преимущества использования систем реального времени. Системы реального времени обладают следующими свойствами:

а) гарантированное время реакции на внешние события;

б) жёсткая подсистема планирования процессов;

с) повышенные требования к времени реакции на внешние события.

Существуют 3 вида архитектур операционных систем реального времени (ОСРВ).

1) Монолитная архитектура. Определяется как набор модулей, взаимодействующих между собой внутри ядра и предоставляющих прикладному ПО интерфейс для обращения к аппаратуре. Недостаток такой архитектуры, вызванный сложным взаимодействием модулей между собой.

2) Уровневая архитектура. Прикладное ПО в такой архитектуре может получить доступ к оборудованию не только через обращение к ядру или его сервисам, но и обращаться к нему напрямую. Отличие от монолитной архитектуры заключается в том, что прикладное ПО может быстро получить доступ к оборудованию. Основной недостаток такой архитектуры является отсутствие многозадачности.

3) Архитектура “клиент-сервер”. Основное её принцип заключается в вынесение сервисов ОС в виде сервисов на уровне пользователя и выполнения микроядром функций диспетчера сообщений прикладного ПО и системными сервисами. Преимущества данной архитектуры: а) повышенная надёжность, простота отладки и обнаружения ошибок, б) улучшенная масштабируемость, в) повышенная отказоустойчивость.

Особенность ядра систем реального времени заключаются в абстрагирование прикладного ПО от особенностей архитектуры процессора или нескольких процессоров и связанного с ним оборудования. Основные сервисы, которые предоставляются ОСРВ:

- Управление задачами. Позволяет разработчика проектировать программные продукты в виде отдельных задач, которые будут выполнятся за отведённый квант времени. Сервисы в данной группе, имеют возможность запускать и присваивать приоритеты задачам.

Основной сервис - планировщик задач. Он контролирует выполнение и запуск задач и следит за режимом их работы.

- Управление таймерами. Предоставляет группу сервисов для управления временем выполнения задач. Эти сервисы измеряют и задают точные промежутки времени и генерируют, прерывая по истечению определенного времени.
- Синхронизация задач. Сервисы данной группы, дают возможность обменивать и синхронизировать данные и согласовывать действия различных задач, для получения большей эффективности.
- Контроль устройств ввода-вывода. Сервисы, представляющие единый интерфейс взаимодействия со множеством драйверов устройств типичных для данных систем.

Отличия от операционных систем общего назначения. Хотя большинство ОСБН имеют вышеперечисленные сервисы, но ключевым отличием систем реального времени является детерминированный характер работы. В данном случае подразумевается заведомо известный временной интервал работы каждого сервиса системы. Эти временные интервалы могут быть вычислены по алгебраическим формулам, исключая все случайные значения, которые могут повлечь нежелательную задержку в работе приложения, тогда следующая задача не вложиться в свое отведенное время и послужить причиной для ошибки. В этом смысле системы общего назначения не являются детерминированными, в их работе могут возникать случайные задержки, которые не являются критичными для работы данных систем.

С развитие технологий системы реального времени нашли применения в областях, где нужно быстро контролировать задачи, и реагировать на события из внешней среды. Эти системы применяют в промышленности, робототехнике, медицине, бытовой технике, транспорте, системах регулирования уличного движения, управление воздушным движением, аэрокосмической техники, а также в военной технике.

Список источников:

1. Зыль С. Операционная система реального времени QNX: от теории к практике. – 2-е изд. - СПб.: БХВ-Петербург, 2004. – 192 с. – ISBN 5-94157-486-X.

2. Зыль С. QNX Momentics. Основы применения. – СПб.: БХВ-Петербург, 2004. – 256 с. – ISBN 5-94157-430-4.

3. Кёртен Р. Введение в QNX/Neutrino 2. – СПб.: Петрополис, 2001. – 512 с. – ISBN 5-94656-025-9.

4. Ослэндер Д. М., Риджли Дж. Р., Рингенберг Дж. Д. Управляющие программы для механических систем: Объектно-ориентированное проектирование систем реального времени. – М.: Бином. Лаборатория знаний, 2004. – 416 с. – ISBN 5-94774-097-4.

АНАЛИЗ ПРИМЕНЕНИЯ КОНЦЕПЦИИ SOLID

Примеров М. В., Солодухина Е. Е.
Научный руководитель – к.т.н, доц. Филиппенко И.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. АПОТ, тел. (057) 702-13-26)
primerovmax@gmail.com, catherinesolodoukhina@gmail.com

The given work describes the conception for effective code writing, managing and refactoring. The conception contains five object-oriented principles chosen by Robert C. Martin.

SOLID – мнемотический акроним, сочетающий в себе пять принципов объектно-ориентированного программирования и проектирования, разработанных Робертом Мартином в 2009 году. Использование данной концепции подразумевает повышение вероятности написания программистом легко поддерживаемой, расширяемой и отлаживаемой системы. Аббревиатуру SOLID составляют:

The Single Responsibility Principle (SRP) – принцип единственной ответственности. Данный принцип обозначает, что каждый класс должен иметь только одну ответственность, и данная ответственность должна быть полностью инкапсулирована в класс. А так же, все методы класса связаны с этой ответственностью.

The Open Closed Principle (OCP) – принцип открытости/закрытости. Использование этого принципа подразумевает, что классы открыты для расширения функциональности, и закрыты – для её изменения. Само расширение функциональности осуществляется с помощью наследования расширяемого класса. Для обеспечения данного принципа проектирование классов должно обеспечивать то, что для изменения их поведения не придется изменять их код. Во всей системе классов должна обеспечиваться гибкость.

The Liskov Substitution Principle (LSP) – принцип подстановки Барбары Лисков. Принцип был предложен Барбарой Лисков в 1987 году.

Формулировка Лисков была следующей: «Пусть q(x) является свойством, верным относительно объектов x некоторого типа T. Тогда q(y) также должно быть верным для объектов y типа S, где S является подтипом типа T».

Существует также альтернативное определение принципа, описанное Робертом С. Мартином: «Функции, которые используют базовый тип, должны иметь возможность использовать подтипы базового типа, не зная об этом».

Таким образом, данный принцип подразумевает замену базовых классов их наследниками без возникновения ошибок с дополнением, но не изменением базового. Кроме того, данный принцип запрещает

использование оператора newметодов класса-наследника и обеспечивает формирование простой иерархии наследования.

The Interface Segregation Principle (ISP) – принцип разделения интерфейса. Принцип, следование которому позволяет системе оставаться гибкой, расширяемой и пригодной для рефакторинга.

Определение Роберта С. Мартина было следующим: «Программные сущности не должны зависеть от методов, которые они не используют».

Следование этому принципу подразумевает отказ от многофункциональных классов и использование большого количества интерфейсов, содержащих специфический функционал, который должен быть минимальным.

The Dependency Inversion Principle (DIP) – принцип инверсии зависимостей. Принцип подразумевает преобладание зависимостей классов от абстракций. Все модули должны зависеть от абстракций. Абстракции же не должны зависеть от деталей, но детали должны зависеть от абстракций. Модули верхних уровней не должны зависеть от модулей нижних уровней.

Выводы. В данном докладе были рассмотрены пять основных принципов концепции SOLID. Использование данной концепции:

1) существенно повышает простоту и читаемость кода, что обеспечивается принципом SRP, 2) обеспечивает совместимость будущих версий с предыдущими и отсутствие ошибок во взаимодействии классов, разрабатываемых различными командами программистов за счет использования OCP, 3) упрощает систему наследования при использовании LSP, позволяет системе оставаться гибкой и, в то же время, 4) легко расширяемой и затрачивать минимальное количество памяти за счёт минимизации интерфейсов, 5) упрощает проектирование системы классов и абстракций, которые они реализуют.

Список источников:

1. Роберт С. Мартин, Джеймс В. Ньюкирк, Роберт С. Косс Быстрая разработка программ. Принципы, примеры, практика — Вильямс, 2004, ISBN 5-8459-0558-3, ISBN 0-13-597444-5.

2. Мартин Р., Мартин М. Принципы, паттерны и методики гибкой разработки на языке C# — Символ-Плюс, 2011, ISBN 5-93286-197-5, ISBN 978-5-93286-197-4, ISBN 0-13-185725-8, ISBN 978-0-13-185725-4.

3. Fenton, Steve (2017). Pro TypeScript: Application-Scale JavaScript Development. p. 108. ISBN 9781484232491.

EMBEDDED CYBERPHYSICAL SYSTEMS DESIGN CHALLENGES AND MODEL-BASED DESIGN APPROACH

Larchenko Bogdan
Scientific Supervisor – Dr. of Technical Science, prof. Svetlana Chumachenko
Kharkiv National University of Radio Electronics
(61166, Kharkiv, Nauky ave, 14, Design Automation Department,
(057) 702-13-26)
e-mail: svetlanachumachenko@nure.ua, fax: (057) 702-13-26

This paper provides a review of commonly faced challenges in embedded cyberphysical systems design and a Model-Based Design Approach which helps address various difficulties and complexities in the process of embedded systems development.

When it comes to developing embedded IoT devices, the hardware design is viewed as a critical component for the success of the IoT product. In order to ensure the embedded IoT product meets the required function, consumes low power, and is secure and reliable, a lot of challenges are faced by the embedded IoT device manufacturers during the hardware designing phase of these devices.

The Internet of Things (IoT) is defined as a process in which objects are equipped with sensors, actuators, and processors that involve hardware board design and development, software systems, web APIs, and protocols, which together create a connected environment of embedded systems. When it comes to designing of these embedded IoT systems, they need to be designed for specific functions, possessing qualities of a good product design like low power consumption, secured architecture, reliable processor, etc.

With the rising demand for connected devices, embedded systems need to work with heterogeneous devices and adapt to different networking architectures to cope-up with new functionalities and performances in the real-time environment. Due to this situation of increasing technology adoption and deployment of new applications, embedded system designers face several problems in terms of flexibility while developing embedded IoT systems such as:

1. Ensuring smooth integration of new services;
2. Difficulty in adapting to new environments;
3. Frequent changes in hardware and software facilities;
4. Integration of small size chip with low weight and lesser power consumption;
5. Carrying out energy awareness operations.

All the IoT hardware products need to perform securely in the real-time embedded environment. Since all the embedded components operate in a highly resource-constrained and in physically insecure situations, engineers often face problems in ensuring the security of these embedded components.

Model-based design (MDB) approach proves to be an effective and efficient means of understanding the product parts such as commercial microcontrollers and processors as well as algorithms and code for the working of both microelectronic and embedded devices. When MBD is used effectively, it provides a single design platform to optimize overall system design. The main advantage of this approach is that it helps embedded software developers to understand the difference between simulator and software development tool in order to create simulation models and check whether algorithms will work before the embedded code is written. Through virtual prototyping, system engineers can easily see whether the whole system will work as intended, even before the hardware is manufactured and available for testing.

The model-based design framework typically unfolds in the following way. System modelling activities involve creating a mathematical and behavioural representation of the embedded system under consideration. It refers to a visual method for designing complex control systems, communication systems, and signal processing systems within an MBD framework. With MBD continuous testing as algorithms and real-time computational models are created and refined. During simulation, continuous-time systems are solved using numerical integration. MBD provides a rapid prototyping method of a product. It is a fast and cost-effective way for engineers to control signal processing, verify design at the early stage, and evaluate design trade-offs. After rapid prototyping, a detailed software design activity is performed to convert the controller model to a detailed, executable software specification. Embedded code (often highly optimized) is then generated from the model for the detailed controller model and downloaded to the actual embedded microprocessor or ECU as part of the production software build. To combine hardware and production code into model-based testing, one can compare dynamic outputs of models with data collected through software-in-the-loop and processor-in-the-loop test or with data measured in the test lab, using the data inspector or logging tools.

The main benefit of MBD is the auto-generation of code, which can eliminate human errors and allow code reusability. In addition, model-based design usage consistently provides the benefits of faster time to the first demonstration, faster time to market with a qualitative product, quick turnaround of iterations without the need of hardware, design and continuous testing in order to improve development effectiveness, reusable models which can improve development time and cost.

References.

1. Susanna Pantsar-Syväniemi. (2012). Architecting Embedded Software for Context-Aware Systems. Embedded Systems – Theory and Design Methodology. Rijeka, Croatia.

2. Komal Chauchan, (2018). Why Model-Based Design is important in embedded systems. “eInfochips” . Austin, Texas.

ВІРТУАЛЬНИЙ КОМП’ЮТІНГ

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ АНАЛИЗА ТВИТОВ В СОЦИАЛЬНОЙ СЕТИ TWITTER

Бондарев А.В
Научный руководитель – к.т.н. доцент Аксак Н.Г.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. ЭВМ, тел. (057) 702-13-54)
e-mail: santura1295@gmail.com, тел. 096-323-1042

This work is created to research opportunities of technologies in the Big Data space. Considered technology such as Apache Storm and Azure SQL DB created for calculating a big amount of data and applying real-time analytics. The main purpose described here is to use tweets from Twitter as the main flow of data and calculate them in real-time using technologies mentioned above. As a kind of sentiment analysis using Twitter we can count how often people are tweeting about certain hashtag, topic in a given period of time. It's interesting because we can take a huge amount of data and make a forecast in nearest future.

Технология Big Data нуждается в разработке новых методов обработки, сбора и анализа непрерывных потоков данных в реальном времени.

В работе предлагается сценарий обработки потока твитов социальной сети Twitter с использованием ключевого инструмента Apache Storm, который обеспечивает непрерывную аналитику в реальном времени. Система анализирует записи в соцсети Twitter на предмет того, что люди пишут в заданный промежуток времени. Используя такой подход, можно оптимально выявлять тренды, например, активные политические события могут показывать, каким настроением живут люди данной области или страны; быстро локализировать пострадавшие районы от погодных катаклизмов или землетрясений.

Система анализа основана на потоковой топологии, которая выбирает некоторое количество твитов, вычисляет метрики, сохраняет данные в репозиторий и публикует необходимые результаты. Анализ происходит при помощи соответствия ключевым словам. Рассчитанные метрики представляют собой количество твитов, соответствующих критериям выбора.

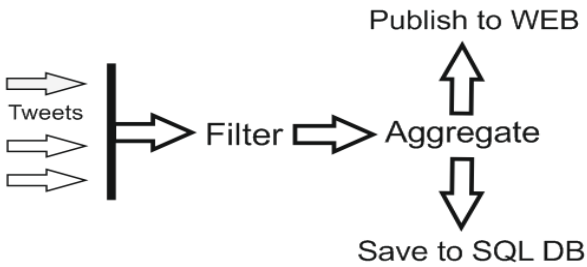


Рисунок 1 – Топология системы анализа

Выбранные твиты предлагается хранить в базе данных Azure SQL с учетом служб Storm (рис. 1). Apache Storm представляет собой инструмент распределенных вычислений в реальном времени над потоками больших данных. Azure настраивает вычислительный кластер, в который загружены компоненты Storm.

Топология системы представлена компонентами Spots и Bolts, где Spots – набор программного кода, который собирает, генерирует данные и выдает их частями – потоками кортежей (набор пар типа и значения), Bolts – набор программного кода, который принимает кортежи данных, выполняет их очистку и вычисляет статистику, а также выдает поток статистических данных, хранящихся в репозитории. Каждый из компонентов выполняет множество параллельных задач, за счет чего достигается масштабируемость.

Преимущество Storm заключается в том, что можно самому задавать степень параллелизма для каждого из компонентов. Данная топология исполняется в наборе рабочих процессов, технология Storm обеспечивает отказоустойчивость при большом масштабе выполнения аналитики в реальном времени.

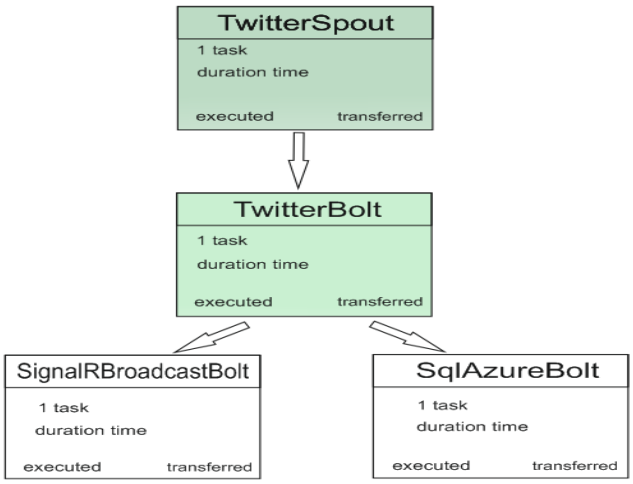


Рисунок 2 – Работа компонентов топологии

Архитектура задействована для повторного использования компонентов, но вместе с этим она создает проблему разворачивания по мере увеличения количества компонентов Spots и Bolts. Среда разработки Visual Studio немного упрощает способ управления кодом и компонентами конфигурации, необходимыми для создания топологии.

Список источников:

1. Azure SDK Hadoop [Электронный ресурс] https://msdn.microsoft.com/magazine/dn890370.

2. Apache Storm Documentation [Электронный ресурс] http://storm.apache.org/releases/1.2.2/index.html.

АЛГОРИТМИ САМООРГАНІЗАЦІЇ БЕЗДРОТОВИХ СЕНСОРНИХ СИСТЕМ

Бєлоусов В.О.
Науковий керівник – к.т.н, доц. Філіппенко І.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: vladyslav.bielousov@nure.ua

Today, the task of building distributed data collection, management and monitoring systems is never more relevant in a wide variety of applications, but the use of traditional wired solutions is not always effective because of the high cost of assembly, commissioning and maintenance. The sensor network has a number of advantages in terms of scalability and autonomy.

Сьогодні завдання побудови розподілених систем збору даних, управління і моніторингу як ніколи актуальна в самих різних прикладних галузях. Крім того, в деяких ситуаціях взагалі неможлива прокладка кабелів з технічних, економічних або організаційних причин. Тому бездротові системи передачі даних виглядають вельми привабливо для вирішення поставленого завдання. Але зараз бездротові системи збору даних і моніторингу стали реальністю завдяки технології так званих бездротових сенсорних мереж.

Сенсорна мережа – розподілена самоорганізована бездротова мережа, що складається з малогабаритних інтелектуальних сенсорних пристроїв. Задля рішення задач збору, обробки і передачі інформації з високими вимогами по автономності, надійності, масштабованості і розподіленості мережі.

Ad Hoc – децентралізований режим бездротової мережі, коли клієнтські станції взаємодіють безпосередньо один з одним без точки доступу або Wi-Fi роутера. Для режиму Ad Hoc потрібно мінімум устаткування – досить, щоб кожна станція була оснащена бездротовим адаптером Wi-Fi. При такій конфігурації не потрібно створення якої-небудь мережевої інфраструктури [1]. Також у роботі розглянуті стандарти Wi-Fi, Bluetooth, HomeRF, ZigBee засобами, яких можна побудувати та налаштувати бездротову сенсорну мережу та виявлений найбільш

відповідний стандарт для побудування самостійної та масштабованої сенсорної мережі за допомогою алгоритмів самоорганізації[2].

До теперішнього часу розроблені більше 100 різних алгоритмів самоорганізації у БСС, які можна умовно розбити на групи [3].

1) Створення кластерів.
2) Створення ланцюжків зв’язків.
3) Створення деревовидної структури .
4) Географічні підходи .
5) Підхід, що використовує різнорідність вузлів мережі [4].

В рамках цієї роботи досліджені основні перевага сенсорних систем – оперативність і економічність розгортання; відсутність необхідності в постійному техобслуговуванні; тривала автономна робота; відмовостійкість і надійність в жорстких умовах експлуатації; широка область застосувань. Порівняні різні стандарти зв’язку та виявлений найоптимальніший. Розглянуті види алгоритмів самоорганізації та їх алгоритми.

Список джерел:

1. Ad-hoc Networks [Електронний ресурс] – Режим доступу до ресурсу: http://www.acorn.net.au/telecoms/adhocnetworks/adhocnetworks.cfm.

2. Fernandez, E.B. & VanHilst, M., Chapter 10, WiMAX Standards and Security (Edited by M. Ilyas & S. Ahson) [Електронний ресурс] – June 2007. Режим доступу до ресурсу: http://www.crcpress.com.

3. Dressler F. A Study of Self-Organization Mechanisms in Ad Hoc and Sensor Networks / F. Dressler // Computer Communications / F. Dressler., 2008. – P. 3018–3029.

4. Handy M. Low energy adaptive clustering hierarchy with deterministic Cluster-Heads selection / M. Handy, M. Haase, D. Timmermann, 2002. – (Proc. 4th International Workshop on Mobile and Wireless Communications Network). – P. 368–372.

ПРИМЕНЕНИЕ ОБАЧНЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ «УМНОГО ДОМА»

Казьмина Д.Р.
Научный руководитель – ст. пр. Росинский Д.Н.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки,14, каф. ЭВМ, тел. (057) 702-13-54)
e-mail: d_ec@nure.ua

This work is devoted to the development of smart home technology based on cloud technology SaaS. The work uses the concept of Internet technology. Based on the analysis, we can conclude that the SaaS cloud model is most suitable for implementing smart home systems using the Internet of Things, since this cloud technology is currently the most common in the world, and everyone who has access to the Internet. The main advantage of the SaaS model for the end user is that there is no need to install and update software.

Внедрение в жизнь современного человека различных технологий автоматизации набирает всё большую популярность. Одна из подобных технологий, называемая термином «умный дом», позволяет оснастить обычное жилое пространство неким «помощником», который упростит отслеживание его состояний. Здесь следует отметить, что основной задачей системы умного дома является повышение безопасности и обеспечение максимального комфорта его обитателей. Несмотря на ряд имеющихся минусов, данная технология используется все чаще.

Стремительное развитие мобильных устройств с постоянным доступом к сети, а также развитие облачных вычислений позволяет технологиям умного дома все больше соответствовать концепции «Интернет вещей», предложенной в 1999 году основателем исследовательского центра Auto-ID Center в Массачусетском технологическом институте Кевином Эштоном. Под этим понятием подразумевается сеть физических объектов-вещей, содержащих встроенную технологию, которая позволяет этим объектам-вещам измерять параметры собственного состояния, состояния окружающей среды и передавать соответствующую информацию [1].

Применительно к системам умного дома концепция «Интернет вещей» выступает в роли способа реализации самой системы. Аппаратная часть системы состоит из множества используемых датчиков, то есть объектов-вещей, информация с которых отправляется на облако. Облако является частью программной системы, которая позволяет управлять объектами-вещами, собирать, редактировать и сохранять полученную от них информацию. Контроль за системой умного дома выполняется через специально разработанный интерфейс в виде веб-сайта или мобильного приложения.

На основе проведенного анализа можно сделать вывод о том, что облачная модель SaaS больше всего подходит для реализации систем умного дома с использованием «Интернета вещей», поскольку данная облачная технология в настоящий момент является наиболее распространенной в мире. При этом доступна она всем, кто является пользователем сети Интернет. Особым образом следует отметить, что основное преимущество модели SaaS для конечного пользователя заключается в отсутствии необходимости установки и обновления программного обеспечения [2].

Применение облачной технологии SaaS для систем умного дома включает в себя два варианта. В первом варианте контроллер (сервер) для управления устройствами умного дома может быть расположен не в самом доме (эту функцию возьмет на себя облако), благодаря чему управление системами умного дома может осуществляться откуда угодно при наличии доступа к Интернету. Во втором варианте контроллер может располагаться дома, но при этом через облако будет обеспечиваться только удаленное управление; всё программное обеспечение будет установлено на облачном сервере.

Для успешного взаимодействия облачного сервера с устройствами умного дома оба этих компонента должны общаться друг с другом посредством одного языка. Наиболее простым и распространенным решением является обмен данными с помощью XML-сообщений. Одним из протоколов, использующих XML для обмена данными, является SOAP, основным преимуществом которого является обеспечение непрерывного взаимодействия веб-сервиса (облака или контроллера) с объектами-вещами.

Среди недостатков использования данной технологии можно выделить относительно невысокое быстродействие, ненадежность доступа к системе умного дома в связи с проблемами Интернет-соединения и неполное обеспечение безопасности данных, в том случае, если SaaS-модель предоставлена сторонним провайдером. Преимущества заключаются в полной мобильности пользователя, достаточно коротких сроках внедрения в эксплуатацию и кроссплатформенности.

Список источников:

1. Найдич А. «Интернет вещей» – реальность или перспектива? [Электронный ресурс] / Андрей Найдич // КомпьютерПресс. – 2013. – Режим доступа к ресурсу: https://compress.ru/article.aspx?id=24290.

2. Виды облачных сервисов: IaaS, PaaS, SaaS и другие модели [Электронный ресурс]. – 2018. – Режим доступа к ресурсу: https://oblako.kz/iaas-blog/samye-populjarnye-oblachnye-servisy-v-mire.

ПОРІВНЯННЯ МЕТОДІВ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ

Ковріжний О.В.
Науковий керівник – д.т.н., проф. Кривуля Г.Ф.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: oleksii.kovrizhnyi@nure.ua, тел. 380979836976

This paper focuses on the problem of load balancing network traffic. Review of existing methods of load balancing, identifying their strength and weaknesses.

З проблемою балансування навантаження зустрічається будь-який веб-проект, бо відмова роботи серверу через велику кількість вхідних запитів може відбутися несподівано та призвести до небажаних матеріальних втрат. Стійкість серверу до навантаження можна вирішувати різними шляхами: будь-то зміна апаратної складової чи оптимізацією використовуємих алгоритмів та програмних кодів. Великі веб-проекти вирішують цю проблему шляхом кластеризації декількох серверів, навантаження між якими розподіляється за допомогою спеціальних методик з використання, як апаратних, так і програмних інструментів. Мета дослідження – визначити можливі переваги та недоліки балансування навантаження на різних рівнях мережевої моделі OSI. Задача – полягає у порівнянні існуючих методів балансування навантаження, можливості їх комбінування та визначення області використання.

Балансування навантаження - це метод для розподілу роботи між декількома обчислювальними ресурсами, такими як комп’ютери, кластери, мережі, центральні процесори та диски (носії інформації). Мета балансування полягає у оптимізації використання ресурсів, максимізація пропускної здатності, мінімізація часу відповіді та запобігання перенавантаження.

Рішення з балансування навантаження часто поділяють на дві категорії: L4 та L7, які відповідають транспортному та прикладному рівням мережевої моделі OSI. Стосовно категорії L4 балансування відбувається шляхом TCP-з’єднання клієнта з балансувальником, який в свою чергу завершає з’єднання, обирає найбільш доступний сервер та встановлює з ним зв'язок. Таким чином всі маніпуляції відбуваються на рівні з’єднання/сеансу протоколів TCP/UDP.

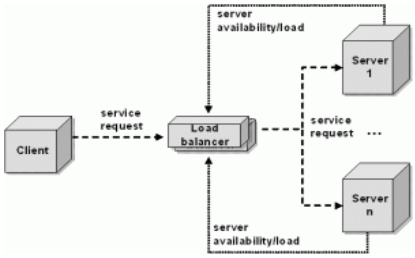


Рисунок 1 – Класична архітектура балансування навантаження

Слід зазначити, що балансувальник на рівні L4 робить одне вихідне TCP-з'єднання для кожного вхідного, приводячи до двох вхідних и двох вихідних з'єднань у ланцюгу клієнт-сервер. Розглянемо ситуацію, коли клієнт А відправляє 1 запит в хвилину, а клієнт Б – 50 запитів у секунду по вже встановленому з'єднанню. В результаті сервер, який був обраний для клієнта А, буде оброблювати приблизно в 3000 разів менше, ніж сервер обраний для клієнта Б. Тому безперервне TCP-з'єднання порушує перш за все мету балансування навантаження і є недоліком.

Балансування категорії L7 працює на прикладному рівні моделі OSI, орієнтовані на роботу з високорівневими протоколами такими як HTTP/HTTPS. В процесі балансування відбувається аналіз запитів клієнта та перенаправлення на різні сервери в залежності від характеру контенту (за такими принципами працює модуль Upstream веб-серверу Nginx). Оскільки L7 балансувальник виконує значно складніший аналіз, перетворення та маршрутизацію трафіку веб-додатку, тому навантаження на апаратну складову значно збільшується, що приводить до зменшення продуктивності обробки навантаження (яка вимірюється у оброблених пакетах за секунду), порівняно з оптимізованими L4 балансувальниками. Слід зазначити про значну складність розробки алгоритмів аналізу трафіку, серед яких вірогідність програмної помилки значно більша.

Підводячи підсумки можна зазначити, що важливу роль для сучасних мережевих протоколів відіграє балансувальники категорії L7. Хоча порівнюючи функціонально категорія L7 може повністю замінити L4, але кожний метод балансування виконує свою задачу і займає відповідне місце. Балансування категорії L4 використовується не менше, бо майже всі розподілені архітектури використовують дворівневу систему балансування навантаження L4/L7 для інтернет-трафіку. Тому для найбільш продуктивного балансування навантаження на сервери слід поєднувати можливості різних методів.

Список джерел:

1. Bourke T. Server Load Balancing // O'Reilly & Associates. – 2001. – V.126/ – N 2. – P. 182.

2. Introduction to modern network load balancing and proxying [Електронний ресурс] – Режим доступу: www / URL: https://blog.envoyproxy.io/introduction-to-modern-network-load-balancing-and-proxying-a57f6ff80236.

ПОШУК ІСНУЮЧИХ РІШЕНЬ ПОВЯЗАНИХ ІЗ ЕЛЕКТРОННИМ ДОКУМЕНТООБЕРТОМ. ІННОВАЦІЇ ДЛЯ ПОКРАЩЕННЯ СУЧАСНИХ МЕТОДІВ.

Єрченко А. В.
Науковий керівник – д.т.н., проф. Чумаченко С.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: anastasiia.yerchenko@nure.ua, тел. 380954334626

Cyberculture, technologies and services of cyber-physics digital online monitoring and cloud metric control of social groups and structural components of the university.

Електронний документообіг – організаційно-технічна система, що забезпечує процес створення, управління доступом і поширення електронних документів в комп'ютерних мережах, а також що забезпечує контроль над потоками документів в організації. Часто електронний документообіг позначається терміном workflow, який характеризує рух документів як потік робіт, виконуваних в рамках того чи іншого бізнес-процесу. Система електронного документообігу (СЕД) – це програмне забезпечення, головними завданнями якого є організація і підтримка життєвого циклу електронних документів. Мета дослідження – розробка комп’ютингової системи безпаперового електронного документообігу кіберуніверситету для збереження ресурсів та екології в масштабах держави. Задачі дослідження – створення комп’ютингової системи безпаперового електронного документообігу кіберуніверситету.

Система електронного документообігу FossDoc - рішення на платформі FossLook, призначене для створення електронного архіву документів, організації корпоративного документообігу (workflow) і автоматизації бізнес-процесів на підприємствах, в установах і організаціях будь-якого роду діяльності. Програма дозволяє вирішити велику кількість завдань, реалізація яких покладена на відповідні модулі. Система може бути легко перенастроєна з урахуванням специфіки роботи кожного конкретного підприємств (рис 1.1).

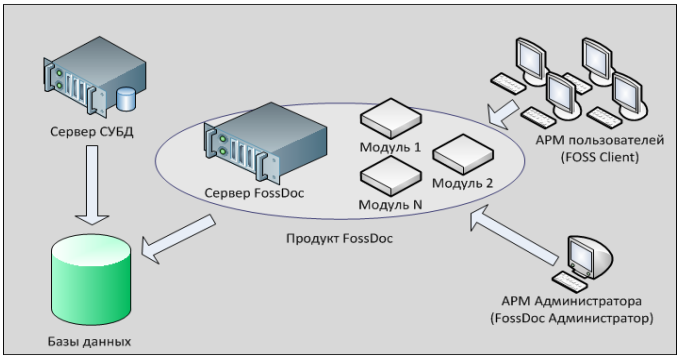


Рисунок 1.1 - Схема реалізації ПО FossDoc

Дана система дозволяє гнучко налаштувати маршрути руху документів між підрозділами вашого підприємства, вказати їх порядок виконання, узгодження, підписи, реєстрації. Ви можете налаштувати реєстрацію в декількох канцеляріях вашої організації. Підтримується ефективний механізм створення документа на основі його проекту з фіксацією кожної стадії узгодження в окремій версії проекту.

Все різноманіття документів, з якими працюють користувачі, розділяється на окремі категорії - типи документів. В системі існують зумовлені типи документів: вхідні та вихідні листи, звернення громадян, службові записки, накази. Документи можуть посилатися на інші документи або бути дочірніми по відношенню до головних.

Поштовий сервер призначений для створення "внутрішніх" поштових скриньок користувачів (на вашому домені) і роботи з ними – прийому / відправки повідомлень. Сервер також ініціює прийом повідомлень з інших поштових серверів (mail.ru, gmail.com) а також відправку ними повідомлень, якщо у користувачів, зареєстрованих на сервері, є зовнішні поштові скриньки.

В системі підтримується робота з електронним цифровим підписом (ЕЦП). Ви можете підписувати документи і їх поля за допомогою електронного цифрового підпису. Такий підпис гарантуватиме цілісність і автентичність відбитку даного документа. Ніхто, крім автора документа, не зможе внести зміни в нього так, щоб про це не стало відомо під час перевірки ЕЦП. [2]

Ідея впровадження електронного документообігу існувала вже давно. Основою електронного документообігу є легітимні інтелектуальні транзакції потоків оцифрованих документів в замкнутій кібер-системі (наприклад, Smart Cyber University). Електронний документообіг повинен вилучити паперові носії шляхом використання: цифрового електронного підпису, ключа, ID-card, E-mail і мобільного телефону. Для надійності документів пропонується його дублювання в кіберфізичному просторі. Доступ до документів будуть мати усі зареєстровані в системі користувачі, це не суперечить законодавству країни. Наукова новизна полягає у створенні інтелектуальної комп'ютингової системи моніторингу та управління, де усі дії будуть прозорими.

Список джерел:

1. Хаханов, В.И. Киберсервисы активного управления университетом [Текст] / В.И. Хаханов, А.С. Мищенко, С.В. Чумаченко, С.А. Зайченко // Радиоэлектроника и информатика. – 2014. – №4. – С. 56-61.

2. Электронный документооборот [Електронний ресурс] – Режим доступу: www/URL: https://club.directum.ru/post/72195.

ЗОВНІШНЯ ОХОРОННА СИСТЕМА КІБЕРУНІВЕРСИТЕТУ

Гарбузов Д.С.
Науковий керівник – к.т.н., проф. Немченко В.П.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: volodymyr.nemchenko@nure.ua

External security system. An overview of the components of the system and the processes to ensure correct operation. Projecting the system based on the infrastructure of the cyber university.

Зовнішня охоронна система (рис. 1) містить компоненти «інфраструктура, сенсори та датчики, хмарне сховище, БПЛА (Безпілотний літальний апарат)». Всі компоненти тісно пов’язані між собою в реальному часі та формують чітку структуру перетікання з одного процесу до іншого. В системі задіяні процеси обробки поточної інформації, сигналізування, запуску та моніторингу руху, контролювання коректності роботи БПЛА та заряду. Джерела: розподілення обчислювальної потужності та реальний час, великий об’єм зовнішніх даних, бездротовий доступ, підтримка аналітики та взаємний зв’язок з хмарами.

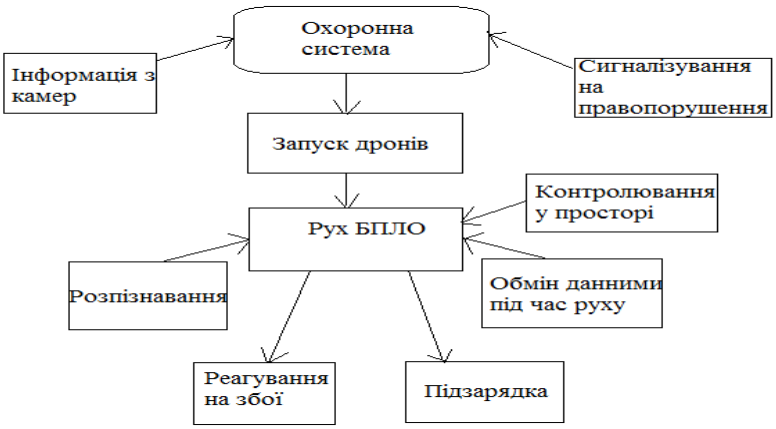


Рисунок 1 – Схема роботи охоронної системи

Мета дослідження – розробка зовнішньої охоронної системи університету для підвищення безпеки, покращення реагування на правопорушення або проникнення на територію, та зниження ризику здоров’я охоронців, що дає змогу швидше розпізнавати загрозу та ступінь правопорушення, за рахунок моніторингу ділянки в реальному часі. Задача – розробка моделі системи, яка буде поєднувати користувача та компоненти системи за допомогою обробки різних видів даних через хмарне сховище.

Зміст дослідження. Основою для проектування системи є інфраструктура університету з умовними камерами спостереження, які

направлені на входи університету та внутрішню територію. За допомогою камер і датчиків руху, що згруповані за відповідними зонами, можна легко ідентифікувати необхідну територію для початку роботи системи та початку руху дронів. В разі проникнення на територію, або іншого порушення порядку, знімаючи показання з камер, система реагує, сигналізувавши про це охоронцю, або оператору, який на своє передбачення запускає або не запускає охоронних квадрокоптерів. Запуск дронів надає оператору вибір індексу, якому відповідає певна камера відео спостереження. По цьому ідентифікатору дрон або декілька дронів відправляються до місця правопорушення. Дрони спроможні за короткий відрізок часу дістатися до заданої ділянки, що дає змогу детальніше розгледіти злочинця, без ризику для здоров'я оператора, який в свою чергу вирішує, чи визивати поліцію.

Пересування квадрокоптерами до заданих ділянок можливо виконувати різними алгоритмами, тобто при необхідності замінити на деякий не значний час камеру спостереження, використовується «1» режим, при якому до камери відправляється один чи два дрони, залежно від складності обзору ділянки та куту огляду камер на дронах. При необхідності патрулювати або перевірити стан цілого комплексу або ділянки – одночасно. Впроваджується «2» режим (рис. 2), згідно за яким до ділянки відправляються декілька дронів, які приймають форму піраміди для детальнішого огляду території з усіх сторін. В цьому випадку в алгоритмі є головний дрон, який знаходиться у вершині піраміди. Його метою є спостереження за іншими дронами та коректування їх на просторі.

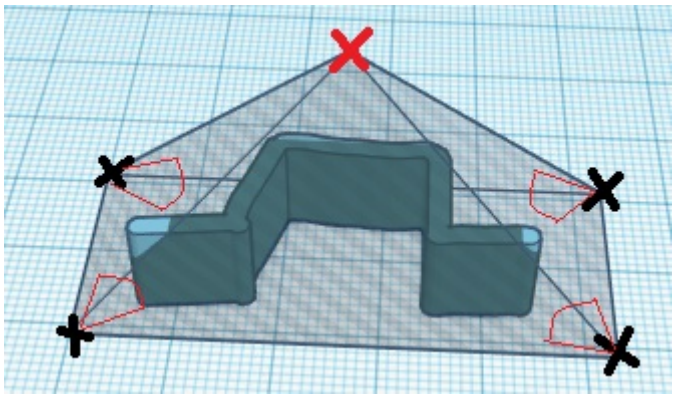


Рисунок 2 – Огляд ділянки при режимі «2»

При ускладнених кутах огляду, основа піраміди рухається по колу, а головний дрон залишається на місці. В цьому випадку оператору надається повний огляд будівлі або ділянки різної форми за короткий час.

Наукова новизна полягає у розробці моделі формування системи контролю території, моніторингу та реагування на різні типи ситуацій в реальному часі з запобіганням риску для здоров'я оператора та робітників закладу.

РАЗРАБОТКА ВЕБ-САЙТА С УЧЕТОМ КРИТЕРИЕВ ДОСТУПНОСТИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ С НАРУШЕНИЕМ ЗРЕНИЯ

Литвишко П.В
Научный руководитель – к.т.н., проф. Немченко В. П.
Харьковский национальный университет радиоэлектроники
(61202, Харьков, пр. Науки,14, каф. АПВТ, тел. (057) 702-13-26
e-mail: pavlo.lytvyshko@nure.ua, тел (099) 247-32-22

This work explains how to develop a website with available content for the blind people.

В Украине проживает 240 тысяч слепых и слабовидящих. Всего в мире насчитывается около 314 миллионов человек, имеющих нарушения зрения, вызванные разными причинами, 45 миллионов из них являются слепыми Они пользуются интернетом с помощью программ чтения с экрана, экранных луп и клавиатуры. Чтобы им было удобно пользоваться сайтами, нужно по-особому оформлять разметку, иллюстрации, формы ввода и таблицы. Предприятиям было бы неразумно намеренно игнорировать 10 или даже 5 процентов своих потенциальных клиентов. Для школ, университетов и государственных учреждений это было бы не только негуманно, но и во многих случаях нарушало бы закон. *Цель исследования* – повышение уровня доступности разрабатываемых сайтов за счет использования семантически верных HTML элементов и их атрибутов, что позволяет значительно расширить аудиторию пользователей веб-ресурса, а также уменьшить затраты на поддержку сайта в дальнейшем. Рекомендации помогут разработчикам делать сайты для людей с нарушениями зрения. Они основаны на официальных источниках - руководство WCAG 2.0 от W3C и Section 508 . Способы, описанные в рекомендациях, не влияют на внешний вид сайта и не мешают работе пользователей с нормальным зрением. *Задача* – проектирование и разработка структурных элементов сайта, соответствующих современным стандартам доступности.

При разработке доступных веб-страниц не обходимо обращать особое внимание на следующие структурные элементы: 1) изображения; 2) формы ввода; 3) текст; 4) таблицы; 5) навигация; 6) метаданные ресурса.

К изображениям необходимо всегда добавлять альтернативное описание с помощью атрибута alt тега img, это поможет слепым и слабовидящим пользователям понять, что представлено на картинке. Описание зависит от типа – информативное, график или диаграмма, декоративное или группа. Информативные передают краткую информацию к тексту, дополняют или обозначают его. Декоративные изображения необходимо добавлять с помощью свойства CSS background-image, чтобы скринридеры их игнорировали. Если декоративный элемент

представлен в виде изображения, например, внутри ссылки, добавьте к нему пустой alt или атрибуты role="presentation" и aria-hidden="true". Для сложных изображений – карт, диаграмм, графиков – добавьте краткое описание в атрибут alt и полное описание на отдельную страницу, в тег figcaption. Для групп изображений, которые представляют одну и ту же информацию, например, звездочки рейтинга, добавьте описание в alt только к первому изображению.

Формы ввода следует описывать с помощью тега label или атрибута title. Необходимо добавить инструкции и ошибки в текстовом виде. Не следует использовать в подсказках визуальные свойства элементов. Это поможет слепым и слабовидящим заполнить форму – узнать названия полей и формат данных, получить результат отправки формы. Оформление текста должно выполнятся посредством CSS, оформление содержательного текста изображением - недопустимо. Расшифруйте аббревиатуры и дайте определения сложным терминам. Добавьте аббревиатуры в тег abbr, расшифровку в атрибут title.

Дайте пользователю возможность управлять сайтом с клавиатуры без ограничений по времени на нажатие клавиши. Это поможет пользователям, которые не могут пользоваться мышкой, работать со страницей без препятствий – листать страницу, переходить по ссылкам, заполнять формы. Обеспечьте правильную последовательность перехода фокуса – проверьте семантику верстки, правильную последовательность содержимого на странице и добавьте визуальное отображение фокуса на активных элементах. Переход на следующий элемент – одно нажатие на клавишу Tab, на предыдущий - Shift+Tab. Для определения очередности выбора элементов при навигации по сайту с клавиатуры используйте атрибут tabindex.

Интернет предлагает много решений для людей с ограниченными возможностями, которые недоступны через любую другую среду. Он предлагает независимость и свободу. Однако, если страница создана без учёта доступности интерфейсов, он может затруднить доступ населению, которое больше всего выиграет от интернета. По мере того, как организации и дизайнеры узнают о доступности и реализуют ее, они будут обеспечивать доступ к своему контенту для более широкой аудитории.

Список источников:

1. Макеев В. А. Веблайнд - рекомендации по разработке сайтов для людей с нарушениями зрения [Електронный ресурс] / В. А. Макеев – Режим доступа к ресурсу: https://weblind.ru/.

2. Introduction to Web Accessibility [Електронный ресурс] – Режим доступа к ресурсу: https://webaim.org/intro/.

ИНТЕЛЛЕКТУАЛЬНОЕ ОБУЧЕНИЕ ИГРОВЫХ ПЕРСОНАЖЕЙ

Усачов В.С.
Научный руководитель – к.т.н. доцент Аксак Н.Г.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. ЭВМ, тел. (057) 702-13-54)
e-mail: hotrodvadim@gmail.com, тел. 099-527-6559

Environmental machine learning is one of the most important branches of AI-learning to date. The main purpose is to create game-environment with running course for AI-driven game-characters, which will try to finish course by using neuron networks and evolutionary algorithms. Learning process will be main focus of this work with task of finding fastest learning algorithm for AI to use. This technology may be useful for creating smarter AI-driven machines in the future.

Машинное обучение - это обширный раздел искусственного интеллекта, построенный на алгоритмах, способных к самообучению. Одним из подразделов машинного обучения является «обучение с подкреплением», который, в работе, представлен динамическим взаимодействием персонажа (Agent) со игровой средой (Environment). При этом, обучающийся персонаж может выполнять действия из определенного набора. Игровая среда меняется в результате выполнения этого действия, и персонаж воспринимает новое состояние среды (рис.1).

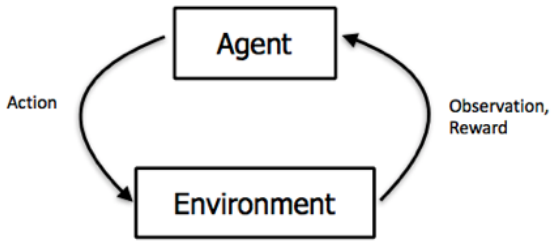


Рисунок 1 – Обучение с подкреплением

Один из элементов этого состояния – некоторое скалярное число, которое представляет собой вознаграждение (Reward). Это вознаграждение говорит о том, правильно ли обучающийся персонаж выполняет те или иные действия на игровом уровне. Целью персонажа является максимизация суммарного вознаграждения, которое он получает в результате достаточно длинного взаимодействия в этой среде.

Реализованный игровой уровень состоит из платформ и преград, а игровые персонажи наделены базовым набором действий - бег в двух направлениях и прыжок.

Нейронные сети предлагается использовать для анализа текущего положения персонажей на игровом уровне. В качестве входных параметров используются данные о ближайших преградах вокруг игрового

персонажа. С помощью этой информации персонаж принимает решение о том, какое действие выполнить – пойти вперед, назад или прыгнуть.

Для тестирования создается несколько игровых персонажей. Результатом является дальность прохождения уровня – чем дальше персонаж дошел, тем лучше он справился с поставленной задачей. Первое поколение строится на случайных настройках каждого индивидуального персонажа. Настройки заключаются в определении минимальных и оптимальных значений расстояния между игровым персонажем и преградой, при которых он должен принять то или иное решение.

Для генерации следующего поколения предлагается выбирать 20% лучших результатов предыдущего поколения (рис. 2). Процесс генерации нового поколения основан на смешивании настроек лучших результатов случайными способами с целью достижения улучшений в следующем тесте. Этот процесс называется скрещивание.

Предлагается также использовать явление мутации (рис. 2), которое меняет настройки нескольких игровых персонажей случайным образом с целью получить лучший результат и ускорить процесс решения задачи.

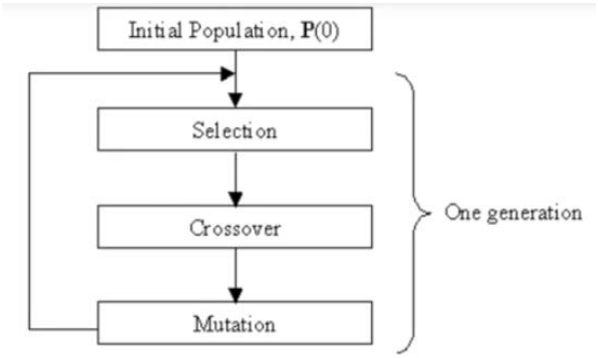


Рисунок 2 – Алгоритм эволюции

Данный процесс продолжается до полного прохождения уровня одним из персонажей. Критериями оценки работы алгоритма машинного обучения предлагается взять время работы алгоритма, точность и количество полученных поколений. Целью работы является достижение как можно меньшего количества произведенных поколений перед полным решением поставленной задачи.

Список источников:

1. Reinforcement learning [Электронный ресурс] https://medium.freecodecamp.org/an-introduction-to-reinforcement-learning-4339519de419.

2. Иерархическое машинное обучение с подкреплением [Электронный ресурс] https://postnauka.ru/video/9027

IOT СИСТЕМА ЕНЕРГОСПОЖИВАННЯ ЕЛЕКТРОТРАНСПОРТНИХ ЗАСОБІВ

Куликівська Ю. С.
Науковий керівник – проф., к.т.н., доцент Немченко В.П.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: yuliia.kulykivska@nure.ua, тел. (095) 345-32-92

The problem of loading and power consumption in the country is considered in connection with the growing number of electric vehicles. The innovative smart-system based on the Internet of Things technology (IoT), for its application in SmartGrid systems and the combined power system (UPS) of Ukraine on the basis of the analysis, is offered.

Автономна батарея транспортного засобу (далі – EV) є широко використовуваним пристроєм для зберігання енергії, обчислення статусу заряду грає життєво важливу роль в економіці країни [1].

EV використовує електродвигуни для руху. Для звичайної зарядки транспортного засобу зазвичай використовується власне зарядний пристрій, підключений безпосередньо до мережі АС.

Зарядна станція EV живиться від розетки зарядного пристрою (рис. 1, а). Двонаправлений інвертор забезпечує двонаправлений потік потужності між мережею і акумулятором, що дозволяє відокремити електричний заряд від мережі. Вся система контролюється одиницею вимірювання, контролю та зв'язку. Отже, силова секція активної зарядної станції повинна задовольняти наступним вимогам: високий динамічний режим управління робочими умовами, чотири квадранта щодо електромережі, активна фільтрація, реверсування впливу електричних зарядних пристроїв, висока ефективність перетворення електричної енергії.

Це дозволяє покрити потреби зарядки електричної енергії в момент, коли відмова мережі здійснюється за допомогою живлення від допоміжної батареї активної зарядної станції, та пригнічувати негативні ефекти зворотного зв'язку зарядки EV на енергосистему, як основної гармоніки, реактивної потужності і в більш високих порядках гармонік. Перевагою рішення є також те, що в разі нестачі енергії в допоміжному акумуляторі станція може працювати тільки як так званий паралельний активний фільтр.

Більшість власників приватних автомобілів зазвичай покладаються на домашню зарядку вночі. Відмітимо, що найкраща електрозаправка – це трифазна розетка вдома.

Ще один важливий висновок: якщо сукупна частка витрат на електроенергію та інші комунальні послуги перевищує 20% від сукупних доходів домогосподарств, рівень оплати починає стрімко падати, що призводить до кризи неплатежів по всьому ланцюжку системи

енергозабезпечення: від житлово-комунального господарства до усієї економіки країни.

Отже зараз існує потреба у впровадженні системи зарядки EV в парковочних системах або мережах.

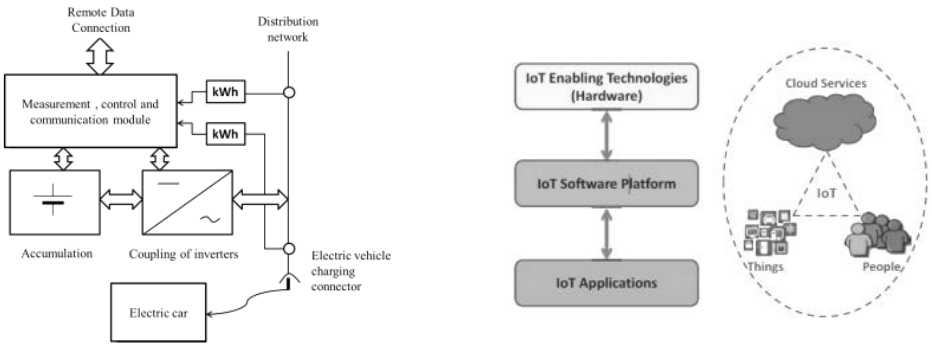


Рисунок 1 – а) Структура зарядного пристрою для електричних транспортних засобів; б) Смарт-система на базі IoT

Запропонована смарт-схема на основі технології Інтернету речей (IoT) дозволяє відстежувати стан батареї в системах SmartGrid (рис. 1, б) і має можливість увімкнути/вимкнути подачу живлення, встановити потрібний режим економії електроенергії, отже й коштів, як у “звичайному режимі” так і у “режимі подорожі”. Система має використовувати хмарну платформу та мобільну платформу Android/iOS чи веб-інтерфейс. Крім того, користувач може визначити місце розташування найближчої зарядної станції за допомогою програми. Як тільки користувач дізнається напруга свого акумулятора занизька, він може легко вирішити, чи варто продовжувати подачу енергії в мережу або брати енергію з мережі на основі тарифних ставок. Тарифна ставка буде відрізнятися для подачі електроенергії в мережу і отримання енергії від мережі. Сітка буде мати двонаправлені перетворювачі для передачі потужності [2] [3]. Є кілька сіток, які також використовують сонячну енергію як джерело. Відправка, калькуляція та зберігання даних повинно відбуватися за допомогою хмарних технологій.

Таким чином, використання запропонованої системи дозволяє не тільки зменшити витрати коштів власників EV на підзарядку, а й оптимізувати усю систему ОЕС України.

Список джерел:

1. Friansa, Koko, Irsyad Nashirul Haq, Bening Maria Santi, Deddy Kurniadi, Edi Leksono. ”Development of Battery Monitoring System in Smart Microgrid Based on Internet of Things (IoT).” Procedia engineering 170 (2017): 482-487.

2. Kim, Ho-Sung, Myung-Hyo Ryu, Ju-Won Baek, and Jee-Hoon Jung. ”High-efficiency isolated bidirectional ACDC converter for a DC distribution system.” IEEE Transactions on Power Electronics 28, no. 4 (2013): 1642-1654.

ПОРІВНЯННЯ СПОСОБІВ ПОЗИЦІОНУВАННЯ АВТОНОМНОГО ТРАНСПОРТНОГО ЗАСОБУ В ТРАНСПОРТНОМУ ПОТОЦІ

Кривицький А. О.
Науковий керівник – к.т.н., доц. Філіппенко І.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Автоматизації проектування обчислювальної техніки, тел. (057) 702-13-26)
e-mail: andrii.kryvytskyi@nure.ua, тел. (057) 702-13-26

The given work is devoted to the modern developments in the field of autonomous driving vehicles positioning in small range environment, not far than hundreds of meters. Comparing main technologies, such as cameras, radars and lidars. Cameras are best ones in visible range. Radars much better in distance measurement, but lidars can create detailed 3d maps of surrounding world. On the other hand lidars are very expensive technology and not very stable. So, probably, best solution is a composite of two technologies, for example, radar and cameras.

Транспорт завжди був рушієм розвитку технологій, особливо автомобілі, адже, за статистикою це найнебезпечніший транспорт і розробники завжди прагнуть виправити цю невтішну тенденцію. Проте на скільки б не був безпечним автомобіль, ним завжди керує людина, з чим пов’язана найбільша небезпека тому й зародилася тенденція розробки безпілотних транспортних засобів.

При розробці перших повноцінних безпілотних авто основним способом сприйняття простору навколо машини були камери. Вони дозволяють швидко отримувати зображення у видимому діапазоні з широким кутом огляду. Проте однієї картинки з камери для успішного функціонування автономного автомобіля недостатньо, безпілотнику потрібний електронний аналог людського мозку, тобто спеціалізований процесор обробки зображень.

Створенням таких процесорів займаються як великі досвідчені компанії, так і стартапи, скажімо, Mobileye, що став частиною Intel, інші великі компанії, такі як NVIDIA та Toshiba. Більшість подібних процесорів обробляють інформацію з чотирьох камер, оцінюючи зображення відразу по за кількома факторами : розмітка, авто, що рухаються і припарковані, світлофори і знаки, зустрічне світло фар, пішоходи і велосипедисти.

Проте ж, у підходу з використанням тільки камер є великий мінус - камери не здатні розпізнавати віддалені об'єкти і будувати деталізовані карти, до того ж їх функціональність безпосередньо залежить від погодних умов. Виправити ці недоліки можуть радари, випромінюючі радіосигнали з частотою в десятки гігагерца. Вони ідеально визначають перешкоди в просторі. Радари з частотою випромінювання в 24 ГГц і 77 ГГц вже застосовуються в дорогих системах ADAS для завчасного гальмування при

виявленні перетину курсів руху з пішоходом або іншим авто. При усій точності і швидкості роботи у застосування радарів є велике обмеження - на відміну від камер, у радарів дуже вузький кут дії, обернено пропорційний до бажаної дальності дії. До того ж радар має високу собівартість (на рівні 1000 доларів США), що відразу обмежує поле його застосування виключно дорогими автомобілями. Тобто, радари ідеально підходять для завдання локалізації об'єктів, без визначення їх геометричних параметрів, в дуже обмеженому куті огляду.

Ще одним способом позиціонування сканування простору є використання лідарів Вони визнані найефективнішим, але при цьому неоднозначним сенсором для автономних автомобілів. Причому лідари, завдяки лазерним променям будують детальну картину світу навколо роблять з точністю, недосяжною для інших систем, проте недоліків у лідара поки більше, ніж позитивних аспектів. По-перше, вони стають безпорадними під сильним дощем або під час снігопаду. По-друге, лідар повинен мати повний круговий огляд, тобто він створює "горб" на даху авто. По-третє, ця технологія не просто дорога, а дуже дорога: ранні зразки виробництва компанії Velodyne куштували 75 тисяч доларів, сучасні розробки Waymo коштують 7500 доларів. Проте найбільшою проблемою лідарів є помилки в їх роботі, а саме – невиявлення, і неправдиве спрацьовування. В окремий клас помилок варто виділити повну відмову системи. Датчики, або їх програмні компоненти можуть відмовити, або несправно працювати і такі помилки, на жаль частіші за будь які інші, що унеможливлює їх використання звичайних авто.

З усіх наведених властивостей стає очевидним, що для компенсації недоліків найкращим варіантом є використання декількох систем одночасно. Приміром, використання камер у комбінації з радаром дозволяє мати чітку оточуючу картину світу з відеопотоку і надточну дистанцію до об’єктів навколо транспортного засобу. Комбінуючи ці потоки інформації стає можливим точно позиціонувати автомобіль, а головне надійніше ніж одна система та дешевше ніж, наприклад, з використанням лідара.

Список джерел:

1. A Medium Corportaion – URL: https://medium.com/@cacheop/advanced-lane-detection-for-autonomous-cars-bff5390a360f – Advanced Lane Detection for Autonomous Cars.

2. Habr.com – URL: https://habr.com/company/toshibarus/blog/431388/ – Мир глазами автомобиля. Каким его видят беспилотники.

3. Lane depature system Mathworks – URL: https://www.mathworks.com/help/vision/examples/lane-departure-warning-system-1.html – Lane Departure Warning System by Mathwork.

РОЗРОБКА IOT ПРОЕКТУ ЗА ДОПОМОГОЮ Wi-Fi МОДУЛЯ ESP8266

Кравцов К.Р.
Науковий керівник – к.т.н, доц. Філіппенко І.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. АПОТ, тел. (057) 702-13-26)
e-mail: nekravtsovkirill@gmai.com

Internet of things (IoT) is not something new: high technology companies and experts have been discussing the idea for many decades, and the first Internet-connected toaster was introduced to the conference in 1989. In essence, IoT is simple: it's about connecting devices over the Internet, allowing them to communicate with us, applications and with each other.Broadband Internet is becoming more widely available, the cost of connectivity decreases, more and more devices are created with Wi-Fi capabilities and sensors embedded in them, technology costs are reduced, and a smart phone is rapidly penetrating everywhere. All these things create the "perfect storm" for the IoT.

При розробці проектів з використнням стандарту зв’язку Wi-Fi 802.11 необхідно мати розуміння принципі його роботи в бездротовій мережі. На високому рівні, Wi-Fi - це бездротова мережа для з'єднань TCP / IP. Wi-Fi - це набір протоколів бездротової мережі, описаних у стандарті IEEE 802.11.

Пристрій, що називається Wireless Access Point (AP) - бездротовою точкою доступу (точкою доступу) працює як вузол комунікацій. Зазвичай воно підключено або працює в режимі роутера. Наприклад, Wi-Fi роутер в кожному домі працює в такому режимі.

У роботі пропонується загальна модель з використанням стандарту Wi-Fi 802.11, яка може бути взята за основу при розробці різноманітних проектів з використанням бездротової системи зв`язку. Як технічне рішення даної задачі був використаний модуль ESP8266.

Модуль ESP8266 може працювати як в режимі точки доступу (Access Point), так і в режимі клієнта - робочої станції (Station), а може і в обох режимах одночасно. Найчастіше точка доступу має підключення до інтернету і працює як міст між пристроєм і інтернетом. Кілька робочих станцій у локальній мережі спілкуються між собою також через точку доступу. Станція одночасно може бути підключена тільки до однієї точки доступу. Кожен пристрій в мережі має власний унікальний MAC-адресу - 48-бітове значення.

Якщо в межах видимості знаходиться кілька точок доступу, їх потрібно якось розрізняти, тому у кожної точки доступу є мережевий ідентифікатор, званий SSID (Service Set Identifier, іноді також званий BSSID) - це ім'я мережі, що має довжину до 32 символів.

При написанні програми дуже часто вони працюють не так як очікувалося. Для модуля ESP8266 налагодження (отримання службової

інформації і стану системи) полегшується наявністю послідовного порту спеціально для виведення налагоджувальної інформації. Ви можете надрукувати в UART1 (GPIO2) що хочете за допомогою функції os_printf (). Якщо підключити на піну GPIO2 модуля перетворювач UART-USB, то ви зможете бачити цю інформацію на екрані комп'ютера в реальному часі. Таким чином, маючи один порт UART для прошивки модуля, а другий для налагодження, вам не доведеться нічого перемикати при створенні своєї програми.

Найшвидший спосіб поспілкуватися з модулем ESP8266 - це передати йому АТ-команду і отримати відповідь. Набір АТ-команд - це спеціальний набір інструкцій, які "знає" наш модуль і може виконувати певні дії при їх отриманні і видавати в термінал результат їх виконання. Програма, яка називається процесор АТ-команд, вже встановлена в модулі ESP8266 і готова до їх прийому по послідовному порту. Ці команди починаються з символів "AT".

Запропонована бездротова модель з використанням модулю ESP8266 була протестована у декількох проектах. Модель показала гарні показники у ефективності, надійності та зручності використання. Запропонована система зв`язку покриває великий функціонал і проста у використані. Програмна частина проекту є універсальної, що робить її придатною для широкого ряду задач.

Список джерел:

1. Сообщество разработчиков – URL: https://esp8266.ru/.
2. Habr.com – URL: https://habr.com/ru/post/394535/ – ESP8266 с чего начать или первый опыт.
3. IoT – URL: http://mikrotik.kpi.ua/index.php/courses-list/iot/79-what-is-the-internet-of-things-and-why-is-it-important – Що таке IoT.

INTERNET OF THINGS

Шостак М.В.
Науковий керівник – ст. викл. Мовсесян Я.С.
Харківський національний університет радіоелектроніки
(61166б Харків, пр. Науки, 14, каф. ЕОМ, тел (057) 702-13-54),
E-mail maksym.shostak@nure.ua

The Internet of things (IoT) is the network of devices such as vehicles, and home appliances that contain electronics, software, sensors, actuators, and connectivity which allows these things to connect, interact and exchange data.

В наш час в наших домівках є велика кількість пристроїв, які спрощують нам життя. З'єднання їх в єдину мережу називають Розумною будівлею. Ця концепція стала можлива після створення Internet of things.

Internet of things (інтернет речей) – концепція виміру, в якому різні прилади та датчики з'єднані між собою дротовими та бездротовими каналами зв'язку та підключені до мережі Інтернет. Також це дуже тісна інтеграція реального та віртуального світу, в якому спілкування відбувається між людьми та приладами.

Інтернет речей являє собою чотири рівні: 1-й рівень пов'язаний з ідентифікацією кожного об'єкту, 2-й рівень представлений сервісом з обслуговування потреб споживача, 3-й рівень пов'язаний з урбанізацією міського життя, 4-й рівень – сенсорна планета.

Тобто Інтернет речей можна розглядати, як мережу мереж, в якій невеликі мережі створюють набагато більші.

Для об'єднання пристроїв в одну мережу необхідно кожному надати унікальну IP-адресу. В наш час найбільш популярним є IPv4 протокол. Він має обмежені адресні простори. Для рішення цієї проблеми вдало підходить підтримка IPv6, яка забезпечує унікальними адресами мережевого рівня не менше 300 млн пристроїв на одну людину.

Для бездротової передачі даних дуже важливу роль в побудові інтернету речей відіграють такі характеристики, як ефективність, відмовостійкість, адаптивність, можливість самоорганізації. Основне зацікавлення в цьому сенсі представляє стандарт IEEE 802.15.4, що управляє доступом для організації енергоефективних персональних мереж і є основою для таких протоколів, як ZigBee, WiFi, Bluetooth, 6LoWPAN.

Особливу роль в інтернеті речей відіграють засоби вимірювання, що забезпечують перетворення відомостей про зовнішнє середовище в машинозчитувані дані і, тим самим, здатні наповнити обчислювальну середу значущою інформацією. В рамках концепції Інтернету речей принциповим є об'єднання засобів вимірювання в мережі (такі, як бездротові датчикові мережі, вимірювальні комплекси), за рахунок чого можлива побудова систем межмашинної взаємодії.

Практична проблема впровадження «інтернету речей» – це необхідність забезпечення максимальної автономності засобів вимірювання і, перш за все, проблема енергопостачання датчиків. Знаходження ефективних рішень, що забезпечують автономне живлення сенсорів (використання фотоелементів, перетворення енергії вібрації, повітряних потоків, використання бездротової передачі електрики), дозволяє масштабувати сенсорні мережі без підвищення витрат на обслуговування.

Серед провідних технологій важливу роль у розповсюдженні інтернету речей відіграють рішення PLC — технології побудови мереж передачі даних по лініях електропередач, оскільки у багатьох додатках присутній доступ до електромереж. 6LoWPAN, який реалізує шар IPv6 як над IEEE 802.15.4, так і над PLC, будучи відкритим протоколом стандартизованих IETF, відзначається як особливо важливий для розвитку інтернету речей.

Інтернет речей може викликати величезні зміни у повсякденному житті, надавши звичайним користувачам абсолютно новий рівень комфорту. Але якщо елементи такої системи не будуть належним чином захищені від несанкціонованого втручання за допомогою надійного криптографічного алгоритму, то замість користі вони принесуть шкоду, надавши кіберзлочинцям лазівку для підриву інформаційної безпеки. Оскільки речі із вбудованими комп'ютерами зберігають дуже багато інформації про свого власника, а зокрема можуть знати його точне місцезнаходження, доступ до такої інформації може допомогти зловмисникам вчинити злочин. Відсутність на даний час стандартів для захисту таких автономних мереж дещо сповільнює впровадження інтернету речей у повсякденне життя.

Хоча в області стандартів досягнуто значного прогресу, але попереду ще велика робота, особливо в областях безпеки, захисту інформації, архітектури та комунікації. IEEE – одна з організацій, яка намагається вирішити зазначені проблеми за рахунок стандартизації методів передачі пакетів IPv6 по мережах різних типів. З розвитком Інтернету речей все більше пристроїв будуть підключатися до глобальної мережі, тим самим створюючи нові можливості в сфері безпеки, аналітики та управління, відкриваючи нові і більш широкі перспективи та сприяючи підвищенню якості життя населення.

Список джерел:

1. Amiot, Emmanuel. "The Internet of Things. Disrupting Traditional Business Models". Oliver Wyman. Retrieved 14 October 2018.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТУМАННИХ ОБЧИСЛЕНЬ В СУЧАСНИХ МЕРЕЖАХ

Горохов О.С., Герасименко К.В.
Науковий керівник – Герасименко Костянтин Васильович
м. Київ, Київський національний університет ім. Тараса Шевченка, факультет Інформаційних технологій, кафедра Мережевих та Інтернет технологій
(04116, м. Київ, вул. Богдана Гаврилишина, 24, тел. (098) 439-92-55)
e-mail: c.herasymenko@gmail.com, gorokhovalex00@ukr.net\gmail.com,

Fog computing performs better than cloud computing in meeting the demands of the emerging paradigms. Hence, we can come to the conclusion that fog computing and cloud computing will complement each other while having their own advantages and disadvantages. Fog computing will grow in helping the emerging network paradigms that require faster processing with less delay and delay jitter, cloud computing would serve the business community meeting their high end computing demands lowering the cost based on a utility pricing model.

На сьогоднішній день до Інтернету приєднуються мільярди пристроїв, що призвело до певних досягнень в області технологій електроніки та телекомунікацій. Тому виникає потреба нового бачення в комунікації M2M, яка дозволяє підключати «речі» до глобальної мережі Інтернет. Ця технологія відома як Internet of Things (IoT).

IoT – це мережа фізичних об'єктів, вбудованих з електронікою, датчиками та підключенням, які дозволяють їй досягати цінності та обслуговування, обмінюючись даними з оператором та/або іншими підключеними пристроями через вдосконалені протоколи комунікації без втручання людини.

Наприклад, програма інтелектуальної транспортної системи (ITS), розумні домашні програми та програми електронного здоров'я. Величезна кількість даних генерується мільярдами підключених пристроїв і передається по мережі в Інтернет.

Що таке хмарні обчислення (Cloud Computing)?

Cloud Computing – це нова технологія, що спрощує обчислювальну роботу клієнтів, орендуючи ресурси та послуги. Раніше, щоб використати якусь програму, нам треба було встановити і запустити її. Тепер же ми можемо зайти на сайт компанії і відразу почати працювати з усіма даними і ресурсами, які нам потрібні.

Дана технологія має ряд проблемних питань. Серед них є такі, що суттєво впливають на якість обслуговування, а саме затримка мережі, безпека та конфіденційність.

Існує нова платформа, яка забезпечує новий набір веб-додатків і послуг кінцевим користувачам. Ця платформа називається туманні обчислення (Fog Computing) і також відома як Fogging**.**

Що таке «Fog Computing»?

Термін «Fog Computing» був введений компанією Cisco Systems як нова модель для полегшення бездротової передачі даних розподілених між

пристроями в IoT. Подібно до Cloud, Fog надає кінцевим користувачам послуги з передачі даних, обчислень, зберігання та застосування.

Особливістю Fog є його близькість до кінцевих користувачів, його щільне поширення та підтримка мобільності. Послуги розміщуються на кінцевих пристроях – точках доступу. Таким чином, Fog зменшує затримку сервісу та покращує параметри якості обслуговування (Quality of Service, QoS).

Таблиця 1 –Порівняльна таблиця вимог хмарних і туманних технологій

Параметри	Cloud Computing	Fog Computing
Затримка	Висока	Низька
Розташування служби	В Інтернеті	На межі локальної мережі
Безпека	Не визначено	Може бути визначена
Атаки на дані по маршруту	Висока ймовірність	Дуже низька ймовірність
Розпізнавання місцезнаходження	Ні	Так
Гео-розподіл	Централізований	Розподілений
Кількість вузлів сервера	Мало	Дуже багато
Підтримка мобільності	Обмежена	Підтримується
Взаємодія в реальному часі	Підтримується	Підтримується
Тип підключення	Виділена лінія	Бездротовий

Отже, використання технологій Fog computing є більш перспективним, ніж Cloud computing, у задоволенні вимог нових тенденцій. Але, звичайно, ця технологія не може замінити хмарні обчислення, оскільки вона все ще буде кращою для високоякісних пакетних процесів обробки, які дуже поширені в діловому світі. Отже, можна зробити висновок, що Fog computing і Cloud computing доповнюватимуть один одного, маючи свої переваги та недоліки. Дослідження, що стосуються безпеки, конфіденційності та надійності системи в Fog computing, є темою для подальших досліджень і повинні бути обов’язково з’ясовані.

Список джерел:

1. Abdelshkour M. IoT, from Cloud to Fog Computing [Електронний ресурс] / Maher Abdelshkour – Режим доступу до ресурсу: https://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing.

ЗАХИСТ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ В ІКС

КВАНТОВИЙ АЛГОРИТМ ШОРА ДЛЯ ВИРІШЕННЯ ПРОБЛЕМИ ФАКТОРИЗАЦІЇ ЧИСЛА

Островський А.М.
Науковий керівник – к.т.н., проф. Качко О.Г.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14,
каф. Системотехніки, тел. (057) 702-13-06)
e-mail: albert.ostrovskyi@nure.ua, факс (099) 728-75-48

The given work is devoted to the modern developments in the field of quantum computer algorithms related to cryptanalysis. The major topic of the work is a research of the Shor quantum algorithm that is designed to solve a factorization problem. The work also contains information about the current state of quantum computing technologies and known non-quantum solutions to the factorization problem. The aim of the work is to demonstrate that nowadays-cryptographic systems based on impossibility to find factors of the big number are vulnerable to quantum algorithms or will be vulnerable in the near future.

Несиметричні алгоритми шифрування широко використовуються у сучасних криптосистемах. Найвідомішим є алгоритм RSA, стійкість якого базується на складності задачі факторизації. Для забезпечення безпеки, RSA вимагає, щоб добуток випадкових простих чисел був більше ніж 300 десяткових цифр. Навіть при використанні найшвидшого комп'ютера, доступного на сьогодні, розкладання на множники цілого числа такого розміру вимагає нездійсненно великого часу. Це означає, що RSA безпечний, поки не буде знайдений ефективний алгоритм розкладання на множники.

Досліджені алгоритми розкладання числа на множники для звичайних ЕОМ. Найкращі мають субекспоненціальні складність, це метод квадратичного решета (складність $L_n(0.5,1)$) та метод Ленстра з використанням еліптичних кривих (складність $L_n(0.5,\sqrt{2})$), де L_n це нотація прийнята для позначення субекспоненціальної складності. Тобто жоден з сучасних алгоритмів не може знайти співмножники великого цілого числа з поліноміальною складністю часу [1].

Найвірогідніше рішення цієї проблеми є використання квантових обчислень. Квантова система з L дворівневих кубітів має 2^L лінійно незалежних станів, тобто квантовий обчислювальний пристрій розміром L кубіт може виконувати паралельно 2^L операцій [2]. Компанією Google вже реалізований квантовий процесор з 72 кубітів.

Вивчено квантовий алгоритм Шора для факторизації (розкладання числа на прості множники), реалізація якого, дозволяє розкласти число M за час $O(\lg^3 M)$, використовуючи O(lgM) логічних кубітів. Сутність

алгоритму - знайти період функції $f(x) = a^x (mod\ M)$, де a довільний параметр, M число, яке необхідно факторизувати. Знайшовши період функції, можемо знайти множники числа за допомогою формули $factor_{1,2} = \gcd(a^{r/2} \pm 1, M)$, де $\text{factor}_{1,2}$ – множники числа M, gcd – формула для обчислення найбільшого спільного дільника, r – період. Парадигма квантових обчислень дозволяє знайти період функції з поліноміальною складністю, чого не можна зробити в рамках класичної обчислювальної моделі [3].

Обрана обчислювальна схема для реалізації квантової частини алгоритму, яка представляє собою два квантових регістра m та n, які спочатку знаходяться у нульовому стані. На першому кроці за допомогою операції Уолша-Адамара первинний стан $|0\rangle$ регістра n переводиться в рівно імовірнісну суперпозицію усіх булєвих станів N. На другому кроці до двух регістрів застосовується унітарне перетворення (оракул S_f), яке переводить стан $|x, 0\rangle$ у $|x, f(x)\rangle$. На третьому кроці виконується квантове перетворення Фур'є (QFT), яке уявляє собою унітарне перетворення стану квантового регістра, яке задається N-мірним вектором стану. В результаті ми отримуємо $\frac{1}{N}\sum_{x=0}^{N-1}\sum_{k=0}^{N-1} \exp(2\pi\ i\ kx/N)\ |k, a^x\ mod\ M\rangle$, що є перетвореним першим регістром, де N – кількість усіх можливих булєвих станів. На четвертому кроці виконується вимірювання регістра X відносно ортогональної проекції. Результатом є $|k, a^k\ mod\ M\rangle$, де k ∈ [0, N-1]. Далі знаходимо найкраще приближення (знизу) до k/N, що і буде періодом функції, який потім використовується для знаходження множників числа за допомогою класичних обчислень. Також треба зазначити, що алгоритм є ймовірнісним, де ймовірність знаходження відповіді є $\frac{1}{N}\sum_{x:a^x \equiv a\ mod\ M}^{N-1} \exp(2\pi\ i\ kx/N)$ [4].

Алгоритм є теоретично обґрунтованим та вже використовувався для факторизації числа 15 на справжньому квантовому комп’ютері. Для подальшого дослідження алгоритму буде виконана його реалізація за допомогою однієї з мов програмування для квантових обчислень (Q# та QCL) та аналіз його роботи на більш великих числах.

Список джерел:

1. Ишмухаметов Ш.Т., Методы факторизации натуральных чисел [Текст]: учеб. пособие / Ш.Т. Ишмухаметов.– Казань:Казан.ун., 2011.- 201с.

2. Роман Душкин Квантовые вычисления и функциональное программирование / Р.В. Душкин.-М.: ДМК Пресс, 2015. – 232 с.

3. К.А. Валиев Квантовые компьюетры и квантовые вычесления/К.А. Валиев.-М.:Insitute of Physics and Technology, 2005.- 37с.

4. Shor P. Algorithms for quantum computation [Text]/Shor P.// Foundations of Computer Science.–1994.–№10.-124–134pp.

МОДИФІКОВАНИЙ КВАНТОВИЙ АЛГОРИТМ ШОРА ДЛЯ ПОШУКУ ДИСКРЕТНОГО ЛОГАРИФМУ

Максутов Д.С
Науковий керівник – к.т.н., проф. Качко О.Г.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Системотехніки,
тел. (057) 702-13-06)
e-mail: dmytro.maksutov@nure.ua, факс (057) 702-11-13

The given work is devoted to the modern developments in the field of quantum computer algorithms related to cryptanalysis. The major topic of the work is a modification of the Shor quantum algorithm that is designed to solve a discrete logarithm problem. The work also contains information about the current state of quantum computing technologies and known non-quantum solutions to the discrete logarithm problem. The aim of the work is to demonstrate that nowadays-cryptographic systems based on Elliptic-curve cryptography (ECC) are vulnerable to quantum algorithms or will be vulnerable in the near future.

З розвитком технології виробництва та емуляції квантових комп'ютерів, а також стрімкого розвитку технологій що покладаються на засоби асиметричної криптографії з використанням еліптичних кривих, таких як шифрування даних у пристроях компанії Blackberry та деякі імплементації Blockchain, нагальним стає питання крипто аналізу криптографії на еліптичних кривих та пошук і вдосконалення алгоритмів пошуку дискретного логарифму, який лежить в її основі.

На сьогодні існує декілька не квантових алгоритмів для пошуку дискретного логарифму, які досягають теоретичного максимуму швидкодії можливого на звичайних ЕВМ. Це таки алгоритми, як модифікація загального методу решета числового поля (GNFS) [1] з асимптотичною оцінкою $O(e^{(\frac{64}{9})^{\frac{1}{3}}(\ln p)^{\frac{1}{3}}(\ln\ln p)^{\frac{2}{3}}})$ та p-алгоритм Поларда [2] з асимптотичною оцінкою $O(\sqrt{q})$, де q – це порядок підгрупи F_p і p – порядок поля Галуа F_p.

З появою теорії квантових комп'ютерів почалася активна розробка квантових алгоритмів для ефективного вирішення проблем факторизації та пошуку дискретного логарифму. В 1994 році Пітер Шор опублікував перший варіант квантового алгоритму для вирішення вищеозначених проблем. Через три роки був опублікований докладний опис алгоритму [3]. Шор описав алгоритм поліноміальної складності для пошуку дискретного логарифму лише для певного випадку, а саме, пошук дискретного логарифму у мультиплікативній групі F_p^* поля F_p.

Це залишило простір для вдосконалення алгоритму з метою покращення асимптотичної оцінки складності, кількості задіяних кубітів і

застосування його в інших групах поля F_p. Одним з таких вдосконалень є адаптація алгоритму Шора для пошуку дискретного логарифму в групі G з відомим простим порядком q, і груповою операцією $\odot$ [4]. Вдосконалений алгоритм складається з двох кроків:

1. Власне квантовий алгоритм, який приймає на вхід генератор групи g і елемент $x = [d]g$ і повертає, як результат пару (k, j) і $[e]g$, що ігнорується.
2. Класичний алгоритм, що приймає на вхід пару (k, j) і повертає, як результат шуканий дискретний логарифм d, якщо пара «хороша», тобто відповідає певним вимогам.

Описаний алгоритм потребує $2[\log_2 q]$ регістрів для індексу і обчислення двох квантових перетворень Фур'є розміру $2^{[\log_2 q]}$. Теоретична нижня границя вірогідності отримання шуканого дискретного логарифму з першого запуску дорівнює 2^{-10}. Практична вірогідність має бути вищою, але це ще необхідно перевірити.

Алгоритм теоретично обґрунтовано, тому подальше дослідження буде стосуватися вивчення поведінки алгоритму на практиці, а саме його реалізацію і запуск на емуляторі або одному з доступних квантових комп'ютерів (IBM), з подальшим відстеженням його роботи під впливом можливої декогеренції та квантового шуму.

Список джерел:

1. O. Schirokauer, "Discrete Logarithms and Local Units", in Philosophical Transactions of the Royal Society of London, volume A 345, 1993, pp. 409-423.
2. S. C. Pohlig, M. E. Hellman, "An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance", in IEEE Transactions on Information Theory, volume IT-24, no 1, 1978, pp. 106-110.
3. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", in SIAM Journal of Computing, volume 26, no 5, 1997, pp. 1484-1509.
4. Martin Ekerå, "Modifying Shor's algorithm to compute short discrete logarithms", in IACR Cryptology ePrint Archive, 2016

АНАЛІЗ НЕБЕЗПЕКИ АПАРАТНИХ ЗАКЛАДНИХ ПРИСТРОЇВ

Гриньов Р.С.
Науковий керівник – к.т.н., доцент Сєвєрінов О.В
Харківський національний університет радіоелектроніки
(61166, м. Харків, пр. Науки, 14, каф. Безпеки інформаційних технологій,
тел:+38 (057) 702-14-25)
e-mail: rost_grin@rambler.ru

Attacks on organizations using hardware embedded devices are a serious threat. Especially in Ukraine, where such things are still not widespread and are not perceived as a serious danger.

В даний час питання безпеки в сучасних операційних системах, захисту персональних комп’ютерів та корпоративних мереж від шкідливого програмного забезпечення та проникнень не втрачає своєї актуальності. Проведений аналіз показав, що тенденція глобального розповсюдження вірусів прихованих в неліцензійному програмному забезпеченні та масового зараження притаманна територіям з високим рівнем “піратства”. Ці атаки спрямовані на звичайних користувачів і зловмисник не має намірів отримати доступ до інформації якоїсь конкретної людини.

Існують методи, що дозволяють приховувати віруси в усіх типах виконуваних файлів, у текстових файлах та файлах формату PDF. Вірусні атаки спрямовані проти конкретних людей, компаній, регіонів, країн та об’єктів інфраструктури заздалегіть сплановані, чітко продумані та мають більш складний характер. Спочатку зловмисники збирають дані. Потім їх можуть використати, наприклад, для проведення поштової спам-розсилки. Електронний лист оформлюється спеціальним чином, наприклад, лист від департаменту безпеки з прикріпленим файлом, в якому зазначені зміни політики безпеки. За допомогою макровірусу, що міститься у прикріпленому файлі зловмисник може отримати доступ до конфіденційної інформації компанії, встановити додаткові шкідливі програми з метою контролю інформаційних потоків організації або вивести з ладу обладнання, що спричинить значні збитки. Однак подібні атаки можна легко виявити через те, що вони мають масовий характер. Крім того, уважні працівники, звернувшись в департамент безпеки, дізнаються, що оновлення політики безпеки не було. Це дозволить швидко локалізувати розповсюдження вірусу, виправити всі наслідки та провести інструктаж з персоналом, що підвищить рівень безпеки організації. Все це можливо, бо відомий час проникнення в систему, спосіб який використовувався і найголовніше, що відбувся факт проникнення.

Зловмисники можуть використовувати різноманітні методики соціальної інженерії. Шахраї можуть використовувати звичайні флеш

накопичувачі, CD диски з вірусним програмним забезпеченням. Часто використовуються запрограмовані мікроконтролери. Якщо замаскувати подібний пристрій під виглядом маніпулятора “миша”, клавіатури або флеш накопичувача, то існує імовірність, що ним скористається хтось із співробітників організації. Таким чином зловмисник зможе проникнути, навіть в ізольовану систему, що не має доступу до глобальної мережі. Захиститися від подібних атак можна за допомогою регулярних інструктажів. Варто розуміти, що велика кількість витоків інформації з організації може відбуватись через неправильну утилізацію обладнання або під час ремонту. Наприклад, коли до ремонту потрапив комп’ютер, на жорсткому диску якого є фінансова звітність або розробки нового проекту. Проте правильна утилізація і виключення схожих ситуацій не гарантує безпеку. В будь-якій організації може виникнути ситуація, коли виходить з ладу устаткування. Це може бути мережевий пристрій, клавіатура. Після ремонту або заміни звичайного маніпулятора “миша” ніхто не помітить в ній наявності зайвого мікроконтролера, що може виконувати шкідливі дії. Такі атаки досить специфічні і мало розповсюджені, проте є найнебезпечнішими. Послуги таких центів можуть дорого коштувати, а з точки зору звичайної людини маніпулятор “миша” або клавіатура не можуть становити небезпеки для персонального комп’ютера або організації.

Подібні апаратні закладки можуть бути досить різноманітними. Одні можуть мати бездротові інтерфейси, інші доступ до Інтернету, що дозволить зловмиснику під’єднуватися до них дистанційно. Більш прості варіанти запрограмовані на виконання певних дій. Такі пристрої можуть бути приховані в системному блоці комп’ютера, маршрутизаторі, периферійному та іншому обладнанні. Небезпека атак, що використовують подібні пристрої полягає у важкості виявлення факту проникнення.

Таким чином, для захисту організації від вірусів, витоку інформації та проникнень в систему недостатньо мати сертифіковану операційну систему, фаєрволи та антивіруси. Необхідно на регулярній основі проводити інструктажі з метою підвищення рівня обізнаності персоналу у методах захисту персональних та корпоративних даних та з метою формування базових знань принципів інформаційної безпеки. Працівники повинні знати як діяти під час інцидентів інформаційної безпеки, розуміти ступінь відповідальності та можливе покарання за порушення правил політики безпеки. Крім того, необхідно чітко контролювати доступ персоналу, а особливо сторонніх людей, до різних департаментів та устаткування.

Список джерел: 1. Гриньов Р.С. Шкідливий USB HID-емулятор // Радіоелектроніка та молодь у XXI столітті: між. форум. Харків, 2018. С. 120-121.

АЛГОРИТМЫ МНОГОРАЗОВОЙ ПОДПИСИ НА ОСНОВЕ ХЕШ-ФУНКЦИ Й

Марухненко А.С.
Научный руководитель – д.т.н., проф. Халимов Г.З
Харьковский национальный университет радиоэлектроники (61166, Харьков, пр. Науки,14, каф. Безопасности информационных технологий), тел. (057) 702-14-25 e-mail: oleksandr.marukhnenko@nure.ua

Modern asymmetric cryptography is vulnerable to quantum computing. A possible solution is to use hash-based digital signatures. This class includes various algorithms: one-time and few-time signatures and schemes based on their composition. This paper discusses a reusable signature algorithm with a decrease in the security: HORS and its modifications PORS and FORS. When creating a new signature, these algorithms reveal a part of the secret key, so the key pair can be used to sign a limited number of messages, this number depends on chosen system parameters.

Стойкость большинства используемых асимметричных криптосистем базируется на сложности решения задач факторизации, дискретного логарифма в простом поле или группе точек эллиптической кривой. В случае использования алгоритма Шора на квантовом компьютере, решение будет иметь полиномиальную сложность, следовательно, в обозримом будущем такие криптосистемы будут небезопасны. Целью работы является анализ перспективных постквантовых алгоритмов цифровой подписи на основе хеш-функций.

ЭЦП на основе хеш функций можно классифицировать следующим образом:

- одноразовые (Лампорта, Винтерница);
- многоразовые с использованием деревьев Меркли;
- многоразовые со снижением стойкости (HORS, FORS, PORS);
- многоразовые с использованием гипердеревьев (SPHINCS, SPHINCS+, Gravity-SPHINCS, XMMS-MT).

Рассмотрим алгоритмы многоразовой ЦП со снижением стойкости, основная идея заключается в том, что секретный ключ имеет достаточно большой размер (например, 1 мегабайт) и при создании подписи раскрывается некоторая его часть, таким образом каждая новая подпись снижает стойкость ключа и увеличивает вероятность подделки.

Алгоритм HORS (Hash to Obtain Random Subset – хеш для получения случайного подмножества) [1] помимо используемых хеш-функций имеет два общесистемных параметра $t = 2^{\tau}$ - размер множества ключей, k – количество элементов в подписи, $kt = n$ - длина хеша сообщения. Модификация данного алгоритма – HORST используется в ЭЦП SPHINCS.

Секретный ключ – массив из t случайных чисел, их размерность определяется требуемой стойкостью системы $SK = (sk_0, sk_1, ..., sk_{t-1})$.

Открытый ключ – массив из хешей элементов секретного ключа $PK = (pk_0, pk_1, ..., pk_{t-1}) = (H(sk_0), H(sk_1), ..., H(sk_{t-1}))$, для уменьшения размера открытого ключа может быть использована дерево Меркли, как это реализовано в алгоритме HORST.

Подпись – хеш подписываемого сообщения делится на блоки по τ бит, в подпись включаются элементы секретного ключа, соответствующие значениям блоков $H(M) = (h_0, h_1, ..., h_{k-1})$, $\sigma = (sk_{h_0}, sk_{h_1}, ..., sk_{h_{k-1}})$.

Проверка – элементы подписи хешируются и сравниваются с соответствующими элементами открытого ключа.

Подпись HORS имеет недостаток, заключающийся в том, что при совпадении значений блоков в хеше сообщения в подписи будут использованы одни и те же элементы ключа, что приводит к снижению стойкости. Алгоритм PORS (PRNG to obtain a random subset – генератор псевдослучайных чисел для получения случайного подмножества) используется в криптосистеме Gravity-SPHINCS [2] и устраняет описанный недостаток. Системные параметры и ключи остаются без изменений, в алгоритмы создания и проверки подписи после разбиения хеша сообщения добавляется следующая проверка: если $h_i = h_j$, $i > j$, h_i отбрасывается, генерируется новый блок длины τ и добавляется в конец последовательности, операция повторяется до тех пор, пока все блоки не будут уникальными. Генерация осуществляется при помощи ГПСЧ, инициализируемым сообщением.

Алгоритм FORS (Forest Of Random Subset) также является модификацией HORST, используемой в схеме SPHINCS+ [3]. Его основное отличие заключается в том, что для каждого подписываемого блока используется свой массив случайных чисел, т.е. размер секретного ключа увеличивается в k раз, но благодаря использованию деревьев Меркли размер открытого ключа остаётся неизменным.

Цифровые подписи PORS и FORS являются альтернативными модификациями алгоритма HORST, устраняющими возможность повторения компонентов подписи. Алгоритм FORS сложнее в реализации, однако позволяет создать больше подписей без потери стойкости.

Список источников:

1. Leonid Reyzin and Natan Reyzin. Better than BiBa: Short one-time signatures with fast signing and verifying. 2002.

2. Jean-Phillippe Aumasson and Guillaume Endignoux. Gravity-SPHINCS – Submission to the NIST's post-quantum cryptography standardization process, 2017.

3. Daniel J. Bernstein and others. SPHINCS+ – Submission to the NIST's post-quantum cryptography standardization process, 2017.

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ЗА ДОПОМОГОЮ ЗАШИФРОВАНОЇ ОБРОБКИ ЗАПИТІВ

Ахтирцев І.І.
Науковий керівник – к.т.н., доцент Федюшин О.І.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Безпеки інформаційних технологій,
тел.702-14-25, e-mail: illia.akhtyrtsev@nure.ua, тел. (099) 797-20-40)

This work presents CryptDB, a system that explores an intermediate design point to provide confidentiality for applications that use database management systems (DBMSes). CryptDB leverages the typical structure of database-backed applications, consisting of a DBMS server and a separate application server In this work we discuss the threats that CryptDB defends against. Next, we describe prototype implemntation and evaluate the performance and security of CryptDB, as well as the effort required for application developers to use CryptDB, also we compared time of queries performance with using CryptDB and without. We made some conclusions.

Втрата приватної інформації є актуальною проблемою, у тому числі для інтернет-додатків. Зловмисник може використовувати спеціальне програмне забезпечення для отримання несанкціонованого доступу до серверів, адміністратори хостингу або постачальники програмного забезпечення можуть зловживати повноваженням та мати доступ до особистих даних або зловмисники з фізичним доступом до серверів можуть отримати доступ до всіх даних на диску та в пам'яті.

Нині існує велика кількість векторів атак та вразливостей в мережі, описанням яких займається спільнота OWASP. OWASP створив список з 10 найнебезпечніших векторів атак в мережі. Деякі з них несуть безпосередню загрозу для персональних даних користувачів на віддалених серверах.

Таким методом є SQL-ін’єкція, яка нараховує п’ять основних технік: оператор UNION, логічний метод, на основі помилок, метод з альтернативним каналом передачі даних, Time delay. Захист від атак такого типу вимагає фільтрації вхідних даних. І все це працюватиме, якщо адміністратори добросовісно робитимуть свою роботу. Та все ж існують ситуації, коли цього досягти неможливо.

Нині існує певна кількість робіт, які освітлюють цю проблему, у тому числі це роботи [1–3]. В них аналізуються загальні поняття гомоморфного шифрування, яке є основою для реалізації шифрованих запитів, а також наводиться опис принципів роботи додатку CryptDB, який є реалізацією даного механізму. Додаток CryptDB дозволяє приховувати персональні дані користувачів навіть від адміністраторів бази даних.

Метою даної роботи є виявлення ефективності гомоморфного шифрування для захисту особистих даних в інтернет-додатках за

критеріями швидкості виконання базових операцій і ступеню захищеності даних, тобто швидкості криптоаналізу. Також завданням роботи є пошук шляхів подальшого розвитку даного принципу для захисту особистих даних в інтернет-додатках.

В ході даної роботи була проведено налаштування додатку CryptDB. В якості тестового середовища була обрана операційна система Ubuntu 16.4., сервер бази даних MySQL 5.7, проксі CryptDB, а також клієнт бази даних. Ці додатки були встановлені в межах однієї системи. Для експерименту створена база даних, проводилося порівняння виконання запитів до MySQL бази даних безпосередньо, бази даних CryptDB та двох варіацій баз CryptDB proxy. Основними критеріями оцінки ефективності роботи CryptDB була швидкодія виконання запитів. Тобто в ході роботи ми порівнювали час виконання запитів. Результати заміру часу затримки виконання запитів до різних серверів, отримані в роботі [2], були підтверджені практично й мають наступний вигляд: час виконання запиту select до серверу MySQL з використанням CryptDB більший на 10%, delete – 14%, insert – 20%, update – 27%.

Таким чином, система CryptDB надає достатній рівень захищеності особистих даних, при цьому впливає на швидкодію виконання запитів не значною мірою. Це дає можливість забезпечувати конфіденційність даних в інтернет-додатках без відчутної для користувача втрати швидкодії. І найголовніше, система гомоморфного шифрування виключає будь-які погрози з боку адміністраторів бази даних.

Список джерел:

1. Poteya Manish M. Homomorphic Encryption for Security of Cloud Data / Poteya Manish M., Dhoteb, C. A., Sharmac Deepak H. //Procedia Computer Science 79, 2016,- P. 175–181. DOI: https://doi.org/10.1016/j.procs.2016.03.023.

2. Stupen, P. Application of homomorphic encryption for the protection of numerical data in cloud storage / Stupen P., V. Sokolov, S. O., Zolkina, O. Yu. //Scientific works of the Petro Mohyla Black Sea State University of the Kyiv-Mohyla Academy complex. Series: Computer Technology, Vol. 266, No. 254, P. 71–75, available at : http://nbuv.gov.ua/UJRN/Npchduct_2015_266_254_13 (last accessed: 28.11.2018).

3. R. A. Popa CryptDB: Apractical encrypted relational DBMS / R. A. Popa, N. Zeldovich, and H. Balakrishnan. //Technical Report MITCSAIL-TR-2011-005, MIT Computer Science and Artificial IntelligenceLaboratory, Cambridge, MA, January 2011.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Курбатов А.С.
Научный руководитель – доцент кафедри БИТ, к.т.н. Петренко О.Е.
Харьковский национальный университет радиоэлектроники
(61166, Харків, просп. Науки,14, каф. Безопасности информационных технологий, тел.: т. 093-510-55-49)
email: olkurbatov@gmail.com

Traditional accounting systems require complete user trust. A centralized approach in building payment systems, property accounting registers, voting platforms has its advantages, but at the same time it forces the end user to blindly believe the final state of the accounting system database. Therefore, it is not surprising that the community was interested in the systems, which made it possible to guarantee the compliance of the accounting system's database with the conducted transactions, while trusting only the mathematical methods on which they are based. The blockchain technology has become the key to building such systems.

Целью данной работы является анализ технологии, которая применяется в децентрализованных системах голосования, и постановка задач, которые требуют решения перед внедрением таких систем.

Децентрализованная система электронного голосования – децентрализованная учетная система, в которой идентификаторы пользователей строго привязаны к их личностям, но все действия пользователей должны быть анонимны (связать личность и идентификатор пользователя можно, но связь идентификатора пользователя с действиями в учетной системы, не является возможной без явного желания пользователя). Все действия участников системы записываются в распределенную базу данных в виде отдельных транзакций. При подтверждении, транзакции объединяются в блоки образуя неизменяемую цепочку блоков, доступ к которой имеет любой желающий [1].

Как было определено выше, идентификаторы пользователей должны быть строго привязаны к их личностям. Единственный на сегодняшний день способ обеспечения этого требования – предварительное внедрение государством системы digital identity и предоставление сертификата открытого ключа каждому из голосующих. На сегодняшний день получение сертификата открытого ключа не является проблемой. Поэтому стоит рассматривать два подхода: одноразовая предвыборная сертификация (одноразовое получение ключей для возможности проголосовать) либо использование ранее полученных сертификатов. Оба подхода имеют свои преимущества, однако каждый из них также сопровождается рядом проблем.

Обеспечить тайну голосования достаточно просто. Для этого можно использовать механизм кольцевой подписи, позволяющий пользователю скрыть свой голос среди участников группы [2]. Важно отметить при этом, что каждый голос должен обладать свойством fungibility, то есть должен быть неотличимым от других голосов, иначе тайну голосования обеспечить будет невозможно. Поэтому структура транзакции должна быть строго определена и должна исключать возможность добавления каких-либо произвольных данных.

Теперь стоит рассмотреть кто может быть валидатором на платформе голосования. Потенциально роль валидатора может выполняться теми же комиссиями, которые на данный момент проводят голосование. Количество комиссий должно быть строго ограничено, валидаторы должны быть идентифицированы (и связаны с сформированными ими блоками).

Таким образом, можно сделать вывод, что децентрализованная система электронного голосования – система, которую вполне реально построить при использовании математических методов и алгоритмов достижения консенсуса. Однако, на сегодняшний день построение надежной децентрализованной платформы голосования невозможно по причине отсутствия надежного механизма цифровой идентификации. Для решения данной проблемы возможно изучение опыта Эстонии, которая успешно решила данную задачу [3].

Список источников:

1. Блокчейн и децентрализованные системы : учеб. пособие для студ. заведений высш. образования : в 3 частях. Ч. 1 / П. Кравченко, Б. Скрябин, О. Дубинина. – Харьков : ПРОМАРТ, 2018. – 441 с.
2. Van Saberhagen N. CryptoNote v 2.0 [Электронный ресурс] / Nicolas van Saberhagen. – Oct. 2013. – Режим доступа: https://cryptonote.org/whitepaper.pdf.
3. D. Springall. Security Analysis of the Estonian Internet Voting System / Drew Springall, Travis Finkenauer, Zakir Durumeric. – University of Michigan, Ann Arbor, MI, U.S.A., 2011, – 13 с.

АНАЛІЗ АЛГОРИТМІВ ПОБУДОВИ ЭЦП SPHINCS ТА SPHINCS+

Нечволод К.В.
Науковий керівник –доцент кафедри БІТ, к.т.н. Петренко О.Є.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф.БІТ, тел +38 (057) 702-14-25)
e-mail: kostiantyn.nechvolod@nure.ua

As e-commerce has become more important in society, the need to certify the origin of exchanged information has arisen. Modern digital signatures enhance security based on the difficulty of solving a mathematical problem, such as finding the factors of large numbers. Unfortunately, the task of solving these problems becomes feasible when a quantum computer is available. To face this new problem, new quantum digital signature schemes are in development to provide protection against tampering, even from parties in possession of quantum computers and using powerful quantum cheating strategies. Object of a research is the two post-quantum algorithms of the digital signature SPHINCS and SPHINCS+, which were submitted to the NIST post-quantum crypto project.

Квантова криптографія – єдина, яка може реалізувати беззастережну безпеку в пост квантовий період. Наукове співтовариство по-різному оцінює перспективи побудови повноцінного квантового комп'ютера. Деякі вважають, що на це піде не менше десятка років, інші – що повноцінний квантовий комп'ютер не буде побудований ніколи. Проте, співтовариство, не покладаючись на велику кількість фізичних проблем по розробці квантових обчислювальних систем, заздалегідь потурбувалося завданням боротьби з майбутніми квантовими комп'ютерами і створило напрямок – пост-квантова криптографія. Цей напрямок розробляє криптографічні системи, які є криптостійкими для майбутніх квантових комп'ютерів. Зокрема, пост-квантова криптографія пропонує захищені системи передачі інформації на основі хеш-функцій.

Мета роботи: на основі порівняльного аналізу алгоритмів SPHINCS+ та SPHINCS визначити найкращій алгоритм для застосування в пост квантовий період.

Алгоритм SPHINCS [1] є надійною системою електронного цифрового підпису, що заснована на на хеш-функціях [2]. Ця система дозволяє забезпечити достатній рівень стійкості в пост квантовий період, застосовуючи довжину, що дорівнює 128 біт та може бути реалізована на базі звичайних комп'ютерів.

Система SPHINCS+ [1] будується на SPHINCS, вносячи кілька покращень, а саме:

1. Здібність захисту від багатоцільової атаки, застосовуючи методи зм'якшення за допомогою функцій хешування ключа. Кожен виклик функцій хешування набирається з іншим ключем і застосовується інша

бітова маска. Ключі та бітові маски генеруються псевдовипадково з адреси, що визначає контекст виклика та публічного seed [1].

2. Здійснено стиснення відкритого ключа WOTS+ на відміну від алгоритму, що застосовано в SPHINCS без L-дерева: останні вузли ланцюгів WOTS+ не стискуються за допомогою L-дерева, але використовують виклик однієї хеш-функції, що настроюється. Цей виклик знову отримує адресу та публічний seed для запуску цього виклика та генерації бітової маски такої ж довжини, як і вхід.

3. Пара ключів FORS, на відміну від алгоритму SPHINCS, не складається більше з одного монолітного дерева. Замість цього вона складається з дерев висоти *a*. Листя цих дерев являють собою хеші секретних ключових елементів 2^a. Публічний ключ - це хеш конкатенації всіх кореневих вузлів, як для відкритого ключа WOTS+, може використовуватися для підписування $k2^a$ бітових повідомлень.

4. Алгоритм SPHINCS+, на відміну від SPHINCS спроможний здійснювати вибір індексу верифікації наступним чином:

- детерміновано генерується випадкове *R = PRF (SK.prf, OptRand, M)*. Де *OptRand* має значення 256 біт, за замовчуванням 0, але може бути заповнений випадковими бітами, наприклад. взятих з *TRNG*, що дозволяє уникнути детерміністичного підписання та протидіяти атакам бічних каналів;
- обчислюється дайджест повідомлення та індекс як *(md || idx) = Hmsg (R, PK, M)*, де *PK = (PK.seed, PK.root)* містить верхній кореневий вузол та публічний seed.

Отже, алгоритм SPHINCS+ є покращеною версією SPHINCS, яка дозволяє генерувати та веріфікувати стійкі до криптоаналітичних атак електронні цифрові підписи в пост квантовий період. Використання впроваджених змін дозволяє швидше генерувати менші за розміром підписи ніж в алгоритмі SPHINCS.

Список джерел:

1. Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe. SPHINCS+, 2017

2. 2. Merkle R. C. A Digital Signature Based on a Conventional Encryption Function [Електронний ресурс] / Ralph C. Merkle // Advances in Cryptology – CRYPTO '87, Lecture Notes in Computer Science. – Вид. 293. – с. 369–378.

АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В «ОБЛАЧНЫХ» ВЫЧИСЛЕНИЯХ

Наумов А.Н.
Научный руководитель – доцент кафедры БИТ, к.т.н. Петренко О.Е.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр.Науки 14, каф.Безопасности информационных технологий, тел. (096)-220-54-86)
e-mail: num4ik@yandex.ru,

Cloud computing is one of the main focuses of development in infocommunications sphere of recent years. This is a technology of distributed data processing, in which computer resources and facilities are provided to the user as an Internet-service. However, due to the fact that the user does not own the infrastructure, a number of problems arise because the safety of user data depends on the provider. Cloud computing based on virtualization technology but this is the main cause of vulnerabilities.

Одним из основных направлений развития последних лет в мире инфокоммуникаций являются облачные вычисления. Это технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как интернет-сервис. Однако, в связи с тем, что пользователь не является владельцем инфраструктуры, возникает ряд проблем, т.к. сохранность пользовательских данных напрямую зависит от провайдера.

Контроль и управление облаками является проблемой безопасности облачных вычислений. Гарантий, что все ресурсы облака посчитаны и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов и не нарушена взаимная конфигурация элементов облака нет. Это высокоуровневый тип угроз, т.к. он связан с управляемостью облаком, как единой информационной системой и для него общую защиту нужно строить индивидуально. В облачных вычислениях важнейшую роль платформы выполняет технология виртуализации.

Целью данной работы является анализ существующих способов обеспечения целостности и конфиденциальности данных в облачных вычислениях.

Для сохранения целостности данных и обеспечения защиты рассмотрим основные известные угрозы для облачных вычислений:

1. Трудности при перемещении обычных серверов в вычислительное облако.
2. Динамичность виртуальных машин.
3. Уязвимости внутри виртуальной среды.
4. Защита бездействующих виртуальных машин.
5. Защита периметра и разграничение сети.

Наиболее эффективные способы защиты в области безопасности облаков опубликовала организация Cloud Security Alliance (CSA). Проанализировав опубликованную компанией информацию, предложены следующие решения:

1. Шифрование – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным, должен шифровать информацию клиента, хранящуюся в центре обработки данных, а также в случае отсутствия необходимости, безвозвратно удалять.

2. Защита данных при передаче. Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или сделать изменения, даже в случаи доступа через ненадежные узлы. Такие технологии достаточно известны, среди них оптимальными для решения поставленных задач безопасности являются алгоритмы и надежные протоколы AES, TLS, IPsec.

3. Аутентификации — защита паролем. Для обеспечения более высокой надежности, лучшим вариантом является использования токенов и сертификатов. Для прозрачного взаимодействия провайдера с системой индетификациии при авторизации, также рекомендуется использовать LDAP (Lightweight Directory Access Protocol) и SAML (Security Assertion Markup Language).

4. Изоляция пользователей. Использование индивидуальной виртуальной машины и виртуальную сеть. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service). Часто провайдеры изолируют данные пользователей друг от друга за счет изменения данных кода в единой программной среде. Данный подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющему получить доступ к данным. В случае возможной ошибки в коде пользователь может получить данные другого.

Итак, описанные решения по защите от угроз безопасности облачных вычислений позволяют значительно снизить количество случающихся инцидентов. Но многие проблемы, связанные с защитой виртуализации до сих требуют тщательного анализа и проработанного решения.

Список источников:

1. Peter Mell, Timothy Gance. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, 2010.

2. Крупинин А. Cloud Computing: высокая облачность. Компьютерра, 2009.

МЕХАНІЗМИ АВТЕНТИФІКАЦІЇ ЗА ВІДБИТКОМ ПАЛЬЦЯ

Морозов О.Ю.
Науковий керівник – к.т.н., доц. Гріненко Т.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. БІТ, тел. (057) 702-14-25)
e-mail: oleksii.morozov@nure.ua

The object of research was the authentication without password. The results of the analysis and research of some methods of authentication are given in the work. They are based on people physical characteristics such as unique fingerprint.

Надійна авторизація та автентифікація стають необхідними атрибутами сучасного життя. Біометричні системи розпізнають людей на основі їх анатомічних особливостей. Оскільки ці риси фізично пов'язані з користувачем, біометричне розпізнавання є дуже надійним механізмом автентифікації. Роль механізму – стежити, щоб тільки ті, хто пройшов автентифікацію, могли отримати доступ до інформації. Таким чином, при грамотній реалізації у відповідних додатках біометричні системи забезпечують високий рівень захищеності [1,2].

Механізми автентифікації поділяються на оптичні, ультразвукові та напівпровідникові, останні в свою чергу діляться на ємкісні, радіочастотні та з використанням термосканерів [1,2]. При оптичному методі автентифікації світло, що випромінюється світлодіодами, відбивається від пальця і потрапляє на світлочутливу матрицю, яка перетворює оптичний сигнал в цифровий. Зчитується, аналізується і порівнюється не саме зображення відбитка, а його геометрія – відстань між лініями, форма, кривизна. Є два основних типа оптичного сканера. Перший – коли робиться знімок потрібної області пальця при дотику до сканера. У другому типі оптичного сканера ми повинні проводити пальцем по сканеру. Сканер робить серію знімків і програмно об'єднує їх в один. Такий метод називається протяжним. В силу необхідності використання більшої матриці для повного знімка відбитка пальця перший тип оптичного сканера є більш дорогим, але, в той же час, більш зручним для кінцевого користувача. Загальним недоліком оптичних сканерів є схильність забруднення, подряпин, впливу фізичного стану пальця (наприклад, вологість). Крім того, перевірку сканера можна обійти за допомогою знімка відбитка пальця.

Напівпровідниковий метод автентифікації заснований на заряді і розряді конденсаторів в залежності від відстані до шкіри в кожній окремій точці поля – якщо конденсатор розташований під горбом, він посилає один вид сигналу, а якщо під впадиною, то інший. Сигнали об'єднуються і порівнюються із зашифрованою інформацією про відбиток, яка зберігається на пристрої. Такі сканери бувають ємкісними,

радіочастотними та термічними. Ємкісні сканери є сьогодні найбільш поширеними напівпровідниковими пристроями для отримання зображення відбитка пальця. Перевага таких сканерів – низька собівартість та надійність, а недолік – неефективний захист від муляжів.

Перевагою радіочастотних сканерів є те, що ймовірність обману даного сканера прагне до нуля (оскільки аналізуються фізіологічні властивості шкіри). Недолік – нестійка робота при поганому контакті з пальцем.

Метод автентифікації на основі термосканерів має безліч переваг: висока стійкість до електростатичного розряду; стійка робота в широкому температурному діапазоні; ефективний захист від муляжів. До недоліків даного методу можна віднести те, що зображення швидко зникає. При прикладанні пальця в перший момент різниця температур значна і рівень сигналу, відповідно, високий. Після закінчення короткого часу (менше однієї десятої частки секунди) зображення зникає, оскільки палець і датчик приходять до температурної рівноваги.

Найперспективнішим методом роботи сканера відбитків пальців є ультразвуковий метод розпізнавання [1,2]. Ультразвукові сканери використовують принцип медичного УЗД для того, щоб створити візуальний образ відбитку пальця. На відміну від оптичних, ці сканери використовують дуже високі частоти звукових хвиль, які здатні проникати в епідермальний шар шкіри. А він має неповторну структуру. Це виключає потребу в чистому, сухому, непошкодженому пальці. Ультразвуковий сканер неможливо обдурити за допомогою знімка відбитка, так як він формує 3D-картину будови шкіри.

Порівняльний аналіз методів автентифікації наведено у табл. 1.

Таблиця 1 – Порівняльний аналіз методів автентифікації

Методи автентифікації	Складність реалізації	Ефективність захисту	Собівартість
Оптичні	Середня	Висока	Середня
Полупровідникові	Низька	Середня	Низька
Ультразвукові	Висока	Висока	Висока

За результатами дослідження можна зробити висновок, що розглянуті методи автентифікації мають свої переваги та недоліки. При цьому оптичний метод автентифікації є найбільш ефективним за характеристиками складності та ціни. Він частіше за все застосовується в мобільних телефонах та забезпечує високу надійність.

Список джерел:

1. Задорожный В.Г. Идентификация по отпечаткам пальцев, Часть 1, 2004, 400 с.

2. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. Политехника, 2001, 240 с.

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ НЕЗВІДНОСТІ ТА ПРИМІТИВНОСТІ ПОЛІНОМІВ

Назарук Р.Р.
Науковий керівник – к.т.н., доцент, Мельникова О.А.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Безпеки інформаційних технологій, тел. (057) 702-14-25)
e-mail: 97roman@gmail.com, факс (050) 346-05-96

Irreducible and primitive polynomials in $Z_2[x]$ are widely used in modern cryptography. For example many stream and block ciphers use such polynomials with big degrees of the form 2^k. Reduction with modulus of this type can be performed faster if smaller non-zero coefficients are placed in one computer word, mostly the lowest one. Algorithms for generating polynomials with such properties are considered in this paper. As a result, it was found 596 primitive pentanoms of power 128, 271 primitive pentanoms of power 256, and 145 primitive pentanoms of power 512 whose smaller non-zero coefficients are less than 64.

В ряді криптографічних алгоритмів і стандартів, у тому числі потокових та блокових шифрах (наприклад, ДСТУ 7624:2014 [1]), використовуються незвідні та примітивні поліноми.

У даному досліджені був проведений пошук примітивних та незвідних поліномів у кільці $Z_2[x]$. Для цього використовувався адаптований алгоритм перевірки властивостей поліному з [2]:

1. $g(x) = x$;
2. *for* ($i = 0; i < l/2; ++i$)
   2.1 $g(x) = g(x)^2 \bmod f(x)$;
   2.2 $d(x) = GCD(f(x), g(x)+x)$;
   2.3 *if* ($d(x) \neq 1$)
      ret "поліном не незвідний (і не примітивний)";
3. $T = 2^l - 1 = q_1 \times q_2 \times \ldots \times q_k$;
4. *for* ($i = 1; i \leq k; ++i$)
   4.1 $d(x) = x^{T/qi} \bmod f(x)$;
   4.3 *if* ($d(x) == 1$)
      ret "поліном не примітивний (але незвідний)";

ret "поліном примітивний (та незвідний)";

В цьому алгоритмі: l — степінь поліному $f(x)$, який тестується, *GCD* — найбільший спільний дільник, q_i — прості множники числа T.

На 3 кроці алгоритму використовується факторизація великого числа T. Факторизація є складною розрахунковою задачею, однак у криптографічних алгоритмах потокових та блочних шифрів [1] використовуються поліноми, степені яких являються степенями числа 2

(наприклад, 128, 256, 512). Такі числа можна розкласти на множники за різницею квадратів ($a^2 – b^2 = (a + b) \times (a - b)$).

Наприклад, для поліному степеню $l = 128$ маємо:

$$T = 2^{128} – 1 = (2^{64})^2 – 1^2 = (2^{64} + 1) \times (2^{64} – 1) = F_6 \times (2^{64} – 1);$$

де F_6 — 6-те число Ферма (F_6 = 0x42f01 × 0x3d30f19cd101), а $(2^{64} – 1)$ далі розкладується за різницею квадратів:

$(2^{64} – 1) = (2^{32})^2 – 1^2 = (2^{32} + 1) \times (2^{32} – 1) = F_5 \times (2^{32} – 1);$

F_5 = 0x281 × 0x663d81;

$(2^{32} – 1) = (2^{16})^2 – 1^2 = (2^{16} + 1) \times (2^{16} – 1) = F_4 \times (2^{16} – 1);$

F_4 = 0x10001;

$(2^{16} – 1) = (2^{8})^2 – 1^2 = (2^{8} + 1) \times (2^{8} – 1) = F_3 \times (2^{8} – 1);$

F_3 = 0x101;

$(2^{8} – 1) = (2^{4})^2 – 1^2 = (2^{4} + 1) \times (2^{4} – 1) = F_2 \times (2^{4} – 1);$

F_2 = 0x11;

$(2^4 – 1) = 15$ = 0x5 × 0x3;

Дані про числа Ферма та результати їх факторизації/доказу простоти чисел взяті з [3].

В результаті маємо 9 співмножників у факторизації значення $T = 2^{128} – 1$ = 0x42f01 × 0x3d30f19cd101 × 0x281 × 0x663d81 × 0x10001 × 0x101 × 0x11 × 0x5 × 0x3.

Операції приведення за модулем $f(x)$ виконуються значно швидше, коли його менші ненульові коефіцієнти розташовані у молодшому слові, тобто на бітових позиціях менших 32 або 64, в залежності від розрядності обчислювальної техніки. Алгоритми одночасної редукції особливо ефективні, якщо степінь поліному $f(x)$ вирівняна по границі слова, тобто є степеню числа 2. У роботі сформовані варіанти пентаномів та триномів з бітовими позиціями ненульових коефіцієнтів менших 64.

За результатами дослідження було виявлено 596 примітивних пентаномів степеню 128, 271 примітивних пентаномів степеню 256, та 145 примітивних пентаномів степеню 512.

Список джерел:

1. ДСТУ 7624: 2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. — Перше видання; Введ. 01.07.2015. — К.: Мінекономрозвитку України, 2015 р. — 238 с.

2. ДСТУ 4145 – 2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. — Перше видання; Введ. 1.07.2003. — К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003 р. — 36 с.

3. Fermat factoring status [Електронний ресурс]: Режим доступу: http://www.prothsearch.com/fermat.html (24.01.2019).

АНАЛИЗ СУЩЕСТВУЮЩИХ СИСТЕМ ИНТЕРНЕТ ЦЕНЗУРЫ

Кочанов М.А.
Научный руководитель – к.т.н., доц. Гриненко Т.А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки, 14, каф. БИТ, тел. +38 (057) 702-14-25)
e-mail: sir.cochanov1998@ukr.net

In work was explored the world's Internet censorship systems, find the strongest censorship, describe its work technologies and possible ways to circumvent it.

Интернет-цензура – это контроль или запрещение материалов, которые кто-либо может публиковать в Интернете или скачивать из него. Интернет-цензура имеет ту же юридическую основу, что и цензура печати. На основе анализа данных исследований американкой компании Freedom House был составлен список стран по степени контролируемости государством интернета [1]. Наименьшая степень свободы использования Интернета оказалась в Китае.

В Китае для ограничения интернета используется проект «Золотой щит». Этот проект включает информационную систему: управления безопасностью, криминальную, выхода и входа, управление трафиком. Частным подпроектом системы «Золотой щит» является «Великий брандмауэр Китая», который отвечает за цензуру и наблюдение за входящими из-за границы данными политического характера.

Контроль данных осуществляется благодаря следующим технологиям [2]. Первое, что власти используют для контроля действий пользователей Интернета, является «зеркальная» технология. Контроль осуществляется посредсвом использования специальных устройств на шлюзах данных, называемых tapper или network sniffer, которые отражают каждый одиночный пакет данных, входящий или исходящий из страны.

Следующей ступенью блокировки информации является DNS (Domain Name System) блокировка. Существует список сайтов, содержание которых полностью закрыто для просмотра случайным интернет-пользователям. Третьей ступенью является проверка сайта вторым уровнем "зеркальной" технологии. Четвёртая ступень блокировки – это блок ключевых слов URL (Uniform Resource Locator). Финальная проверка делается с использованием третьего уровня “зеркальной” технологии.

Обобщая, можно составить схему доступа к веб-ресурсу в Китае, представленную на рис. 1. Сталкиваясь со столь жёсткой системой цензуры может показаться, что способов её обхода нет, но это не так. На основании различных исследований были выявлены и проанализированы самые популярные и эффективные методы обхода «Золотого щита» Китая и индекс их относительной простоты применения [2].

Индексы расположены в порядке от 1 до 3, где 1 – действия, которые может сделать любой рядовой пользователь ПК, а 3 – действия, которые по силам только людям со специальными знаниями в данной области. Данные представлены в табл. 1.

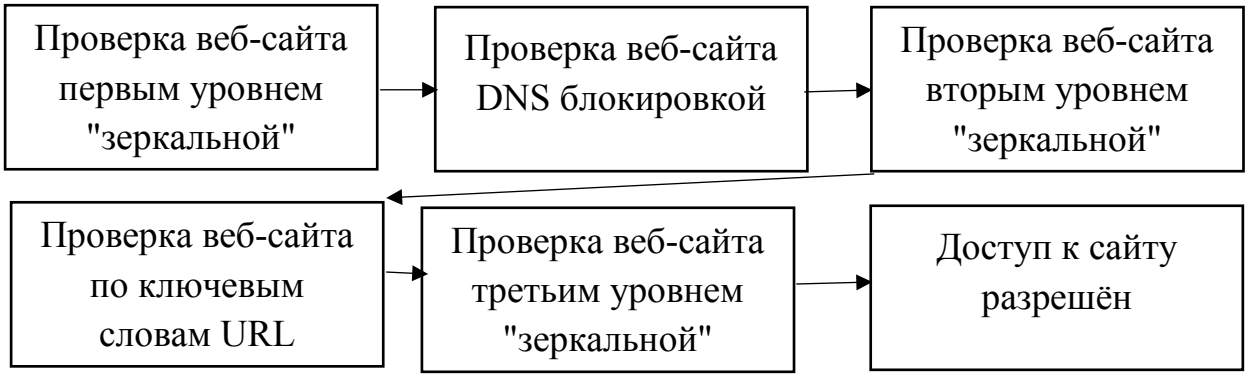


Рисунок 1 – Процесс доступа к веб-сайту в Китае

Таблица 1 – Анализ методов обхода Интернет цензуры Китая

Название метода обхода	Индекс
Использование службы VPN	1
Использование зеркал веб-сайтов	1
Взлом сетевого стека	3
Использование инструментов Tor и DPI	3
Непреднамеренные методы	3
Использование аналогии для обхода фильтров ключевых слов	1
Использование стеганографии	3

Наиболее простыми способами обхода для рядового пользователя являются: использование служб VPN, использование зеркал и аналогов сайтов. Однако применение данных способов не дает возможности полностью обойти защиту, а лишь позволяет избежать определённых трудностей, вызванных ею. Наиболее эффективным и сложным способом для полного обхода брандмауэра является использование браузера Tor в сочетании с различными оболочками и пакетами. Таким образом, на примере анализа самой совершенной системы контроля Интернета государством можно сделать вывод, что на данный момент невозможно создать полную локальную цензуру Интернета.

Список источников:

1. Freedom House [Електронний ресурс] – Режим доступу до ресурсу: https://gtmarket.ru/ratings/freedom-on-the-net/info.

2. Golden Shield Project [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Golden_Shield_Project.

АНАЛИЗ ОПАСНОСТИ ГРУПП ЭКСПЛОЙТОВ

Поддубный В.О.
Научный руководитель – к.т.н, доц. Федюшин А.И.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Безопасности информационных технологий, тел. (097) 232-81-66)
e-mail: vadym.poddubnyi@nure.ua

When creating software , it is impossible not to make mistakes, sometimes they can be almost useless, but some can be used to attack the software or the system. An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware. Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack. The aim of the work was to determine the most dangerous exploits group. The result of the work shows that at this point in time browser exploits are the most dangerous and require further study and work with them.

На этапе конфигурирования и настройки автоматизированной системы (АС) требуется проверить, правильно ли подобраны и настроены средства защиты информации, выбрана ли верная политика безопасности. Во время эксплуатации системы также следует регулярно осуществлять аудит безопасности, так как любая система со временем меняется, добавляются новые компоненты, и, следовательно, появляются новые угрозы. Но даже при выполнении всех норм безопасности нельзя гарантировать, что АС будет защищена от атак с использованием эксплойтов, так как ошибки на этапе создания и эксплуатации программного обеспечения (ПО) очень трудно предугадать. Каждый день появляются сотни новых эксплойтов для различных приложений операционных систем (ОС), и несмотря на своевременное обновление баз сигнатур антивирусов и средств защиты, атаки наносят колоссальный урон. Количество веб-сайтов и спам-рассылок с эксплойтами увеличивается. Так, число атак, совершенных с помощью эксплойтов, в 2016 году выросло по сравнению с 2015–м практически на четверть. А корпоративных клиентов, подвергшихся подобным нападениям, за тот же период оказалось больше на 28% – их количество выросло с 538 тысяч до 690 тысяч.

За период 12.02.19–19.02.19 было обнаружено 482 новых уязвимостей из них 37% высокой степени угрозы, 11,5%средней, 51,5% низкой. Из них 5,4% не были исправлены [1].

Эксплойты фактически предназначены для выполнения сторонних действий на уязвимой системе и могут быть разделены между собой следующим образом:

1) Эксплойты для операционных систем;

2) Эксплойты для прикладного ПО (музыкальные проигрыватели, офисные пакеты и т. д.);

3) Эксплойты для браузеров (Internet Explorer, Mozilla Firefox, Opera и другие);

4) Эксплойты для интернет-сайтов (facebook.com, hi5.com, livejournal.com);

5) Эксплойты для интернет-продуктов (IPB, WordPress, VBulletin, phpBB);

6) Другие эксплойты.

Оценивать будем только первые 4 группы, поскольку они имеют наибольшее распространение.

Для определения опасности группы эксплойтов будем брать совокупную оценку исходя из опасности эксплойта и оценки CVSSv2.

Общая система оценки уязвимостей (Common Vulnerability Scoring System – CVSS) – это система, позволяющая осуществлять сравнение уязвимостей ПО с точки зрения их опасности. При выставлении оценки используются базовые, временные и контекстные метрики.

Существует 4 вида эксплойтов по степени опасности это низкая, средняя, высокая, критическая.

Максимальная оценка опасности –20 (в случае если все уязвимости критические), минимальная 0. Распределение угроз: 0-5– малая степень угрозы, 5-10, – средняя, 10-15 –. высокая, 15-20 – критическая.

В работе исходя из критериев оценки уязвимостей промышленного стандарта CVSSv2, а также дополнительных контекстных метрик был проведен сравнительный анализ опасности групп эксплойтов и получены статистические оценки. Результаты свидетельствуют, что наиболее опасная группа эксплойтов это эксплойты для браузеров: общий коэффициент опасности – 9,78 по сравнению с 5,42 – для ОС, 7,31 – для прикладного ПО и 3,05 – для сайтов. Таким образом, можно сделать вывод, что эксплойты для браузеров обладают предпороговой с высокой средней угрозой, для ОС и ПО средней угрозой, для сайтов низкой.

Браузерные эксплойты являются довольно распространенным явлением, они могут получать информацию пользователя и использовать ресурсы компьютера. Основная угроза, это угроза конфиденциальности, так как браузер хранит файлы cookies, историю посещений, пароли к сайтам и т.п., которые могут быть похищены и использованы злоумышленником. Дыры в защите существуют у таких браузеров как Microsoft Edge, Mozilla Firefox, Google Chrome, регулярное их обновление и применение защитных мер способны улучшить ситуацию.

Список источников:

1 База данных уязвимостей.– Режим доступа: URL: https://www.cybersecurity-help.cz/vdb/– 19.02.2019г. — Загл. с экрана.

АНАЛІЗ ДЕЦЕНТРАЛІЗОВАНОГО ПРОТОКОЛУ ОБМІНУ ПОВІДОМЛЕННЯМИ BITMESSAGE

Гріненко Т.О., Мандич Д.Р.
Науковий керівник – д.т.н., проф. Олійников Р.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. БІТ, тел. +38 (057) 702-14-25)
e-mail: madr0310@gmail.com

In the work will been represented an idea of peer-to-peer decentralized message protocol, its properties, characteristics, need for the modern world and possible ways to use.

Після повідомлення Едварда Сноудена про те, що за більш ніж мільярдом людей в 60 країнах ведеться глобальне стеження, виникла необхідність створення дійсно конфіденційного засобу комунікації. Вже через рік, а саме 21 березня 2013 року, вийшла перша бета-версія клієнта BitMessage [1,2]. Ключовою інновацією протоколу BitMessage стала відсутність центральних серверів або будь-якого центру, який обробляє дані. Протокол працює за схемою peer-to-peer, тобто кожен вузол є і клієнтом, і сервером одночасно, а єдиний сервер відсутній [1,2].

Протокол підтримує обмін зашифрованими повідомленнями, використовуючи end-to-end шифрування. Це означає, що повідомлення може прочитати тільки відправник і одержувач, а жодна проміжна ланка не має такої можливості.

Варто зазначити, що для кожного повідомлення, яке передається по мережі BitMessage, використовується алгоритм доказу виконання роботи proof-of-work. Щоб відправити повідомлення, автор повинен виконати деяку ресурсномістку роботу. Складність proof-of-work залежить від обсягу повідомлення і обсягу вкладень, що входять в нього.

BitMessage використовує модель анонімності, яку можна охарактеризувати як «всі отримують все», що є формою приватного пошуку інформації, яка, як відомо, є теоретично безпечною, але також неефективною. Ця модель ускладнює, якщо не унеможливлює, визначення повідомлень, призначених для користувачів. У поєднанні з відсутністю метаданих BitMessage здається близьким до досягнення цієї властивості в практичному сенсі. Протокол приховує відправника і одержувача. Ця властивість досягається за рахунок того, що ні відправник, ні одержувач не розголошують ніякі ідентифікатори (наприклад, відкриті ключі, BitMessage-адреси або мережеві адреси користувачів). Крім цього, будь-який користувач може використовувати Tor для підключення до інших учасників мережі. Підключення через Tor дозволяє приховати сам факт використання BitMessage с точки зору зовнішнього спостерігача. У протоколі також є можливість підпису повідомлення для підтвердження авторства тексту повідомлення і для забезпечення цілісності. Передбачена

підтримка відкритих каналів, наприклад, для новинних або інформаційних ресурсів. Тобто, існує адреса, яку може прослуховувати будь-який бажаючий користувач. Ця функція працює аналогічно каналам в Telegram або розсилкам в звичайній пошті. Також є підтримка закритих групових чатів. Тобто серед бажаючих користувачів створюється загальний секрет, за допомогою якого шифруються повідомлення в цьому чаті. Причому, для цього необов'язково вказувати одну зі своїх адрес. Закритий чат неможливо цензурувати, видалити або заблокувати.

У протоколі Bitmessage для зашифрування даних використовується алгоритм AES з довжиною блоку 256 біт, який працює в режимі CBC (Cipher Block Chaining) [3]. В даному випадку ключ розраховується як загальний секрет між відправником і отримувачем за схемою ECDH (Elliptic-curve Diffie-Hellman). Такий секрет відправник може отримати автономно без взаємодії з одержувачем. Для цього йому необхідно використовувати свій особистий ключ і відкритий ключ одержувача. Одержувач, використовуючи свій особистий ключ і відкритий ключ відправника, зможе отримати аналогічний секрет. Таким чином, обидва учасники мають однаковий секрет для зашифрування повідомлень. Також, для підвищення рівня безпеки алгоритму ECDH може використовуватися рандомізатор для генерації нового ключа шифрування для кожного нового повідомлення. Реалізація шифрування в BitMessage заснована на бібліотеках з відкритим вихідним кодом, що вважається гарною практикою. BitMessage використовує бібліотеки OpenSSL для реалізації генерації випадкових чисел, шифрування і гешування.

Протокол BitMessage може використовуватися в додатках, в яких необхідно забезпечувати анонімність і конфіденційність. Протокол також є можливою гарною альтернативою звичайній електронній пошті. BitMessage представляє систему, яка об'єднує електронну пошту і безпеку PGP.

Протокол BitMessage забезпечує високий рівень безпеки та анонімності, але є специфічним в роботі: відсутня миттєва відправка повідомлень, також необхідна стабільна робота ПК та інтернету.

Список джерел:

1. BitMessage Wiki [Електронний ресурс] – Режим доступу до ресурсу: https://bitmessage.org/wiki/Main_Page.

2. Jonathan Warren, Bitmessage: A Peer-to-Peer Message Authentication and Delivery System, 2012.

3. Fips 197 «Advanced Encryption Standard», 2001.

РЕАЛІЗАЦІЯ АЛГОРИТМУ ЕЛЕКТРОННО-ЦИФРОВОГО ПІДПИСУ ECDSA НА PYTHON 3.7

Щербина Д.В.
Науковий керівник – к.т.н, доц. Ляшенко О.С.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Радіотехніки, тел. (057) 702-13-06)
e-mail: denys.shcherbyna@nure.ua, факс (057) 702-11-13

The given work is devoted to one of the standard digital signature algorithm named Elliptic Curve Digital Signature Algorithm (ECDSA), which is widely used is TLS, SSL, PGP, Bitcoin and elsewhere. ECDSA is the elliptic curve analogue of the DSA and has been standardized by many standards organizations around the world including NIST, IEEE, ANSI and ISO [1]. Unlike the ordinary discrete logarithm and the integer factorization problem, no subexponential-time algorithm is known for the elliptic curve discrete logarithm problem. For this reason, the strength-per-key-bit is substantially greater in an elliptic curve.

Рукописні підписи здавна використовуються як доказ авторства документу або повідомлення та згоду з його змістом. Їхніми основними властивостями є достовірність, непідробність, неможливість зміни після підписання і т. д [2].

На жаль, ті проблеми, які присутні у реальному житті так само переносяться у світ електронної передачі інформації. Для подолання цих проблем був розроблений електронно-цифровий підпис (ЕЦП), що представляє собою невеликий обсяг даних, переданих разом з документом або повідомленням при його пересиланні.

ECDSA (Elliptic Curve Digital Signature Algorithm) – це алгоритм з відкритим ключем для створення цифрового підпису, аналогічний за своєю будовою DSA, але визначений, на відміну від нього, не над полем цілих чисел, а в групі точок еліптичної кривої.

Стійкість цього алгоритму ґрунтується на проблемі дискретного логарифмування в групі точок еліптичної кривої [1]. На відміну від проблеми простого дискретного логарифма і проблеми факторизації цілого числа, не існує суб-експоненціального алгоритму для проблеми дискретного логарифма в групі точок еліптичної кривої. З цієї причини «сила на один біт ключа» набагато вище в алгоритмі з еліптичними кривими.

У 1998 році алгоритм ECDSA був прийнятий стандартом ISO. Пізніше був прийнятий як стандарт ANSI у 1999 році, а у 2000 році – як стандарт IEEE і NIST.

ECDSA працює з хешем повідомлення, а не з самим повідомленням. У програмній реалізації, написаній на мові Python 3.7, була використана хеш-функція SHA-512 з модуля hashlib. Хеш повідомлення необхідно урізати,

щоб бітова довжина хеша була такою ж, як і бітова довжина порядка підгрупи n. Урізаний хеш – це ціле число, позначене, як z.

Алгоритм який виконується Алісою для підписування повідомлення, виглядає так:

1. Беремо випадкове ціле k, вибране у діапазоні від 1 до $n-1$, де n – порядок підгруппи. За це відповідає функція make_keypair.

2. Обчислюємо точку $P = kG$, де G – базова точка підгруппи. Функція scalar_mult відповідає за цей крок.

3. Обчислюємо число $r = x_P \, mod \, n$, де x_P – координата x точки P.

4. Якщо $r = 0$, то обираємо інше k і повторюємо кроки, починаючи з другого.

5. Обчислюємо $s = k^{-1}(z + rd_A) \, mod \, n$, де d_A – закритий ключ Аліси, k^{-1} – мультиплікативна інверсія k за модулем n (обчислюється функцією inverse_mod).

6. Якщо $s = 0$, то обираємо інше k і повторюємо кроки, починаючи з другого.

Пара (r, s) і є підписом. За генерацію підпису відповідає функція sign_message.

Для перевірки підпису необхідний відкритий ключ Аліси H_A, урізаний хеш z і підпис (r, s):

1. Обчислюємо ціле $u_1 = s^{-1}z \ \ mod \, n$.
2. Обчислюємо ціле $u_2 = s^{-1}r \ \ mod \, n$.
3. Обчислюємо точку $P = u_1G + u_2H_A$.

Підпис дійсна, якщо $r = x_P \, mod \, n$. За перевірку підпису відповідає функція verify_signature.

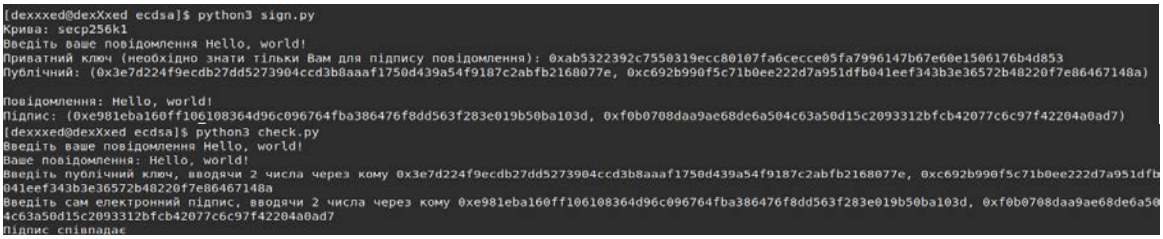


Рисунок 1 – Результат роботи скриптів

Для генерування та перевірки підписів були написані скрипти на мові Python 3.7. нижче.

Список джерел:

1. D. Brown, Generic groups, collision resistance, and ECDSA, Designs, Codes and Cryptography, 35 (2005), 119-152 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: Триумф, 2002. – 40 с.

АНАЛИЗ АУДИТА В ОПЕРАЦИОННОЙ СИСТЕМЕ FREEBSD

Мищеряков А.Ю.
Научный руководитель – проф., Халимов Г.З.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, проспект Науки, 14, каф. Безопасности информационных технологий. Тел.702-14-25)
e-mail: anton.mishcheriakov@nure.ua

In this paper we consider the audit log integrity monitoring, and protection it against unauthorized access. We consider the possibilities of an attacker to modify the audit log in order to hide his presence in the system. Some solutions to this problem and the rationale for their adoption are given. The problems that may arise in connection with the implementation of the proposed solutions are considered.

На сегодняшний день операционная система FreeBSD обрела популярность в использовании, как для повседневной жизни, так и для рабочих целей. В работе данная система рассматривается в качестве сервера.

Данная операционная система является достаточно защищенной, надежной. В связи с этим поднимается вопрос безопасности системы, отслеживания работы пользователей с файлами, изменения файлов и т. д.

Одним из важнейших средств контроля событий в системе является журнал аудита. Его главным назначением является отслеживания событий о действиях пользователя и программного обеспечения, запускаемого пользователями. Журнал хранит информацию о том, кто, когда, с какими правами использовал файлы, запускал программы и т. д.

Журнал аудита является эффективным методом наблюдения за важными файлами утечка, изменение или удаление которых может нанести непоправимый ущерб.

Однако, реализация аудита в FreeBSD имеет известные ограничения. Не все события в настоящий момент протоколируемые. Также, некоторые механизмы входа в систему, такие как оконные менеджеры X11 или демоны от сторонних производителей, не настраивают аудит пользовательских сессий должным образом [1].

Для настройки журнала аудита используются конфигурационные файлы в которых прописывается какие файлы отслеживать, где хранятся файлы журнала аудита, резервные копии этих файлов и т. д.

Так как в журнале аудита хранятся действия над многими файлами возникает потребность ограничить доступ к этому файлу для всех сотрудников, для избегания нежелательной его модификации.

Вместе с тем, модификация, изменение или повреждение журнала аудита может происходить ненамеренно в результате сбоя программно-аппаратного обеспечения или злоумышленником.

В результате сбоя программно-аппаратного обеспечения, например, перебой электропитания, могут быть недоступны файлы системы. В следствии этого должен присутствовать механизм восстановления работоспособности системы и журналов аудита.

Злоумышленник может модифицировать файлы журнала аудита для сокрытия своих действий в системе. Для противодействия этому необходимо их защитить.

Для защиты журнала аудита можно хранить файлы в нестандартных местах и так же использовать шифрование. Для этих целей может использоваться как симметричное, так и ассиметричное шифрование.

Однако при применении шифрования возникает дополнительная нагрузка на систему. Таким образом администратору необходимо обеспечить выбор баланса между стойкостью шифрования и нагрузкой на вычислительную систему.

Вышеуказанную проблему можно решить шифрованием не самих файлов аудита, а путей к ним. Это серьезно затруднит злоумышленнику возможность определить расположение файлов аудита, следовательно, убрать все признаки своего присутствия в системе будет намного сложнее.

Несмотря на применяемые средства защиты существует вероятность того что злоумышленник все же может почистить следы своего пребывания в системе. Во избежание этого необходимо принять дополнительные меры проверки корректности, целостности файлов аудита. Для этих целей могут быть применены следующие решения: выполнять резервное копирование в реальном времени, желательно на другой сервер сети, для каждой вносимой в журнал аудита записи сохранять в отдельный скрытый файл отметки расположения записи в журнале, времени ее внесения в журнал, а также хеш-значение. Такой подход позволит отслеживать целостность файлов аудита и выявлять несанкционированные изменения в них.

Таким образом контроль действий пользователей и программного обеспечения и отслеживания целостности этих данных повышает нагрузку на систему, и каждый администратор должен решить для себя, повысить нагрузку на систему и повысить безопасность, или же пожертвовать безопасностью в пользу быстродействия системы.

Список источников:

1. Аудит событий безопасности. / Руководство FreeBSD [Электронное издание]. – Режим доступа: https://www.freebsd.org/doc/ru/books/ handbook/audit.html.

БЕЗОПАСНОЕ ХРАНЕНИЕ ЦЕЛЕВЫХ ДАННЫХ В BITCOIN С ПРИМЕНЕНИЕМ ДЕЦЕНТРАЛИЗОВАННОЙ СЕТИ ОБМЕНА ФАЙЛОВ INTERPLANETARY FILE SYSTEM

Гриненко Т.А., Скичко Д.В.
Научный руководитель – д.т.н., проф. Олейников Р.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки, 14, каф. БИТ, тел. +38 (057) 702-14-25)
e-mail: meksvinz@gmail.com

In this work discusses the method of ensuring the properties of information security, which is based on the joint use of the Bitcoin decentralized accounting system and the decentralized IPFS data exchange network.

Существует множество способов обеспечения свойств информационной безопасности. В работе рассмотрен способ, который базируется на совместном применении децентрализованной учётной системы Bitcoin и децентрализованной сети обмена данных IPFS (InterPlanetary File System). Совместное применение этих двух систем может дать довольно мощный инструмент по обмену файлами.

База данных децентрализированной учётной системы Bitcoin состоит преимущественно из транзакций [1]. У каждой транзакции может быть один или несколько входов, каждый из которых содержит поле scriptSig (доказательство владения монетами) и один или несколько выходов, каждый из которых содержит поле scriptPubKey (условие траты монет). Эти поля представляют собой набор операций, написанных на языке описания сценариев для траты монет Bitcoin Script. Под выполнением сценария подразумевается последовательное выполнение операций (OP-кодов) над некоторыми данными, которые содержатся в том же скрипте, а при выполнении помещаются в стек.

Рассмотрим OP-код OP_RETURN. Код OP_RETURN позволяет поместить в выход транзакции до 80 байт произвольных данных. Это может быть хэш-значение, данные в открытом или зашифрованном виде и т.д. Плюсы в помещении какой-либо произвольной информации в выход транзакции в том, что после распространения такой транзакции по сети и при условии, что она попадает в блок, который будет добавлен к самой длинной цепочке блоков, эти данные фактически будут храниться на всех узлах децентрализированной учётной системы Bitcoin, а это около 10115 узлов. Информация, которая была добавлена в цепочку блоков таким способом, будет храниться там до тех пор, пока владельцы большей части вычислительной мощности не решат переписать историю (предложат альтернативную цепочку блоков, что очень маловероятно). Поэтому наиболее вероятно, что произвольно записанные данные останутся доступными любому желающему навсегда. Это обеспечивает целостность и доступность информации, даже при условии, что субъект, который

отправил транзакцию, потерял доступ к целевым данным. Стоит заметить, что одна транзакция может включать более чем один выход с кодом OP_RETURN (возможное количество выходов зависит от размера данных, записываемых в транзакцию. В Bitcoin максимальный размер транзакции ограничен размером ¼ от максимального размера блока) [1]. С помощью такой транзакции можно сохранить, к примеру, доказательство совершения какого-либо действия (оплаты, сделки) и получить к нему доступ в любой момент времени, просто просмотрев транзакцию, в которой оно записано. Но есть определенные недостатки хранения информации в базе учётной системы Bitcoin таким способом, так как любой субъект может просмотреть информацию, записанную в OP_RETURN-выходе. Чем больше данных записывается в выходы с OP-кодом OP_RETURN, тем большую комиссию придется заплатить за отправку транзакции (если вообще не установить комиссию, то вероятность попадания транзакции в блок стремится к нулю, а если установить слишком маленькую комиссию, то возможна ситуация, когда узлы-валидаторы просто не станут включать транзакцию в блок из-за маленькой комиссии). Для обеспечения конфиденциальности информации, записанной в OP_RETURN-выходе транзакции, можно применять асимметричную криптографию.

В транзакцию невозможно поместить информацию большого объёма (документ, видеофайл и т.д.). Но при этом в транзакцию можно поместить hash значение файла, который необходимо отправить. Например, hash значение любого файла, который хранится в децентрализированной сети обмена данных IPFS.

Рассмотрим пример типичного обмена файлами в связке Bitcoin и IPFS: Алиса выбирает файл, который хочет отправить Бобу, и загружает его в сеть IPFS, получая в ответ хэш-значение (hash), по которому другой пользователь сети IPFS может скачать данный файл. Далее Алиса берёт публичный ключ Боба и шифрует на нём hash целевого файла, после чего записывает уже зашифрованный hash в выход bitcoin-транзакции (при помощи OP_RETURN). После чего сообщает идентификатор транзакции (txid) Бобу, по нему Боб находит транзакцию с зашифрованным hash и успешно расшифровывает его при помощи своего личного ключа, тем самым получая расшифрованный hash файла в сети IPFS, по которому может скачать файл, который Алиса ему адресовала. При таком обмене, третьей стороне будет трудно сказать, был ли обмен вообще, так как однозначно определить кому адресованы данные в OP_RETURN-выходе невозможно. А также, невозможно будет определить содержится ли именно hash в OP_RETURN-выходе, а не любые другие данные.

Список источников:

1. Блокчейн и децентрализованные системы: учеб. пособие для студ. Ч.1 /П. Кравченко, Б. Скрябин, О. Дубинина.– Харьков: ПРОМАРТ, 2018. – 440 с.

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФРАСТРУКТУРІ ХМАРНИХ ОБЧИСЛЕНЬ

Коханевич Є.Г.
Науковий керівник – к.т.н., доцент Федюшин О.І.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Безпеки інформаційних технологій, тел.702-14-25)
e-mail: yevhenii.kokhanevych@nure.ua, тел. (066) 189-79-17)

In this work the features of information security of cloud infrastructure are considered. Also we created a test environment using the OpenStack program, and simulates the work of cloud computing services to identify the major threats.

Then, we identified the main metrics with which you can identify the incident of information security in the cloud. In the end, a neural network was created that was capable of responding to information security incidents in accordance with data obtained from metrics.

Широке розповсюдження мереж з високою потужністю, низька вартість комп'ютерів та приладів збереження даних, а також масове впровадження віртуалізації, сервіс-орієнтованої архітектури призвело до дуже великого зростання хмарних обчислень. Хмарні обчислення – це модель забезпечення зручного доступу до обчислювальних ресурсів через мережу, які оперативно надаються та звільняються з мінімальними зусиллями з боку клієнта.

Але через те, що користувачі не мають доступу до роботи обладнання технологічної інфраструктури, яка їх підтримує, приватна інформація користувача фактично стає доступна третій стороні – провайдеру, окрім цього данні стають вразливими під час їх передачі по каналам зв'язку. Хоча великі постачальники і роблять все можливе для забезпечення високого рівня безпеки всередині хмари, але особливості побудови хмарної інфраструктури, використання технології віртуалізації та пов'язана з нею можливість порушення ізоляції віртуальних машин, а також паралельна обробка великих об'ємів інформації різних споживачів хмарних послуг, призводить до виникнення нових можливих загроз інформаційної безпеки, які будуть специфічними лише для хмарних обчислень.

На сьогодні провідними організаціями, що займаються питаннями безпеки в хмарі, є Альянс безпека в хмарі (Cloud Security Alliance, CSA), що складається з представників IT-індустрії, а також дві державні організації Європи та США: Європейське агентство мережної та інформаційної безпеки (ENISA) і Національний інститут стандартів і технологій (NIST). Кожна з організацій створила відповідний документ з класифікацією всіх існуючих проблем інформаційної безпеки в хмарі[1-3].

Найбільш поширена проблема інформаційної безпеки, яка виникає при роботі в хмарному середовищі, пов’язана з некоректною конфігурацією інфраструктури та не своєчасним реагуванням на інциденти, що виникають.

Метою даної роботи є реалізація ефективного засобу аудиту інформаційної безпеки в інфраструктурі хмарних обчислень та оперативного реагування у випадку виявлення потенційних загроз.

Під час виконання роботи було створено тестове хмарне середовище з допомогою інструменту OpenStack. В тестовій інфраструктурі була змодельована робота декількох споживачів хмарних послуг та проведений аналіз безпеки в середині кожної з них та їх вплив один на одного. В ході аудиту безпеки були визначені основні метрики, які дозволяють найбільш ефективно визначити інциденти інформаційної безпеки.

Наступним етапом роботи було розроблення ефективного засобу реагування на виникаючі загрози. Була створена нейронна мережа, яка здатна активно реагувати на інциденти інформаційної безпеки згідно з показниками метрик, які їй надаються. Таким чином, нейронна мережа здатна виконувати певні визначені дії по налаштуванні роботи інфраструктури у випадку отримання результатів метрик, що свідчать про виникнення чи існування певного інциденту в інформаційній безпеці даної інфраструктури. Робота нейронної мережі була реалізована згідно з алгоритмом, що детально описаний в [4].

Як результат ми отримали засіб оперативного реагування на інциденти та загрози інформаційної безпеки, що виникають в інфраструктурі хмарних обчислень. Ця система дозволяє забезпечити ефективний аналіз безпеки в інфраструктурі з врахуванням особливостей хмарних технологій та оперативні дії у випадку виявлення загроз інформаційній безпеці.

Список джерел:

1. Cloud Security Alliance “Treacherous 12: Top Threats to Cloud Computing” – 2016 [Electronic resource]. – URL: cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-deep-dive.

2. European Union Agency for Network and Information Security “Cloud Security Guide for SMEs” – 2015 [Electronic resource]. – URL: www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

3. National Institute of Standards and Technology “Guidelines on Security and Privacy in Public Cloud Computing” – 2011 [Electronic resource]. – URL: nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-144.pdf.

4. Сенцова А. Ю. Модели и метод экспертного аудита информационной безопасности в системе облачных вычислений: дис. канд. техн. наук: 05.13.19 / Сенцова Алина Юрьевна. – Уфа, 2016. – 208 с.

ПРОБЛЕМИ ЗАХИЩЕНОСТІ КОМПОНЕНТІВ СУЧАСНОГО АВТОМОБІЛІВ ВІД КІБЕРАТАК

Фесенко Д. О.
Науковий керівник – проф., Халімов Г.З.
Харківский національний університет радіоелектроніки
(61166, Харків, проспект Науки, 14, каф.Безпеки інформаційних технологій. Тел.702-14-25)
e-mail: dmytro.fesenko@nure.ua

Nowadays automotive industry has need in development of additional methods that would improve security of auto systems to achieve much more proficient security and trust levels. For this full understating of threads that would lead to improper operations with car components is needed, to understand what could cause road accidents or driving away of a vehicle.

Автоіндустрія потребує наразі розроблення додаткових методів захисту компонентів транспортного засобу та розроблення комплексних засобів захисту для систем авто для підвищення рівня захищеності та довіри, для цього необхідно розглянути можливі загрози, що могли б спричинити неправильну роботу компонентів автомобіля і як наслідок – привести до дорожньо-транспортної пригоди чи викрадення транспортного засобу.

Більшість сучасних транспортних засобів має на борту мультимедійну систему, яка дозволяє використовувати його як повноцінний персональний комп'ютер з можливістю виходу в мережу інтернет через вбудований модем, який підтримує використання SIM-карт для доступу до GSM мереж та вбудованим Wi-Fi модулем 802.11/n. Це дає можливість використання більш зручних та високотехнологічних засобів, що дозволяють користувачу отримувати інформацію про стан вузлів авто в режимі реального часу, дивитись фільми або працювати з іншими даними та навіть передавати їх по P2P мережі автомобіля. В той же час використання таких технологій можливість хакерських атак на системи авто для перехоплення даних, їх підміни та компрометації роботи систем та вузлів транспортного засобу через збільшення кількості атак даного виду в останній час. Данні атаки є можливими через використання давно відомих технологій, для яких виявлено багато вразливостей, які переходять до нових розробок від старих, наприклад багато мультимедійних систем використовує в якості операційної системи ОС Android, часто не останніх версій.

Мультимедійна система автомобіля з'єднана з іншими найчастіше через мережу CAN, що дозволяє зробити більш легким та ефективним з'єднання електричних елементів транспортного засобу, але в той же час на даний протокол з'єднання розроблено багато атак, які оновлюються з апгрейдом захищеності протоколу.

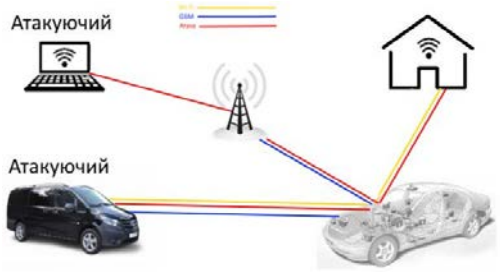


Рисунок 1 – Схема бездротових з`єднань авто з мережею інтернет

Розглянемо вид атак, що направлений на отримання керування пристроями автомобілю дистанційно. На рисунку 1 представлено приклад з'єднання мультимедійної системи з мережею інтернет через різні бездротові канали зв'язку через які можливі атаки на мережі, як підтримуються даним транспортним засобом – це мережа Bluetooth, вектором атаки який використовує помилки реалізації протоколу та дозволяє виконати атаку спарювання пристрою атакуючого з пристроєм встановленим на авто Wi-Fi мережу, яка найчастіше буде використовуватися для доступу до мережі інтернет з метою серфінга інтернет сторінок, оновлення навігаційних карт. Тут атаки можуть бути різноманітні: від реалізації атаки на стек до можливостей проведення Fake AP/MITM атаки. В разі успішно проведеної атаки атакуючий отримує доступ до компонентів транспортного засобу, що дозволяє йому керувати ними в своїх цілях.

Виходом з ситуації може бути розроблення комплексної системи захисту інформації для сучасного транспортного засобу, що є надзвичайно важливим етапом для покращення захищеності життя водія та пасажирів, оскільки під час створення такої системи проводиться обстеження всіх середовищ функціонування ІТС та розглядаються всі можливі варіанти взаємного впливу елементів різних середовищ на безпеку системи.

RULES ARE MEANT TO BE BROKEN, THE SECURITY SYSTEM TO BE HACKED

Ivanitskiy Mikhail Aleksandrovich
Scientific supervisor – Ph.D., professor Zabolotny V. I.
Kharkiv National University of Radio Electronics
(61166, Kharkiv, 14 Nauka Ave., CEC Dept., Tel. (057) 702-14-21)
e-mail: malyuvin@gmail.com

The work is devoted to the principles that cybersecurity is based on. In this article is analyzed an up-to-day state of forever contradictory forces through the prism of intruder and security officer.

From the beginning up to now, the values always are under the risk to be stolen. And the ones are surrounded by the walls. Each wall has its hole. That the way the defense based on. Does exist the safety or don't? That's the question.

Not every vulnerability is an Achilles heel. But the one is a vulnerability. That's what under lock and key. And the leakage of such information will cause irrevocable damage to the security system.

The term Achilles Heel refers to an area of weakness which, when applied to Information Security means the weak link in the security safeguards. An example of an Achilles Heel would be where substantial effort has been made to secure data on the server, and yet virtually anyone is able to walk in to the systems room and remove the disk sub-systems. The appropriate action for the Security Officer in your organization, is to identify the Achilles Heel, and to take action against it.

What are the existing security vulnerabilities, the methods of attacks and consequences, range of potential insider and outsider actions that could be exploited?

The digital networking and increasing exchange of data currently taking place in many firms is making their IT systems vulnerable to attack. Companies with a digital infrastructure such as computer networks are vulnerable to cyber-attacks, that is, targeted attacks on their digital infrastructure from outside. These attacks can paralyse computer networks or destroy customer and employee data. The intentional manipulation of IT infrastructure and data by outsiders was perceived by companies as the most significant risk associated with cyber security, closely followed by increasingly complex IT systems, which often make it difficult to identify potential security flaws and fix vulnerabilities in the system as soon as they appear. At least two thirds of the firms surveyed view security flaws in hardware and software as well as the increasing exchange of data as cyber security risks.

This increasing awareness of cyber security risks has led many companies to take action. Almost a quarter of companies already spend more than five per cent of their IT budget on cyber security.

60 per cent of companies also encrypt their data and just as many regularly check their logfiles for cyber-attacks. Encrypted email communication is used in 59 per cent of the companies surveyed. Half of all firms are already providing their management staff with cyber security training and 40 per cent do this for other employees as well. Meanwhile, 38 per cent of the firms agreed that IT staff need to be given regular training to keep up-to-date with new developments and have already implemented such training.

In order to ensure the security of their IT systems, firms must be willing to constantly engage with the issue. As technologies continue to develop, so too must firms' security frameworks and measures. This requires considerable effort but is essential for ensuring the continued success of digital transformation

According to recent studies and international organizations' reports, violent extremists are trying to obtain insider position that may increase the impact of any attack on the critical infrastructure and there is also a probability that any terrorist group attacks may cause the collapse of any major critical infrastructure organization's data. Based on these reports it is clear that their actions pose a significant threat that could potentially impact critical services, financial impact, people lives and even democracy. It is of utmost importance to adopt important measures in order to secure critical infrastructure and thus lower the level of threats while preserving the rights of citizens. States have an extreme interest in detecting malicious insiders and to counter human threats. Different agencies have invested billions of dollars in different technical measures for years now. Such as, access control implemented through passwords, authentication, biometric authentication and physical certification is recognizable as usernames and passwords pairs and firewalls, data leakage prevention and behavioral-pattern threat detection. However, various studies and researches demonstrate that security software devices are normally failed as these measures are normally designed to defend against external threats to secure critical infrastructure and do not protect against internal and external attacks aided by internal help in the organization.

Every wall has its door. Therefore, if the wall has no hole just go through the door.

References:

1. The information Security Glossary of Terms [Электронный ресурс]./ https://public.ccsds.org/Pubs/350x8g1.pdf.
2. Computerworld [Электронный ресурс]/ https://www.computerworld.com.
3. Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice.
4. Schlienger, Thomas; Teufel, Stephanie (December 2003). "Information security culture - from analysis to change".

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ПРОБЛЕМИ ІНТЕЛЕКТУАЛЬНИХ ОБЧИСЛЕНЬ

RECURRENT NEURAL NETWORKS FOR POWER LINE PARTIAL DISCHARGES DETECTION

Bogdanova A.
Supervisor - Ph.D., Associate Professor O. Turuta
Kharkiv National University of Radio Electronics
61166, Kharkiv, Nauky ave, 14, Software Engineering Department,
e-mail: alina.bohdanova@nure.ua, mob. 099-367-06-08

This paper is focused on the use of recurrent neural networks for detecting partial discharges of medium voltage overhead power lines. Developing a solution to detect partial discharge can help reduce maintenance costs, and prevent power outages. Proposed approach includes the feature extraction and classification steps with tuning such parameters as the number of epochs and number of windows.

Breakdowns of electrical insulation when electrodes are only partially transferred are known as partial discharges. If left unrepaired, they can lead to the downfall of the power lines or damage the equipment to the point that it stops functioning entirely.

The challenge is to detect partial discharges given the voltage measurements of the power line. The dataset contains 8712 signals. Each measurement is represented by 800 000 integer values taken over a single grid cycle (~ 20 milliseconds). Since the data comes from the real environment, there are significantly less positive samples than negative, making an additional challenge to deal with a highly imbalanced dataset. The results are evaluated on the Mattews correlation coefficient (MCC) between the predicted and the observed values. It returns a value between -1 and +1, where +1 represents a perfect prediction, -1 indicates total disagreement between prediction and observation.

Detecting partial discharges is a subject of many areas of study, including signal processing, time series analysis, statistics, applied math and machine learning. Most of the studies use 2 steps for detecting partial discharges: feature extraction and classification. The most popular approach for feature extraction is to divide a signal into subsequences and extract different statistics from them. Usually, the models applied for the final classification are machine learning algorithms: random forest, convolutional neural networks, recurrent neural networks. The latter shows the best quality on cross-validation.

Rerunning a feature extraction algorithm and classifier training takes time, making it hard to test hypotheses quickly. So, the goal of the experiment is to test which parameters of the algorithms work best. The parameter of the feature extraction algorithms is the number of windows. For each subsequence the following statistics are calculated: min, median, max values; mean, standard deviation, skewness and kurtosis.

Table 1 – MCC increase depending on the number of windows

Number of windows	**Best MCC**	**Time to achieve the best MCC, sec**	**10^6 * MCC increase per sec**
500	0.6831	1310	521.45
400	0.6534	915	714.1
320	**0.6635**	**605**	**1096.69**
200	0.6271	695	902.30
160	0.6216	460	1351.30

The more windows are used - the better features approximate the original sequence. But too many features lead to more computing time for training the neural network and possibly to underfitting due to the small number of samples. The best MCC value achieved with 500 windows. However, it takes more time to fit the model on this data. The fastest increasing MCC is observed using 320 windows making it the optimal value for feature extraction.

The parameter of the classifier is the number of epochs. RNN architecture was chosen for handling sequences with 3 dense layers as a classifier head.

Table 2 – MCC increase per second depending on the epoch number

Number of epochs	**AVE epoch time, sec**	**10^6 * MCC increase per sec**
10	19.7	-
20	20.15	9197.89
30	20	2070.92
35	19.74	1333.69
40	**19.98**	**450.60**
45	20.02	-1515.12
50	19.72	1162.57

Best metric increase per second is observed at the very beginning of the training process when the model starts adjusting its weights for the dataset. After a certain amount of epochs, each following epoch gives a smaller increment to metric but takes the same computing time. Thus, it’s reasonable to stop the learning process when the metric increase becomes not significant. In this case, 40 epochs are enough.

КОНТРОЛИРУЕМЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

Ивановская К.А., Шостак М.В.
Научный руководитель – к.т.н., ст. преп. Мовсесян Я.С.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф. ЕОМ, тел (057) 702-13-54),
E-mail kseniia.ivanovska@nure.ua, maksym.shostak@nure.ua

The concept of "detection of anomalies" appeared relatively recently and immediately attracted the attention of experts in the field of network security. In mid-2003, the first Western and domestic anomaly detection systems appeared on the information security market, and network security service providers began to actively offer appropriate solutions. What methods and algorithms for the detection of anomalies can be useful for the practice of information protection services?

На данный момент актуальна проблема, связанная с сетевыми вторжениями – неавторизованным доступом в компьютерную систему или сеть либо несанкционированным управлением ими в основном через Интернет.

Обнаружение аномалий – динамический метод работы антивирусов, хостовых и сетевых систем обнаружения вторжений. Программа, использующая метод обнаружения аномалий, наблюдает определённые действия (работу программы/процесса, сетевой трафик, работу пользователя), следя за возможными необычными и подозрительными событиями или тенденциями.

Задачей выявления является создание набора данных, по которому происходит поиск, определение характеристик поиска и анализ исходных значений для определения вторжений. Все существующие методы машинного обучения выявления аномалий можно разделить на два класса: контролируемые и неконтролируемые методы.

Контролируемые методы машинного обучения – те, которые предусматривают наличие для каждого входного вектора данных выходной вектор значений (откликов). Неконтролируемое обучение – один из способов машинного обучения, в котором испытываемая система спонтанно учится выполнять поставленную задачу, без вмешательства экспериментатора используя типы алгоритмов, которые пытаются найти корреляции без каких-либо внешних данных, кроме необработанных данных.

Рассмотрим методы контролируемого машинного обучения, так как именно имея вектора входных/выходных данных наиболее наглядно видны аномалии:

Метод k-ближайших соседей (K-NN) – один из простых алгоритмов, часто применяется с непараметрическим методом. Он вычисляет

приблизительное расстояние границ различными точками входных векторов, а затем присваивает незамеченную точку к классу k-ближайшего соседа. В процессе создания K-NN классификатора k является важным параметром и разные значения k могут вызывать различные последствия. Ключевой особенностью метода K-NN является простой и быстрый в реализации алгоритм, но имеется недостаток – высокая чувствительность к настройке параметров, что сильно влияет на точность.

Байесовская сеть (BN) представляет собой модель, которая кодирует вероятностные отношения между переменными. Данный метод обычно используется для обнаружения вторжений в сочетании со статистическими схемами. Имеет ряд преимуществ, среди которых – возможность кодирования зависимости между переменными и предвидением события, а также возможность включать предварительные знания и данные.

Контролируемые нейронные сети (NNS) предсказывают поведение различных пользователей и демонов в системах. Основным преимуществом NNS является толерантность к неточным данным и неточной информации, а также способность строить решения без предварительного знания закономерностей данных, что в сочетании со способностью к обобщению изученных данных сделало их целесообразными для ID.

Дерево принятия решений (DT) – эффективный и распространенный инструмент для классификации и прогнозирования, он может быть применено для классификации точки данных, начиная от корней дерева и перемещаясь вниз, пока лист узла, обеспечивающий классификацию точки данных, не будет достигнут. Главным недостатком является большое время выполнения вычислений.

Метод опорных векторов (SVM) преобразует входной вектор в многомерное пространство признаков, а затем получает оптимальную разделяющую гиперплоскость в высокой размерности пространства признаков.

Исходя из проведённого анализа, все эти методы борьбы с сетевыми вторжениями эффективны для решения проблемы с обнаружением сетевых вторжений. Лучше всего со своей задачей справляются контролируемые нейронные сети, из-за своей возможности охватить весь спектр входных данных и быстрого отклика при обнаружении проблемы.

Список источников:

1. Paulo M., Vinicius M. and Joni. 2010. Octopus-IIDS: An Anomaly Based Intelligent Intrusion Detection System. Proceedings of Computers and Communications (ISCC).

АНАЛИЗ ИММУННЫХ АЛГОРИТМОВ КЛОНАЛЬНОГО ОТБОРА ДЛЯ РЕШЕНИЯ ЗАДАЧ ОПТИМИЗАЦИИ

Чуприна А.А., Малюков Р.Р.
Научный руководитель – д.т.н.,проф. Кораблев Н.М.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр.Науки,14, каф. ЭВМ, тел. (057) 702-13-54)
e-mail: chupina2610@gmail.com, rash1369@mail.ru

Artificial Immune Systems (AIS) have emerged during the last decade. They are incited by many researchers to design and build immune-based models for a variety of application domains. This report investigates the different AIS based clonal selection algorithms.

Задачи оптимизации могут решаться с использованием различных подходов. Для этих достаточно эффективным является использование искусственных иммунных систем (ИИС). Существуют различные модели ИИС, одной из которых является модель клонального отбора. Анализ этой модели и ее развитие приведено ниже.

Л. Кастро и Ф. Зубен предложили алгоритм клонального отбора CLONALG для обучения и оптимизации. CLONALG генерирует популяцию из N антител, каждая из которых определяет случайное решение для процесса оптимизации. На каждой итерации в соответствии со значением аффинности антител к антигенам отбираются лучшие антитела, клонируются и мутируются, чтобы получить новую популяцию-кандидата. Затем новые антитела-кандидаты оцениваются по степени их близости к антигенам и к исходной популяции добавляется определенный процент лучших антител. Наконец, процент наихудших антител предыдущего поколения заменяется на новые случайно созданные.

В работе Л. Руочена, Д. Хайфенга и Д. Личенга введен алгоритм иммунной клональной стратегии (ICS), который включает в себя алгоритмы моноклональной стратегии иммунитета (IMSA) и алгоритм поликлональной стратегии иммунитета (IPSA). ICS используется для решения задачи многокритериальной оптимизации..

С. Гарретт предложил алгоритм адаптивного клонирования (ACS) в качестве модификации CLONALG, который предполагает некоторые изменения в CLONALG на основе анализа операторов для выбора количества мутаций и количества клонов для преодоления недостатков CLONALG, таких как большое число используемых параметров и двоичное представление. Алгоритм адаптивной иммунной клональной стратегии (AICSA), предложенный Р. Лью , Л. Джао и Х. Ду для решения задач численной оптимизации, динамически назначает иммунную память и популяцию антител в соответствии с аффинностями как между антителами, так и между антителами и антигенами, интегрируя локальный поиск вместе с глобальным поиском.

С. Хоу и Ю. Ю представили улучшенный алгоритм выбора клонов, основанный на алгоритме CLONALG. Был введен иммунный оператор для улучшения механизма обучения CLONALG и повышения эффективности обнаружения. Ф. Кампело, Ф. Гуимараес, Х. Игараши и Д. Рамирез предложили вещественное кодирование антител, клонов и антигенов (RCSA) для оптимизации электромагнитного проектирования. RCSA предлагает некоторые модификации алгоритма клонального отбора, и имеет некоторые функции такие как количество клонов, диапазон мутаций и долю популяции, выбранной для каждого поколения.

В. Кателло, Г. Нарцисси, Г. Никосия и М. Павоне разработали иммунологический алгоритм для задач непрерывной глобальной оптимизации OPT-IA, основной особенностью которого являются оператор клонирования, исследующий окрестность в каждой точке в пространстве поиска. В алгоритме используется обратно пропорциональный оператор гипермутации, где число мутаций обратно пропорционально значению аффинности. Ими была представлена улучшенная версия OPT-IA – opt-IMMALG. Основными модификациями в этом алгоритме являются замена представления двоичной строки на вещественно закодированное значение и введение нового обратно пропорционального оператора гипермутации.

М. Гонг, Л. Джао, Л. Джанг и В. Ма представили усовершенствованный алгоритм отбора клонов на основе CLONALG с новым мутационным методом – самоадаптивной хаотической мутацией. Основные модификации заключаются в том, что новый алгоритм использует логистическую хаотическую последовательность для генерации первоначальной совокупности антител, в то время как гипермутация принимает самоадаптивную хаотическую мутацию. В развитие этого алгоритма ими был предложен алгоритм дифференциального иммунноблокового отбора (DICSA) для решения глобальных задач оптимизации. Он объединяет теорию отбора клонов и дифференциальную эволюцию и использует три иммунных оператора: оператор клонирования, дифференциальную кроссоверную мутацию и стандартный оператор отбора.

Х. Лу и М. Джичун предложили алгоритм корректировки клонального хаоса (CCAA) для оптимизации мультимодальной функции. В целях повышения эффективности глобальной конвергенции CLONALG он использует преимущества эргодических и динамических свойств системы хаоса и вводит в CLONALG хаотический механизм поиска.

Таким образом, каждый последующий предлагаемый алгоритм является модификацией предыдущих с добавлением дополнительных операторов и свойств, что позволяет повысить эффективность получения желаемого результата. Предполагается проведение экспериментальных исследований по сравнительному анализу рассмотренных алгоритмов с целью выработки рекомендаций по их использованию.

ЗАСТОСУВАННЯ МЕТОДІВ БІНАРНОЇ КЛАСИФІКАЦІЇ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

Коновалов В.С.
Науковий керівник – к.т.н., доц. Гибкіна Н.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Прикладної математики,
тел. (057) 702-14-36)
e-mail: vladyslav.konovalov@nure.ua

Due to the increased capabilities of modern computing technology, it became possible to process large amounts of data and performs complex calculations. Thanks to this, most calculations, as well as work with the large amounts of data can be shifted from the people to the machine. Particularly work with people in the bank. Every day employees need to analyze big amount of data. So that's why we need to create a program that will analyze data instead of him and give recommendations to accept decision.

Сучасні можливості та вимоги до організації діяльності призводять до стрімкого збільшення обсягів даних, які необхідно швидко опрацьовувати для безперебійного надання послуг. Розвиваються не тільки потужності пристроїв, але й методи роботи з ними. Через це одними з найактуальніших напрямів інформаційних технологій, що набули стрімкого розвитку, стають аналіз даних та методи машинного навчання. Завдяки аналізу даних з’явились можливості обробляти великі обсяги даних майже без втручання людини. Це допомагає збільшити продуктивність праці за рахунок перекладання аналізу великого масиву даних на комп’ютерну техніку.

Задачі обробки великих масивів даних виникають у різних сферах діяльності, зокрема, у банківській діяльності під час аналізу фінансових потоків та операцій, балансу активів та пасивів тощо. Одніми з найактуальніших задач банківської діяльності є задача про надання кредитних послуг та інвестування коштів у бізнес-проекти.

Розв’язання цих задач може бути здійснено методами машинного навчання, що реалізують бінарну класифікацію об’єктів. Розглянемо процедуру видачі споживчого кредиту. Клієнт банку, який бажає отримати кредит, повинен надати до установи велику кількість різних документів, посвідчень, довідок тощо. Кожен з документів містить статистичну інформацію, що певним чином характеризує даного клієнта (вік, безперервний стаж роботи на останньому місці роботи, заробітна плата, соціальний рівень, умови проживання тощо). Після надання всієї необхідної інформації, необхідні документи потрібно проаналізувати й видати вердикт стосовно кожного клієнта. Очевидно, що ймовірність прийняття правильного рішення щодо можливості видачі кредиту можна

суттєво підвищити, якщо під час аналізу використовувати інформацію про видання і повернення аналогічних кредитів у минулі періоди.

Одним з методів бінарної класифікації є логістична регресія.

Розглянемо множину пар (x_i, y_i), $i = \overline{1,m}$, де $x_i \in \mathbb{R}^n$ – вектор параметрів i-го об'єкта, $y_i \in \{-1;+1\}$ – його ознака. У задачі кредитування такими об'єктами будуть попередні клієнти зі своїми характеристиками, термін кредитування яких уже завершений і про яких відомо, що вони повернули (+1) або не повернули (–1) кредит. Алгоритм бінарної класифікації матиме вигляд:

$$a(x, w) = sign\left(\sum_{j=1}^{n} w_j x_j\right) = sign\langle x, w\rangle,$$

де w_j – ваги, що підлягають визначенню. Задача навчання лінійного класифікатора полягає у визначенні ваг w_j, $j = \overline{1,n}$, за заданою вибіркою (x_i, y_i), $i = \overline{1,m}$. Для цього необхідно розв'язати задачу мінімізації емпіричної функції похибок

$$Q(w) = \sum_{i=1}^{m} \ln(1 + e^{-\langle x_i, w\rangle y_i}) \to \min_{w_j, j=\overline{1,n}}.$$

Побудований таким чином лінійний класифікатор дозволяє робити висновки щодо можливості видачі кредиту будь-якому новому клієнту, що описується вектором параметрів x, та оцінювати ймовірність повернення чи неповернення їм цього кредиту $\mathrm{P}\{y \mid x\} = \dfrac{1}{1 + e^{-y\langle x, w\rangle}}$.

Ця ймовірність буде коливатися від 0 до 1 і чим вона вище, тим більша ймовірність того, що гроші будуть повернені до банку. У залежності від ймовірності, розрахованої за допомогою алгоритму, співробітник банку зможе висунути рішення стосовно клієнта. У залежності від банку можна буде встановити різні порогові значення, починаючи з яких співробітникам буде дозволятися надавати кредитні послуги банку.

Таким чином, завдяки такій модифікації банківської системи, можна буде оптимізувати робочий процес всередині банку, зменшити час, необхідний на обробку даних, та мінімізувати можливі втрати через те, що клієнти не повертають гроші до банку.

Список джерел:

1. Айвазян С.А., Бухштабер В.М., Енюков И.С., Мешалкин Л.Д. Прикладная статистика: классификация и снижение размерности. – М.: Финансы и статистика, 1989. – 607 с.

2. Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных. – М.: ДМК Пресс. – 400 с.

ДОСЛІДЖЕННЯ РЕЗУЛЬТАТІВ ЗОВНІШНЬОГО НЕЗАЛЕЖНОГО ОЦІНЮВАННЯ МЕТОДОМ КОМПОНЕНТНОГО АНАЛІЗУ

Малищак Т.О.
Науковий керівник – к.т.н., доц. Гибкіна Н.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Прикладної математики,
тел. (057) 702-14-36)
e-mail: tetiana.malyshchak@nure.ua

In a modern world it is preferable for everyone to have higher education. Therefore, it would be good for universities to know about schoolchildren's' preferences in choosing the future profession. This requires an assessment of the quality of the secondary education. It's quite a difficult task but possible. Modern computer systems allow us to operate by huge amount of data. So in the context of our We can research data about schoolchildrens' desirable carrier path in order to find the way that will help us to agitate them to enter the particular university or college.

Оцінювання якості середньої освіти все більш стає актуальним для нашої країни, адже кожного року тисячі школярів обирають свій шлях у майбутнє. Для випускників постає складна задача вибору: які предмети складати та де отримувати вищу освіту, а заклади вищої освіти, у свою чергу, мають планувати агітаційну роботу з урахуванням рівня та особливостей середньої освіти у регіонах за профільними предметами.

Аналіз результатів ЗНО дає можливість зробити висновки про якість навчання у різних регіонах України, побудувати картину розподілу областей за гуманітарними та технічними напрямами. Проаналізувавши дану інформацію, заклади вищої освіти зможуть зкорегувати свої дії стосовно абітурієнтів, правильно розгорнути свою агітаційну компанію для збільшення кількості абітурієнтів, бажаючих вступити до даного закладу, і мінімізувати кошти, що витрачаються на проведення самої агітації. Також, це певним чином зможе підвищити якість підготовленості абітурієнтів, бо агітувати їх будуть з тих областей, де буде більша кількість необхідних даному закладу вищої освіти абітурієнтів певного технічного чи гуманітарного напряму.

Задача аналізу результатів ЗНО пов’язана з обробкою великих масивів даних як за кількістю предметів, так і за кількістю областей, тому для статичної обробки можна використовувати методи аналізу даних, зокрема, метод головних компонент. Він є ефективним методом зниження розмірності, який дозволяє наочно подати данні у двовимірній площині та стиснути обсяг наявної інформації, що аналізується, без видимих втрат інформативності.

У якості вихідних параметрів були взяті статистичні данні з офіційного сайту ЗНО в Україні для 2017 року з предметів за областями [1]. У роботі було проведено аналіз відсотку людей у кожній області

України, що обирали для складання наступні предмети: історія України, математика, англійська мова, німецька мова, французька мова, іспанська мова, географія, біологія, фізика, хімія. Методом компонентного аналізу було обчислено власні вектори за головними компонентами. Відповідно до них, було побудовано значення перших двох головних компонент:

$$y_1 = -0,446x_1 + 0,431x_2 + 0,402x_3 - 0,201x_4 - 0,233x_5 +$$
$$+0,111x_6 - 0,338x_7 - 0,194x_8 + 0,432x_9 + 0,086x_{10};$$
$$y_2 = -0,181x_1 - 0,221x_2 + 0,341x_3 + 0,472x_4 + 0,317x_5 +$$
$$+0,389x_6 + 0,065x_7 - 0,505x_8 - 0,123x_9 - 0,230x_{10}.$$

На рисунку 1 наведено отримане методом головних компонент взаємне розташування областей України відповідно до вибору предметів ЗНО у 2017 році. Як видно з розрахунків, на формування першої компоненти найбільший вплив мають відсотки вибору предметів, що відповідають історії України, математиці, англійській мові та фізиці, а на другу – німецькій мові та біології.

Отримані данні дають змогу аналізувати переваги абітурієнтів за областями України з вибору майбутнього напряму професійної діяльності і робити попередні висновки про вибір подальшого профілю навчання.

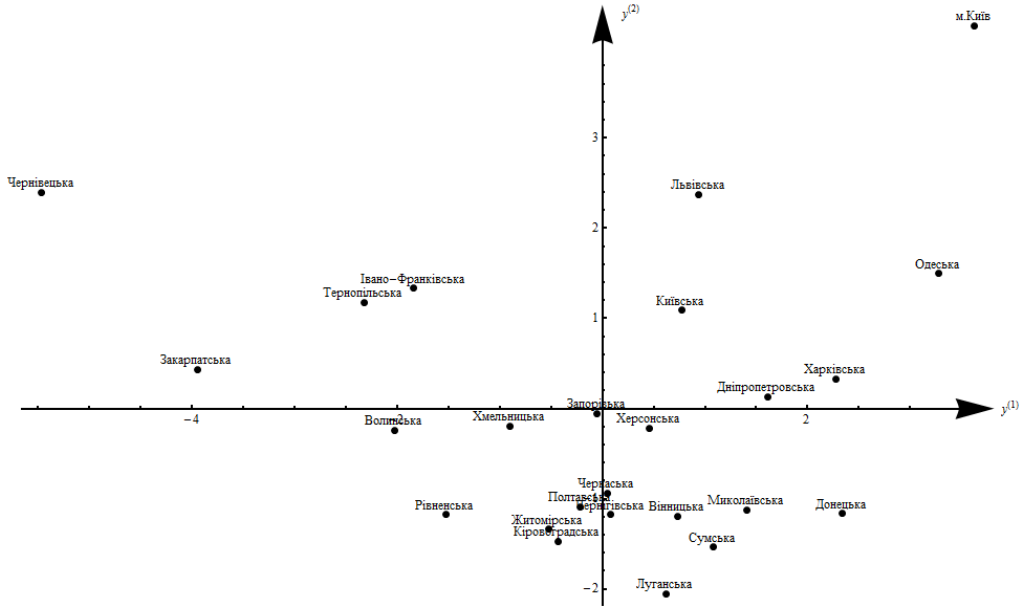


Рисунок 1 – Розташування областей України за результатами ЗНО у 2017 р.

Література:

1. Офіційні звіти/Український центр оцінювання якості освіти [Електронний ресурс]. – Режим доступу: http://testportal.gov.ua/ofzvit/.

2. Айвазян С.А., Енюков И.С., Мешалкин Л.Д. Прикладная статистика и основы эконометрики. – М.: Статистика, 1998. – 1006 с.

3. С.А. Айвазян,В.М. Бухштабер, И.С. Енюков, Л.Д. Мешалкин. Прикладная статистика: Классификация и снижение размерности. – М.: Финансы и статистика, 1989. – 607с.

FEATURES OF CONTROLLED TRAINING OF ARTIFICIAL NEURAL NETWORKS

Okhmak Valeriia
Scientific supervisor—Dr. Techn. Sc., Prof. Yamnenko J.S.
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
(Industrial Electronics Department, 37, Peremohy ave., Kyiv, Tel. (+38 044) 236-21-17)
e-mail: valeriiaokhmak@gmail.com; Tel (067) 59-171-84

This article describes the main features of the neural nervous system, that is about working with them. Principles of organization and processing of information in the management of neural networks. This approach allows you to analyze the main directions of further development and the key issues that need to be addressed in order to improve the performance of such systems in order to make it more effective.

Artificial neural networks are the object of development of advanced control systems and interactive tasks of artificial intelligence. They are models of the neural structure of the brain that can perceive, process, store and generate information. The main feature of the brain is the ability to learn and improve the results of their work as a result of self-improvement. Recurrent systems based on artificial intelligence systems allow you to successfully solve image recognition problems, generate forecasts, implement associative memory enhancements and, in particular, management.

Neural Networks, as an analogue of the biological brain, are original in the ability to learn by the examples that make up the training set. Neural network learning process is considered as configuration of architecture and weight coefficients of synaptic connections in accordance with the data of the training set for effective solution of the task. Training can be:

- Controlled (training with teacher)
- Uncontrolled (training without a teacher)

Some researchers believe that a system with a teacher based on their work can not be a prototype, albeit artificial, neural network. Therefore, it is important to have a detailed study of the peculiarities of such a controlled approach to work with information and the future development of use in artificial intelligence systems. Although most of the implemented neural networks use controlled learning. The main idea is to compare the running output with the desired output. The network initialization is set randomly, and during the next iterations, adjustments are made to achieve maximum correspondence between the desired and running output. The main task of such methods is to minimize running errors caused by the continuous change of synaptic weights to achieve the accepted accuracy of the network.

Before use, the neural network must be trained. The training may be rather long, and it is considered complete when the user-defined level of efficiency and desired statistical accuracy is attained. After which the weight coefficients of the

connections are fixed. There are networks that allow you to continue learning while using, which allows the network to adapt to the conditions of use.

Typically, training sets are gigantic to contain all the information you need to identify relationships and features. The weighting factors for one example are changed for the following. When learning the following examples, the previous ones are simply forgotten. The system should learn all together, looking for the best weighting factors for a large number of examples. The principle of controlled learning is depicted in Figure1.

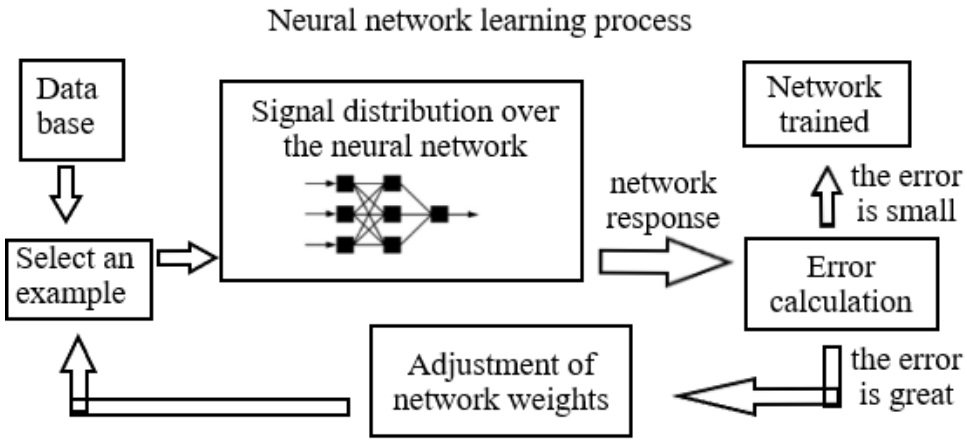


Figure 1. – Illustration of the training process of NN

No less important is the encoding and presentation of input and output data. Artificial neural networks work only with numerical input data, that is, data coming from the environment must be transformed. All values must be brought to the same range, that is, normalized. This transformation is performed by dividing each component of the input vector into a vector length, which converts the input signal into a single one. These data are common and easily accessible for standard computers.

If the neural network effectively processes the data of the training set after the training, it is checked whether it can be suitable for working with data that was not used for training. In case of unsatisfactory results the training continues. Testing is necessary to ensure stable work with data, not just the training set.

References:

1. Artificial Neural Networks. [Electronic resource]. – Access mode: https://neuronus.com/theory/nn/238-obucheniya-nejronnoi-seti.html

2. Neural Network Training. [Electronic resource]. – Access mode: https://studfiles.net/preview/5740125/

3. Rumelhart D.E. Learning internal representation by error propagation. In Parallel distributed processing/ Rumelhart D.E., Hinton G.E., Williams R. // Data Science Guide – 1986. – Vol. 1 – pp. 310–328.

ГЕНЕРАЦІЯ СХЕМ РОЗПІЗНАВАННЯ ДИСКРЕТНИХ ОБ‘ЄКТІВ НА ОСНОВІ АПРОКСИМАЦІЇ НАВЧАЮЧОЇ ВИБІРКИ

Пастор Н.Е., Повхан І.Ф.
Науковий керівник – к.т.н., доц. Повхан І.Ф.
ДВНЗ “Ужгородський національний університет”
(88000, Ужгород, вул. Заньковецької 89Б, каф. ПЗС, тел. (068)-555-44-59)
e-mail: f-it@uzhnu.edu.ua тел. +38 (0312) 65-52-50

One of the most important requirements that are superimposed on the standard language for solving a complex problem is the condition that the final algorithm (scheme) for solving a complex problem is quite simple and efficiently constructed with local algorithms. Practice has shown that the most effective means of automatic design of recognition systems of discrete objects that meet this requirement is to create a software system that uses for the design of recognition systems, the method of mathematical modeling. The main idea of functioning of the designed model of recognition system is the implementation of an interactive procedure, which provides by successive approximations the generation of the system, the efficiency of which, in principle, is quite close to the potentially achievable. This work is devoted to this problem.

На відміну від існуючих методів, головною особливістю систем розпізнавання (які базуються на основі дерев класифікації) є те, що важливість окремих ознак (групи ознак) визначається відносно функції, яка задає розбиття об‘єктів на класи. Причому слід пам‘ятати, числова величина вказаної важливості характеризує собою помилку розподілу об‘єктів на класи [1,2]. Нехай на першому кроці побудови дерева розпізнавання використовується довільний алгоритм розпізнавання, в результаті застосування якого отримуємо деяку формулу (узагальнену ознаку). Дана формула реалізує визначений рівень розпізнавання. Вона приймає декілька значень в залежності від значень ознак. Дані значення характеризують собою шляхи (класи), причому є шляхи, по яких формула “працює добре“, а є і такі, по яких – “погано” і покращення рівня розпізнавання далі немає. Зрозуміло, що саме на цих значеннях ознак (шляхах) необхідно взяти інший алгоритм, який створить іншу формулу (узагальнену ознаку) і т.д. Отже в методах та алгоритмах на основі дерев необхідно до тих пір повторювати такий вибір алгоритмів, доки ми не отримуємо необхідний рівень якості розпізнавання [3,4].

Особливість дерев класифікації, полягає в тому, що для того, щоб побудувати економічну загальну схему розпізнавання, необхідно використовувати лише “найкращі” ознаки [5]. Так, поклавши в основу метод дерева класифікації та принцип модульності, в Ужгородському національному університеті був розроблений програмний комплекс “Оріон ІІІ” для генерації автономних систем розпізнавання, базовою задачею для

якого було конструювання автономної системи розпізнавання на основі геологічних даних (задача про розділення нафтоносних пластів).

Для розпізнавання об‘єктів використовувалися система з 22 елементарних ознак, в даному випадку навчаюча вибірка складалася з 1250 об‘єктів (з них нафтоносні 756 об‘єктів), причому ефективність сконструйованої системи розпізнавання оцінювалася на тестовій виборці об‘єму 240 об‘єктів. Дані навчаючих та тестових вибірок отримані на основі геологічної розвідки на території Закарпатської області в період з 2001 року по 2011 рік. В якості фіксованого алгоритму використовувався метод апроксимації навчаючої вибірки на основі гіперкуль (результуюча кількість узагальнених ознак склала 18 на 756 об‘єктів класу розпізнавання). Відмітимо лише, що якщо оцінювати ефективність (відносно стиснення – описання даних навчаючої вибірки) сконструйованої схеми системи розпізнавання дискретних об‘єктів за формулою $\rho = 100\% - (\frac{кількість \text{ узагальнених ознак}}{кількість \text{ об`єктів НВ}} \cdot 100\%)$, то вона склала $\approx 92.32\%$.

Зауважимо, що побудова даної системи розпізнавання було проведено на двох різних конфігураціях (*Conf №1* Intel I5 8500/ Ram 8GB; *Conf №2* AMD FX8370 / Ram 16GB), і весь процес зайняв відповідно 128 с. та 106 с., що в значній мірі пояснюється підвищенням частотами процесора, швидкості дискової підсистеми та асемблерною оптимізацією.

Список джерел:

1. Повхан І.Ф. Проблема оцінки складності логічних дерев розпізнавання та загальний метод їх оптимізації / Ф.Г. Ващук, Ю.А. Василенко, І.Ф. Повхан // Науково технічний журнал “European Journal of Enterprise Technologies”. – 2011. – 6/4(54). – С. 24-28.

2. Повхан І.Ф. Загальна оцінка мінімізації деревоподібних логічних структур / Ф.Г. Ващук, Ю.А. Василенко, І.Ф. Повхан // Науково технічний журнал “European Journal of Enterprise Technologies”. – 2012. – 1/4(55). – С. 29-33.

3. Повхан, І.Ф. Мінімізація логічних деревоподібних структур в задачах розпізнавання образів / І.Ф. Повхан, Ю.А. Василенко, Е.Ю Василенко, М.Й. Ковач, О.Д. Нікарович // Науково технічний журнал “European Journal of Enterprise Technologies”. – 2004. – 3[9]. – С. 12-16.

4. Повхан І.Ф. Концептуальна основа систем розпізнавання образів на основі метода розгалуженого вибору ознак / Повхан І.Ф., Василенко Ю.А., Василенко Е.Ю. // Науково технічний журнал “European Journal of Enterprise Technologies”. – 2004. – №7[1]. – С. 13-15.

5. Povhan I. Designing of recognition system of discrete objects / Povhan I.F. // 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, pp. 226-231, 2016.

МЕТОДИ ТА ЗАСОБИ ОБРОБКИ ДАНИХ У ГЕТЕРОКОМПОНЕНТНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

SPECIFIC FEATURES OF FANET OPERATION WITH SEPARATE RESERVATION IN MODE OF AN INTEGRAL MULTIPLE RESERVE

[1]Karasiov A.O., [1]Kosherdan O. E., [2] Volotka V.S.
Research supervisor – Ph.D., Senior Lecturer Tkachov V.M.
Kharkiv National University of Radio Electronics
[1](61166, Kharkiv, Nauky Ave. 14, Department of Electronic Computers, tel. (057) 702-13-54)
[2](61166, Kharkiv, Nauky Ave. 14, Department of Infocommunication Engineering, tel. (057) 702-13-20)
e-mail: [1]d_ec@nure.ua, [2]d_ts@nure.ua

In the given paper, a method of increasing the reliability of FANET by applying an integral multiple reserve is considered. The mathematical apparatus is given and the mean time between system failures is determined.

The task of ensuring a high level of reliability in FANETs is quite widely described in a number of papers [1-4]. Let us consider the model of FANET operation, in which the separate reservation is performed in an integral multiple reserve mode. The calculation and logic scheme for this type of reservation is presented in Fig. 1

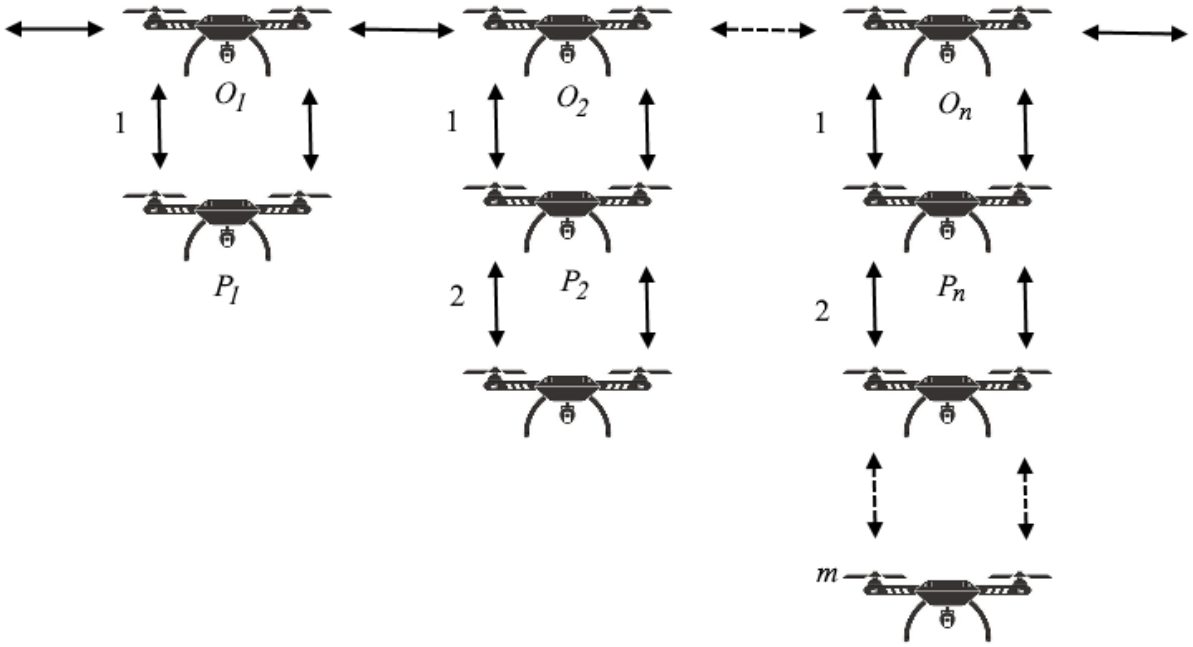


Figure 1 – Separate reservation with permanently enabled reservation

With separate reservation, each element of the main chain O_i has its own backup elements P_i and, respectively, its multiplicity of the reservation m_i (Figure 1). In a particular case, the multiplicity of reservation may be the same for all primary nodes of the FANET. Thus, in the case of loaded reserve when calculating the reliability of such reserved FANETs, it is possible to use the

mechanism described in [5] for the main elements of the chain, and then using the mechanism of partially enabled reservation.

Given the above mentioned, the probability of failure-free FANET operation with separate reservation will be defined as:

$$P_{TC}(t) = \prod_{i=1}^{n} \left\{ 1 - \left[1 - P_i(t) \right]^{m_i+1} \right\}.$$

Under the exponential distribution, it will be equal to:

$$P_{TC}(t) = \prod_{i=1}^{n} \left\{ 1 - \left[1 - e^{-\lambda_0 t} \right]^{m_i+1} \right\}.$$

In a separate case, with equal reliability of the primary and backup nodes and with the same multiplicity of reservation, we obtain:

$$P_{TC}(t) = \left\{ 1 - \left[1 - e^{-\lambda_0 t} \right]^{m_i+1} \right\}^{n}.$$

In addition, the mean time between system failures will be determined from the following formula:

$$T_{TCcp} = \int_0^{\infty} P_{TC}(t)dt = \frac{(n-1)!}{\lambda(m+1)} \sum_{i=0}^{m} \frac{1}{v_i(v_i+1)...(v_i+n+1)},$$

where $v_i = \dfrac{i+1}{m+1}$.

However, this approach to ensuring the reliability requires experimental research to identify the optimal probabilistic models of FANET operation with permanently enabled reservation.

References:

1. Ткачов В.М. Підвищення живучості мережної складової рою БПЛА / В.М. Ткачов, Д.Є. Мітін, Я.В. Дух // Комп'ютерні інтелектуальні системи та мережі. Матеріали XI Всеукраїнської науково практичної WEB конференції аспірантів, студентів та молодих вчених (21-23 березня 2018 р.). – Кривий Ріг: ДВНЗ «Криворізький національний університет», 2018. – С. 98-100.

2. Churyumov G.I. Method for Ensuring Survivability of Flying Ad-hoc Network Based on Structural and Functional Reconfiguration / G.I. Churyumov, V.M. Tkachov, V.V. Tokarev, V.O. Diachenko // Информационные технологии и безопасность. Материалы XVIII Международной научно-практической конференции ИТБ-2018. – ИПРИ НАНУ, 2018. – 145-159 с.

3. Ткачов В.М. Проблема передачі даних типу Big Data у мобільній системі «мультикоптер-сенсорна система» / В.М. Ткачов, В.В. Токарєв, В.О. Радченко, В.О. Лебедєв // Системи управління, навігації та зв'язку. – Полтава: Полтавський національний технічний університет ім. Ю. Кондратюка, 2017. – № 2 (42). – С. 154-157.

4. Tkachov V.M. Problems of reliability in creating complex infocommunication systems / V.M. Tkachov, V.S. Volotka // Шоста міжнародна науково-технічна конференція «Проблеми інформатизації». – Черкаси-Баку-Бельсько-Бяла-Харків. – 14-16 листопада 2018 р. – С. 27.

ОСОБЛИВОСТІ ПОБУДОВИ ХМАРНИХ БРАНДМАУЕР-СИСТЕМ ЗАХИСТУ ВЕБ-РЕСУРСІВ

Гунько М.А.
Науковий керівник – к.т.н., ст. викл. Ткачов В.М.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. ЕОМ, тел. (057) 702-13-54)
e-mail: d_ec@nure.ua

Existing cloud firewall systems for protecting web resources are analyzed in this paper. The conclusions are formulated regarding the features of the cloud firewall systems construction. A new solution that allows you to optimize access to web resources by minimizing delayed response is suggested. The solution is based on the principle of sorting IP addresses by geographic features.

Сучасні інфраструктурні рішення побудови веб-ресурсів засновані на принципах віртуалізації та застосування хмарних технологій. Важливим питанням забезпечення надійності функціонування веб-ресурсів є застосування підсистеми захисту від несанкціонованого доступу, різного роду мережних атак тощо. Однією з таких підсистем є хмарна брандмауер-система.

В даній роботі розглядається принцип побудови хмарної брандмауер-системи на прикладі системи мережного захисту інфраструктурних рішень компанії Amazon [1]. Згідно запропонованої моделі функціонування [1], запит до веб-ресурсу надходить через ряд проміжних вузлів, поєднаних між собою за допомогою хмарних технологій. Тобто хмарний брандмауер представлений сукупністю віртуальних машин, які, як правило, є монотипними та виконують функції сортування та відсіювання трафіку, який генерується сукупністю користувачів. При цьому частина брандмауер-системи, що виконує функції оркестратора хмари координує шляхи (маршрути) проходження запитів до веб-ресурсу всередині, власне, хмари. У разі виходу з ладу віртуального частини брандмауер-системи, координатор хмари приймає рішення клонування віртуальної машини в критичну точку. Важливо зауважити, що така хмарна інфраструктура є збитковою, а кількість віртуальних вузлів дещо більша за ту, яка може обробити запити від всіх користувачів, що можуть максимально завантажити вхідний канал зв’язку [2, 3].

Пропонується розробити віртуальну систему сортування, яка буде частиною хмарної брандмауер-системи. До спектру її задач належить задача сортування трафіку, що надходить до хмари в залежності від інтенсивності надходження запитів з однієї IP-адреси. Також віртуальна система сортування повинна ідентифікувати IP-адресу вузла запиту відносно географічного місцерозташування даного вузла. Після проходження через віртуальну систему сортування, кожен запит, в

залежності від вищевказаних критеріїв, проходить декілька етапів перевірки.

Наприклад, якщо запит виконано зі Сполучених Штатів Америки (США) віртуальна система відправить його до серверу в найкоротший час. Це пояснюється тим, що з США, згідно стастистичних даних безпечності IP-адрес, найчастіше надходить безпечний трафік. В противагу – якщо трафік йде з IP-адрес з низькою репутацією, то перевірка та обробка запиту буде значно довшою, бо віртуальна система сортування ідентифікує IP-адресу як небезпечну (тобто, може завдати шкоди) та відправить команду хмарному брандмауеру задіяти усі ступені перевірки.

Окремо можна вирізнити системи блокування в хмарному брандмауері IP-адрес анонімних проксі-вузлів, VPN-каналів та сегментів Інтернету, що класифікуються як DarkNet. Тобто запити з таких вузлів будуть автоматично блокуватися без подальшої обробки, що знижує завантаженість на хмарний брандмауер. Як виключення можуть бути блоки IP-адрес, які не ідентифікуються за географічною ознакою (наприклад, IP-адрес супутникових операторів Інтернет-послуг, як то Iridium, Thuraya тощо).

Таким чином, в даній роботі розглянуто приклади побудови хмарних брандмауер-систем захисту веб-ресурсів та запропоноване рішення, що дозволяє оптимізувати доступ до веб-ресурсів з мінімізацією затримки відклику на базу сортування IP-адрес за географічними ознаками.

Подальший напрям дослідження полягає у розробці прототипу програмної системи даного рішення.

Робота виконана на базі науково-навчальної лабораторії Реконфігурованих і мобільних систем кафедри Електронних обчислювальних машин ХНУРЕ.

Список джерел:

1. Ryan J. S., Stevenson J., Nahhas B. Cloud-based multi-layer security architecture with hub and spoke development environment : пат. 9419857 США. – 2016.

2. Ткачев В.Н. Особенности использования облачного оркестратора при построении систем сетевого мониторинга / В.Н. Ткачев, В.О. Лебедев // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали сьомої міжнародної науково-технічної конференції. – Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ДП «ХНДІ ТМ», 2017. – С. 16.

3. Tkachov V.M. Problems of reliability in creating complex infocommunication systems / V.M. Tkachov, V.S. Volotka // Шоста міжнародна науково-технічна конференція «Проблеми інформатизації». – Черкаси-Баку-Бельсько-Бяла-Харків. – 14-16 листопада 2018 р. – С. 27.

АНАЛІЗ АЛГОРИТМІВ СТІЙКОЇ КЛАСТЕРИЗАЦІЇ

Носик К.А., Сумцова А.Д.
Науковий керівник – к.т.н., с.н.с. Носик А.М.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. ЕОМ, тел. (057) 702-13-54)
e-mail: kateryna.nosyk@nure.ua, sumtsova.anna@gmail.com

This work considers issues of the cluster analysis. The principles of the construction of clustering algorithms were analyzed here. The given analysis allows us to identify the strengths and weaknesses of their application. In the framework of these studies, sustainable clustering algorithms were analyzed. Research and testing of algorithms on real data made it possible to evaluate their advantages and disadvantages and formulated recommendations for building new algorithms with specified properties.

Кластеризація - це розбиття множини об'єктів на деякі однорідні підмножини (кластери), параметри яких спочатку невідомі. Для конкретного завдання кількість кластерів може бути довільною або фіксованою. Для кластера характерні внутрішня однорідність (об'єкти одного класу схожі між собою за певними ознаками) і зовнішня ізольованість (об'єкти різних класів суттєво відрізняються).

До складнощів кластерного аналізу відносяться:

- вибір досить ефективного для вирішення певної задачі методу кластеризації вимагає достатнього знання алгоритмів і умов їх застосування;
- вибір характеристик, на підставі яких проводиться кластеризація: метрики, початкових значень центрів, умов зупинки алгоритму;
- вибір початкового числа кластерів;
- інтерпретація результатів кластеризації.

Алгоритми кластеризації зазвичай діляться на два види: ієрархічні і неієрархічні.

Принцип роботи ієрархічних алгоритмів полягає в послідовному об'єднанні маленьких кластерів в великі або навпаки поділі великих кластерів на маленькі. До переваг цієї групи методів можна віднести їх наочність і можливість отримати детальне уявлення про структуру даних. До недоліків - негнучкість отриманих класифікацій, обмеження обсягу аналізованих даних, а також те, що велика складність даних алгоритмів робить їх непридатними при значній кількості досліджуваних.

Неієрархічні методи засновані на поділі набору даних на певну кількість кластерів і виконанні ітеративного процесу оптимізації деякої цільової функції, яка визначає оптимальність (обумовлену особливостями алгоритму) даного розбиття множини об'єктів на кластери. До переваг цього типу методів можна віднести більш високу стійкість по відношенню до шумів, вибору метрики, додаванню груп незначущих об'єктів у вихідні

дані, що беруть участь в кластеризації. До недоліків – те, що заздалегідь необхідно визначити параметри кластеризації (кількість кластерів, а також кількість ітерацій або правило зупинки та інші параметри).

До найбільш поширених класів задач кластеризації відноситься визначення кількості кластерів, при відсутності припущень щодо їх числа та обсягу даних це не дозволяє скористатися ієрархічними методами. Одним із можливих шляхів вирішення цієї проблеми є проведення ряду експериментів з ітеративними алгоритмами для різної кількості кластерів.

В рамках цього завдання були досліджені алгоритми стійкої кластеризації. До основних підходів з дослідження стійких алгоритмів і визначення кількості кластерів в безлічі даних можна віднести [1]:

- оцінку щільності розподілів;
- індекси, що порівнюють ступені «розкиду» даних усередині кластерів і між кластерами;
- статистики, що визначають найбільш ймовірне рішення;
- розрахунок значень евристичних характеристик (функцій стійкості), що показують відповідність призначених кластерів для вибіркових елементів множини.

У роботі в якості засобів аналізу роботи алгоритмів стійкою кластеризації розглядалися наступні індексні методи: Calinski-Harabasz, Hartigan і Krzanowski та Lai [2-4].

Дослідження і апробація існуючих алгоритмів на реальних даних дозволила оцінити їх переваги та недоліки. Головним недоліком даних методів є зростаюча обчислювальна складність, що залежить як від збільшення числа кластерів так і від збільшення числа об'єктів входять в дані. До переваг можна віднести те, що дані методи оптимізації добре описані математично, що так само дозволить розробити нові методи з заданими властивостями.

Список джерел:

1. Шалымов Д.С. Алгоритмы устойчивой кластеризации на основе индексных функций и функций устойчивости // Стохастическая оптимизация в информатике, 2008, №4, - С. 236–248.

2. Calinski R. B., Harabasz J. A dendrite method for cluster analysis // Communications in Statistics. 3. – 1974. – pp. 1–27.

3. Kaufman L., Rousseeuw P. Finding Groups in Data: An Introduction to Cluster Analysis. — Hoboken, N.J. : Wiley,. – 2005. – 342 p.

4. Hartigan J. A. Clustering Algorithms. — Wiley. –1975. – 369 p.

ГЕНЕРАТОР БОЛЬШИХ СЕТЕВЫХ СИСТЕМ

Пономаренко О.Е., Коткова О.Н., Абдулрахман Котаеба Батиаа
Научный руководитель – к.т.н., проф. Горбачев В.А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Электронных вычислительных машин,
тел. (057) 702-13-54)
e-mail: valeriy.gorbachov@nure.ua, olha.ponomarenko@nure.ua

The work is devoted to the problem of analyzing large network systems, among which. Existing methods and approaches to solving traditional problems of networks of smaller scales are unsuitable for large-scale networks. When analyzing and evaluating the performance of such systems, the problem of generating a large-scale network structure is relevant.

The paper proposes to develop a generator of a network structure based on the initial characteristics such as the number of elements of the system, connections between them and the values of channel capacities. The generator is implemented in the Java programming language.

Множество систем, например, Интернет, социум, биологические системы, обладают общими свойствами и относятся к классу сложных систем. Такие системы характеризуются большой размерностью и вычислительной сложностью [1]. Данная работа посвящена анализу больших систем с сетевой структурой. Целью работы является создание инструмента оценки показателей эффективности таких систем.

Работа [2] посвящена исследованию безмасштабных сетей (scale-free network), которые содержат важные узлы или хабы. Эти сети характеризуются большим количеством других узлов, являются стойкими к случайным отказам, но уязвимы к управляемым атакам. Данная модель предполагает, что число вершин известно заранее, до соединения узлов дугами.

Анализу важного класса случайных сетей посвящена работа [3]. Сущность заключается в том, что узлы сети соединяются друг с другом случайным образом, поэтому большинство узлов имеет приблизительно одинаковое число связей. В таких сетях очень редко можно встретить узел, число связей которого намного меньше или намного больше чем среднее значение.

Для больших систем с сетевой структурой характерным является такой процесс как «преимущественное присоединение» (preferential attachment), который заключается в том, что если у узла есть много связей, то скорее всего к нему будет присоединен новый узел. Таким образом, выделяют два механизма, которые объясняют существование хабов: рост и преимущественное присоединение. В процессе функционирования, новый узел, который появляется в системе, имеет тенденцию соединяться с узлом, который имеет наибольшее количество связей. В результате чего с

течением времени такой узел – хаб – приобретает все больше связей в отличие от других узлов.

В работе [4] рассматривается метод, который уменьшает размерность и вычислительную сложность больших систем. Предложенная технология была протестирована на небольших системах.

Исследуемые системы имеют сложную структуру и большую размерность, в следствие чего процесс создания, обработки и анализа тестовых примеров вручную затрудняется. Решением этой проблемы является создание генератора структур системы.

Генератор структур систем реализован на языке программирования Java. Генерация осуществляется в несколько этапов. На первом этапе создается граф, входными данными является количество вершин. Так как осуществляется работа с графом, который представляет соединение элементов в системе, учитываются некоторые ограничения, такие как минимальное количество входящих и исходящих дуг, возможность соединения определенных вершин графа. Учитывая данные особенности структуры системы, осуществляется формирование матрицы графа. Алгоритм заключается в обходе строк и столбцов матрицы и соединении вершин графа дугами с помощью генерации случайных чисел. На втором этапе осуществляется преобразование графа в систему. Алгоритм заключается в последовательном анализе дуг графа. Для каждой вершины графа, из которой выходит дуга, и вершины, в которую дуга входит, создается элемент системы, если такой не был создан ранее. В ходе перебора дуг создаются входные и выходные контакты элементов системы. Также учитываются случаи, когда из одного выходного контакта системы исходит несколько связей. Таким образом, формируются соединения элементов системы. Выходными данными программы является таблица сопряжения элементов в системе.

Таким образом, был получен генератор структур системы, который в комплексе с ранее разработанной технологией позволяет анализировать системы с большой размерностью.

1 Mark Newman, Networks: An Introduction, Oxford University Press, 2010.

2 A. Barabási and E. Bonabeau, «Scale-Free Networks», Scientific American, vol. 288, no. 5, 2003, pp. 60-69.

3 P. Erdös, A. Rényi, «On random graphs», I Publicationes Mathematicae, Debrecen, Vol. 6, 1959, pp. 290-297.

4 V. Gorbachov, Abdulrahman Kataeba Batiaa, O. Ponomarenko, Y. Romanenkov. Formal transformations of stuctural models of complex network systems. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies «DESSERT’2018». Conference proceedings. – Kyiv: 2018, pp. 473-477.

ПОРІВНЯННЯ ПРОДУКТИВНОСТІ ПОСЛІДОВНИХ І ПАРАЛЕЛЬНИХ АЛГОРИТМІВ СОРТУВАННЯ НА МОВІ С++

Риндик І.В.
Науковий керівник– к.т.н. Барковська О.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Електронних обчислювальних машин, тел. (057) 702-13-54) e-mail: olesia.barkovska@nure.ua

The given work is devoted to the comparison of the most famous data sorting algorithms in parallel and sequence format, which are associated with a significant amount of computation and requires a solution in the shortest time, close to the real-time mode. This determines the relevance of high-performance processing of big arrays using C++ programming language. The technology used for parallelizing is OpenMP, that supports multi-platform shared memory multiprocessing programming. Research presents by comparison executable time five sorting algorithms in parallel and sequence form.

Алгоритми сортування масиву чисел – одні з найбільш важливих процесів, які використовуються у обчислювальній техніці, оскільки сортування та пошук є найбільш загальними складовими частинами систем програмування. Останнім часом інтерес до методів та засобів сортування великих масивів інформації зростає, що тісно пов’язано з новими досягненнями в області комп’ютерних технологій, а також з розширенням сфери застосування самих алгоритмів сортування. Часова складність алгоритмів сортування та обсяг пам’яті, що використовується для сортування, значно впливають на ефективність комп’ютерної обробки даних. Велике значення має масштабованість цих алгоритмів, можливість їх застосування для обробки великих даних (англ. Big Data), придатність для впорядкування складних інформаційних структур.

Ідея паралельної обробки даних як потужного резерву збільшення продуктивності обчислювальних апаратів була висловлена Чарльзом Беббіджем приблизно за сто років до появи першого електронного комп'ютера. Сучасні паралельні технології відрізняються одна від одної не скільки мовами програмування, стільки архітектурними підходами до побудови паралельних систем. Паралельні обчислення – одночасне використання кількох ресурсів ЕОМ для розв’язування обчислювальних задач:

– задача розбивається на підзадачі, які можуть виконуватися у один і той самий момент часу;

– кожна підзадача в свою чергу розбивається на послідовність інструкцій;

– інструкції кожної підзадачі виконуються одночасно на різних процесорах;

Реалізовано п’ять алгоритмів сортування: Шелла, швидке

сортування, сортування злиттям, бітонічне сортування та парне непарне. Паралельні версії виконані за допомогою відкритого стандарту для розпаралелювання програм – OpenMP. Виконаний порівняльний аналіз ефективності виконання алгоритмів на різних об'ємах даних, шляхом заміру часу виконання послідовної та паралельної версії алгоритму. Заміри проводилися на комп'ютері з процесором Intel Core i5-8250u 2.3 Ghz, up to 3.8 Ghz, з 4 ядрами та 8 потоками, з об'ємом ОЗП 8 Gb.

Таблиця 1 – Результати реалізації алгоритму швидкого сортування

Швидке сортування			
Розмір масиву	Послідовний час, с	Паралельний час, с	Прискорення
10 000	0,000621	0,005921	0,104880932
50 000	0,003443	0,002822	1,220056697
200 000	0,01505	0,011571	1,300665457
1 000 000	0,085064	0,067093	1,267852086
5 000 000	0,467472	0,305758	1,528895401
10 000 000	0,959759	0,62031	1,547224775
15 000 000	1,457437	0,908183	1,604783397
20 000 000	1,97628	1,149775	1,718840643
50 000 000	5,2510457	3,0543118	1,719223853
100 000 000	12,1529271	7,5818173	1,60290424
150 000 000	20,9432202	11,8453861	1,76804876
250 000 000	38,8624897	21,0903868	1,842663677

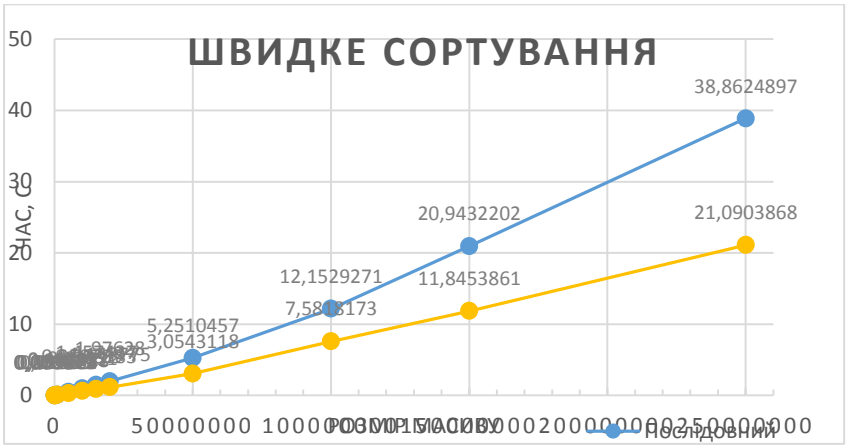


Рисунок 1 – Графік залежності швидкості виконання швидкого сортування від розміру масиву

За результатами аналізу, паралельна реалізація методів сортування є обґрунтованою. Найефективнішим є алгоритм швидкого сортування, реалізація якого на багатопроцесорній системі із загальною пам'яттю дає прискорення до 1.8 разів для великих обсягів вхідних даних (таблиця 1).

СРАВНЕНИЕ СКОРОСТИ ВЫЧИСЛИТЕЛЬНЫХ ОПЕРАЦИЙ С МАТРИЦАМИ БОЛЬШИХ РАЗМЕРОВ С ИСПОЛЬЗОВАНИЕМ РАЗНЫХ ТЕХНОЛОГИЙ ПРОГРАММИРОВАНИЯ ГРАФИЧЕСКОГО ПРОЦЕССОРА

Порошенко А.И.
Научный руководитель – к.т.н. Барковская О.Ю.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Электронных вычислительных машин, тел. (057) 702-13-54) e-mail: olesia.barkovska@nure.ua

The given work is devoted to comparing the performance of different technologies for GPU-programming: CUDA, PyCUDA and NumbaCUDA technologies by calculating the matrix multiplication of floating-point numbers on thousands of streaming processors. The use of these technologies has shown that CUDA is the fastest technology, but with proper experience with PyCUDA, the same results can be achieved. NumbaCUDA is the simplest technology in terms of use, but it loses more than 2 times in performance in comparing to other technologies.

С течением времени появляется все больше и больше технологий для выполнения вычислений на графическом процессоре. Хотя все они работают по одному и тому же принципу, их характеристики значительно отличаются. Платформа параллельных вычислений CUDA обеспечивает набор расширений для языков C и C++, позволяющих параллелизм данных на уровне мелких и крупных структурных единиц. Библиотека PyCUDA является расширением для языка Python, и, как и сам Python, является интерпретатором. Написание программы с использованием PyCUDA требует знаний языка C для программирования ядра CUDA. Пакет Numba дает возможность ускорить программы с помощью функций, написанных непосредственно на языке Python. Использование специальных аннотаций (декораторов с различными параметрами) при функциях позволяет компилировать код прямо во время исполнения (just-in-time) в машинные инструкции. Пакет создан компанией Anaconda, Inc. (ранее - Continuum Analytics). С некоторых пор Numba может взаимодействовать с CUDA - ядра CUDA и функции, выполняемые на устройстве GPU, могут быть откомпилированные с помощью декоратора @cuda.jit.

В качестве задачи для анализа производительности подходит умножение матриц чисел с плавающей точкой, так как при большой размерности матриц, является очень трудоемкой задачей и программную модель этой задачи легко сопоставить с аппаратной моделью графической карты. Самым нативным вариантом реализации будет вариант, когда каждый поток вычисляет один элемент результирующей матрицы, а сами матрицы представлены в виде двумерного массива.

Для эксперимента использовался ноутбук Dell Inspiron 15 7000 с графическим процессором Nvidia GeForce GTX 1060 With Max-Q Design,

центральным процессором Intel Core i5-7300HQ. Замерялось только время выполнения алгоритмов умножения, запись данных в память графического устройства и чтение из нее в результат не вошли. Замеры выполнялись для различных программных моделей, с использованием 64, 256 и 1024 потоков в блоке. Результаты работы программы с использованием CUDA приведены в таблице 1.

Таблица 1 – Время выполнения программы с использованием CUDA

Размерность матрицы	Время, мс		
	64 потока в блоке	256 потоков в блоке	1024 потока в блоке
256	1.673	1.102	1.938
512	2.053	2.054	3.198
1024	2.792	2.965	6.202
2048	3.741	3.199	10.931
4096	5.554	5.856	20.343

Результаты работы программы с использованием PyCUDA приведены в таблице 2.

Таблица 2 – Время выполнения программы с использованием PyCUDA

Размерность матрицы	Время, мс		
	64 потока в блоке	256 потоков в блоке	64 потока в блоке
256	0.999	0.809	0.634
512	1.863	1.544	1.338
1024	2.713	2.174	1.991
2048	4.773	4.672	4.175
4096	19.433	18.932	18.345

Результаты работы программы с использованием NumbaCUDA приведены в таблице 3.

Таблица 3 – Время выполнения программы с использованием NumbaCUDA

Размерность матрицы	Время, мс		
	64 потока в блоке	256 потоков в блоке	64 потока в блоке
256	0.709	0.679	0.734
512	1.270	1.349	1.538
1024	3.480	3.540	3.420
2048	11.100	11.169	11.189
4096	41.416	40.889	40.640

Таким образом, результаты тестирования показали, что CUDA является самой быстрой технологией, но при надлежащем опыте работы с PyCUDA можно достичь тех же результатов. NumbaCUDA является самой простой технологией с точки зрения использования, но по сравнению с другими технологиями она проигрывает в производительности более чем в 2 раза.

АНАЛІЗ РОБОТИ ПАРАЛЕЛЬНОГО ТА ПОСЛІДОВНОГО АЛГОРИТМІВ ПОШУКУ ТА ЗАМІНИ ЕЛЕМЕНТІВ У ТЕКСТОВОМУ РЕДАКТОРІ

Зайцева С.Г.
Науковий керівник - к.т.н Барковська О.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Електронних обчислювальних машин, тел. (057) 702-13-54) e-mail: olesia.barkovska@nure.ua

The object of the research is the development of a "Text Editor". As a result, a text editor was developed for working with text files. The main task of this work was to compare the speed of the “searching element’s” functions and “searching and replacement of elements” in a parallel and sequential algorithm of work. And as a result you can see that the “search and replace” operation is much faster than “searching element’s” function because of lack of graphic procedures using for the is time-consuming text highlighting.

Невід'ємною частиною роботи комп'ютера є "RTF текстовий редактор". Це програма, яка дозволяє проводити набір тексту, редагувати його, а також візуально оформлювати.

Текстові редактори призначені для роботи з текстовими файлами в інтерактивному режимі. Вони дозволяють переглядати вміст текстових файлів і здійснювати над ними різні дії - вставку, видалення і копіювання тексту, контекстний пошук і заміну тощо. Часто інтерактивні текстові редактори містять додаткову функціональність, покликану автоматизувати дії по редагуванню або відображають текстові дані спеціальним чином.

На сьогодні є сотні різноманітних текстових редакторів, і їхня кількість продовжує зростати. Функціональні можливості різних програм підготовки текстів істотно різняться, водночас більшість із них має багато спільних властивостей. Деякі текстові редактори мають розширені функції форматування тексту, впровадження в нього графіків, формул, таблиць та об'єктів. Такі редактори часто називають текстовими процесорами й призначені вони для створення різного роду документів — від особистих листів до офіційних паперів. Класичні приклади — Microsoft Word і Libre Office.

Основною задачею даної роботи було порівняння швидкості роботи функцій пошуку елементів та пошуку і заміни елементів при паралельному та послідовному алгоритмі роботи.

Для пошуку та заміни елементів використовувався алгоритм прямого пошуку, тобто порівнюэться *I*-й символ початкової строки з першим символом строки для пошуку; якщо вони співпадають, порівняння продовжується для наступних символів; якщо символи відрізняються, переходимо на наступний символ.

Алгоритм буде завершено, коли буде порівняно останній символ початкової строки.

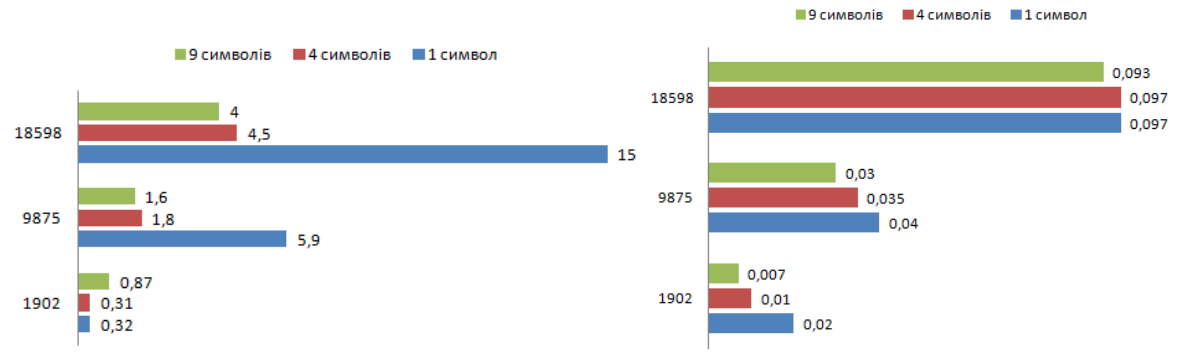
Для паралелізації даного алгоритму було використано інструменти мови C#: Parallel.For(...).

Клас Parallel також є частиною TPL і призначений для спрощення паралельного виконання коду. Parallel має ряд методів, які дозволяють распаралелити завдання.

Параметр Parallel.For працює над декількома потоками, і обробка відбувається паралельно. Цикл Parallel.For не є основною функцією C # і доступний з C # 4.0 і вище. Перед C # 4.0 ми не можемо його використовувати. Його виконання відбувається швидше, ніж у більшості випадків. Для використання циклу Parallel.For нам потрібно імпортувати System.Threading. Це директиви простору імен у використанні.

Тестування функції пошуку та пошуку і заміни елементів було проведено на різному наборі даних. Для початкового тексту було обрано три файли розміром 1, 5 та 10 сторінок. Також було обрано різних розмір слів для пошуку - 1, 4 та 10 символів у слові.

Підсумуємо результати виконання програми у нижче наведених графіках, де рисунок 1.а відображає час виконання функції пошуку елементів, рисунок 1.б - пошуку та заміни елементів.



а) б)

Рисунок 1 - а) діаграма результату пошуку елементів;
б) - діаграма результату пошуку та заміни елементів

Таким чином, було виявлено, що зі збільшенням розміру слова для пошуку, прямопропорційно зменшується час на його пошук по усьому тексту через використання більшої кількості ядер обчислювача. Такі самі результати були отримані для функції пошуку та заміни елементів. Також можна побачити, що функція пошуку та заміни елементів відбувалася значно швидше - це відбувається завдяки тому, що використовується зміна кольору тексту, а як відомо, будь-яка графічна операція займає значене більше часу аніж обчислювальна (заміна тексту) операція.

РАЗРАБОТКА УСКОРЕННОЙ СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ С ИСПОЛЬЗОВАНИЕМ РЕСУРСОВ ГРАФИЧЕСКОГО ПРОЦЕССОРА

Гомелев А.А.
Научный руководитель – к.т.н. Барковская О.Ю.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Электронных вычислительных машин, тел. (057) 702-13-54) e-mail: olesia.barkovska@nure.ua)

The given work is devoted to the development of the accelerated image processing program, which methods are associated with a significant amount of computation and requires a solution in the shortest time, close to the real-time mode. This determines the relevance of high performance processing of two-dimensional images. Common technologies are not appropriate for computation data using algorithms such as Viola-Jones' detection algorithm. However, the use of a graphics processor's resource in conjunction with the CUDA technology gives significant acceleration.

Класс задач с использованием цифровых изображений стремительно расширяется. Одним из направлений является регистрация и обработка двумерных изображений с целью извлечения информации об объектах, находящихся на нём. Обработка изображений сопряжена со значительным объёмом вычислений. Многие задачи обработки изображений необходимо решать в строго ограниченное время, так как конкретные данные могут извлекаться из видеопотока в реальном времени.

Компьютерное зрение – теория создания систем, которые могут проводить выявление, наблюдение и классификацию объектов. Исходные данные могут быть представлены в виде видеопотока, изображения с разных камер или трёхмерные данные сканеров, например данные медицинского сканера ультразвуковой диагностики.

Компьютерное зрение также может восприниматься как дополнение биологическому зрению. В биологии изучается зрительное восприятие человека, в результате создаются модели работы систем в терминах физиологических процессов. Компьютерное зрение изучает и описывает системы компьютерного зрения, выполненные аппаратно или программно. Междисциплинарный обмен между биологическим и компьютерным зрением оказался продуктивным для различных научных отраслей.

Такие задачи подразумевают большой объем обработки данных. Методы параллельных вычислений дают значительный прирост в скорости и производительности, однако не могут полностью реализовать свой потенциал при использовании обычных процессоров с небольшим количеством физических ядер и архитектурой MIMD. С другой стороны, в графических процессорах, основной блок – это мультипроцессор с восемью – десятью ядрами и сотнями ALU в целом, несколькими

тысячами регистров и определённым количеством разделяемой общей, глобальной, локальной, а также специальной памятью для констант. Эти несколько ядер являются SIMD ядрами. Ядра выполняют одни и те же инструкции одновременно. Такой подход позволяет увеличить количество исполнительных блоков за счет их упрощения.

Задачей работы является разработка компьютерной программы, цель которой – автоматический анализ зображений, полученных с камеры наблюдения с использованием технологий и методов параллельного программирования, а также заполнение списка присутствующих в аудитории людей. Сферой использования данной программы является регистрация присутствия студентов как на различных видах занятий в высших учебных заведениях, так и учет времени работы персонала различных компаний. Преподавателю понадобится меньше времени на выполнение организационной работы и больше времени становится доступным для подачи материала.

Способом анализа информации является алгоритм Виолы-Джонса на основе каскадов Хаара, реализованный посредством библиотеки OpenCV, инкапсулирующей технологию CUDA для различных языков программирования.

Исследование проводилось на графических картах NVIDIA GTX 720M и NVIDIA GTX 1060. Лица представлены в виде черно-белых изображений формата BMP размером 100 на 100 пикселей. Для каждой вариации было проведено по 1000 замеров времени из которых выведено среднее значение.

Таблица 1 – Время выполнения алгоритма Виолы-Джонса

Количество людей в базе данных	Графический процессор	
	GTX 720M	GTX 1060
	Время выполнения процедуры распознания (сек)	
1	0,0615611432	0,0405858220
5	0,0599416942	0,0405689913
15	0,0686475458	0,0484050662
25	0,1043391698	0,0583295351
45	0,1298241204	0,0693510549
80	0,1584274128	0,0838194554

На процессорах GTX 1060 заметен существенный прирост производительности за счёт увеличения количества CUDA ядер. Однако такая скорость уже является значительной при обработке изображений в сравнении с CPU, где различие может достигать десятков раз.

АНАЛІЗ ІСНУЮЧИХ СКБД ДЛЯ ПІДСИСТЕМИ ІНФОРМАЦІЙНОГО ТА НАВЧАЛЬНО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ ОСВІТНЬОГО ПРОЦЕСУ

Васюк Д.В.
Науковий керівник – д.т.н. Барковська О.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Електронних обчислювальних машин, тел. (057) 702-13-54) e-mail: olesia.barkovska@nure.ua

The given work is devoted to the development of the software complex for distance learning of students and gives the opportunity to access to the electronic abstract of lectures, quick communication with teacher via e-mail, quick access to the schedule of lectures and consultations, self-control of knowledge by testing. To store personal data, data for student's testing and other tasks, it is necessary to have quick and correct-working database. The most popular databases were analyzed in this work - MySQL, PostgreSQL, SQLite, Oracle Database, MongoDB. The result of the analysis showed that MySQL has more advantages over the others - free and easy to using.

Підсистема інформаційного та навчально-методичного забезпечення (ПІНЗ) передбачає наявність бази даних, щоб зберігати інформацію про студентів, їх оцінки, інформацію що до тестів тощо. На сьогоднішній день існує безліч різних систем керування базами даних (СКБД), найпопулярніші з них це MySQL, PostgreSQL, SQLite, Oracle Database, MongoDB. Кожна з них по своєму унікальна, але щоб обрати найоптимальнішу необхідно розібрати кожну з них окремо.

MySQL – реляційна СКБД, яка використовує дуже легку мову запитів SQL. Має відкритий код, що робить її безкоштовною. Дуже легко інтегрується в різні додатки та легко взаємодіє з різними мовами програмування, підтримує майже всі типи даних. В MySQL використовується багатопотокова система обробки інформації, що робить її швидкою при обробці та виконанні команд. Окрім цього, система підтримує необмежену кількість користувачів, що одночасно працюють з базою даних (БД). MySQL має власну просту але дуже ефективну систему безпеки, що робить її дуже захищеною від різноманітних атак.

PostgreSQL – об'єктно-реляційна СКБД, так само як і MySQL використовує мову запитів SQL та має відкритий код, що робить її безкоштовною. Існує великий список типів даних, які підтримуються в PostgreSQL, але якщо цих типів буде замало, то PostgreSQL надає можливість створювати власні типи даних. З версією 9.6 в PostgreSQL з'являється паралелізація послідовного зчитування, що пришвидшує виконання запитів. Окрім цього, PostgreSQL має безліч інших можливостей таких як робота з функціями на мові SQL та на PL/pgSQL, підтримка індексів типу B та R дерева, хеш, GIST, GIN, можливість успадкування характеристик та наборів полів від інших таблиць тощо.

SQLite – вбудована реляційна СКБД, яка має відкритий код, що робить її безкоштовною. Основними характеристиками SQLite є високий рівень мобільності (база даних зберігається в одному крос-платформному файлі на диску), простота використання, ефективність надійність, не потребує адміністрування, не має зовнішніх залежностей. SQLite має досить невеликий розмір близько 300 кілобайт, що дозволяє використовувати цю СКБД на малопотужних пристроях.

Oracle Database – об'єктно-реляційна СКБД, є платним продуктом корпорації Oracle. Основні характеристики Oracle Database це надійність, безпечність, висока продуктивність. Кількість інформації, яка може знаходитись в базі даних майже безмежна, це відбувається за рахунок масштабування, з цією інформацією може працювати безмежна кількість людей. Однією з відмінних особливостей Oracle Database це можливість зберігання та обробка текстових, аудіо та відео файлів, зображень тощо. Oracle Database підтримує велику кількість типів даних, але при необхідності можна створити нові, також має власну мову структурного програмування PL\SQL.

MongoDB – документо-орієнтована СКБД, що має відкритий код. Основні можливості MongoDB це здатність зберігати дані у форматі JSON, досить гнучка мова для формування запитів, що дуже схожа на мову JavaScript, динамічність запитів, підтримка індексів, ефективне зберігання бінарних даних в великих обсягів таких як фото або відео, профілювання запитів, зберігання даних про здійснені операцій, асинхронна реплікація, паралельна обробка великих масивів даних з використанням кластерів.

У роботі було розглянуто п’ять СКБД. Найкращі результати при аналізі на основі висунутих критеріїв – швидкість обробки запитів, простота користування, вартість програмного за стосунку, показала СКБД MySQL, бо саме MySQL більш легка в використанні (дуже проста конструкція запитів) ніж інші СКБД та більш підходить саме для невеликих проектів, також велику роль зіграло те, що MySQL є безкоштовною СКБД.

У ході розробки проекту було створена тестова база даних opfi_test, що має вигляд, наведений на рисунку 1.

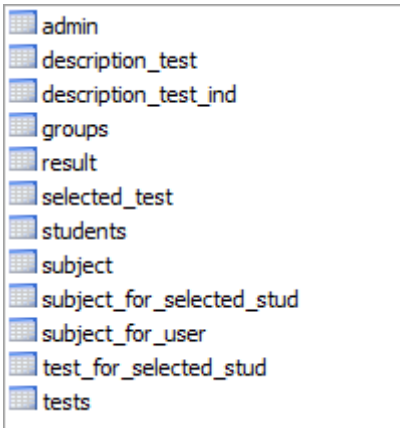


Рисунок 1 – Тестова база даних, що використана у ПІНЗ

ПОРІВНЯННЯ ПРОДУКТИВНОСТІ ПОСЛІДОВНИХ І ПАРАЛЕЛЬНИХ АЛГОРИТМІВ СОРТУВАННЯ НА МОВІ C#

Ботнар П.Д.
Науковий керівник – к.т.н. Барковська О.Ю.
Харківський національний університет радіоелектроніки
(61166, Харьків, пр. Науки,14, каф. Електронних обчислювальних машин, тел. (057) 702-13-54) e-mail: olesia.barkovska@nure.ua

The purpose of the work is to compare most famous sorting algorithms in parallel and sequence format on C# programming language. Sorting the large data arrays by various methods of sorting and their parallel versions, and determining the most efficient algorithm. In the researching used C# programing language and for parallel version modern Task Parallel Library, which allows run program with multiple threads. The research supports 5 sorting algorithms in sequential and parallel form: quick sorting, Shell sorting, odd-even sorting, bitonic-sorting, merge sorting.

Однією з найважливіших операцій і найбільш часто використовуваних у комп'ютерній науці, навіть сьогодні, є операції сортування.

Сортування даних - це будь-який процес, який передбачає впорядкування даних у певному значенні, щоб полегшити розуміння, аналіз або візуалізацію.

Алгоритм сортування - це алгоритм, який допомагає впорядкувати набір даних в певну послідовність. Зазвичай, масиви сортують за зменшенням і зростанням.

У зв'язку з різноманітністю завдань на сортування даних, існує багато різних методів сортування, які доцільно використовувати в різних ситуаціях, з метою економії коштів комп'ютера і часу користувача.

У дослідженні підтримуються 5 алгоритмів сортування у послідовному та паралельному вигляді : швидке сортування, сортування Шелла, парне-непарне сортування, бітонічне сортування, сортування злиттям.

Ймовірно, найголовнішим серед нових засобів, впроваджених в версію 4.0 середовища .NET Framework, є бібліотека розпаралелювання завдань (TPL). Ця бібліотека удосконалить багатопоточний програмування двома основними способами. По-перше, вона спрощує створення і застосування багатьох потоків. І по-друге, вона дозволяє автоматично використовувати кілька процесорів. Іншими словами, TPL відкриває можливості для автоматичного масштабування додатків з метою ефективного використання ряду доступних процесорів.

В роботі проаналізовані такі алгоритми сортувань, як сортування Шела, швидке сортування, сортування злиттям, біонічне сортування. Тестування проводилось на масивах різного розміру від 10000 елементів до 250000000 елементів. Найбільше прискорення було отримано при реалізації задачі на основі алгоритму швидкого сортування, результати наведені у таблиці 1.

Таблиця 1 - Результати швидкого сортування

Розмір масиву	Час послідовного виконання	Час паралельного виконання	Прискорення
10,000	0.0010207	0.000775	1.317032258
200,000	0.0247197	0.011786	2.097378245
1,000,000	0.134346	0.049426	2.718124064
5,000,000	1.0880588	0.32847	3.312505861
10,000,000	1.970997	0.738108	2.670336861
50,000,000	10.615045	4.344549	2.44330194
100,000,000	21.163807	9.999964	2.116388319
150,000,000	33.42381	17.824116	1.875201553
250,000,000	57.674523	32.07301	1.798226079

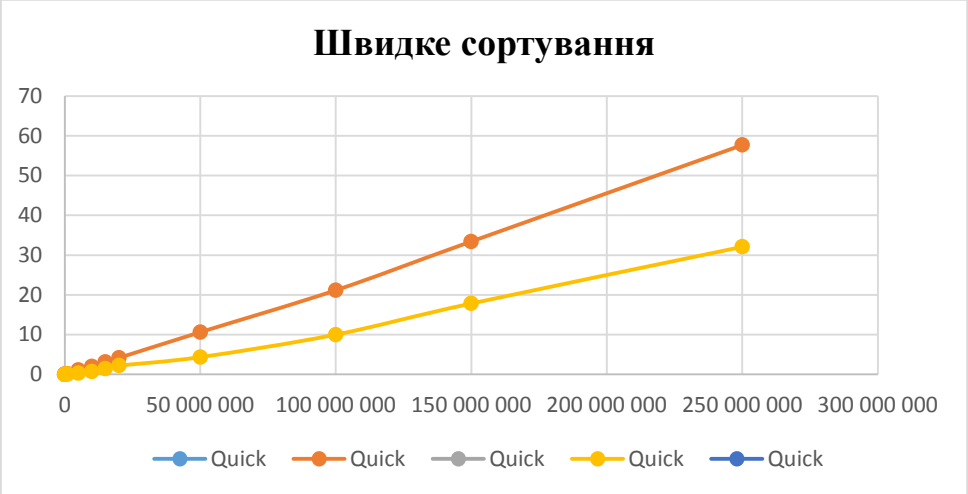


Рисунок 1 – Аналіз продуктивності паралельних обчислень на системі із загальною пам’яттю

Отримані результати підтверджують необхідність використання існуючих програмних та апаратних рішень для паралельної реалізації чисельних методів із великим обсягом вхідних даних із метою отримання результату у короткий час.

АКТУАЛЬНІСТЬ ПРОБЛЕМИ РОЗШИРЕННЯ МОЖЛИВОСТЕЙ СИСТЕМ БАТЬКІВСЬКОГО КОНТРОЛЮ

Сердечний В.С.
Науковий керівник – к.т.н. Барковська О.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Электронных вычислительныхЕлектронних обчислювальних машин, тел. (057) 702-13-54) e-mail: olesia.barkovska@nure.ua)

The given work is devoted to the analysis of the existing parental control systems for protecting children in the Inernet. In order to create a software application that can take into account the disadvantages of existing parental control systems, they were reviewed and analyzed. As a result of the research, no software product passed all the proposed tests. The results are very heterogeneous for all software solutions. No product was able to block the proposed pages in Study No. 2, while in the researches No. 1 and No. 3 are leaders - Kaspersky Total Security 2017 (Study No.3) and Mobicip (Study No.1).

Інформація, що отримується з глобальної мережі Інтернет, будучи однією зі складових інформаційно-освітнього середовища суспільства, значно впливає на освіту дитини. Бурхливий розвиток інтернет-технологій в останнє десятиліття привів до того, що діти мають повний доступ до всесвітньої мережі починаючи з малечку. При спробі знайти інформацію в електронних виданнях (наприклад, підручники, довідники, енциклопедії), діти стикаються з небажаною нецензурною інформацією. Перегляд подібних ресурсів може завдати удар по психіці дитини і мати відображення у майбутньому.

Тому, забезпечення можливості вберегти дитину від впливу небажаної інформації - одна з вимог, що пред'являються до інтернет-ресурсів різного характеру, а завдання розробки ефективних і простих у використанні засобів для фільтрації інтернет-трафіку з метою виявлення небажаних ресурсів і забезпечення безпеки в мережі є актуальною в сучасному світі.

Задля створення програмного застосунку, здатного враховувати недоліки існуючих систем батьківського контролю, було виконано їх огляд та аналіз.

Сучасні фільтри інтернет-трафіку, які забезпечують безпеку дітей, більш відомі, як «батьківський контроль» реалізується переважно в двох формах: спеціалізовані додатки для веб-браузерів і відповідні модулі в рамках антивірусних пакетів. Існують і самостійні програмні рішення, але вони на поточний час не знайшли широкого застосування в порівнянні з антивірусними пакетами.

Розширення для браузерів є безкоштовними і абсолютно не вимогливими до системних ресурсів. Однак, в силу своїх платформних

особливостей, функціонал таких доповнень є досить небагатим, часто обмежуючись лише наявністю чорних списків. Крім того, якщо в системі встановлено два і більше браузерів, необхідно окремо встановлювати доповнення, створені спеціально для конкретного веб-оглядача. Ще одним недоліком є те, що такий додаток дуже легко видалити, в той час як антивірусні рішення видалити дитині буде доволі складно, тому що батьки можуть заблокувати їх модифікацію за допомогою пароля. Передові антивірусні пакети, такі як ESET Smart Security (далі ESS) і Kaspersky Internet Security містять в собі вбудовані модулі, що реалізують функціонал батьківського контролю. Це потужні інструменти, ефективно блокують потенційно небажані веб-ресурси. Такі пакети не є безкоштовними і поставляються з платної підпискою. У зв'язку із закритістю технічних деталей реалізації функціоналу в антивірусних пакетах, важко точно сказати, як працюють модулі фільтрації. Для визначення ефективності існуючих програмних рішень, була розроблена спеціальна група тестів (досліджень):

- дослідження №1. Сторінки містять англійський текст і зображення, які відносяться до категорії «18+». Для дослідження була написана проста HTML-сторінка, яка включала недопустимі для дитини фрази. Результати показали, що програмне забезпечення Mobicip пройшло тест на 100%, заблокувавши всі 3 сторінки. ESS Premium не заблокував жодну з тестованих сторінок, тим самим ставши аутсайдером дослідження. Всі інші програмні продукти впоралися з тестом, в середньому, на 41,64%;
- дослідження №2. Сторінки містять англійський текст і зображення, які відносяться до категорії «18+». Для дослідження була написана найпростіша HTML-сторінка, яка включала недопустимі для дитини зображення та текст. Особливість сторінки - відсутність будь-яких натяків в title і meta на небажаний тематичниій зміст. Жодне з програмних рішень (ESS, Kaspersky TS, Child Web Guardian, Mobicip) не пройшло даний тест. Усі розглянуті програмні продукти не заблокували жодної розробленої сторінки;
- дослідження №3. Сторінки містять російський текст, який відноситься до категорій «18+» та «нецензурна лексика». Даний тест пройшов на 100% програмний продукт Kaspersky Total Security 2017, евристичний аналіз якого дозволив визначити нецензурну лексику на сторінці та її тематичний зміст. Всі інші учасники дослідження не пройшли тест.

В результаті проведених досліджень не було виявлено жодного програмного продукту, який би пройшов всі запропоновані тести. Результати дуже неоднорідні для всіх програмних рішень. Жоден продукт не зміг заблокувати запропоновані сторінки в дослідженні №2, в той час, як в дослідженні №1 і №3 є конкретні лідери – Kaspersky Total Security 2017 (дослідження №3) і Mobicip (дослідження №1).

АНАЛИЗ ПРОБЛЕМ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ И ОСНОВНЫЕ ВОПРОСЫ БЕЗОПАСНОСТИ

Корниенко А.Ю.
Научный руководитель – ст. преп. Партыка С.А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. ЭВМ, тел. (057) 702-13-54)
e-mail: oleksii.korniienko@nure.ua

This paper focuses on studying and analyzing the Cloud Computing technology in concept and its security, which is still a developing technology with great convenience and portability for exchanging information over the Internet via different platforms. Cloud Computing provides virtualized and scalable resources dynamically based on the network built with a great number of distributed computers instead of local computer or remote server. Meanwhile, the utilization and application of Cloud Computing is growing dramatically, which boosts a great number of new IT industries by integrating traditional computing technologies.

Облачные вычисления становятся популярными как способ виртуализации данных, растет популярность распределенных вычислений с сервером кластера. IT инфраструктура нуждается в технологиях, предоставляемых облачными вычислениями, что ускоряет их развитие. Виртуализация – это создание виртуального образа или «версии», ресурсов, которые можно было бы использовать на нескольких компьютерах одновременно [1].

Основной целью виртуализации является управление рабочей нагрузкой с помощью преобразования традиционных вычислений для того, чтобы сделать их более масштабируемыми, эффективными и экономичными.

Новые данные Synergy Research Group показывают, что в семи ключевых сегментах рынка облачных услуг и инфраструктуры доходы операторов и поставщиков за 2018 год превысили рубеж в 250 миллиардов долларов, увеличившись на 32% по сравнению с 2017 годом.

Во всей облачной экосистеме наиболее значимыми среди лидеров сегмента рынка в 2018 году были компании Microsoft, Amazon/AWS, Dell EMC и IBM. За ними последовали Salesforce, Cisco, HPE, Adobe и VMware [2].

Технология виртуализации позволяет легко управлять ресурсами облачных вычислений. Она абстрагирует и изолирует базовое оборудование и сетевые ресурсы в единой среде хостинга. Виртуализация повышает безопасность облачных вычислений, защищая как целостность виртуальной машины, так и облачных компонентов, виртуализированные машины могут быть масштабированы по требованию и могут обеспечивать надежность данных. Она обеспечивает совместное использование ресурсов, высокую степень задействования объединенных ресурсов,

быстрое распределение ресурсов, изоляцию рабочей нагрузки. Последние тенденции в виртуализации – это консолидация центров обработки данных, что снижает затраты на управление.

Одним из наиболее важных свойств облачных вычислений является то, что пользовательские данные не хранятся на локальном устройстве, а хранятся в облаке, в результате чего некоторые данные могут быть подвержены потере конфиденциальности. Несмотря на многочисленные рекомендации в отношении облачных вычислений о том, как не загружать конфиденциальные данные в облако, это не идеальное решение и, вероятно, нейтрализует определенные преимущества, которые приносит облако. Кроме того, это мешает развитию облачных вычислений.

До сих пор довольно популярно объединять хеш-дерево Меркле [3] и зашифрованный блок для реализации конфиденциальности и целостности документа в зашифрованной сетевой системе на основе случайного доступа. Пользователь должен рассчитать токен аутентификации заранее, после того как сервер получает запрос аутентификации от пользователя, в соответствии с сгенерированной подписью и отправляет его обратно пользователю. Затем пользователь может определить действительность путем сравнения этой подписи и предварительно рассчитанного токена. Этот метод отлично подходит для проверки достоверности данных, а также поддерживает безопасный и эффективный обмен динамическими данными, включая обновление, добавление и удаление данных.

В работе были рассмотрены тенденции развития облачных вычислений. В частности, проведен анализ такой технологии как виртуализация данных, главными преимуществами которой являются: изолированность пользователей, совместное использование ресурсов, использование динамических ресурсов, агрегирование ресурсов. В целом, рост облачных вычислений знаменует собой начало новой эры информационных технологий. Между тем, это приводит к преобразованиям приложений из локальной в облачную среду, что приносит огромную пользу и комфорт для повседневной жизни и работы.

Список источников:

1. Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, Jan 2011.

2. Swathi T, Srikanth K, Reddy SR (2014) Virtualization In Cloud Computing, IJCSMC, Vol. 3.

3. Lombardi L, Pietro RD (2011) Secure virtualization for cloud computing, Journal of Network and Computer Applications 34: 1113-1122.

РЕШЕНИЕ ВОПРОСОВ ИНФРАСТРУКТУРЫ С ПОМОЩЬЮ «ОБЛАЧНЫХ» ВЫЧИСЛЕНИЙ

Билоус А.В.
Научный руководитель – ст. преп. Партыка С.А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. ЭВМ, тел. (057) 702-13-54)
e-mail: oleksandr.bilous@nure.ua, тел.: (099) 607-61-66

The given work is devoted to the modern trend of cloud technologies and computing. Cloud computing is a clustered pool of computer system resources, that provides the high-quality services. Its main purpose is to allow users all over the world to get access to the high-level API with stable uptime and vast computational power. It may be used for wide various of tasks such as data storage, online computing, data partitioning, remote OS etc. The providing of high-capacity networks, low-cost computing power, and storages as well as perfect adaptation for almost every possible type of architecture makes cloud services grow fast in almost all human working spheres.

Глобальная урбанизация, устаревшая инфраструктура и сильно ограниченные энергетические ресурсы оказывают сильное влияние на качество жизни человечества как сейчас, так и в будущем. Говорят: «Необходимость – это источник инновации»,– в наши дни нет большей необходимости, нежели создание мира, где 7 миллиардов человек сможет иметь прекрасную жизнь, минимизировав отрицательное влияние на планету. Человечество всегда использовало проектирование как средство решения проблем – это важный инструмент, который позволяет работать с воображением, представить, какой наша планета будет в будущем. Хорошая новость в том, что уже в скором времени всё будет по-другому, благодаря облачным вычислениям – инструментарию, который открывает доступ к невероятным объёмам данных и вычислительным мощностям.

Облачные вычисления – это набор аппаратных средств и программных сервисов доступных через интернет и состоящих из серверов, которые занимаются обработкой и хранением данных. Возможности облака огромны, поэтому они были разделены на три группы в зависимости от типа использования:

Software as a Service (SaaS) – Программное обеспечение как услуга – является достаточно популярным способом доступа к программному обеспечению. Вместо того, чтобы устанавливать ПО на своих собственных серверах, имеется возможность получить к нему доступ удалённо, через, как правило, тонкий клиент (браузер), по ежемесячной или годовой подписке. Отличительной чертой такого решения является то, что плата за приложение, обычно, не становится больше, но при этом возникает экономия на инфраструктуре, а также присутствует доступ к продукту с высокой надежностью, доступностью и масштабируемостью.

Infrastructure as a Service (IaaS) – Инфраструктура как услуга – модель обслуживания в облачных вычислениях по которой в рамках ежемесячной или годовой подписки клиентам предоставляется доступ к фундаментальным информационным ресурсам – виртуальным удаленным серверам с большой вычислительной мощностью и предустановленной операционной системой. Данная модель облачных вычислений является основным конкурентом традиционным выделенным серверам в дата центре, так как предоставляет аналогичную инфраструктуру, но с большей вычислительной мощность, доступностью и масштабируемостью за меньшую стоимость.

Platform as a Service (PaaS) – Платформа как услуга – широкий набор сервисов инфраструктурных приложений (промежуточного программного обеспечения). Данная модель облачных вычислений подразумевает доступ ко всему перечню информационно-технологических платформ: операционным системам, системам управления базами данных, системам автоматизированного тестирования, средствам разработки приложений и т.д., которые размещены у облачного провайдера.

Значение облачных технологий в современном мире возрастает в геометрической прогрессии. Исследовательская компания Gartner прогнозирует рост рынка облачных вычислений на 17,3% в 2019 году, а к 2022 году 90% организаций будут использовать облачные вычисления [2].

Таблица 1 – Рынок облачных вычислений (млрд. долл. США)

Модель	2017 г.	2018 г.	2019 г.	2020 г.	2021 г.
Platform as a Service	11.9	15.2	18.8	23.0	27.7
Infrastructure as a Service	23.6	31.0	39.5	49.9	63.0
Software as a Service	58.8	72.2	85.1	98.9	113.1

Подводя итоги, можно сказать, что человечество уже начало свой стремительный путь в мир, где вычисления, совместная работа и общение находятся в облаке. Гибкость, эффективность и простота для понимания, обеспечиваемые облачными вычислениями, способствуют их внедрению в повседневные процессы быстрее, чем когда-либо прежде.

Список источников:

1. Michael J. Kavis Architecting the Cloud: Design Decisions for Cloud Computing Service Models [Текст] : книга / Michael J. Kavis. – New York, 2014. 224 с.

2. Исследовательская компания Gartner [Электронный ресурс]. – Режим доступа : https://www.gartner.com.

ЗАСОБИ АНАЛІЗУ BIG DATA

Смірнов Н.М.
Науковий керівник – ст. викл. Партика С.О.
Харківський національний університет радіоелектроніки
(61103, Харків, прос Науки 14, каф. ЕОМ, тел. (057) 702-1354)
e-mail nikita.smirnov@nure.ua, тел. +380954718030

The given work is deticated to research of modern approaches and tools for Big Data analyze. The amount of data accumulated worldwide is close to 300 exabytes and continues to grow by approximately 50% per year. Moreover, IDC analysts predicted an increase in data volumes around the world to 35 thousand exabytes by 2020[1]. Thus, organizations that want to succeed in these conditions are simply obliged to adapt to the new strategies of market analyze. Although the rules of the game in the field of data accumulation and their exchange are still being formed, today it has become clear to everyone that the need for Big Data is not determined by individual companies, but by an entire era of the computer industry.

С развитием технологий и увеличением количества поступающей информации, возникает необходимость в быстрых и эффективных способах анализа и обработки данных. Обычные базы данных уже не обеспечивают достаточно высокую эффективность хранения и обработки информации [1]. Поэтому возникает необходимость в новых инструментах и методах, специализирующихся на анализе и обработке больших объёмов данных.

Big Data подразумевает наличие средств и методов анализа больших массивов данных, которые позволяют организовывать различные хранилища данных, инструменты управления и обработки, инструменты и методы аналитики, а также визуализацию и оценку различных этапов процесса принятия решений [2].

В настоящее время набирают популярности базы данных, такие как Not Only SQL (NoSQL), которые были разработаны для хранения и управления неструктурированными данными [3]. Базы данных NoSQL нацелены на масштабирование, гибкость модели данных и упрощенное развертывание. В отличие от реляционных баз данных, базы данных NoSQL разделяют возраст и хранение данных. Такие базы данных скорее ориентированы на высокую производительность и отлично подходят для нужд хранения больших данных.

Существует четыре критических требования для обработки Big Data. Первое требование – быстрое чтение и запись, чему сильно мешает медленный дисковый и сетевой трафик. Второе требование это быстрая обработка запросов для того, чтобы удовлетворять запросам в реальном времени и запросам, которые критичны по времени ответа. Третье требование – высокоэффективное использование хранилища данных, так как быстрый рост активности пользователей может потребовать

масштабируемой емкости и вычислительной мощности. Наконец, четвертое требование – сильная адаптивность к высокодинамичным моделям рабочей нагрузки.

В докладе рассмотрена программная среда Apache Hadoop с открытым исходным кодом, используемая для разработки приложений обработки больших данных, которые выполняются в распределенной вычислительной среде, что отличает её от обычных реляционных баз данных (см. табл. 1).

Таблица 1 – Сравнение основных характеристик классических БД и Hadoop.

	Традиционные реляционные БД	Hadoop/MapReduce
Объемы данных	Гигабайты, терабайты	Петабайты и более
Доступ	Интерактивный, пакетный	Только пакетный
Обновления	Многократные чтение и запись	Однократная запись, многократное чтение
Структура	Статическая схема	Изменяемая схема
Масштабируемость	Нелинейная	Линейная
Скорость ответа	Стремится к нулю	Имеется задержка из-за пакетной обработки

В случае традиционных реляционных БД запись данных – это синхронный процесс, классифицируемый как атомарная транзакция, которая завершается только после подтверждения принятия. Это может привести к нежелательным задержкам для любых приложений, которые не готовы ждать этого подтверждения. Платформы Big Data, такие как Hadoop , напротив, используют при написании асинхронные методы, которые не зависят от фиксации со стороны ядра базы данных и, следовательно, не страдают от задержек, что значительно ускоряет процесс [4].

Показано, что Hadoop обеспечивает наиболее распространенные передовые методы анализа данных, такие как правила ассоциации, кластеризации, классификации и деревья решений.

Список источников:

1. The digital universe in 2020 : big data, bigger digital shadows, and biggest growth in the far east. – Gants J., Reinsel D. – IDC iView – 2012.

2. Elgendy, N.: Big Data Analytics in Support of the Decision Making Process. MSc Thesis, German University in Cairo, p. 164 (2013).

3. Considerations for Big Data: Architecture and Approaches. – Bakshi, K. – Proceedings of the IEEE Aerospace Conference, pp. 1-7 – 2012.

4. He, Y., Lee, R., Huai, Y., Shao, Z., Jain, N., Zhang, X., Xu, Z.: RCFile: A Fast and Spaceefficient Data Placement Structure in MapReduce-based Warehouse Systems. In: IEEE International Conference on Data Engineering (ICDE), pp. 1199–1208 (2011).

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

Зінченко С.В.
Науковий керівник – ст.викл. Партика С.О.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. ЕОМ, тел. (057) 702-13-54)
e-mail: serhii.zinchenko@nure.ua

This work is devoted to the analysis of the concept of enterprise information security, types of threats and ways to eliminate them. All work aimed at building, maintaining and developing the information security system has one goal - to minimize the possibility of inflicting damage to the information infrastructure of the enterprise, and in case of emergencies - minimizing the consequences of the damage. Today, there are many methods of combating threats to information security. For each type of threat there are own methods and processes that control certain nodes of the information system and prevent any failures in them.

У наші дні практично всі підприємства переходять до використання інформаційних послуг, і в зв'язку з цим виникає загроза витоку даних на ринок конкурентів, тим самим підвищуючи рівень важливості інформаційної безпеки в компаніях і на підприємствах.

Для повного розуміння поняття «інформаційна безпека підприємства» треба спочатку вияснити, що означає термін «інформаційна безпека». Інформаційна безпека – це стан збереження інформаційних ресурсів і захищеності законних прав особистості і суспільства в інформаційній сфері [1]. Наданий стан складається з двох головних аспектів:

− безпосередньої інформаційної безпеки – стану захищеності інформаційного середовища;

− забезпечення захисту інформації – діяльності, спрямованої на запобігання витоку інформації, що захищається, недопущення несанкціонованих і ненавмисних дій з цією інформацією [2].

Знаючи визначення інформаційної безпеки можна сформувати визначення поняття інформаційна безпека підприємства.

Інформаційна безпека підприємства полягає в здійсненні цілеспрямованої діяльності органів управління та посадових осіб підприємства з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [2].

Усі роботи, що орієнтовані на побудову, підтримку та розвиток системи інформаційної безпеки мають одну мету – звести до мінімуму можливість нанесення шкоди інформаційній інфраструктурі підприємства, а у виникненні надзвичайних ситуацій – зведення до мінімуму наслідків отриманої шкоди.

Відповідно до концепції забезпечення інформаційної безпеки компанії тільки виявлення і контроль повного спектру загроз дозволяє побудувати

ефективну систему захисту інформації. Усі погрожуючі фактори можна поділити на декілька видів:

− загрози від авторизованих користувачів – умисні або неумисні дії співробітників компанії;

− зовнішні цілеспрямовані атаки – не санкціоноване проникнення до комп'ютерної мережі зовні;

− комп'ютерні віруси;

− спам;

− форс-мажорні обставини – псування обладнання у результаті неправильного використання або зовнішніх чинників.

Сьогодні існує велика кількість методів боротьби із загрозами інформаційної безпеки. Для кожного виду загроз існують власні методи та процеси, які контролюють певні вузли інформаційної системи та запобігають будь-яким збоям у них.

Основними засобами та методами захисту інформації є система автентифікації, системи шифрування, міжмережевий екран, віртуальні приватні мережі (VPN), фільтрація електронної пошти, контроль працездатності вузлів, антивірусний захист, використання систем виявлення слабких місць, резервне копіювання.

Однак, максимального ефекту можна досягти лише використовуючи усі наведені методи в комплексі. Тобто, проектування, побудова, впровадження та підтримка систем інформаційної безпеки підприємств являє собою комплексне завдання, що потребує аналізу потенційних загроз, вибору боротьби з ними та налагодження взаємодії між цими методами.

У представленій роботі було з'ясовано визначення інформаційної безпеки, інформаційної безпеки підприємства та їх складові, були визначені види загроз на інформаційну систему підприємства та методи боротьби з ними, і було зроблено висновок щодо використання наведених методів для різних видів загроз

Список джерел:

1. Build a Security Culture – Roer K. – 2015.

2. IT Governance - An International Guide to Data Security and ISO27001/ISO27002, Sixth Edition - Calder A., Watkins S.- 2015

АНАЛІЗ ЧЕТВЕРТОГО ТА П'ЯТОГО СТРУКТУРНОГО ПОКОЛІННЯ КОМП'ЮТЕРНИХ СИСТЕМ

Ляшова А.О.
Науковий керівник – ст. викл., к.т.н. Єрьоміна Н.С.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки14, каф. ЕОМ, тел. (057) 702-13-54)
e-mail: anastasiia.liashova@nure.ua

The analysis of fourth and fifth structural generation of computer systems (CSs) has been performed. The current state of CSs is the result of long-term evolution. The challenges set for the fourth generation of CSs developers were the increasing of productivity, enlarging the storage space. The main goal of fifth generation of CSs developers are the creation of the architectural intelligence of machines, the development of the intellectual performance of the computers.

У наш час важко уявити собі, що без комп'ютерних систем (КС) можна обійтися. Використання комп'ютера означає появу нових форм мислення, творчої діяльності, що можна розглядати як історичний розвиток психічних процесів людини, формування таких якостей, як експериментування, гнучкість, структурність [1, с. 25]. Сучасний стан КС являє собою результат багаторічної еволюції. У традиційному трактуванні еволюцію обчислювальної техніки уявляють як послідовну зміну поколінь КС. Значно більшого поширення набула прив'язка поколінь до зміни технологій. Прийнято говорити про «механічну» еру (нульове покоління) і про п'ять наступних за нею поколінь обчислювальних систем [2]. Перші чотири покоління традиційно пов'язують з елементною базою КС: електронні лампи, напівпровідникові прилади, інтегральні схеми малого ступеня інтеграції (ІМС), великі (ВІС), надвеликі (НВІС) і ультравеликі (УВІС) інтегральні мікросхеми [3]. П'яте покоління асоціюють не стільки з новою елементною базою, скільки з інтелектуальними можливостями КС.

Якщо розглядати КС четвертого покоління, то для нього були характерні логічні інтегральні схеми створені на основі уніполярних польових CMOS-транзисторів з безпосередніми зв'язками, застосовувалися великі інтегральні схеми, потужністю приблизно 1000 ІС. Швидкодія таких комп'ютерів досягала 100 мільйонів операцій за секунду, ємність їхньої оперативної пам'яті (ОЗП) зросла до 500 млн. двійкових розрядів, ємність оперативної пам'яті близько 1-64 Мбайт. З точки зору структури КС цього покоління є багатопроцесорними і багатомашинними комплексами, що працюють на загальну пам'ять і загальне поле зовнішніх пристроїв.

Перед розробниками КС попередніх поколінь стояли завдання збільшення продуктивності в області числових розрахунків і досягнення великої місткості пам'яті, тоді як основним завданням розробників КС п'ятого покоління є створення штучного інтелекту (ШІ), сприймання

інформації з рукописного або друкованого тексту, з бланків, з людського голосу, розпізнавання користувача за голосом, здійснювання перекладу з однієї мови на іншу. Це має сприяти усуненню бар'єру в спілкуванні між людиною і комп'ютером.

Вважалося, що архітектура комп’ютерів п’ятого покоління буде містити два основні блоки. Один з них – власне комп’ютер, у якому зв’язок з користувачем здійснює блок, так званий «інтелектуальний інтерфейс»[4]. Об’єм ОЗП КС п’ятого покоління збільшився до 256 ГБ, швидкодія комп’ютерів зросла до 9 мільярдів операцій за секунду.

Хід розробок п’ятого покоління представлявся так, що комп'ютерний інтелект, набираючи потужність, повинен змінювати сам себе, а метою було створити таке комп'ютерне середовище, яке саме почне виробляти наступне, причому принципи, на яких буде побудований остаточний комп'ютер, були заздалегідь невідомі, ці принципи потрібно виробити в процесі експлуатації початкових комп'ютерів.

Для різкого збільшення продуктивності, пропонувалося поступово замінювати програмні рішення апаратними, тому не робилося різкого поділу між завданнями для програмної і апаратної бази.

Для вирішення завдань штучного інтелекту, зокрема для створення інтелектуальних систем підтримки прийняття рішень (ІСППР), все ширше застосовуються нетрадиційні розділи математики, такі як теорія нечітких множин та нечітка логіка, а також теорія можливостей і теорія ймовірностей. Таким чином ШІ є потужним засобом обробки даних і може знаходити рішення складних завдань швидше, ніж традиційні алгоритми, написані програмістами.

Сучасні КС і інформаційні технології знаходять і знаходитимуть все більш широке застосування в самих різних областях людського буття - в науці і техніці, в освіті і культурі, в виробництві, на транспорті і в сфері обслуговування. Вони формують стиль життя сучасної людини, його культуру, сприйняття світу і образ дій.

Список джерел:

1. Литвин А. В. Комп’ютерні технології у професійно-технічній освіті. Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми : зб. наук. пр. / Київ–Вінниця, 2005. Вип. 8. С. 151-157.

2. Таненбаум Э. Архитектуракомпьютера. СПб.: Питер, 2007. 848 с.

3. Тарарака В.Д. Архітектура комп'ютерних систем: навчальний посібник. Житомир : ЖДТУ, 2018. 383 с.

4. А. В. Геза Основні етапи обчислювальної техніки як підґрунтя для становлення та розвитку кібернетики. Наука та наукознавство. 2015. № 2. С.134 – 140.

ПРОЕКТИРОВАНИЕ РАСПРЕДЕЛЁННЫХ БАЗ ДАННЫХ ПРИМЕНИТЕЛЬНО К ЗАДАЧАМ УПРАВЛЕНИЯ СИСТЕМАМИ ИНТЕРНЕТА ВЕЩЕЙ

Лукашёв С.А.
Научный руководитель - д.т.н., доц. Михаль О.Ф.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф ЭВМ, тел. (057)70-21-354)
e-mail: serhii.lukashov@nure.ua

The Internet of Things is the concept of a computing network of physical objects equipped with embedded technologies for interacting with each other or with the external environment. Within of this concept, issues of designing distributed databases are considered in relation to the organization of control systems for individual segments of the Internet of things.

Интернет вещей (ИВ) - (IoT - internet of things) – представляет собой глобальную сеть подключенных к интернету физических устройств (так называемых «вещей»), оснащенных сенсорами, датчиками и устройствами передачи информации. Все устройства могут быть объединены подключением к центрам контроля, управления и обработки информации. ИВ есть концепция вычислительной сети физических предметов, оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой. В связи с ИВ, рассматривается организация таких сетей как явление, способное перестроить экономические и общественные процессы. То есть, последствия появления ИВ будут весьма серьёзными и уже сейчас начинают сказываться. Поэтому актуальным является технический аспект проблемы- исследования применительно к проектированию и использованию распределенных баз и других хранилищ данных в связи с концепцией ИВ.

Среда, в которой разворачивается ИВ и которая видоизменяется под воздействием ИВ может быть охарактеризована как многоцелевая информационная структура (МИС). Отдельные блоки МИС обозначены на приведённой блок-схеме понятиями, отстранёнными от тематики ИВ. Целесообразность этого состоит в интерпретационной обособленности. На определённом этапе могут проявиться понятия «иные», чем соотносимые сейчас с ИВ.

Прикладная область (ПО) есть реальный мир, «заселённый» подключёнными к ИВ «вещами». По мере разрастания числа «вещей», ПО видоизменяется. Информация о прикладной области (ИПО) есть реальный контент ИВ. Элементами ИПО являются, в частности, записи в различных БД, совокупность которых является «статической частью» ИВ. Транзакции между БД есть «динамическая часть» ИВ. Она реализуется в процессоре информации о прикладной области (ПИПО), с которым пользователи (П)

работают через два интерфейса: интерфейс работы с информацией (ИРИ) и интерфейс реконфигурирования работы с информацией (ИРРИ).

П ИВ есть контингент разнородный. Сюда входят по крайней мере 4 группы: (1) люди-потребители услуг ИВ; (2) «вещи»-потребители услуг ИВ; (3) люди-операторы (исполнители), работающие в сфере ИВ и (4) «вещи», реализующие ИВ. 1 и 2 работают с ПИПО через ИРИ, 3 и 4 – через ИРРИ. Сведение людей и «вещей» в единый список отражает тот факт, что «вещи», фигурирующие в ИВ, наделены известной долей интеллекта (более уместно слово smart), т.е. компьютеризи-рованы, т.е. по определению являются усилителями функций человеческого интеллекта.

ИВ есть интеллектуализация человеческого окружения, т.е. перенос туда часть человеческих интеллектуаль-ных функций. Процесс этот необратим (никто не станет «забирать» эти свои функции назад, потому что это будет сознательный отказ от определённых аспектов комфортности окружения) и по своим темпам – не соизмерим с процессом эволюции человеческого мозга. Поэтому у человечества – нулевые шансы, что оно будет «умнеть» быстрее, чем компьютеризируемое им человеческое окружение. Поэтому уход человечества в боковую (не основную) ветвь развития – вопрос реально обозримого времени. ИВ есть концепция вычислительной сети физических предметов, оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой. В рамках этой концепции, людьми рассматриваются в настоящее время вопросы проектирования распределённых баз данных применительно к организации систем управления отдельными сегментами ИВ. Но, как и всякая концепция, ИВ ограничен во времени уже в силу того, что ограничен в своём концептуальном развитии возможностями человеческого мозга. Достаточно очевидно, что исследования проектирования распределенных баз данных и использования веб-технологий для создания современных интерфейсов приложений возможны только до определённого уровня сложности. Эти функции будут постепенно и плавно перенесены на компьютерные системы, которые будут поддерживать более высокий уровень сложности, и это будет знаменовать смену носителя самой концепции ИВ, т.е. уход человечества в боковую ветвь развития.

ЗАДАЧА КОНВЕРТАЦИИ ГОЛОСОВЫХ ДАННЫХ. ГЕНЕРАТИВНО-СОРЕВНОВАТЕЛЬНЫЙ ПОДХОД

Логвин А.А.
Научный руководитель - д.т.н., доц. Михаль О.Ф.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф ЭВМ, тел. (057)70-21-354)
e-mail: logvin.anton.work@gmail.com

Within the problem of creating a speech interface, for the task of voice conversion, two methods are compared: GAN and DNN. MCD is selected as the evaluation metric. It is shown that the metric is highly sensitive, but weakly correlates with the real quality perceived by a human person.

Традиционное концептуальное требование к человеко-машинному интерфейсу (ЧМИ) – максимальная комфортность, естественность и предельное приближение к характеристикам межчеловеческого взаимодействия. Затраты значительных творческих усилий на разработки в этом направлении – оправданы. Они обусловлены тем, что высокое качество ЧМИ – это более низкая утомляемость (более продолжительное сохранение работоспособности) работающего с ним персонала. Одновременно, - это снижение вероятности ошибок операторов и, как следствие, - повышение эффективности работы человеко-машинной системы в целом.

Важной составляющей общей проблематики разработки ЧМИ является речевой интерфейс. В информационном плане, речевой канал человека существенно меньше по объёму, чем зрительный. Но в плане важности (ценности) передаваемой по нему информации, - соотношение противоположное. Объяснение этому следующее. Человек – существо социальное. Поэтому традиционно многие важные задачи решаются группами людей. Обычно, группа бывает пространственно распределена, так что каждый индивид получает уникальную информацию. Реальны ситуации, при которых только один индивид получает информацию, критическую для всей группы (об опасности или, наоборот, о достижении существенного выигрыша). Речевой канал – важное средство передачи критической (сигнальной или командной) информации. Результат – выигрыш всей группы.

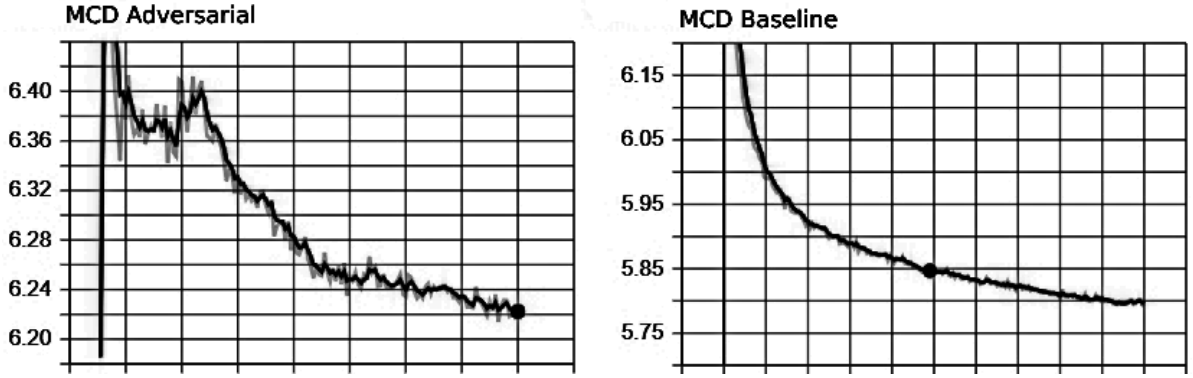
На текущем этапе развития масштабы применения компьютеров в качестве усилителей человеческого интеллекта становятся столь значительными, что группа - становится человеко-машинной. Отсюда важность речевого человеко-машинного интерфейса - максимальный комфорт передачи критической информации.

Ключевая составляющая проблемы - задача конвертации голоса (voice conversion). Традиционное решение - на основе глубоких нейронных сетей (DNN - deep neural network) в качестве акустических моделей для TTS

(text-to-speech) и VC (voice-conversion). Они могут достаточно точно моделировать соотношение между входными данными модели и звуковыми характеристиками. Однако речевые параметры имеют тенденцию к сверх-сглаживанию, и результирующее качество речи - не высоко по сравнению с естественной речью.

Рассматривается - использование генеративно-состязательной сети (GAN - generative-adversarial networks). Она представляет собой модель, которая может воспроизводить сложную взаимосвязь между вектором входных данных случайного шума и выходных параметров с помощью состязательного процесса. Используются две подмоделей: генератора и дискриминатора. Задача генератора - получить на вход случайный шум и сгенерировать данные, подчиняющиеся некоторому вероятностному распределению. Функция дискриминатора - показывает вероятность того, что данные, которые были поданы на его вход, получены из тренировочного датасета или созданы генератором.

В качестве метрики оценивания на данном этапе выбрана MCD (Mel-cepstral distortion). Она показывает насколько различаются две последовательности мел-кепструма. Чем меньше MCD между синтезированными и естественными мел-кепструмами, тем ближе синтетическая речь к воспроизведению естественной речи. На рисунке представлены графики MCD для GAN и DNN, демонстрирующие качественное совпадение.



Резкий скачок на первом рисунке объясняется тем, что были проведены 50 эпох предварительного обучения для улучшения работы генератора и дискриминатора. В остальном – MCD, хотя и демонстрирует более высокую чувствительность, но не позволяет выделить реальных «человеческих» преимуществ GAN, непосредственно воспринимаемых на слух. Это показывает, что MCD не сильно коррелирует с качеством речи. Для оценки качества синтезированной речи. должна использоваться MOS (mean opinion score) - численная мера оцениваемого человеком общего качества события или опыта. В последующей работе по данному направлению должно будет быть проведено более качественное полноценное тестирования при помощи MOS.

ЛОКАЛЬНО-ПАРАЛЛЕЛЬНЫЙ АЛГОРИТМ ПОСТРОЕНИЯ ФУНКЦИИ ПРИНАДЛЕЖНОСТИ ЧЕТКОГО МНОЖЕСТВА, СРЕДНЕКВАДРАТИЧЕСКИ МИНИМАЛЬНО УДАЛЕННОГО ОТ ИСХОДНОГО НЕЧЕТКОГО МНОЖЕСТВА

Федоренко К.И.
Научный руководитель - д.т.н., доц. Михаль О.Ф.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф ЭВМ, тел. (057)70-21-354)
e-mail: mesomix@gmail.com

A locally parallel (LP) version of the algorithm for constructing the membership function of a distinct set, the root mean square minimum distance from the original fuzzy set, is considered. An LP entry is composed of adjacent non-intersecting bit segments. The efficiency of the LP algorithm, in comparison with the sequential, grows in proportion to the number of segments.

Сохранение баланса черного и белого (ч/б) при преобразовании тонового (серого) изображения в контрастное двухцветное ч/б, - актуально, и перспективно для ряда приложений, поскольку обеспечивает сокращение объема информации при сохранении основного содержания. В более широком контексте, преобразование гладкого профиля функции принадлежности (ФП) нечеткого множества (НМ) в ступенчатый (дискретный) профиль ФП четкого множества (ЧМ), есть задача принятия четких решений при нечетких исходных данных. Технические приложения – разнообразны и многочисленны, а полезный эффект – очевиден.

В теории НМ имеется теорема, согласно которой обычное, традиционное ЧМ, построенное по правилу

$$\text{if } (\mu_{\text{нм}} \le 0{,}5) \text{ then } (\mu_{\text{чм}} = 0) \text{ else } (\mu_{\text{чм}} = 1)\,, \qquad (1)$$

минимально (в среднеквадратическом смысле) удалено от исходного НМ. Здесь $\mu_{\text{нм}}$ и $\mu_{\text{чм}}$ - значения ФП для НМ и ЧМ, соответственно.

Согласно определению, ФП (обозначается μ) находится в интервале [0, 1] (т.е. $\mu \in [0, 1]$ с включением концов интервала) и изображает (описывает) в теории НМ степень принадлежности элемента (в рассматриваемом интерпретационном варианте – значение пиксела серого изображения) к некоторому множеству (в рассматриваемом варианте - к множеству значений оттенков серого). Ситуация $\mu = 1$ соответствует полной принадлежности; $\mu = 0$ – полной непринадлежности. Т.е. частичная принадлежность описывается дробными значениями μ. Множество возможных дробных значений в интервале [0, 1] – бесконечно велико. В математике оно называется континуумом и характеризуется (описывается) не понятием «число точек», а понятием «мощность множества». В частности, в математике доказано, что может быть предложена процедура,

с помощью которой для любой пары точек из интервала [0, 1], сколь угодно близко расположенных друг к другу, может быть указана точка, находящаяся между ними.

Математика – наука абстрактная, для реальной же действительности - характерна конкретность. Степень освещённости объекта воспринимается человеческим глазом и обрабатывается человеческим мозгом. Достаточно давно экспериментально показано, что эта система не обеспечивает распознавания (различения) бесконечно большого набора оттенков серого. Классиком в данной области является Пьер Бугер (1698-1758), проводивший опыты с наборами восковых свечей и экранов и подсчитывавший число различаемых глазом оттенков тени. По результатам проведения подобных экспериментов, оказалось, что разные люди различают разное число градаций. Кроме того, глаз адаптируется, поэтому различающая способность меняется во времени. Но усреднённо – речь может идти не более чем о нескольких десятках градаций.

Опираясь на эти (достаточно традиционные) представления, в реальных технических системах целесообразно перейти от непрерывного ряда возможных значений ФП к дискретному набору значений. Тогда - конкретное значение коэффициента серого реально может быть описано двоичным числом длиной, допустим, 5 – 6 бит. Учитывая, что в настоящее время доминирует 64-битная компьютерная техника, реально представить отрезок (фрагмент) изображения, содержащий 10 – 12 пикселов, в виде одного числа. В нём могут соседствовать без пересечения 5-ти – 6-ти битовые сегменты. Такое представление информации называется локально-параллельным (ЛП). В ЛП-представлении значения ФП $\mu_{нм}$ и $\mu_{чм}$ хранятся компактно, в сегментах регистровых представлений (РгП). Множественность представления информации предполагает соответствующее сокращение времени обработки.

Алгоритм, реализующий логику (1), включает разделение исходного РгП на два, содержащих чётные и нечётные сегменты. Далее эти РгП вычитаются из образцовых РгП (РгП-констант), содержащих в соответствующих сегментах значения, соответствующие $\mu = 0{,}5$. Превышение уровня 0,5 приводит к заимствованию из старшего разряда (младшего разряда соседнего левого сегмента), где в РгП-константе предусмотрительно стоит специальная «резервная» единица. Картина расходования «резервных» единиц позволяет построить маски, по которым из исходного РгП формируется «ч/б – РгП» согласно (1).

На текущем этапе – концепция алгоритма разработана, программное обеспечение отлажено. Согласно плану экспериментов, исследуется выигрыш в производительности в зависимости от параметров модели. Эффективность ЛП алгоритма по сравнению с последовательным растет пропорционально числу сегментов.

СИНТЕЗ АДАПТИВНЫЕ КЛЕТОЧНЫЕ АВТОМАТЫ В МОДЕЛИРОВАНИИ ДИНАМИЧЕСКИХ СИСТЕМ

Севостьянова Е.Н.
Научный руководитель - д.т.н., доц. Михаль О.Ф.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф ЭВМ, тел. (057)70-21-354)
e-mail: fuzzy16@pisem.net

The prospects of cellular automata are discussed, as an apparatus for modeling the behavior of cluster systems. Hierarchical cellular automata are proposed for consideration. Conceptually developed a two-dimensional two-level scheme. The expected results are discussed for promising areas of modeling.

Клеточные автоматы перспективны, как апарат для моделирования поведения кластерных систем. Согласно определению, *кластер* есть объединение нескольких однородных элементов, которое может рассматриваться как самостоятельная единица, обладающая определёнными свойствами. Принадлежность элементов к определённым кластерам понимается как систематизация, классификация, распознаванием образов и др., что является статическим аспектом кластеризации. Прикладные области –техника, информатика, лингвистика, социология, экология, биология и др. В статическом варианте - работа с элементами сводится к соотнесению их с определёнными кластерами. Представляет интерес поведение кластерных систем (КС) в динамике: формирование, рост, эволюционирование, деградация. При этом, статический аспект есть набор временных срезов динамического аспекта.

Перспективным для изучения поведения КС во времени, является моделирование. Представляют интерес модели, минимально затрагивающие конкретику прикладной области. В качестве инструмента, перспективны клеточные автоматы (КА). Их возможности и «изобразительные средства» КА варьируются в широких пределах, базируясь на малых наборах правил. При этом, средствами КА может быть продемонстрирован ряд общих (универсальных) свойства КС.

Перспективны для изучения иерархические структуры на КА. Интерес к ним вызван тем, что окружающая действительность (внешний мир, живая природа, социальные структуры, техника, информационные системы) организована иерархично. Соответственно, моделирование элементов окружающего мира (с различной степенью интерпретационной конкретизации) может быть целесообразно (перспективно, полезно, обладает предсказательной силой) именно с учётом принципов иерархичности. В качестве инструмента моделирования, могут быть предложены КА с многоуровневой иерархической организацией, варьирующейся в зависимости от масштаба рассмотрения. Начального

этапа, может быть представлен к рассмотрению двумерный иерархический двухуровневый клеточный автомат (ИДКА).

Поле ИДКА подразделено на соседствующие не пересекающиеся ячейки. В матричной интерпретация, это битовое поле размером M×N ячеек; каждая ячейка размером $m_i \times n_j$ элементов, где $i \in (1, 2, \ldots, M)$, $j \in (1, 2, \ldots, N)$. Ячейки изображают отдельные кластеры; поле вцелом – всю КС. Параметр модели, – кластеры могут быть разных размеров.

Кроме конфигурации поля, другим важным параметром является функция соседства конкретных кластеров. Для всех или некоторых ячеек ИДКА, битовые поля могут случайно или детерминировано заполняться единичными элементами «1», обозначающими «кластерный признак». В зависимости от конкретных условий моделирования, «1» могут перемещаться внутри ячеек случайным образом или детерминировано. Они могут проходить «сквозь стенки ячеек» (переходить из данной ячейки в соседнюю); «отражаться от стенок» (оставаться в своей ячейке); либо, например, раздваиваться - превращаться в два экземпляра, один из которых остаётся в ячейке, а второй – переходит в соседнюю. Так же, в зависимости от условий машинного эксперимента, при столкновениях, «1» могут сливаться или рекомбинировать.

В выборе вариантов правил поведения «1» есть значительная свобода. Следовательно, имеется возможность параметрического расширения модели. Может быть особо оговорено, например, что при столкновении «1» на границе раздела ячеек происходит многократное размножение «1». Ещё одна возможность наращивания параметров – повышение числа состояний «кластерного признака», – переход от битового состояния элементов КА к многоразрядному.

Изучаемыми характеристиками модели являются «населённости» отдельных ячеек (кластеров), а также КС вцелом. Один из ожидаемых эффектов – достижение состояния насыщения при неполном заполнении ячеек ИДКА. Интересно так же изучение эволюции заполнения кластеров от единственной «1» до «насыщения».

Одно из известных прикладных явлений, которое может быть смоделировано в рассматриваемой системе, – «закон Амдала» – наличие порога прироста производительности многопроцессорной вычислительной системы с общей памятью. Данный закон является эмпирическим, а следовательно, интересен для моделирования применительно к конкретным наборам условий, определяющих структуру системы. Развитием изучения этого явления может быть моделирование на ИДКА трафика компьютерных сетей.

Текущее состояние дел – разработана представленная концепция, программно реализованы (этап отладки) ключевые элементы модели, идёт планирование машинных экспериментов.

BIG-DATA. ОБРАБОТКА БОЛЬШИХ ОБЪЕМОВ ДАННЫХ

Даценко А.С., Скрипка В.В.
Научный руководитель – д.т.н., проф. Смеляков К.С.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, каф ЭВМ, тел. (095) 465-51-03)
e-mail: anton.datsenko@nure.ua

Big data is a term that describes the large volume of data – both structured and unstructured – that inundates a business on a day-to-day basis. But it's not the amount of data that's important. It's what organizations do with the data that matters. Big data can be analyzed for insights that lead to better decisions and strategic business moves. The importance of big data doesn't revolve around how much data you have, but what you do with it. You can take data from any source and analyze it to find answers that enable cost reductions, time reductions, new product development and optimized offerings, and smart decision making. When you combine big data with high-powered analytics, you can accomplish business-related tasks.

Большие данные (англ. big data) — серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объёмов и значительного многообразия для получения воспринимаемых человеком результатов, эффективных в условиях непрерывного прироста, распределения по многочисленным узлам вычислительной сети, сформировавшихся в конце 2000-х годов, альтернативных традиционным системам управления базами данных и решениям класса Business Intelligence.

Таким образом под Big Data мы будем понимать не какой-то конкретный объём данных и даже не сами данные, а методы их обработки, которые позволяют распредёлено обрабатывать информацию. Эти методы можно применить как к огромным массивам данных (таким как содержание всех страниц в интернете), так и к маленьким.

Можно сформулировать основные принципы работы с данными: горизонтальная масштабируемость, отказоустойчивость, локальность данных.

Горизонтальная масштабируемость. Поскольку данных может быть сколь угодно много – любая система, которая подразумевает обработку больших данных, должна быть расширяемой. В 2 раза вырос объём данных – в 2 раза увеличили количество железа в кластере и всё продолжило работать;

Отказоустойчивость. Принцип горизонтальной масштабируемости подразумевает, что машин в кластере может быть много. Например, Hadoop-кластер Yahoo имеет более 42000 машин. Это означает, что часть этих машин будет гарантированно выходить из строя. Методы работы с

большими данными должны учитывать возможность таких сбоев и переживать их без каких-либо значимых последствий;

Локальность данных. В больших распределённых системах данные распределены по большому количеству машин. Если данные физически находятся на одном сервере, а обрабатываются на другом – расходы на передачу данных могут превысить расходы на саму обработку. Поэтому одним из важнейших принципов проектирования BigData-решений является принцип локальности данных – по возможности обрабатываем данные на той же машине, на которой их храним.

Все современные средства работы с большими данными так или иначе следуют этим трём принципам. Для того, чтобы им следовать – необходимо придумывать какие-то методы, способы и парадигмы разработки средств разработки данных.

К основным методам анализа и обработки данных можно отнести следующие:

- методы класса или глубинный анализ (Data Mining) – данные методы достаточно многочисленны, но их объединяет одно: используемый математический инструментарий в совокупности с достижениями из сферы информационных технологий;
- краудсорсинг – данная методика позволяет получать данные одновременно из нескольких источников, причем количество последних практически не ограничено;
- A/B-тестирование – из всего объема данных выбирается контрольная совокупность элементов, которую поочередно сравнивают с другими подобными совокупностями, где был изменен один из элементов;
- прогнозная аналитика – специалисты в данной области стараются заранее предугадать и распланировать то, как будет вести себя подконтрольный объект, чтобы принять наиболее выгодное в этой ситуации решение;
- машинное обучение (искусственный интеллект) – основывается на эмпирическом анализе информации и последующем построении алгоритмов самообучения систем;
- сетевой анализ – наиболее распространенный метод для исследования социальных сетей – после получения статистических данных анализируются созданные в сетке узлы, то есть взаимодействия между отдельными пользователями и их сообществами.

Список источников:

1. Smolan R. The Human Face of Big Data/ Erwitt J. – 2012. – 224 с.
2. Adams M. Perspectives on Data Mining// International Journal of Market Research. – 2010. – С. 11–19.

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ ВЫЧИСЛЕНИЯ

Ахундов А.Я., Усков Е.В.
Научный руководитель – д.т.н., проф. Смеляков К.С.
Харьковский национальный университет радиоэлектроники
(61174, Харьков, пр. Л.Свободы, 51Б, тел. (095) 465-51-03)
e-mail: ahanur.akhundov@nure.ua

High-performance computing comes to the rescue in cases where you need to reduce the computation time or get access to a big amount of memory. If you divide the program into parts and execute each of them on a separate node, you can speed up the calculations in proportion to the number of nodes involved.

High-performance computing is computing performed on computer systems with specifications that are much larger than regular computers

Высокопроизводительные вычисления (ВВ) приходят на помощь в тех случаях когда нужно сократить время расчётов или получить доступ к большему объёму памяти. Например, ваша программа может проводить необходимые вычисления в течение недели, но вам нужно получить результаты завтра. Если разделить эту программу на части и выполнять каждую из них на отдельном ноде, то теоретически можно ускорить расчеты пропорционально числу вовлеченных нодов. Но это только теоретически, а на практике этому всегда что-то мешает. Тут стоит упомянуть и другой случай, когда ваша программа требует большой объём оперативной памяти. Например, в вашем компьютере установлено только 4 Гб оперативной памяти, но для расчётов нужно хотя бы 64 Гб. В системах ВВ на каждом ноде установлена память определённой ёмкости. Так если каждому ноду доступно 2 Гб памяти, то опять же можно разделить программу на 32 части, каждая из которых будет выполняться на отдельном ноде, будет взаимодействовать с другими частями, обмениваться данными и, в конечном итоге, программа в целом будет иметь доступ к 64 Гб памяти.

Из этих примеров вы наверняка поняли что высокопроизводительные вычисления – это вычисления проводимые на компьютерных системах со спецификациями, которые значительно превышают обычные компьютеры. Это понятие условное, возможно есть и более точное определение, но я его сейчас не смог найти. Существуют параллельные, распределенные ВВ, а также их комбинации.

Параллельные вычисления предусматривают разработку программ, которые во время их выполнения представляют собой несколько параллельных и взаимодействующих между собой процессов. Например, моделирование характеристик ячейки солнечной батареи предусматривает взаимодействие трёх моделей описывающих: перенос носителей заряда, распространение падающего света внутри ячейки, температурные эффекты, растяжение-сжатие. Так перенос носителей, растяжение-сжатие и

показатель преломления материала, который используется в оптической модели падающего света, зависят от температуры и модели, описывающие эти эффекты, должны взаимодействовать друг с другом в процессе расчета. Чтобы ускорить расчёты можно код модели описывающей транспорт носителей выполнять на одном ноде, код отвечающий за распространение света – на другом, температурную модель – на третьем, и так далее. То есть, ноды будут выполнять взаимодействующие расчёты параллельно.

Распределённые вычисления предусматривают использование нескольких не взаимодействующих друг с другом нодов и процессов. Очень часто в таком случае выполняется один и тот же код на разных нодах. Например, нам нужно оценить растяжение и сжатие той же ячейки солнечной батареи в зависимости от температуры. В таком случае, температура – входной параметр модели и один и тот же программный код этой модели можно выполнить на разных нодах для разных значений температуры.

Выбор между распределенными и параллельными расчетами зависит от организации программного кода используемого для расчётов, самой физической модели, доступности систем ВВ для конечного пользователя. Далее в этой заметке:

- как конечный пользователь взаимодействует с системой ВВ;
- какие ВВ системы доступны и какие у них ограничения;
- о кластерах построенных при помощи ПО Кондор (англ. Condor) и МАТЛАБ (выбор пал на них просто по причине опыта автора с ними);
- немного о суперкомпьютерах и гридах;
- и о том как всем этим хозяйством можно можно воспользоваться.

Список источников:

1. “Высокопроизводительные вычисления для многопроцессорных многоядерных систем” Виктор Гергель - 2012. - 212 с.

2. “Университет Лобачевского” В.П. Гергель - 2010. - 475 с.

КОРРЕКЦИЯ ИЗОБРАЖЕНИЙ НА РЕНТГЕНОВСКИХ СНИМКАХ

Янковская Д.А., Шидловский С.И.
Научный руководитель доцент кафедры ЭВМ Янковский А.А.
Харьковский национальный университет радиоэлектроники
(61066, Харьков, пр. Науки, 14 каф. Электронных вычислительных машин, тел. (057) 702-13-54)
e-mail: daria.yankovska@nure.ua

The given work is devoted to the algorithm for image processing on X-ray images in order to improve the visibility of its individual fragments, which allows to more accurately determine the problem of the patient. The work is carried out under a cooperation agreement between the departments of biochemistry and physiology of Kharkov National Medical University and the Department of Computers of the Kharkov National University of Radio Electronics.

Анализ рентгеновских изображений зачастую затруднен вследствие особенностей человеческого зрения (небольшая разрешающая способность, сложности восприятия яркости при переходе от одного фрагмента изображения на другой), а иногда из-за ухудшения изображения, обусловленного процессами старения пленки, вызывающие частичное отслоение эмульсии, «выцветание изображения» и т.п.

Поэтому при работе с рентгеновскими изображениями всегда возникают задачи по улучшению или восстановлению изображения.

Единого алгоритма анализа и улучшения таких изображения нет. Для каждого изображения необходимо применять различные алгоритмы обработки, связанные либо с выделением отдельных компонентов или с попыткой улучшить изображение.

Ниже предлагается метод улучшения изображения, позволяющий сделать более видимыми отдельные участки.

Первоначальное изображение, полученное в результате сканирования рентгеновского снимка специализированным сканером с разрешением 600 dpi, показано на рис.1.а. Изображение сделано при переломе в третьей фаланге пятого пальца левой руки.

Как видно, изображение малоконтрастное, что затрудняет его анализ.

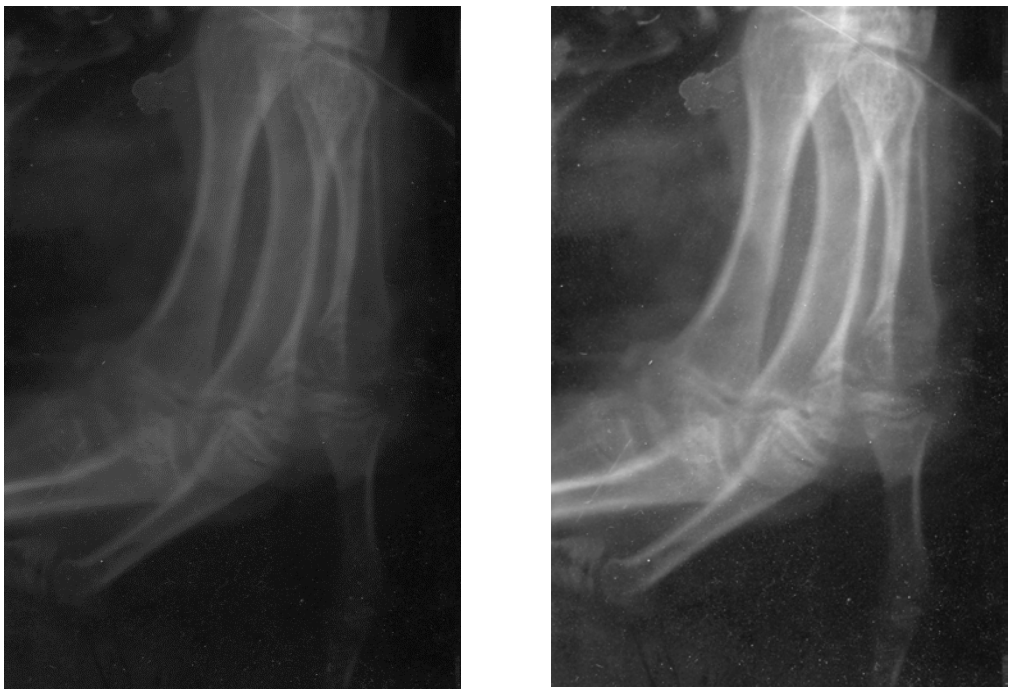
Для улучшения видимости места перелома к данному изображению применили степенное преобразование типа гамма-коррекции:

$$S=cr^{\gamma},$$

где c и γ – положительные числа.

Были проверены различные комбинации значений коэффициента *c* (от 0.1 до 1.5) и показателя степени γ (от 0.1 до 2). Это позволило сделать вывод, что влияние коэффициента *c* на улучшение изображения

незначительно. Основное влияние на улучшение изображения оказывает показатель γ. При этом увеличение значения этого показателя приводит к увеличению яркости пикселов.



а) б)

Рисунок 1 – Результаты процедуры улучшения изображения:
а) исходное изображение, б) обработанное изображение при c=0.6, γ =1.3

Такие действия по улучшению изображения позволяют более точно анализировать изображение при небольшой нагрузке на глаза.

Список источников:

1. Р. Гонсалес, Р. Вудс. Цифровая обработка изображений. СПб.: Питер, 2005.- 1071 с.

2. В.Т. Фисенко, Т.Ю. Фисенко, Компьютерная обработка и распознавание изображений: учеб. пособие. - СПб: СПбГУ ИТМО, 2008. – 192 с.

АЛФАВІТНИЙ ПОКАЗЧИК

ЗМІСТ

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ В XXI СТОЛІТТІ»

Матеріали 23-го Міжнародного молодіжного форуму

Відповідальні за випуск: О.С. Ляшенко

Комп'ютерна верстка Я.В. Дух

Матеріали збірника публікуються в авторському варіанті
без редагування

Підп. до друку 02.04.19. Формат 60x84 1/16. Спосіб друку – ризографія.
Умов.друк.арк. 11,1. Облік. вид.арк. 10,1. Тираж 105 прим.
Ціна договірна Зам № 2-315.

ХНУРЕ. Україна. 61166, Харків, просп. Науки, 14

Віддруковано в редакційно-видавничому відділі ХНУРЕ
61166, Харків, просп. Науки, 14