МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кіровоградський національний технічний університет

Міжнародна науково-практична конференція

«Комп'ютерні технології та інформаційна безпека»

2-3 липня 2015 року

м. Кіровоград
Україна

УДК 003.26;004.49; 004.056; 681.5; 681.323

Комп'ютерні технології та інформаційна безпека: збірник тез доповідей міжнародної науково-практичної конференції, м. Кіровоград, 2-3 липня 2015 року (електронне видання) / Кіровоградський національний технічний університет. – Кіровоград: КНТУ, 2015. – 81 с.

Метою конференції є обмін новими ідеями, отриманими теоретичними і практичними результатами наукових досліджень у галузі інформаційних технологій, програмного забезпечення комп’ютерних систем, інформаційної безпеки держави, суспільства і особистості; обговорення тенденції розвитку сучасних ІТ; встановлення творчих контактів та розширення наукових зв’язків.

МАТЕРІАЛИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«Комп'ютерні технології та інформаційна безпека»

Організаційний комітет

голова:

Левченко О.М. д.е.н., професор

заступники голови:

Смірнов О.А. д.т.н, професор

члени оргкомітету:

Урбанович П. П., д.т.н., професор (Білорусія)

Гуцуляк Е., д.т.н, професор (Молдова)

Стасєв Ю. В.,д.т.н, професор (Украина),

Сидоренко В. В., д.т.н., професор (КНТУ)

Якименко Н. М., к.ф-м.н, доцент (КНТУ)

Коваленко О. В., к.т.н, доцент (КНТУ)

Мелешко Є. В., к.т.н, доцент (КНТУ)

Минайленко Р. М., к.т.н, доцент (КНТУ)

Петренюк В. І., к.ф-м.н, доцент (КНТУ)

Смірнова Н. В., к.т.н, доцент (КНТУ)

Смірнов В. В., к.т.н, доцент – секретар оргкомітету

e-mail: conf-kntu@rambler.ru

*За зміст матеріалів, викладених в тезах доповідей персональну відповідальність несуть автори

ТЕЗИ ДОПОВІДЕЙ ПЛЕНАРНОГО ЗАСІДАННЯ

ТЕЗИ ДОПОВІДЕЙ СЕКЦІЙНИХ ЗАСІДАНЬ

Секція 1. Інформаційна безпека держави, суспільства та особистості

Секція 2. Інформаційні технології та комп'ютерна інженерія

УДК 004.49.5

А.А. Смирнов, докт. техн. наук
Кировоградский национальный технический университет,
assa_s@mail.ru
Мохамад Абу Таам Гани, аспирант
Кировоградский национальный технический университет,
m_aboutaam@hotmail.com
С.А. Смирнов, аспирант
Кировоградский национальный технический университет,
smirnov.ser.81@gmail.com

МЕТОД УПРАВЛЕНИЯ ДОСТУПОМ К ОБЛАЧНЫМ ТЕЛЕКОММУНИКАЦИОННЫМ РЕСУРСАМ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ

Анализ основных угроз информационной и функциональной безопасности телекоммуникационных систем показал явные тенденции к увеличению злоумышленного программного обеспечения, циркулирующего и внедряющегося в средства автоматизированной обработки данных телекоммуникационных систем [1, 2]. Это повышает спрос потребителей на различного рода средства антивирусной защиты данных. В настоящее время в антивирусной индустрии наметилась тенденция перехода на новые, более совершенные, технологии защиты данных от злоумышленного программного обеспечения.

Проведенные исследования показали, что одним из наиболее перспективных направлений совершенствования средств антивирусной защиты данных являются так называемые облачные вычисления (cloud computing), или облачные антивирусы [3]. Это во многом связано с распространением и доступностью телекоммуникационных средств и ресурсов, увеличением числа компьютерных вирусов и повышением стоимости антивирусных средств (обновлений баз данных). В то же время использование подобного рода антивирусных программных ресурсов требует от разработчиков новых технических решений обеспечивающих заданное качество информационного обмена метаданными (специальными сигнатурами файлов) с удаленными облачными системами поддержки и принятия решений. Наиболее сложными, при этом, остаются системы управления телекоммуникационными ресурсами, в которых реализуются методы и процедуры распределения доступа с обеспечением качества передачи телекоммуникационного трафика различного уровня приоритетности.

Таким образом, актуальна задача разработки метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения защиты данных, состоящего из следующих этапов.

На первом этапе разработаны адекватные математические модели ТКС и облачных сетевых ресурсов, в которых моделируется оптимизация распределения информационных потоков в телекоммуникационном оборудовании, усовершенствование процессов функционирования и управления ресурсами ТКС. Эти исследования осуществлялись на основе анализа и систематизации уже известных подходов в предметной области телекоммуникационных сетей, разработки новых методов стратегического и оперативного синтеза (проектирования). Основным методом исследования стал системный метод, который в отличие от других подразумевает комплексное рассмотрение структурных связей, методов, алгоритмов и процедур, а также протоколов и функций ТКС (структурно-функциональный аспект метода), а так же ее поведение в условиях воздействия внешних факторов [4].

Проведенный анализ подходов математического моделирования технологии распространения злоумышленного программного обеспечения, а также процессов информационного обмена в ТКС показал необходимость дальнейшего усовершенствования математической модели технологии передачи данных в процессе информационного обмена специализированными сигнатурами с «облачными» антивирусными системами с целью повышения точности оценки трафика метаданных в ТКС и определения требований оперативности передачи и обслуживания

специальных сигнатур для обеспечения антивирусной защиты данных [4]. Кроме практической составляющей этого этапа исследования, необходимой для разработки метода управления доступом к облачным телекоммуникационным ресурсам, результаты усовершенствования математической модели технологии передачи данных в процессе информационного обмена специализированными сигнатурами с «облачными» антивирусными системами являются входными данными этапа разработки метода управления доступом в интеллектуальных узлах коммутации.

Проведенный анализ существующих моделей интеллектуального узла коммутации, а так же методов решения оптимизационных задач показал необходимость математического моделирования многопротокольного узла коммутации с обслуживанием информационных пакетов различного приоритета, резервированием ресурсов и учётом реальной надёжности обслуживающих приборов. В основу разработки были положены положения теории графов и GERT-моделирования [3]. Это позволило учесть закономерности распределения ресурсов современного сетевого оборудования (интеллектуальных узлов связи) при передаче различного рода информации (в том числе метаданных), а так же внешние факторы (прежде всего изменения интенсивности входного потока информации), и определить функцию распределения случайной величины времени обработки информационных пакетов метаданных и плотность распределения вероятностей времени обработки информационных пакетов метаданных.

Для решения поставленных в результате моделирования оптимизационной задачи были использованы определенные наборы решений, среди которых стоит выделить средства и механизмы обеспечения качества передачи данных реализованные на физическом уровне и уровне доступа модели NGN-сети. В частности методы управления очередями буфера памяти интеллектуального узла коммутации. Поэтому на следующем этапе исследования был разработан алгоритм алгоритма управления доступом к «облачным» телекоммуникационным ресурсам, что позволило обеспечить требуемые значения оперативности при передаче разнородных потоков данных.

Далее была решена задача синтеза исследования позволяющая обосновать направления и способы реализации результатов, обобщенно проведена оценка степени достоверности полученных результатов и определяется их соответствие цели исследования и выдвинутым требованиям [5].

На следующем этапе исследования, на основании результатов решения задачи оптимизации было вынесено общее суждение об эффективности разработанного метода, выявляются закономерности, присущие ТКС. Завершающим этапом исследования было доказательство полноты достижения цели исследования, которое привело к формулированию заключения по теме.

Список литературы

1. Давыдов, В.В. Сравнительный анализ моделей распространения компьютерных вирусов в автоматизированных системах управления технологическим процессом / В.В. Давыдов // Системи обробки інформації. – Харків: ХУПС, 2012. – Вип. 3(101), Том 2. – С. 147-151.
2. Семенов, С.Г. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом / С.Г. Семенов, В.В. Давыдов // Вісник Національного технічного університету «ХПІ». Збірник наукових праць. Серія: Інформатика та моделювання. – Харків: НТУ «ХПІ», 2012. – Вип. 38. – С. 163-171.
3. Смирнов А.А. Математическая gert-модель технологии передачи метаданных в облачные антивирусные системы / В.В.Босько, А.А.Смирнов, И.А.Березюк, Мохамад Абу Таам Гани // Збірник наукових праць "Системи обробки інформації". – Випуск 1(117). – Х.: ХУПС – 2014. – С. 137-141.
4. Смирнов А.А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 4(17). – Харків: ХУПС. – 2014. – С.90-95.
5. Smirnov A.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / , Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.

УДК 681.5.013

К.О. Буравченко, аспірант
Кіровоградський національний технічний університет,
buravchenkok@gmail.com

ОПТИМІЗАЦІЯ ВАРТОСТІ УПРАВЛІННЯ ТА СТАБІЛІЗАЦІЯ СТАНУ СИСТЕМИ ВОДОПОСТАЧАННЯ

Важливим завданням системи управління насосним агрегатом є стабілізація тиску на вході у трубопровід. Значне перерегулювання приводить до не бажаного навантаження на обладнання, збільшення поривів трубопроводів, втрат води і електроенергії. Для забезпечення роботи системи водопостачання у усталеному режимі нами запропоновано використати теорію оптимальної стабілізації. На відміну від існуючих систем даний регулятор мінімізує функціонал вартості, який враховує витрату енергії на керування, відхиленням у реальному часі та відхиленням у кінцевій точці.

Розглянемо завдання регулятора, який підтримує стан системи поблизу заданого значення з мінімальною витратою енергії на управління.

Ставиться завдання знайти такий алгоритм зміни $u(t)$, який би підтримував стан системи на заданому рівні та мінімізував функціонал виду:

$$J(x,u)=\frac{1}{2}\int_{t_0}^{tk}\left[x^T(t)Q(t)x(t)+u^T(t)R(t)u(t)\right]\mathrm{d}t+\frac{1}{2}x^T(t_k)Sx(t_k) \tag{1}$$

Де матриці Q,R,S – симетричні;

R – додатньо визначена,

Q,S – додатньо напіввизначені.

Застосуємо до управління насосним агрегатом в системі водопостачання. Показано, що диференціальне рівняння насосного агрегату:

$$T_1T_2\ddot{x}+(T_1+T_2)\dot{x}+x=ku \tag{2}$$

Приведемо до нормальної системи диференціальних рівнянь, покладемо $x=x_1$.

$$\begin{cases}\dot{x}_1=x_2\\ \dot{x}_2=\dfrac{-x_1-x_2(T_1+T_2)+ku}{T_1T_2}\end{cases} \tag{3}$$

Матриці коефіцієнтів тоді

$$A=\begin{bmatrix}0 & 1\\ -\dfrac{1}{T_1T_2} & -\dfrac{(T_1+T_2)}{T_1T_2}\end{bmatrix};B=\begin{bmatrix}0\\ \dfrac{k}{T_1T_2}\end{bmatrix}$$

$$Q=\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix};R=[1]$$

Враховуючи, що матриця P симетрична, то отримаємо три рівняння:

$$\begin{cases} \dot{p}_{11} = p_{12}\left(\dfrac{2}{T_1T_2} + \dfrac{k^2}{T_1^2T_2^2}\,p_{12}\right) - 1 \\ \dot{p}_{12} = -p_{11} + \dfrac{(T_1+T_2)}{T_1T_2}\,p_{12} + \dfrac{1}{T_1T_2}\,p_{22} + \dfrac{k^2}{T_1^2T_2^1}\,p_{12}p_{22} \\ \dot{p}_{22} = -2\,p_{12} + \dfrac{2(T_1+T_2)}{T_1T_2}\,p_{22} + \dfrac{k^2}{T_1^2T_2^2}\,p_{22}^2 \end{cases} \quad (4)$$

Вирішивши систему диференціальних рівнянь методом Рунге-Кутти знаходимо матрицю P.

Рішення системи відбувається до того моменту поки похідні не стануть константами.

Позначаючи

$$K(t) = -R^{-1}(t)B^T(t)P(t)$$

Отримаємо, що оптимальне управління (14) визначається як

$$u^*(t) = K(t)x(t)$$

Висновки

Для досягнення оптимальної траєкторії руху системи водопостачання в усталеному режимі необхідно мінімізувати функціонал виду (1), вирішивши нелінійне диференціальне рівняння першого порядку типу Ріккаті. Отримавши вектор коефіцієнтів можливо сформувати оптимальний рух системи на всьому відрізку управління.

Список литературы

1. Болтянский В.Г. Математические методы оптимального управления. М., 1968г., 408 стр.с илл.
2. Оптимальное управление движением / В.В. Александров, В.Г. Болтянский, С.С Лемак, Н.А. Парусников, В.М. Тихомиров. – М.: ФИЗМАТЛИТ. 2005. – 376 с.
3. А.А. Воронов. Основы теории автоматического управления. Л. – М. издательство «Энергия», 1966, 364 стр. с. рис.

УДК 004.38

В.В. Смирнов, канд. техн. наук, доцент
Кировоградский национальный технический университет,
swckntu@rambler.ru
Н.В. Смирнова, канд. техн. наук, доцент
Кировоградский национальный технический университет,
snvkntu@rambler.ru

УЧЕБНЫЙ АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ИЗУЧЕНИЯ АРХИТЕКТУРЫ ПРОЦЕССОРОВ

В настоящее время разработано много типов процессоров: от универсальных процессоров общего назначения до специализированных процессоров и контроллеров для выполнения узкого круга задач с высокой скоростью обработки. Изучение архитектур всех видов процессоров в рамках учебного курса является невыполнимой задачей. Тем не менее, у разных процессоров есть общие архитектурные модули, вошедшие в архитектуру процессоров ARM-Cortex. С целью изучения архитектуры процессоров создан учебный аппаратно-программный комплекс для проведения лабораторных работ по дисциплине «Архитектура процессоров» на базе процессора STM32F407.

На рис. 1 представлена структура учебного аппаратно-программного комплекса для изучения архитектуры ARM-процессоров.

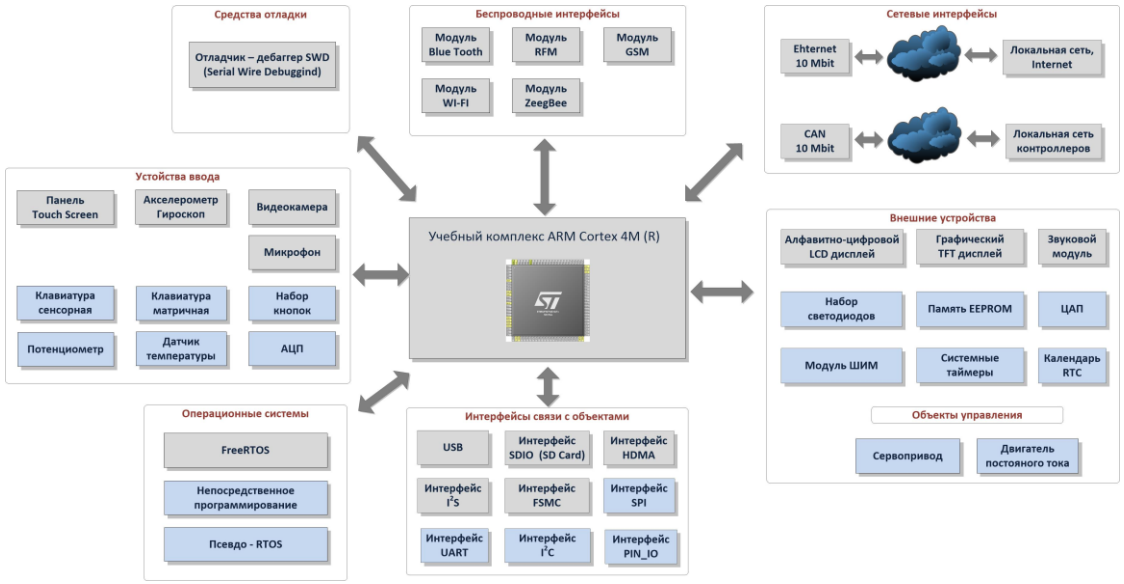


Рис. 1 – Структура учебного комплекса для изучения архитектуры ARM-процессоров

Изучение архитектуры процессора охватывает его внутреннюю структуру на уровне взаимодействия базовых модулей, а также взаимодействие процессора с внешним устройствами и программные средства для реализации его функциональности. Преимуществом данного аппаратно-программного комплекса перед демонстрационными платами является возможность конфигурации схемы любой сложности путем коммутации компонентов комплекса соединительными проводниками и создание соответствующего программного обеспечения, что позволяет реализовать множество задач по изучению архитектуры процессоров в учебных учреждениях.

Список литературы

1. http://www.st.com/
2. Cortex™ - M4F Technical Reference Manual / Cortex™ / Doc ID 022152 Rev 1, 2011, - 164 с.

УДК 681.323

О.Г. Собінов, викладач
Кіровоградський національний технічний університет,
sag_sob@mail.ru

МНОГОЯДЕРНІСТЬ ТА ARM МІКРОПРОЦЕСОРИ. СУЧАСНІСТЬ І ПЕРСПЕКТИВИ

Процесорні архітектури змінюються за законом Мура. Але з 2005 року відмічається призупинення зростання процесорної частоти, тому так цікаві багатопроцесорні системи наступного покоління, повідомлення про які вже з'явилися в пресі. Багатоядерні процесори вже більше десяти років - рушійна сила комп'ютерної революції, яка пов’язана зі стрімким зростанням енергоспоживання одноядерних процесорів.

Багатоядерні ЦПУ спочатку знайшли застосування в серверах. Через відсутність у цей час програмного забезпечення, здатного оптимізувати енергоспоживання багатоядерних пристроїв в ПК, вони з'явилися дещо пізніше. І лише на початку 2011 року почалося виробництво багатоядерних процесорів для мобільних пристроїв. Але темпи їх реалізації в мобільних системах виявилися набагато вище, ніж в комп'ютерах. На виставці CES 2012 вже майже на кожному стенді був представлений смартфон або планшет, оснащений чотирьохядерною ARM-мікросхемою, продуктивність якої було значно вищим, ніж у двоядерних процесорів.

За даними аналітичної компанії Semicast Research в 2015 році кожна людина в світі має має два пристрої на основі ARM процесорів. За період з 2000 по 2015 відвантаження продукції компанії ARM досягли 95 млрд. одиниць, За період з 2000 по 2015 кількість процесорів на основі розробок компанії склали 17 млрд. Проти 0,4 млрд. в 2000 році. У 2011 році щорічні відвантаження процесорів ARM перевищили 7 млрд. одиниць і до 2015 року склали 15 млрд. одиниць. Якщо врахувати, що за даними ООН населення планети до 2016 року складатиме близько 7,5 мільярдів, то такий прогноз відповідає дійсності.

Найперспективніші інноваційні рішення для передових смартфонів і планшетів (що не відносяться до виробів Apple) представляють компанії Qualcomm, Nvidia і, звичайно, ARM. Компанія Qualcomm в 2011 році описала чотирьохядерне ЦПУ, призначене для системи на кристалі наступного покоління Snapdragon S4. Компанія Nvidia розкрила дані про мікропроцесори Tegra 3 (кодове ім'я - Kal El), ARM на конференції ARM Techcon 2012 представила архітектури процесорів Cortex-A7 (Kingfisher) і Cortex-A15 (Eagle), а також розкрила принципи концепції big.little (старший. молодший брат). Всі три архітектури придатні для реалізції багатоядерних структур з високою енергоефективністю і великими обчислювальними можливостями.

Розглянемо біль детальніше їх характеристики.

Чотирьохядерний процесор Snapdragon S4 Pro. На конференції Qualcomm Uplinq 2012 компанія Qualcomm * представила чотирьохядерний процесор APQ8064 (Snapdragon S4 Pro), виконаний на основі принципу асинхронної симетричною мультипроцесорної обробки (Asynchronous Symmetric Multiprocessing, aSMP), з оптимальним співвідношенням продуктивність-енергоспоживання [2, 3]. До переваг асинхронної, самотактуємої архітектури, в якій ядра працюють при різних значеннях напруги і частоти, належить можливість призначення ресурсномістких завдань, що вимагають інтенсивних обчислень, ядру з великим швидкодією, а менш складних завдань - ядру з більш низьким швидкодією.

Архітектура регульованою симетричною мультипроцесорної обробки компанії Nvidia. У лютому 2011 року на найбільшій виставці мобільної промисловості Mobile World Congress компанія Nvidia представила ЦПУ Tegra 3 (Project Kal El) - наступне покоління Tegra 2 - з архітектурою регульованої симетричної мультипроцесорної обробки (Variable Symmetric Multiprocessing, vSMP) [4-6]. Процесор містить чотири ядра високої швидкодії (основні ядра) і ще одне з меншою швидкодією (ядро-компаньйон), тобто так звану компанією 4-плюс-1 чотирьох ядерний пристрій. У систему на кристалі Tegra 3 також

входить 12-ядерний графічний процесор компанії GeForce, який реалізує притаманні ПК ігрові ефекти: динамічне підсвічування, стереоскопічне відтворення.

Архітектура big.little. Аналіз роботи різних мобільних систем показав, що більшу частину часу вони задіяні, коли висока продуктивність зовсім не потрібна, а важливе максимально низьке енергоспоживання. Таким чином, весь час використовувати тільки потужні обчислювальні ядра, які потрібні лише для виконання ресурсоємних додатків (ігор, перегляду відео, веб-серфінгу тощо), невигідно. Так, прийом повідомлень або аудіо інформації успішно виконують процесори на засадах відносно слабких ядер попередніх поколінь, енергія споживання яких менша, ніж у сучасних ЦПУ з потужними ядрами. У підсумку в корпорації ARM народилася концепція big.little, що передбачає спільну роботу у складі однієї системи на кристалі обчислювальних ядер різних поколінь [7]. Таким чином, на відміну від vSMP-архітектури компанії Nvidia в ЦПУ з архітектурою big.little використовуються два типи ядер:

- потужне (big, "велике"), яке виконує завдання, що вимагають обробки великого обсягу даних, наприклад, відтворення відеозапису високої чіткості;
- менш потужне (little, "мале"), що виконує не настільки ресурсомісткі завдання, які вимагають меншої швидкодії, і в результаті більш енергоефективні.

Процесори сімейства Cortex-A50. На конференції ARM TechCon 2012 компанія ARM представила нове сімейство процесорів Cortex-A50, які виконані на основі архітектури ARMv8, набір команд яка підтримує виконання програм Aarch64 і Aarch32, які сумісні з 32-бітним набором команд ARMv7. Процесори сімейства на основі архітектури ARMv8 відрізняються можливістю SIMD-обробки; роботою з командами, які прискорюють програмну криптографію; збільшеним розміром реєстрових файлів; гнучкими режимами адресації; підтримкою тегованих покажчиків; 64-Кбіт сторінками даних; новим режимом обробки виключень; поліпшеним управлінням пам'яттю і вдосконаленою обробкою даних з плаваючою комою (відповідно до IEEE754-2008). Процесори Cortex-A50 працюють спільно з графічним процесором компанії сімейства Mali [6].

Як бачимо, спостерігається цікавість провідних компаній до поліпшення співвідношення споживання енергія-продуктивність високопродуктивних процесорів, які сьогодні представляють собою систему на кристалі і зокрема до архітектури ARM.

Список литературы

1. Pangrle B, Innovation At The Core. - chipdesignmag. com/lpd/pangrle/2011/11/03/ innovation-at-the-core. Snapdragon S4 Processors: System on Chip Solutions for a Mobile New Age. White paper.
2. Qualcomm Announces Next-generation Snapdragon Mobile Chipset Family. Press release. - www.qualcomm.com/media/releases/2011/02/14/qualcomm-announces-next-generation-snapdragon-mobile-chipset-family
3. Variable SMP (4-Plus-1TM) - a Multi-core Architecture for Low Power and High Performance. White Paper. - ttp:// www. nvidia. com/content/PDF/tegra_white_papers/ tegra-whitepaper-091 lb. Pdf.
4. Dean Takahashi. Nvidia launches its Tegra 3 mobile graphics processor - venturebeat.com/2011/ll/08/ nvidia-launches-its-tegra-3-mobile-graphics-processor/#Fbo05uPixSFCdgzw.99 .
5. Shimpi A.L. NVIDIA’s Project Kal-El: Quad-Core A9s Coming to Smartphones/Tablets This Year. - www. anandtech. com/print/4181.
6. Hyun-DukCho, Kisuk Chung, Taehoon Kim. Benefits of the big.LITTLE Architecture. - www.samsung.com/ global/business/semiconductor/minisite/Exynos/data/ benefits.pdf.
7. SemiLex ARM Cortex-A57 и Cortex-A53. - androidtabs.ru/ arm-cortex-a5 7 -i-cortex-a5 3. html
8. Cortex-A50 Series. - www.arm.com/products/processors/ cortex-a5 0/index. php

УДК 004.056

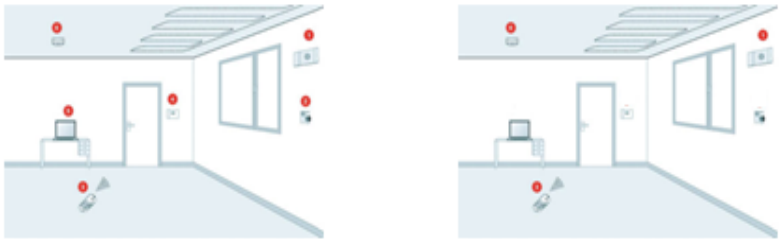
Р.М. Минайленко, канд. техн. наук
Кіровоградський національний технічний університет,
aron70@rambler.ru
С.В. Михайлов, інженер
Кіровоградський національний технічний університет,
schul@rambler.ru

ПРО МОЖЛИВІСТЬ ОБ'ЄДНАННЯ СИСТЕМИ АВТОМАТИЗАЦІЇ І СИСТЕМИ БЕЗПЕКИ ОБ'ЄКТА

Однією з особливостей побудови автоматизованих систем керування (АСК) об'єктами є особливе положення служби безпеки об'єкта, яка вже на рівні технічного завдання вимагає обмеження доступу до всього, що пов'язане з безпекою. Тобто АСК об'єктом відокремлюється від системи контролю доступу, системи відеоспостереження і т.д. [1].

Досвід експлуатації таких систем показує, що використання комплексних рішень під час впровадження АСК об'єктом є значно вигіднішим. Тобто, коли один і той самий датчик використовується і в системі контролю доступу, і для керування мікрокліматом, і в системі протипожежної сигналізації об'єкта [2].

На теперішній час існуючі технології, дозволяють гнучко реалізовувати такі комбіновані системи. В результаті з допомогою лише одного монітора можна відслідковувати параметри роботи АСК об'єктом, а також стан системи відеоспостереження або протипожежної сигналізації об'єкта (рис. 1) [2].



а) б)

Рис. 1 – а) система контролю об'єкта; б) комбінована система контролю об'єкта;
● - датчики контролю об'єкта

Крім того, система безпеки потребує визначених вимог до окремих підсистем. Для прикладу розглянемо АСК мікрокліматом об'єкта. При введенні пожежного режиму, повинна бути відключена система вентиляції, з метою недопущення надходження повітря в задимлену частину приміщення. Частіше всього такі функції реалізуються на рівні шаф керування, але при цьому АСК об'єктом повинна отримувати дублюючий сигнал про введення пожежного режиму тому, що зупинка обладнання буде сприйнята як аварія даного обладнання. [2, 3].

Таким чином, з технічної точки зору система безпеки може бути об'єднана з АСК об'єктом, що приведе до здешевлення таких систем під час їх розробки і впровадження, за рахунок зменшення кількості контролюючого обладнання, а також дасть можливість раціональніше його використовувати.

Список літератури

1. Рыжова В.А. Проектирование и исследование комплексных систем безопасности. – СПб: НИУ ИТМО, 2013. – 156 с.
2. В.В. Панкратов Системы автоматизации и диспетчеризации высотных жилых комплексов / В.В. Панкратов, А.Н. Колубков, Н.В. Шилкин //Автоматизация и регулирование АВОК. - 2005. - № 4.
3. Афанасьев Н. А., Юсипов М. А. Система технического обслуживания и ремонта оборудования энергохозяйства промышленных предприятий. – М.: Энергоатомиздат, 1989.

УДК 519.1

В. І. Петренюк, доцент, канд. фіз.-мат. наук
Кіровоградський національний технічний університет,
petrenjukvi@i.ua

ГРАФ-МОДЕЛІ НА 8-МИ ТА 9-ТИ ВЕРШИНАХ ЯК ОБСТРУКЦІЇ ДЛЯ ТОРА

Основні позначення взяті із [1], [2]. Нехай G неорієнтований скінчений граф без петель і кратних ребер ейлеревого роду $\gamma(G)$, а S - замкнутий 2-многовид роду $\gamma(S)$, де $\gamma(G)=\gamma(S)+1$. Якщо поверхня орієнтована, то позначатимемо її через σ, а якщо це неорієнтована поверхня, то позначатимемо її Σ. Граф G називається таким, що неприводиться над S, або графом-обструкцією роду $\gamma(G)$ для S, якщо для будь-якого власного підграфа H графа G має місце нерівність: $\gamma(H)\le\gamma(S)<\gamma(G)$. Множину всіх графів-обструкцій роду $\gamma(G)$ над S позначимо через ζ(S).

Задача полягатиме у поданні графів-обструкцій роду 2, виписаних в [3], на 8-ми та 9-ти вершинах, у яких кожне ребро є суттєвим відносно роду при операції видалення ребра, як результату φ-перетворення по підмножинам множин точок (точок приєднання із заданими характеристиками – числом досяжності та двостороннім доступом) одного із графів K_5, $K_{3,3}$ (можливо без ребра чи із кількома додатковими ребрами) та квазізірки K із центральним графом M на двох, трьох чи чотирьох вершинах. *Основні результати:* а) теорема 1 для 8-ми вершинних графів-обструкцій роду 2 матимемо $M\in\{K_3,\overline{K_3}\}$; б) теорема 2 про подання графів-обструкцій роду 2 на 9-ти вершинах, як результату φ-перетворення не більше ніж трьох зв'язних графів X,Y,Z одного з наступних випадків:

0) жоден граф із множини $\{X,Y,Z\}$ не гомеоморфний ні K_5, ні $K_{3,3}$, та множини точок приєднання мають число досяжності два та мають розбиватися на пару підмножин із яких одна має число досяжності 2, а та підмножина, що з нею ототожнюється, є досяжною на площині,

1) граф Y гомеоморфний K_5 чи $K_{3,3}$ (можливо із кількома додатковими ребрами) вкладений в тор σ, а інший граф X - є площинним та є 2-мінімальним відносно множини точок приєднання до графа Y на недвоклітці $\sigma\setminus Y$ із нульовими характеристиками θ та $\partial\theta$ для множини точок приєднання до графа Y, або є 3-мінімальним на недвоклітці $\sigma\setminus Y$ із характеристиками θ, $\partial\theta$, де $\theta=1$ чи $\partial\theta=1$ для множини точок приєднання графа X до графа Y, граф Z відсутній;

2) граф Y один з графів K_5 чи $K_{3,3}$, можливо без ребра, вкладений в тор σ, а інший граф X роду 1 є 2-мінімальним відносно множини точок приєднання на недвоклітці $\sigma\setminus Y$ із нульовими характеристиками θ, $\partial\theta$ множини точок приєднання графа X до графа Y, граф Z відсутній;

3) граф Y гомеоморфний K_5 чи $K_{3,3}$ (можливо із кількома додатковими ребрами) вкладений в тор σ, граф Z - проста зірка, граф X є площинною квазізіркою із центральним графом M на двох вершинах, яка не є 2-мінімальним графом на недвоклітці s, $s\in\sigma\setminus Y$, причому існує, принаймні одна, пара вершин простої зірки Z, зформована із елементів множини приєднання графа X до графа Y, що розділяє на ∂s пару кінцевих вершин з множини приєднання графа X до графа Y.

Список літератури

1. Хоменко М. П. φ-перетворення графів. Препринт ІМ НАНУ, Київ, 1971,378с.
2. Хоменко М. П. Топологические аспекти теории графов. Препринт ИМ НАНУ, Киев, 1970.
3. Hur Suhjin. The Kuratowski covering conjecture for graphs of order less than 10. PhD dissertation, Ohio State University, 2008.

УДК 004.925.8

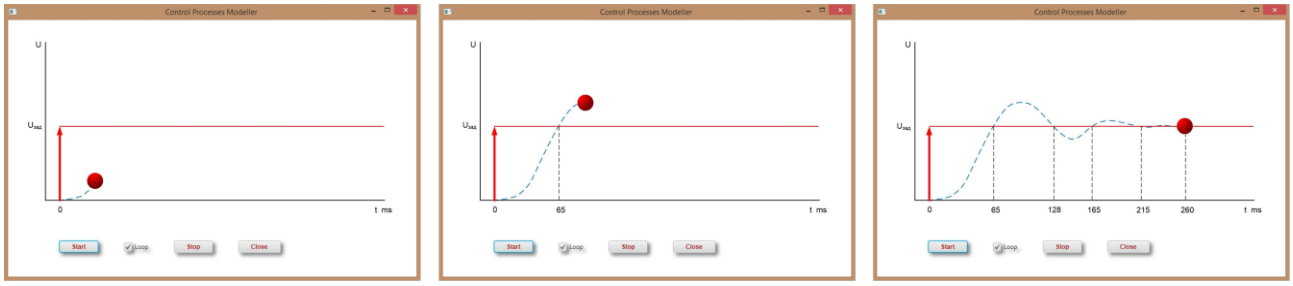
Н.В. Смирнова, канд. техн. наук, доцент
Кировоградский национальный технический университет,
snvkntu@rambler.ru
В.В. Смирнов, канд. техн. наук, доцент
Кировоградский национальный технический университет,
swckntu@rambler.ru

ПРОГРАММИРОВАНИЕ КОМПЬЮТЕРНОЙ ГРАФИКИ ДЛЯ СИСТЕМЫ МОДЕЛИРОВАНИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ

В настоящее время существует много программ, позволяющих моделировать поведение сложных систем, в частности, регуляторов и систем управления. Наиболее известная программа – “Simulink” из программного пакета “Matlab” выполняет возложенные на нее задачи. Однако, при разработке реальных устройств и систем управления, возникает трудность в переносе результатов моделирования из моделирующей программы в конкретную систему управления, и наоборот, из системы управления в моделирующую программу. Результат выполнения задачи в моделирующей программе часто отличается от результата выполнения той же задачи в реальном устройстве.

Нами разработана интерактивная графическая программная система, позволяющая осуществлять исследование, моделирование и разработку систем управления объектом в различных временных масштабах. Переходная характеристика объекта управления может задаваться как в виде аналитического выражения, так и виде траектории. В обоих случаях осуществляется анимация процесса управления объектом в различных временных и амплитудных масштабах.

На рис. 1 представлен результат моделирования процесса управления объектом для ПИД – регулятора.



а) б) в)

Рис. 1 – а) начало процесса б) перерегулирование в) установившийся режим

Графическая программная система создана на платформе JavaFX 8 с использованием классов анимации пакета `javafx.animation`. Использовались классы `Timeline`, а также `Transition`-анимация со встроенной временной шкалой.

Таким образом, использование современных средств программирования компьютерной графики позволяет создавать графические интерактивные системы моделирования процессов управления, что дает возможность проводить экспериментальные исследования на модели объекта в процессе разработки программных систем управления объектом.

Список литературы

1. http://www.oracle.com/
2. Johan Vos Pro JavaFX 8. A Definitive Guide to Building Desktop, Mobile, and Embedded Java Clients / Johan Vos, Weiqi Gao, 2014. – APRESS, 579 с.

УДК 004.056

С.К. Дудник, студент
Кіровоградський національний технічний університет,
dudnik_sy@ukr.net

ІНФОРМАЦІЙНІ ВІЙНИ ТА ЇХ ПАГУБНІСТЬ ДЛЯ СУСПІЛЬСТВА

На даний час великого значення набувають проблеми, пов’язані з веденням інформаційних війн. Різноманітні інформаційні баталії ведуться з використанням комп'ютерних мереж, зокрема в глобальній комп'ютерній мережі Інтернет.

Інформаційні війни, які є природним результатом розвитку світової науково-технічної думки і вдосконалення комп'ютерних і інформаційних технологій, активно включають в свою сферу нові інтернет-технології: соціальні мережі, блоги, електронні журнали, електронну пошту і так далі.

Інформаційні війни - це контентні війни, які мають на меті зміну масової, групової та індивідуальної свідомості. У процесі ведення інформаційних війн йде боротьба за розуми, цінності, установки, поведінкові патерни і т.п.

Інформаційні війни велися задовго до появи Інтернету,і налічують історію, вимірювану навіть не сотнями, а тисячами років. Інтернет перевів ці війни на якісно інший рівень інтенсивності, масштабності та ефективності.

Кіберзброя і кібервійна є важливим, ефективним і економічним компонентом ведення бойових дій в рамках багатовимірної нелінійної війни.

Відповідно, здатність країни вести кібервійну як бойові дії виключно в кіберпросторі, так і використовувати кіберзброю в ході багатовимірної нелінійної сучасної війни є найважливішим показником боєготовності збройних сил держави і гарантом її національної безпеки. З мережевими структурами можуть ефективно боротися тільки інші мережеві структури, здатні працювати в тому ж операційному полі, що і їх противники.

Метою інформаційно-мережевої війни є міцне закріплення більшої частини стратегічно важливих ресурсів країни-супротивника за геополітичним агресором.

При цьому "передача" цих ресурсів агресору здійснюється елітою країни-жертви в значній мірі добровільно, оскільки сприймається нею не як захоплення, а як шлях до розвитку.

Фактично в інформаційно-мережеву війну підключаються практично усі суспільні інститути: в першу чергу, ЗМІ та релігійні організації, заклади культури, неурядові організації. Під деструктивною діяльністю соціальних мережевих структур слід розуміти специфічну людську форму активного ставлення до світу, основний зміст якої складає руйнування або порушення функціонування існуючих об'єктів і систем, що забезпечують нормальне функціонування особистості, суспільства і держави.

Інформаційна зброя являє собою технічні засоби і технології, застосовувані для активізації, знищення, блокування або створення в інформаційній системі процесів, в яких зацікавлений суб'єкт, що застосовує зброю.

Інформація, що посилається може бути спрямована як на зміну фізичного простору, так і на зміну інформаційного простору, але її третьою метою може бути і зміна віртуального простору (ідеологія, релігія, література тощо).

Говорити про якесь самостійне значення кіберпростору як відокремленої сфери ведення війни або відокремленого «театру воєнних дій» не можна. В цілому дії в кіберпросторі у військових цілях являють собою цілеспрямований деструктивний чи інший вплив програмно-апаратними засобами на комп'ютерні мережі, інформацію що зберігається і циркулює в них, особовий склад що обслуговує ці мережі.

Відмінними ознаками дій в кіберпросторі у військових цілях є: наявність чітко сформульованої мети кібервпливу (узгодженої з цілями і завданнями операції, бою, битви);

ретельне планування дій з досягнення поставленої мети і наявність відповідного комплекту сил і специфічних засобів кібервпливу.

Характерними рисами дій в кіберпросторі у військових цілях є:

- високий темп проведення кібервпливу;
- не завжди явний характер деструктивного впливу;
- не завжди явне джерело деструктивного впливу;
- необмежені масштаби впливу;
- непередбачуваність місця і часу кібервпливу противника;
- загроза незворотних катастрофічних наслідків деструктивного впливу.

Можна виділити два види інформаційної боротьби:

- інформаційно-технічна;
- інформаційно-психологічна.

При інформаційно-технічному протиборстві головними об'єктами дії і захисту є інформаційно-технічні системи (системи передачі даних, системи захисту інформації і так далі).

При інформаційно-психологічному протиборстві головними об'єктами дії і захисту є: психіка політеліти і населення протиборствуючих сторін; система формування суспільної свідомості; система формування громадської думки; система ухвалення рішень.

Загалом «полем бою» в інформаційній війні є окрема сучасна людина – саме від її світосприймання, цінностей і мотивацій залежить результат будь-якого впливу. Здавалося б, ера загальних інформаційних свобод і необмеженого спілкування всіх зі всіма в соціальних мережах Інтернету дає всі можливості для самостійного мислення і участі в суспільному житті. Але в реальності інформаційні технології останніх років породили феноменальну керованість суспільної свідомості.

Таким чином треба наголосити на тому, що на сучасному етапі значна увага повинна приділятись тим інформаційним впливам, які спрямовані на зміну думок і вподобань звичайних громадян. Недостатня поінформованість населення та недооцінювання результатів інформаційних впливів можуть призводити до непередбачуваних і згубних наслідків.

Список літератури

1. Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. – Монография, с ил.. – М.: Горячая линия - Телеком, 2003. – 541 с.
2. Панарин И. Н. Технология информационной войны. - М.: Издательство «КСП+», 2003. - 320 с.
3. Бондар Ю.В. Поле битви - інформаційний простір. - К. : МАУП, 2006. - 152с.

УДК 004.056

М.М. Махно, студент
Кіровоградський національний технічний університет,
m.m.mahno@mail.ru

ЗАХИСТ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Поширення інформації – це доведення її до відома хоча б одній особі у будь-який спосіб.

Існує багато різновидів методу ведення інформаційно-психологічної війни та соціального впливу. Обробка підсвідомості людини або групи людей за допомогою навіювання чи спеціальних технічних засобів і прийомів, завдяки яким вони програмуються на беззастережне підпорядкування будь-чиїм наказам, на вчинення будь-яких дій, або на сприйняття якогось навіювання якоїсь ситуації. За допомогою них ми купуємо не потрібні нам товари, йдемо і підтримуємо на мітингах можливо не тих, кого варто було б підтримати, приймаємо карколомні рішення, які вирішують долю зовсім не на краще не лише для нашої сім'ї, а й для країни загалом.

Ми звикли, що ЗМІ використовують як засіб, де можна застосувати теорію «промивання мізків», але знаючи про це, все ж потрапляємо під їхній вплив. ЗМІ працюють зовсім не з переконанням, а з навіюванням. Десятки науково-дослідних центрів розробляють теорію і практику так званого зомбування людей. Основна мета даних практик полягає у створенні слухняної, пасивної людини. Вони мають за мету перетворити народ у масу,створивши з нього легко керовану спільноту.

Засоби масової інформації стали найпотужнішою політичною та ідеологічною зброєю за допомогою якої у народу можуть стерти історичну пам'ять, натомість запропонують щось, зробивши усе так, що народ на це погодиться, ще й буде задоволений.

Телебачення та Інтернет породили свого роду інформаційну наркоманію. Досить підрахувати кількість інформації, яку ми щодня опрацьовуємо, переглядаючи новини в Інтернеті, читаючи газету чи журнал по дорозі додому, дивлячись телевізор за сніданком чи за вечерею, то можна з упевненістю твердити, що ми інформаційні наркомани, які вже не можуть без дози новини чи корисної статті і дня прожити.

Зомбування – це вплив на підсвідомість, підпорядкування людини своїй волі, тобто застосування маніпулятивних методів з метою змінити мислення, поведінку, вірування, емоції або процес прийняття рішень людини, не зважаючи на його волю чи бажання.

Практично будь-який журналіст – це інтуїтивний зомбіст , якщо можна так сказати. Така у них вже професія: вселяти читачеві істину, якою б вона не була.

Інформаційний суверенітет України - це право держави на формування і здійснення національної інформаційної політики відповідно до Конституції і законодавства України, міжнародного права в національному інформаційному просторі України.

Здійснення інформаційного суверенітету України включає:

- законодавче визначення та забезпечення державою стратегічних напрямів розвитку і захисту національного інформаційного простору, цілісної державної інформаційної політики;
- визначення норм, засад і меж діяльності зарубіжних та міжнародних суб'єктів в національному інформаційному просторі України;
- формування та захист інтересів України в світовому інформаційному просторі, міжнародних інформаційних відносинах; гарантування інформаційної безпеки України.

Список литературы

1. ІнформаційнабезпекаУкраїни :http://ua.textreferat.com/referat-7471.html
2. Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. – Монография, с ил.. – М.: Горячая линия - Телеком, 2003. – 541 с.

УДК 004.7.056.53

В.В. Вернигора, студент
Кіровоградський національний технічний університет,
vlad261094@gmail.com

ІНФОРМАЦІЙНА БЕЗПЕКА КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Питання безпеки і захист інформації від несанкціонованого доступу стоїть сьогодні на першому місці за ступенем нагальності. Випадки розкрадання інтелектуальної власності, промислового шпигунства, отримання несанкціонованого доступу до персональних даних і стратегічно важливим інформаційних ресурсів організацій трапляються все частіше і носять все більш серйозний і загрозливого характеру. Масштаби можуть бути самими різними, але суть одна.

Існує два підходи до проблеми забезпечення безпеки комп'ютерних систем та мереж (КС): «фрагментарний» і комплексний.

«Фрагментарний» підхід спрямований на протидію чітко визначеним загрозам у заданих умовах. В якості прикладів реалізації такого підходу можна вказати окремі засоби управління доступом, автономні засоби шифрування, спеціалізовані антивірусні програми і т. П.

Перевагою такого підходу є висока вибірковість до конкретної загрози. Істотний недолік - відсутність єдиної захищеної середовища обробки інформації.

Фрагментарні заходи захисту інформації забезпечують захист конкретних об'єктів КС тільки від конкретної загрози. Навіть невелике видозміна загрози веде до втрати ефективності захисту.

Комплексний підхід орієнтований на створення захищеного середовища обробки інформації в КС, що об'єднує в єдиний комплекс різнорідні заходи протидії загрозам. Організація захищеного середовища обробки інформації дозволяє гарантувати певний рівень безпеки КС, що є безсумнівним достоїнством комплексного підходу.

До недоліків цього підходу відносяться: обмеження на свободу дій користувачів КС, чутливість до помилок установки і налаштування засобів захисту, складність управління.

Сьогодні в області безпеки інформаційних систем застосовуються найрізноманітніші технології захисту інформації. Однак практика показує, що тільки комплекс заходів здатний допомогти в досягненні поставленої мети.

Різні методи захисту інформації повинні застосовуватися паралельно. Синергетичний ефект такого застосування здатний дати серйозні результати.

Для підтримки режиму інформаційної безпеки особливо важливі заходи програмно-технічного рівня, оскільки основна загроза комп'ютерних систем виходить від них самих: збої обладнання, помилки програмного забезпечення, промахи користувачів і адміністраторів і т. д.

В рамках сучасних інформаційних систем повинні бути доступні наступні механізми безпеки :

- ідентифікація та перевірка справжності користувачів;
- управління доступом;
- протоколювання і аудит;
- криптографія;
- екранування;
- забезпечення високої доступності.

Список літератури

1. П. Б. Хорев «Методы и средства защиты информации в компьютерных системах»
2. В.Ф. Шаньгин «Защита информации в компьютерных системах и сетях»

УДК 004.056

Ю.Ю. Гордієнко, студент
Кіровоградський національний технічний університет,
ragehaos@mail.com

СИСТЕМА ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ОСНОВАНА НА АНАЛІЗІ SNMP ПОВІДОМЛЕНЬ

Широке розповсюдження отримала система виявлення несанкціонованого доступу, що грунтується на аналізі SNMP нотифікаційних повідомлень про зміну статусу порту, отримуваних від мережевих комутаторів, і визначення неавторизованих підключень на основі відсутності MAC-адреси пристрою в базі даних авторизованих хостів у мережі.

Протокол SNMP – це протокол, який використовується для управління мережевими пристроями. За допомогою нього програмне забезпечення для управління пристроями мережі може діставати доступ до інформації, яка зберігається пристроях (наприклад, на комутаторі). На цих пристроях протокол SNMP зберігає інформацію про пристрій, на якому він працює, в базі даних [1].

Повідомлення SNMP, що містять, адреси комутатора і номер порту, що знов включився, посилається мережевим комутатором на головний центрадьний сервер моніторингу при зміні статусу будь-якого порту з "OFF" на "ON". Відправку таких повідомлень підтримують навіть найпростіші моделі мережних комутаторів, тому реалізувати інфраструктуру моніторингу всіх портів локальної мережі досить просто. Як серверна частина, що забезпечує збір повідомлень, може виступати сервер мережевого моніторингу (HP Openview, IBM Tivoli, Microsoft MOM, і тому подібне). Далі повідомлення поступають на обробку, де виробляється визначення основних ідентифікаційних параметрів підключення. По-перше, треба визначити всю можливу інформацію про новознайдене з'єднання. Як джерело інформації про з'єднання можуть бути самі мережеві комутатори, база даних структурованої кабельної системи компанії, а також база даних дозволених з'єднань, у якій зберігаються всі будь-коли знайдені підключення.

Основні можливості системи виявлення несанкціонованого доступу, основаної на аналізі SNMP повідомлень:

- при виявленні забороненого підключення НСД автоматично вимикає відповідний порт комутатора;
- при виявленні нового підключення НСД автоматично поміщає відповідний порт комутатора в гостьовий WLAN.
- система реєструє заявку на новий комп'ютер. Після схвалення заявки службою інформаційної безпеки, нове дозволене з'єднання автоматично заноситься в БД з'єднань;
- ведення історії фізичного переміщення пристроїв в мережі [2].

Список літератури

1. Обнаружение несанкционированных подключений к локальной сети в режиме реального времени. [Electronic resourse] / Інтернет-ресурс. - Режим доступу: http://citforum.ru/security/articles/ids/. - Загол. з экрану.
2. Семейство стандартов SNMP. [Electronic resourse] / Інтернет-ресурс. - Режим доступу: http://ru.wikibooks.org/wiki - Загол. з экрану.

УДК 004.056.53

С.А. Стецовська, бакалавр
Одеський національний політехнічний університет
svetastetsovskaya@gmail.com
К.О. Трифонова, ст. викладач
Одеський національний політехнічний університет
katikkatik@gmail.com

РЕАЛІЗАЦІЯ СХЕМИ РОЗДІЛЕННЯ СЕКРЕТУ ДЛЯ МОБІЛЬНОГО ДОДАТКУ

Останні розробки в інформаційних технологіях та техніці надають можливість передавати та зберігати великі обсяги інформації. Тому все більшого значення набуває проблема захисту інформації від несанкціонованого доступу при її передачі чи зберіганні.

Для розв'язку поставленої проблеми застосовують криптографічні методи захисту інформації. Основа криптографічного захисту – секретний ключ, крім очевидних переваг має значний недолік.

Оскільки, якщо зловмисникові вдасться заволодіти цим ключем, то інформація, що захищається, може опинитись в його руках. Потенційним вирішенням цієї проблеми стали схеми розділення секретного ключа.

Пороговой схемою або схемою розділення секрету називається така схема, що дозволяє розділити секрет між кількома учасниками таким чином, щоб заздалегідь задані дозволені групи учасників могли однозначно відновити секрет, а недозволені – не отримали ніякої додаткової інформації про можливе значення секрету [1].

На протязі виконання схеми розділення секрету: для зменшення витрат часу на введення частини секрету для реалізації фази відновлення; для підвищення точності введення частини секрету для реалізації фази відновлення; для зменшення можливості втрати частини секрету – запропоновано використовувати візуальний спосіб зберігання часин секрету учасників.

Тому метою даної роботи є реалізація порогової схеми розділення секрету з візуальним способом зберігання частин для мобільного додатку.

Схема розділення секрету з візуальним способом зберігання частин для мобільного додатку, як кожна схема розділення секрету, побудована у відповідності до протоколу розділення секрету, тому складається з двох основних фаз: фази розділення секрету та фази відновлення секрету.

Фаза розділення секрету з візуальним способом зберігання частин – фаза, коли дилер, якому відомий секрет M, генерує n частин $m_1, m_2, ..., m_n$ секрету, виконує кодування кожної частини в QR код та видає кожному учаснику його частку по захищеному каналу зв'язку.

Роздачу потрібно організувати так, щоб дозволені групи учасників, зібравшись разом, могли однозначно відновити секрет, а недозволені – не могли.

Фаза відновлення секрету з візуальним способом зберігання частин – фаза, коли яка-небудь група з структури доступу Γ об'єднує свої частки секретів і отримує секрет.

Для досягнення поставленої мети розв'язані наступні задачі: реалізована порогова схема розділення секрету Шаміра для мобільного додатку; реалізовано алгоритм кодування та декодування QR коду для зберігання частини секрету учасника схеми розділення секрету Шаміра.

Список літератури

1. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы. Исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2002. – 816 с.

УДК 004.056

П.С.Усік, студент
Кіровоградський національний технічний університет,
mr.usik@ukr.net

СИСТЕМА ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ОСНОВАНА НА АНАЛІЗІ SNMP ПОВІДОМЛЕНЬ

Останнім часом популярною стала система виявлення несанкціонованого доступу, що грунтується на аналізі *SNMP* повідомлень про зміну статусу порту, отримуваних від мережевих комутаторів.

Протокол *SNMP* – протокол, який використовується для управління мережевими пристроями. За допомогою протоколу *SNMP* програмне забезпечення для управління пристроями мережі може діставати доступ до інформації, яка зберігається на керованих пристроях.

На керованих пристроях протокол *SNMP* зберігає інформацію про пристрій, на якому він працює, в базі даних [1]. Повідомлення *SNMP*, що містять, *IP*-адреси комутатора і номер порту, що знов включився, посилається мережевим комутатором на центральний сервер моніторингу при зміні статусу будь-якого порту з "Вимкнений" на "Включений".

Аналіз з'єднання дозволяє визначити важливу інформацію про мережеві властивості (MAC адреса, IP адреса, VLAN, номер порту мережевого комутатора, мережеве ім'я), і місце розташування підключеного комп'ютера.

Після цього, за допомогою бази даних з'єднань, що зберігає інформацію про з'єднання та їх статус "Дозволено / Заборонено", проводиться перевірка з'єднання на легітимність. Якщо оброблюване з'єднання зареєстровано в базі, як дозволене, то на цьому його обробка завершується.

Тобто система просто ігнорує подію, розцінюючи його, як нормальну активність. Якщо ж з'єднання упізнано як Заборонене або непізнане (нове) на консоль Адміністратора безпеки висилається

Тривожне повідомлення, а в Базі Данних З'єднань заноситься інформація про факт нового або забороненого з'єднання. Основні можливості системи виявлення несанкціонованого доступу (НСД), основаної на аналізі SNMP повідомлень:

- при виявленні забороненого підключення НСД автоматично вимикає відповідний порт комутатора;
- при виявленні нового підключення НСД автоматично поміщає відповідний порт комутатора в гостьовий *VLAN*.
- система заявок реєструє заявку на новий комп'ютер. Після схвалення заявки службою інформаційної безпеки інформація про нове дозволене з'єднання автоматично заноситься в БД з'єднань;
- ведення історії фізичного переміщення пристроїв в мережі [2].

Список літератури

1. Обнаружение несанкционированных подключений к локальной сети в режиме реального времени. [Electronic resourse] / Інтернет-ресурс. – Режим доступу: http://citforum.ru/security/articles/ids/.
2. Семейство стандартов SNMP. [Electronic resourse] / Інтернет-ресурс. – Режим доступу: http://ru.wikibooks.org/wiki

УДК 004.056

Н.О. Цимбал, студент
Кіровоградський національний технічний університет,
kroshkanensi@mail.ru

СУТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасні інформаційні технології потребують організації високого рівня захисту даних. Колективне користування інформаційними ресурсами вимагає чіткої постановки задачі захисту окремих папок та файлів та мережевих ресурсів взагалі від несанкціонованого втручання інформаційних зловмисників, вірусів та небезпечних програм. Найважливішим етапом на цьому рівні є фізичний захист самого інформаційного ресурсу. Якщо ж на такому ресурсі зберігаються конфіденційні дані, вони повинні знаходитися у безпечному місці.

Суть інформаційної безпеки - забезпечити безперебійну роботу організації і звести до мінімуму збиток від подій, що таять загрозу безпеки, за допомогою їхнього запобігання і зведення наслідків до мінімуму. Управління інформаційною безпекою дозволяє колективно використовувати інформацію, забезпечуючи при цьому її захист і захист обчислювальних ресурсів. Інформаційна безпека складається з трьох основних компонентів:

- конфіденційність: захист конфіденційної інформації від несанкціонованого розкриття чи перехоплення;
- цілісність: забезпечення точності і повноти інформації і комп'ютерних програм;
- доступність: забезпечення доступності інформації і життєво важливих сервісів для користувачів, коли це потрібно.

Вихідні дані інформаційних систем, що містять секретну інформацію, повинні мати відповідний гриф таємності. Цей гриф повинний відображати категорію таємності найбільш уразливої інформації. Прикладами таких вихідних даних є друковані звіти, інформація, виведена на екрани дисплеїв, дані, збережені на магнітних носіях (стрічках, дисках, касетах), електронні повідомлення і передані файли. Фізичні мітки є найбільш придатною формою маркування. Однак у деяких випадках, наприклад, для електронної передачі даних, можуть знадобитися інші засоби, такі, як процедури, чи контракти поштові повідомлення для виконання функцій маркування.

Також, необхідно забезпечити фізичний захист устаткування від погроз порушення безпеки і небезпек, що представляються навколишнім середовищем. Захист устаткування інформаційних систем (включаючи устаткування, використовуване за межами організації) необхідний як для того, щоб зменшити ризик несанкціонованого доступу до даних, так і для того, щоб не допустити його втрату або ушкодження. Варто також приділити увагу проблемам розміщення устаткування і його утилізації. Можуть знадобитися спеціальні міри для захисту від несанкціонованого доступу й інших небезпек, а також для захисту допоміжного устаткування, наприклад, системи електроживлення і кабельного розведення.

Для запобігання і виявлення випадків впровадження шкідливого програмного забезпечення, потрібно вживання належних заходів обережності. В даний час існує цілий ряд шкідливих методів, що дозволяють використовувати уразливість комп'ютерних програм стосовно їх несанкціонованої модифікації, з такими іменами, як «комп'ютерні віруси», "мережеві хробаки", "троянські коні" і "логічні бомби". Адміністратори інформаційних систем повинні бути завжди готові до небезпеки проникнення шкідливого програмного забезпечення в системи і по необхідності вживати спеціальних заходів по запобіганню або виявленню його впровадження. Зокрема украй важливо вжити заходів обережності для запобігання і виявлення комп'ютерних вірусів на персональних комп'ютерах.

Необхідно реалізувати заходи для виявлення і запобігання проникнення вірусів у системи і процедури інформування користувачів про їхню шкоду. Користувачам варто нагадати, що запобігання вірусів краще, ніж ліквідація наслідків від їхнього проникнення. В основі

захисту від вірусів повинні лежати високі знання і розуміння правил безпеки, належні засоби управління доступом до систем і наступні конкретні рекомендації:

- Організація повинна визначити формальну політику, що вимагає дотримання умов ліцензій на використання програмного забезпечення і заборонити використання несанкціонованих програм.
- Необхідно проводити регулярну перевірку програм і даних у системах, що підтримують критично важливі виробничі процеси. Наявність випадкових файлів і несанкціонованих виправлень повинна бути виявлена за допомогою формальних процедур.
- Дискети невідомого походження варто перевіряти на наявність вірусів до їхнього використання.
- В даний час паролі є основним засобом підтвердження повноважень доступу користувачів до комп'ютерних систем. Призначення паролів необхідно контролювати за допомогою формального процесу управління, що має задовольняти наступним вимогам.
- Вимагати від користувачів підписання зобов'язання по збереженню персональних паролів і паролів робочих груп у секреті.
- У тих випадках, коли користувачі повинні самі вибирати свої паролі, видати їм надійні тимчасові паролі, які вони зобов'язані негайно змінити. Тимчасові паролі також видаються у випадку, коли користувачі забувають свої паролі. Тимчасові паролі повинні видаватися тільки після позитивної ідентифікації користувача.
- Передавати тимчасові паролі користувачам надійним способом. Варто уникати передачу паролів через посередників або за допомогою незахищених (незашифрованих) повідомлень електронної пошти. Користувачі повинні підтвердити одержання паролів.

Ефективний захист інформації є одним з найголовніших аспектів при побудові надійної інформаційної системи будь-якої організації.

Список літератури

1. Попов Л.І., Зубарєв А.В. Основні принципи підвищення ефективності реалізації заходів щодо комплексного захисту інформації. «Альтпресс», 2009. -512с.
2. Купріянов А.І. Основи захисту інформації: навч. Посібник для студ. вищ. навч. закладів / А. І. Купріянов, А. В. Сахаров, В.А. Шевцов - М.: Видавничий центр «Академія», 2006. - 256 с.
3. А.В.Олійник, В.М.Шацька - Навчальний посібник - Львів: "Новий Світ-2000", 2006 - 436 с.

УДК 004.056

Р.В. Гребінка, студент
Кіровоградський національний технічний університет
1995roman12@I.ua

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Вступ. Комп'ютерна мережа – система зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа (КМ) – це система зв'язку через кабельне чи повітряне середовище, самі комп'ютери різного функціонального призначення і мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, як правило – різні види електричних сигналів чи електромагнітного випромінювання. Середовищами передавання у комп'ютерних мережах можуть бути телефонні кабелі, та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали.

Класифікація комп'ютерних мереж за областю дії враховує географічний район, охоплений мережею та, в меншому ступені, розмір мережі. Виділяються типи:

- персональна мережа (Personal Area Networks – PAN)
- локальні мережі (Local Area Networks – LAN)
- кампусні мережі (Campus Area Network – CAN)
- глобальні мережі (Wide Area Networks – WAN)

Безпека ОС базується на двох ідеях:

- ОС надає прямий чи непрямий доступ до ресурсів на кшталт файлів на локальному диску, привілейованих системних викликів, особистої інформації про користувачів та служб, представлених запущеними програмами;
- ОС може розділити запити ресурсів від авторизованих користувачів, дозволивши доступ, та неавторизованих, заборонивши його.

Запити, в свою чергу, також діляться на два типи:

- Внутрішня безпека – вже запущені програми. На деяких системах програма, оскільки вона вже запущена, не має ніяких обмежень, але все ж типово вона має ідентифікатор, котрий використовується для перевірки запитів до ресурсів.
- Зовнішня безпека – нові запити з-за меж комп'ютера, як наприклад реєстрація з консолі чи мережеве з'єднання. В цьому випадку відбувається процес авторизації за допомогою імені користувача та паролю, що його підтверджує, чи інших способів як наприклад магнітні картки чи біометричні дані.

Висновок: В доповнення теми слід зазначити спеціальні випадки, коли вказані типи мереж можуть бути скомбіновані. Наприклад, глобальна мережа може надавати середовище для створення корпоративних мереж, що об'єднують дуже віддалені вузли. Існуючі технології віртуальних мереж забезпечують можливість використання принципів функціонування локальних та корпоративних для комунікацій віддалених об'єктів, з'єднаних через глобальну мережу.

Список літератури

1. Погребняк А.В. «Технології комп'ютерної безпеки» / Погребняк А.В. – Рівне, 2011. - 117 с. – (Книга 3).
2. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

УДК 003.26

В.Г. Андрієнко, студент
Кіровоградський національний технічний університет,
avg94-13@mail.ru

КРИПТОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

У перекладі з грецької мови слово криптографія означає тайнопис. Сенс цього терміна виражає основне призначення криптографії - захистити або зберегти в таємниці необхідну інформацію.

Для забезпечення секретності застосовується шифрування, або криптографія, що дозволяє трансформувати дані в зашифровану форму, з якої витягти вихідну інформацію можна тільки при наявності ключа.

Криптографічні засоби захисту це спеціальні засоби та методи перетворення інформації, в результаті яких маскується її зміст. Основними видами криптографічного закриття є шифрування і кодування даних, що захищаються. При цьому шифрування є такий вид закриття, при якому самостійного перетворенню піддається кожен символ закриваються даних; при кодуванні захищаються дані діляться на блоки, що мають смислове значення, і кожен такий блок замінюється цифровим, буквеним або комбінованим кодом. При цьому використовується кілька різних систем шифрування: заміною, перестановкою, гамуванням, аналітичним перетворенням шифруємих даних. Широке поширення отримали комбіновані шифри, коли початковий текст перетворюється з використанням двох або навіть трьох різних шифрів.

Класичним завданням криптографії є оборотне перетворення деякого зрозумілого вихідного тексту в уявну випадкової послідовність деяких знаків.

Секретність інформації забезпечується введенням в алгоритми спеціальних ключів. Використання ключа для шифрування надає дві суттєві переваги:

- Можна використовувати один алгоритм з різними ключами для відправки послань різним адресатам.
- Якщо секретність ключа буде порушена, його можна легко замінити, не змінюючи при цьому алгоритм шифрування.
- Таким чином, безпека систем шифрування залежить від таємності використовуваного ключа, а не від секретності алгоритму шифрування.
- Можна скористатися одним з відомих методів приховування інформації:
- Приховати канал передачі інформації, використовуючи нестандартний спосіб передачі повідомлень;
- Замаскувати канал передачі закритої інформації у відкритому каналі зв'язку;
- Істотно ускладнити можливість перехоплення, противником переданих повідомлень.

Результатом проведеної роботи є огляд метода криптографій. Було з’ясовано, що криптографія не «ховає» передані повідомлення, а перетворює їх у форму, недоступну для розуміння супротивником.

Список літератури

1. Молдовян А. Криптографія./А. Молдовян, Н. А. Молдовян, Б. Я. Рад - СПб: Лань, 2001
2. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования ГОСТ 28147–89, М., Госстандарт, 1989.

УДК 003.26.09

Р.В. Громов, студент
Кіровоградський національний технічний університет,
the-1975@yandex.ru

ОСОБЛИВОСТІ КРИПТОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Криптографічне перетворення - це перетворення інформації, засноване на деякому алгоритмі, що залежить від змінного параметра (зазвичай називаємого секретним ключем), і володіє властивістю неможливості відновлення вихідної інформації за перетвореною, без знання діючого ключа, з трудомісткістю менше заздалегідь заданої.

Основною перевагою криптографічних методів є те, що вони забезпечують високу гарантовану стійкість захисту, яку можна розрахувати і виразити в числовій формі (середнім числом операцій або часом, необхідним для розкриття зашифрованої інформації або обчислення ключів).

До числа основних недоліків криптографічних методів слід віднести:

- значні витрати ресурсів (часу, продуктивності процесорів) на виконання криптографічних перетворень інформації;
- труднощі спільного використання зашифрованої (підписаної) інформації, пов'язані з управлінням ключами (генерація, розподіл і т.д.);
- високі вимоги до збереження секретних ключів та захисту відкритих ключів від підміни.

Криптографія ділиться на два класи: криптографія з симетричними ключами і криптографія з відкритими ключами.

Симетричні криптосистеми (з секретним ключем - secret key systems) - дані криптосистеми побудовані на основі збереження в таємниці ключа шифрування. Процеси шифрування і розшифрування використовують один і той же ключ. Секретність ключа є постулатом. Основна проблема при застосуванні симетричних криптосистем для зв'язку полягає в складності передачі обом сторонам секретного ключа. Проте дані системи мають високу швидкодію.

В даний час симетричні шифри - це:

- блочні шифри. Обробляють інформацію блоками певної довжини (зазвичай 64, 128 біт), застосовуючи до блоку ключ в установленому порядку, як правило, кількома циклами перемішування і підстановки, які називаються раундами. Результатом повторення раундів є лавинний ефект - наростаюча втрата відповідності бітів між блоками відкритих і зашифрованих даних;
- потокові шифри, в яких шифрування проводиться над кожним бітом або байтом вихідного (відкритого) тексту з використанням гамування. Потоковий шифр може бути легко створений на основі блочного (наприклад, ГОСТ 28147-89 в режимі гамування), запущеного в спеціальному режимі.

Асиметричні криптосистеми (системи відкритого шифрування - в.ш., з відкритим ключем тощо.- public key systems) - сенс даних криптосистем полягає в тому, що для шифрування і розшифрування використовуються різні перетворення. Одне з них - шифрування - є абсолютно відкритим для всіх. Інша ж - розшифрування - залишається секретним. Таким чином, кожен, хто хоче що-небудь зашифрувати, користується відкритим перетворенням. Але розшифрувати і прочитати це зможе лише той, хто володіє секретним перетворенням.

Всі асиметричні криптосистеми є об'єктом атак шляхом прямого перебору ключів, і тому в них повинні використовуватися набагато довші ключі, ніж ті, які використовуються в

симетричних криптосистемах, для забезпечення еквівалентного рівня захисту. Це відразу ж позначається на обчислювальних ресурсах, необхідних для шифрування, хоча алгоритми шифрування на еліптичних кривих можуть пом'якшити цю проблему.

В асиметричних криптосистемах важливо, щоб сеансові і асиметричні ключі були співставні відносно рівня безпеки, який вони забезпечують. Якщо атакуючий дізнається секретний асиметричний ключ, то буде скомпрометована не тільки поточна, але й всі наступні взаємодії між відправником та одержувачем.

Таблиця 1 - Довжина ключа

Довжина симетричного ключа	**Довжина відкритого ключа**
56 біт	384 біт
64 біта	512 біт
80 біт	768 біт
112 біт	1792 біта
128 біт	2304 біта

Для сучасних симетричних алгоритмів (AES, CAST5, IDEA, Blowfish, Twofish) основною характеристикою криптостійкості є довжина ключа. Шифрування з ключами довжиною 128 біт і вище вважається сильним, так як для розшифровки інформації без ключа потрібні роки роботи найпотужніших суперкомп'ютерів. Для асиметричних алгоритмів, заснованих на проблемах теорії чисел (проблема факторизації - RSA, проблема дискретного логарифма - Elgamal) в силу їх особливостей мінімальна надійна довжина ключа в даний час - 1024 біт. Для асиметричних алгоритмів, заснованих на використанні теорії еліптичних кривих (ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002), мінімальної надійною довжиною ключа вважається 163 біт, але рекомендуються довжини від 191 біт і вище.

Кожен з описаних способів реалізації криптографічних засобів захисту інформації володіє як перевагами, так і недоліками. Вибір визначається поставленими завданнями з урахуванням особливостей реалізації, експлуатації та фінансових можливостей. При цьому необхідно брати до уваги апаратні засоби, необхідний ступінь захисту інформації і т.д

Список літератури

1. Х. К. А. ван Тилборг. Основы криптологии. Профессиональное руководство и интерактивный учебник. Мир, М., 2006.
2. О. В. Вербіцький. Вступ до криптології. Видавництво науково-технічної літератури, Львів, 1998 (на укр. яз.).

УДК 003.26

М.М. Махно, студент
Кіровоградський національний технічний університет,
m.m.mahno@mail.ru

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ ТА ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Використання криптографічного захисту інформації при побудові політики безпеки платіжної системи значно посилює безпеку роботи системи.

За принципами використання криптографічний захист може бути вбудованим у платіжну систему або бути додатковим механізмом, який може відключатися. Є дві групи криптографічних алгоритмів:

1) загальні:
- симетричні;
- асиметричні;

2) спеціальні.

Криптографічні алгоритми застосовують із метою:
- шифрування інформації;
- захисту даних і повідомлень (інформації) від модифікації або підробки.

Особливу увагу при вивченні теми потрібно приділити методам розподілу криптографічних ключів між учасниками платіжної системи, а саме методом:
- базово-сеансових ключів;
- відкритих ключів.

Апаратно-програмні засоби криптографічного захисту інформації в СБП забезпечують автентифікацію відправника та отримувача електронних банківських документів і службових повідомлень СБП, гарантують їх достовірність та цілісність, неможливість підроблення або викривлення документів у шифрованому вигляді й за наявності ЕЦП.

Криптографічний захист інформації охоплює всі етапи оброблення електронних банківських документів з часу їх створення до зберігання в архівах банку. Використання різних криптографічних алгоритмів на різних етапах оброблення електронних банківських документів дає змогу забезпечити безперервний захист інформації в СБП.

Криптографічний захист інформації гарантує цілісність та конфіденційність електронної банківської інформації, а також сувору автентифікацію учасників СЕП і їх фахівців, які здійснюють підготовку та оброблення електронних банківських документів.

Для здійснення суворої автентифікації банків (філій), які є учасниками СБП, застосовують систему ідентифікації користувачів, яка є основою системи розподілу ключів криптографічного захисту. Учасник СЕП для забезпечення захисту інформації має трибайтний ідентифікатор, перший знак якого є літерою відповідної території, на якій він розташований; другий та третій знаки є унікальними ідентифікаторами учасника СЕП у межах цієї території.

Ідентифікатори мають бути узгоджені з адресами системи ЕП і бути унікальними в межах банківської системи України. Трибайтні ідентифікатори е складовою частиною ідентифікаторів ключів криптографічного захисту для робочих місць САБ банку (філії), де формуються та обробляються електронні банківські документи. Ідентифікатор ключів криптографічного захисту для робочих місць складається з шести символів, з яких три перші є ідентифікаторами учасника СЕП, четвертий – визначає тип робочого місця (операціоніст, бухгалтер тощо), п'ятий і шостий – ідентифікатор конкретного робочого місця (тобто службовця, який відповідає за оброблення електронних банківських документів на цьому робочому місці).

Трибайтний ідентифікатор учасника СЕП убудований у програму генерації ключів і не може бути змінений учасником СЕП, що забезпечує захист від підроблення ключів від імені

інших учасників СЕП. Ідентифікатори ключів записуються в апаратуру криптографічного захисту інформації (АКЗІ), яка надається учасникам СЕП і забезпечує апаратне формування (перевірку) ЕЦП та апаратне шифрування (розшифрування) на АРМ-НБУ.

Особливої охорони і захисту потребують центри генерації та сертифікації ключів платіжної системи. Вони повинні бути обладнані відповідною обчислювальною технікою, яка пройшла дослідження на побічні електромагнітні випромінювання для захисту від перехоплення і витоку ключової інформації технічними каналами.

Обчислювальна техніка для генерації і сертифікації ключів не повинна входити до локальних мереж центрального банку або повинна бути обладнана відповідною системою захисту від втручання з інших робочих місць локальної мережі. Доступ до приміщень центру генерації і сертифікації ключів повинен бути суворо обмеженим.

Окремо треба подбати про фізичний захист обслуговуючого персоналу платіжної системи та створення безпечних умов їхньої роботи.

Учасник СБП має гарантувати дотримання адміністративних вимог щодо безпечного використання, зберігання та обліку засобів захисту інформації, розподілу повноважень між службовими особами банку (філії), які беруть участь в обробленні електронних банківських документів. Усі засоби захисту інформації Національного банку, що використовуються в СБП, надаються учасникам СЕП територіальними управліннями за умови виконання таких вимог:

- укладення договору про використання криптографічних засобів захисту інформації в системі електронних платежів Національного банку України між банком (філією) і територіальним управлінням тієї області, в якій розташований банк (філія), незалежно від моделі обслуговування консолідованого кореспондентського рахунку;

- забезпечення відповідності приміщень, у яких обробляються електронні банківські документи, використовуються та зберігаються в неробочий час засоби захисту інформації, вимогам до приміщень учасників СЕП, які використовують засоби захисту інформації Національного банку, що визначені нормативно-правовими актами Національного банку щодо правил організації захисту електронних банківських документів;

- призначення службових осіб, які відповідають за зберігання та використання засобів захисту інформації з поданням належно завіреної копії наказу про призначення до територіального управління;

- подання листа-доручення про отримання конкретних засобів захисту інформації.

Засоби захисту інформації для банку (філії) виготовляються Департаментом інформатизації на замовлення територіального управління. Банк (філія) – учасник СЕП не має права передавати засоби захисту інформації іншій установі. Учасник СЕП має забезпечити реєстрацію в окремому журналі такої інформації:

- обліку апаратних та програмних засобів захисту інформації із зазначенням нормативно-правових актів Національного банку, що регулюють порядок їх використання;

- переліку службових осіб, відповідальних за користування та зберігання отриманих засобів захисту інформації;

- переліку службових осіб, на яких, згідно з наказом керівника банку (філії), покладено виконання криптографічного захисту електронних банківських документів.

Список литературы

1. Багриновський К.А. Нові інформаційні технології», М., ЭКО, 2007. – 441с.
2. Крилов І. В. Інформаційні технології: теорія і практика, М., Центр, 2009. – 415с
3. http://pidruchniki.com/12920522/finansi/kriptografichniy_zahist_informatsiyi_zahodi_zahistu_informatsiynoyi_bezpeki

УДК 003.26

Ю.М. Поперека, студент
Кіровоградський національний технічний університет,
yenot2531@gmail.com

ВИМОГИ ДО КРИПТОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Криптографічні методи захисту інформації - це методи захисту даних із використанням шифрування. Криптографічний захист у більшості випадків є більш ефективним і дешевим. Конфіденційність інформації при цьому забезпечується шифруванням переданих документів або всього трафіка.

Перед сучасними криптографічними системами захисту інформації ставлять наступні вимоги:

- зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;
- число операцій, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення і відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;
- число операцій, необхідних для розшифровування інформації шляхом перебору ключів, повинно мати чітку нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень);
- знання алгоритму шифрування не повинне впливати на надійність захисту;
- незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні того самого ключа;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути цілком і надійно сховані в шифрованому тексті;
- довжина шифрованого тексту повинна бути рівна довжині вихідного тексту;
- не повинно бути простих (які легко встановлюються) залежностей між ключами, що послідовно використовуються в процесі шифрування;
- будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації;
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

Сам по собі криптографічний алгоритм, названий алгоритмом шифрування, являє собою деяку математичну функцію, яка використовується для шифрування і розшифровки. Точніше таких функцій дві: одна застосовується для шифрування, а інша - для розшифрування.

Розрізняється шифрування двох типів:

- симетричне (із секретним ключем);
- несиметричне (з відкритим ключем).

При симетричному шифруванні створюється ключ, файл разом з цим ключем пропускається через програму шифрування та отриманий результат пересилається адресатові, а сам ключ передається адресатові окремо, використовуючи інший (захищений або дуже надійний) канал зв'язку.

Адресат, запустивши ту ж саму шифрувальну програму з отриманим ключем, зможе прочитати повідомлення. Симетричне шифрування не таке надійне, як несиметричне, оскільки ключ може бути перехоплений, але через високу швидкість обміну інформацією воно широко використовується, наприклад, в операціях електронної торгівлі.

Несиметричне шифрування складніше, але і надійніше. Для його реалізації потрібні два взаємозалежних ключі: відкритий і закритий. Одержувач повідомляє всім бажаючий свій

відкритий ключ, що дозволяє шифрувати для нього повідомлення. Закритий ключ відомий тільки одержувачеві повідомлення.

Алгоритми, у яких відкритий текст обробляється побітно, називаються *потоковими* алгоритмами або потоковими шифрами. В інших алгоритмах відкритий текст розбивається на блоки, що складаються з декількох біт. Такі алгоритми називаються *блоковими* або блоковими шифрами. У сучасних комп'ютерних алгоритмах блокового шифрування довжина блоку звичайно складає 64 біта.

Симетричні алгоритми при виявленні в них яких-небудь слабкостей можуть бути дороблені шляхом внесення невеликих змін, а для несиметричних - така можливість відсутня.

Симетричні алгоритми працюють значно швидше, ніж алгоритми з відкритим ключем. На практиці несиметричні алгоритми шифрування часто застосовуються в сукупності з симетричними алгоритмами: відкритий текст зашифровується симетричним алгоритмом, а секретний ключ цього симетричного алгоритму зашифровується на відкритому ключі несиметричного алгоритму.

Такий механізм називають цифровим конвертом (digital envelope). Найширше в даний час застосовуються наступні алгоритми шифрування:

- DES (Data Encryption Standard);· Blowfish;
- IDEA (International Decryption-Encryption Algorithm);
- ГОСТ 28147-89;
- RSA (автори: Rivest, Shamir і Alderman);
- PGP.

У симетричних криптоалгоритмах (DES, ДСТ, Blowfish, RC5, IDEA) для шифрування і розшифровки інформації використовується той самий секретний ключ.

У несиметричних криптоалгоритмах (RSA, PGP, ECC) пряме і зворотне перетворення виконуються з використанням відкритого і секретного ключів, що не мають взаємозв'язку, що дозволяє по одному ключу обчислити інший.

Список літератури

1. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ – Петербург; Арлит 2002. – 496 с.;
2. Баранов В.М./Защита информации в системах и средствах информатизации и связи. Учебное пособие. – СПб.: 1996. – 111 с.
3. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика. – 1997. – 364 с.

УДК 004.056.56: 655.25

О.А. Троян, аспірант
Національний університет «Львівська політехніка»,
troyan.oxana@gmail.com

СПОСІБ ЗАХИСТУ ДОКУМЕНТІВ НА ОСНОВІ ЛАТЕНТНИХ ЕЛЕМЕНТІВ ПОБУДОВАНИХ ЗА ДОПОМОГОЮ ФРАКТАЛІВ

Спосіб захисту документів на основі латентних елементів за допомогою фракталів дозволяє захистити та ідентифікувати друковані документи. Метою є розроблення нових методів графічного захисту та створення на їх основі технологій захисту друкованих та електронних документів, які забезпечить високий рівень захисту інформації.

Друковані та електронні документи потребують надійних та ефективних методів та видів захисту від фальсифікації. На сьогоднішній день існує велика кількість способів захисту, які ґрунтуються на використанні нових технологій друку, паперу та фарби, а також післядрукарської обробки. Відомі способи захисту, які є дорогими в реалізації, але є й такі, які не потребують використання вартісних технологій та матеріалів.

Основна стратегія захисту полягає в тому, щоб зробити затрачений час та кошти на виготовлення підробленого документа економічно невигідними. У даній праці розроблено метод захисту, який відноситься до недорогих у реалізації, але трудомістких для підробки, тобто достатньо надійний та ефективний для захисту.

Реалізація методу відбувається на етапі комп’ютерної обробки у додрукарських процесах, що не вимагає використання додаткового спеціального обладнання та може бути використана для захисту як друкованих так і електронних документів.

Упродовж останніх років використовувався цілий ряд методів та технологій захисту документів, зокрема захист криптографічними водяними знаками, гільйошними захисними сітками, латентними елементими, які побудовані на різних теоретичних моделях та структурах.

Проведений аналіз сучасних технологій захисту документів вказує на доцільність розробляння таких методів захисту друкованих та електронних документів, які не потребують застосування особливих технологій та вартісних матеріалів, але разом з тим можуть забезпечити надійний та ефективний захист. У даній роботі розроблено новий метод побудови латентних елементів на основі фракталів для захисту документів, який дозволяє підвищити ефективність захисту.

У побудованому методі латентні елементи формуються на етапі додрукарської підготовки документів. Створюються спеціальні графічні елементи, які містять приховану інформацію, що може бути відтворена тільки при застосуванні відомих розробнику спеціалізованих засобів. В документах під час розробки передбачаються зображення, які підлягають растуванню.

Для забезпечення найвищої поліграфічної якості документів та їх ефективного захисту є необхідність розробити захисні елементи, які базуються на фрактальній основі. Фрактали належать до самоподібних структур, у яких зображення не залежить від масштабу. Опишемо алгоритм побудови захисних елементів на основі фракталів. На рис. 1 подано блок-схему розробленого алгоритму.

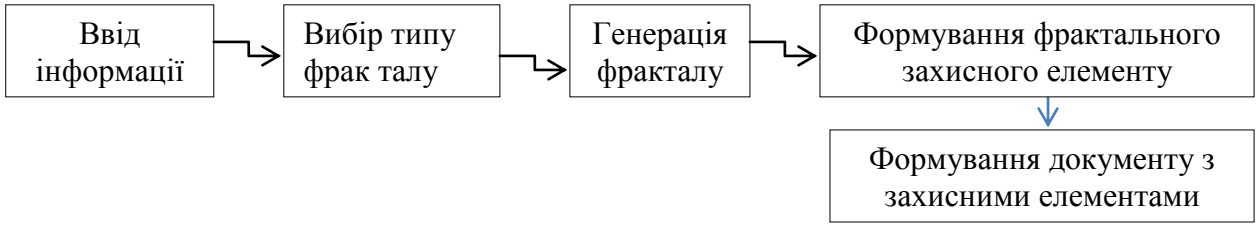


Рис. 1 – Формування захисного елементу на основі фракталу

Побудований алгоритм демонструє процес генерування фракталу для захисту друкованої та електронної інформації. Після обробки вхідних даних генерується фрактал і формується фрактальний захисний елемент, що додається до шаблону документу.

Фракталам притаманні властивості: побудова фрактала здійснюється за допомогою рекурсивної процедури, форма отриманого зображення суттєво залежить від заданих параметрів, самоподібність, тобто подібність частин фракталу до форми усього фракталу, складність фрактального зображення при його збільшенні не змінюється. Саме ці властивості фракталів використовуються для збільшення ефективності захисту розробленим методом.

Цінні папери і документи суворого обліку завжди можуть бути повторені іншими, тому потрібно відтворювати надійні захисти так, щоб підробка обходилася у декілька разів дорожче за оригінал або виробництво займало б багато часу.

Фрактал у вузькому сенсі являє собою складний геометричний об’єкт, який будується в результаті ітераційного циклу, причому окремі частини фрактала подібні за формою усьому фракталу. У широкому сенсі фрактал – це множина точок в евклідовому просторі, що має дробову метричну вимірність, або метричну вимірність, строго більшу від топологічної.

Геометричні фрактали, котрі у двовимірному випадку створюються за допомогою ламаної-генератора. За один крок алгоритму кожен із відрізків ламаної замінюється на ламану-генератор і таким чином у відповідному масштабі створюється геометричний фрактальних образ. До цієї групи фракталів відносяться тріадна крива Коха і дракон Хартера-Хейтуея.

У геометричних фракталів форма описується як послідовність певних геометричних операцій. Наприклад крива Коха стає фракталом в результаті ітерацій, під час яких виконується ділення відрізка прямої на три частини.

Таким образом, проведено дослідження методів, математичних моделей та обчислювальних процедур підвищення якості захисту інформації на основі фрактального підходу. Виявлено, що для створення фракталів необхідно сформулювати обернену задачу моделювання фракталів. Для вирішення поставленої зворотної задачі запропоновано такий спосіб: для заданого зображення або його фрагментів слід підібрати відповідні коефіцієнти перетворення.

Оскільки фрактали представляють дуже складні зображення, а описати їх можна за простими формулами, то для збереження опису цих формул потрібний значно менший обсяг інформації, ніж для збереження відповідних растрових зображень. Наукова новизна виконаних досліджень полягає у тому, що досліджено проблему підвищення якості захисту інформації на основі використання фрактальних функцій для захисту інформації. Потім відбувається перетворення регулярних виразів в кінцеві дані, котрі реалізують необхідні ітераційні цикли. Практична цінність методу полягає в тому, що захист документів стає більш захищеним за рахунок побудови фрактальних елементів в прихованих зображеннях.

Список літератури

1. Кроновер, Р. Фракталы и хаос в динимических системах [Текст] / Р. Кроновер. – М.: Техносфера, 2006. – 488 с.
2. Фрактальный анализ процессов, структур и сигналов [Текст] / Под ред. Р.Э. Пащенко. – Харьков: ЭкоПерспектива, 2006. – 348 с.
3. Уэлстид, С. Фракталы и вейвлеты для сжатия изображений в действии [Текст] / С. Уэлстид. – М.: Триумф, 2003. – 320 с.
4. Назаркевич М. А. Розроблення програмного продукту для захисту інформації на основі плівок із прихованим латентним зображенням / М.А. Назаркевич, О. Троян // Вісник Національного університету «Львівська політехніка». “Комп’ютерні системи та мережі”. – 2014. – № 806. – С. 187–194
5. Назаркевич М. Розробка методу захисту документів латентними елементами на основі фракталів / М. Назаркевич, І. Дронюк, О. Троян, Т.Томащук // Захист інформації, Том 17. – 2015. – № 1. – С. 21–26.

УДК 003.26

П.С.Усік, студент
Кіровоградський національний технічний університет,
mr.usik@ukr.net

МЕТОДИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Сучасним етапом розвитку криптографії, принято вважати той момент, коли вийшла у світ знаменита коротка замітка Діффі і Хеллмана [1] 1976 року. Відомий протокол Діффі і Хеллмана, описаний у зазначеній замітці, вважається першим протоколом з відкритим ключем.

Також визначним в формуванні криптографії є кінець 1970-х рр., в яких відбулися ще дві визначні події в криптографії: поява системи RSA Ривеста, Шаміра і Адлемана і виходом у світ стандарту шифрування DES. Важливо те, що відразу ж було опубліковано опис стандарту, який поклав край монополії надсекретної і всемогутньої організації NSA, котра заперечувала своє власне існування.

Починаючи з того часу, йде бурхливий процес створення, аналізу, дискредитації і знищення численних методів і протоколів шифрування. Все це відбувається паралельно з розвитком і впровадженням обчислювальної техніки.

Саме розвиток обчислювальних можливостей ховає відомі і широко використовувані раніше методи шифрування, криптостійкість яких в справжніх умовах вже не задовольняє необхідним вимогам. Лише окремі методи шифрування витримують потужний натиск аналітиків.

Ясно, що в подібній ситуації істотне значення набувають глибокі математичні теорії. Легко помітити, що багато відомих методи шифрування і складання криптографічних протоколів використовують в якості платформи групи: RSA, дискретний логарифм, еліптичні криві і т.п.

Починають з'являтися публікації, в яких пропонується використовувати ті чи інші абстрактні групи, їх властивості, відомі алгоритми для потреб криптографії. (Див., Наприклад, роботи [2-4], в яких аналізується можливість використання в якості платформи шифрування групи кіс Артинов.

Аналіз даного методу проведено, наприклад, в [5]. В якості ключа в даному методі пропонується використовувати поєднуючий елемент. Деякі загальні напрями використання теоретико-групових властивостей описані в [6].)

Метою цієї доповіді є огляд ряду найбільш відомих методів шифрування і складання криптопротоколів, що базуються на теорії груп. Огляд дозволяє сформулювати ряд принципів, що лежать в основі зазначених методів.

Список літератури

1. Diffie W., Hellman M.E. New directions in cryptography // IEEE Translations on Information Theory, 22, pp. 644–654.
2. Anshel I., Anshel M., Fisher B., Goldfield D. New key agreement protocols in braid group cryptography // Topics in Cryptology – CT-RSA 2001, Lecture Notes in Comput. Sci. 2020, Springer, 2001, pp. 13–27.
3. Anshel I., Anshel M., Goldfield D. An algebraic method for public-key cryptography // Math. Res. Lett. 6, pp. 287–291.
4. Ko K.H., S Lee.J., Han J.W., Kang J., Park C. New public-key cryptosystem using braid groups // Advances in cryptology – CRYPTO 2000 (Santa Barbara, CA), Lect. Notes in Comput. Sci. 1880, Springer, 2000, pp. 166–183.
5. Lee E., Park J.H. Cryptanalysis of the public key encryption based on braid groups // Advances in Cryptology, EuroCrypt 2003, Lect. Notes in Comput. Sci. 2656, Springer, 2003, pp. 477–490.
6. Yamamura A., Saito T. Subgroup membership problem and its applications to information security // Sci. Math. Japonicae, 57 (2003), pp. 23–39.

УДК 004.056.55

Д.А. Горбулінський, студент
Кіровоградський національний технічний університет,
gorbulinskii@gmail.com

ШИФРУВАННЯ, ЗАЛЕЖНЕ ВІД ПОПЕРЕДНІХ БЛОКІВ

Щоб подолати ці проблеми, були розроблені інші режими роботи, встановлені міжнародним стандартом ISO / IEC 10116 і певні національними рекомендаціями, такі, як NIST 800-38A і BSI TR-02102 Загальна ідея полягає у використанні випадкового числа, часто званого вектором ініціалізації (англ. initialization vector, IV).

У популярному режимі зчеплення блоків (англ. Cipher Block Chaining, CBC) для безпеки IV повинен бути випадковим або псевдовипадковим. Після його визначення, він складається за допомогою операції виключає АБО з першим блоком відкритого тексту.

Наступним кроком шифрується результат і виходить перший шіфроблок, який використовуємо як IV для другого блоку і так далі. У режимі зворотного зв'язку за шіфротекста (англ. Cipher Feedback, CFB) безпосередньому шифруванню піддається IV, після чого складається по модулю два (XOR, що виключає АБО) з першим блоком.

Отриманий шіфроблок використовується як IV для подальшого шифрування. У режиму немає особливих переваг в порівнянні з іншими. На відміну від попередніх режимів, режим зворотного зв'язку виводу (англ. Output Feedback, OFB) циклічно шифрує IV, формуючи потік ключів, що складаються з блоками повідомлення.

Перевагою режиму є повний збіг операцій шифрування і розшифрування. Режим лічильника (англ. Counter, CTR) схожий на OFB, але дозволяє вести паралельне обчислення шифру: IV об'єднується з номером блоку без одиниці і результат шифрується.

Отриманий блок складається з відповідним блоком повідомлення.

Слід пам'ятати, що вектор ініціалізації повинен бути різним у різних сенсах. В іншому випадку приходимо до проблеми режиму ECB. Можна використовувати випадкове число, але для цього потрібно досить хороший генератор випадкових чисел.

Тому зазвичай задають деяке число - мітку, відому обом сторонам (наприклад, номер сеансу) і зване nonce (англ. Number Used Once - одноразово використовується число). Секретність цього числа звичайно не потрібно. Далі IV - результат шифрування nonce. У разі режиму лічильника, nonce використовується для формування раунд ключа Ki:

$$K\_i = E\_K (nonce \| i-1), i = 1, .., n,$$ де i - номер раунду.

Якщо довжина самого повідомлення, або останнього блоку, менше довжини блоку, то він потребує доповнення. Просте додаток нульовими бітами не вирішує проблеми, оскільки одержувач не зможе знайти кінець корисних даних. До того ж, такий варіант призводить до атак Оракула доповнення.

Список літератури

1. Diffie W., Hellman M.E. New directions in cryptography // IEEE Translations on Information Theory, 22, pp. 644–654.
2. Anshel I., Anshel M., Fisher B., Goldfield D. New key agreement protocols in braid group cryptography // Topics in Cryptology – CT-RSA 2001, Lecture Notes in Comput. Sci. 2020, Springer, 2001, pp. 13–27.
3. Anshel I., Anshel M., Goldfield D. An algebraic method for public-key cryptography // Math. Res. Lett. 6, pp. 287–291.

УДК 004.056.53

В.Р. Зіновський, студент
Одеський національний політехнічний університет
v.zinovskyi@gmail.com
К.О. Трифонова, ст. викладач
Одеський національний політехнічний університет
katikkatik@gmail.com

АУДИТ ВРАЗЛИВОСТІ ВЕБ-ДОДАТКУ ЗАСОБАМИ СТЕГАНОАНАЛІЗУ

На сьогоднішній день інформатизація є одним з пріоритетних напрямків розвитку всіх економічних галузей. Практично кожна організація має свій інтернет-сайт.

В електронному вигляді зберігаються персональні дані клієнтів і співробітників, фінансова інформація [1]. У зв'язку з цим завдання аудиту та забезпечення безпеки веб-додатків стає важливішим рік від року. Кожного року відкритий проект захисту веб-додатків OWASP проводить дослідження та публікує класифікацію найбільш поширених вразливостей веб-додатків.

На даний час це:

- вставка інструкцій;
- некоректна аутентифікація та управління сеансами;
- міжсайтове виконання сценаріїв;
- небезпечні прямі посилання на об’єкти;
- небезпечна конфігурація оточення;
- витік критичних даних;
- відсутність контролю доступу до функціонального рівня;
- підробка міжсайтових запитів;
- використання компонентів з відомими вразливостями;
- небезпечні переадресування [2].

Але не так давно індійський дослідник безпеки Саум Шах опублікував звіт про розроблений ним метод атаки, заснованому на популярному серед користувачів обміні посилань на зображення.

Спеціаліст зміг приховати виконуваний шкідливий код в пікселях довільної картинки, залишаючи таким чином свій експлоїт на самому видному місці. Дослідник відзначає, що приховати шкідливий код безпосередньо в зображенні було найскладнішим, і для цього йому довелося використовувати стеганографію. Частини шкідливого коду Шах розподілив всередині пікселів картинки, що дозволяє декодувати їх назад за допомогою елемента Canvas в HTML 5, який проводить динамічний рендеринг зображень.

Тому в даній роботі виконана реалізація автоматизованої системи аудиту та визначення вразливості веб-додатку засобами стеганоаналізу. Робота стеганоаналізу полягає в пошуку та аналізі певних характеристик та ознак у досліджуваному цифровому зображенні, визначенні факту наявності або відсутності яких дозволяє отримати відповідь на питання, чи є об'єкт, що розглядається, стеганоповідомленням або ж він не піддавався стеганоперетворенню [3]. В якості стеганоаналітичного алгоритму для реалізації системи використано алгоритм заснований на аналізі кількості близьких пар кольорів та унікальних пар кольорів [3]. Запропонована модифікація алгоритму на основі введення нового визначення кількості унікальних пар кольорів. Для підвищення швидкості роботи алгоритму реалізовано обраний алгоритм засобами паралельного програмування Node.js.

Список літератури

1. Статистика уязвимостей веб-приложений. – Режим доступу: http://www.ptsecurity.ru/download/PT_Web_application_vulnerability_2014_rus.pdf.
2. OWASP Топ 10. Десять найбільш критичних ризиків для безпеки веб-додатків. – Режим доступу: https://www.owasp.org/index.php/Top_10_2013-Top_10.
3. Узун, И.А. Стеганоанализ цифровых изображений, хранящихся в произвольных форматах / И.А. Узун // Информатика и математические методы в моделировании. – Одесса. – Том3,№2. – 2013. – С. 179–189.

УДК 004.056

О.А. Філіппов, студент
Кіровоградський національний технічний університет,
alex.fil25@yahoo.com

СТЕГАНОГРАФІЯ В ОРГАНІЗАЦІЇ ОБМЕЖЕНОГО ДОСТУПУ ДО ВІДЕОДАНИХ

Цифрове представлення матеріалів, захищених авторським правом, таких як фільми, музичні композиції, а також фотографії має безліч переваг. Однак факт необмеженості незаконного копіювання є серйозною загрозою для прав власників та авторів.

До недавнього часу основним інструментом для захисту прав власників вмісту було шифрування. Шифрування захищає вміст при передачі даних від відправника до одержувача, однак, після отримання та наступного розшифрування, дані більше не мають захисту [1].

Стеганографія являє собою сукупність методів заснованих на різних принципах які забезпечують приховування самого факту існування секретної інформації в тому чи іншому середовищі, а також засобів реалізації цих методів [1].

Стеганографічні методи реалізовані на основі комп'ютерної техніки і програмного забезпечення в рамках окремих систем обчислення чи управління, корпоративних чи глобальних обчислювальних мереж складові предмету вивчення комп'ютерної стеганографії. Існують певні відмінності між технологіями цифрових водяних знаків (ВЗ) з одного боку та, власне, стеганографічними технологіями приховування таємної інформації для її подальшої передачі або зберігання. Цифрові ВЗ доповнюють шифрування. Вони вбудовують непомітний сигнал до даних, через що основною перевагою є те, що вміст контейнера нероздільний з ВЗ.

Їх властивості, як, наприклад, реакція на загальні перетворення сигналу або умисні атаки,стали важливими. Розвиток зв'язку через комп'ютерні мережі викликав поширення використання комп'ютерної стеганографіі. Відеозв'язок використовує алгоритми стиснення для забезпечення прийнятної якості навіть на низькій швидкості передачі даних систем, таких як ISDN (Integrated Services Digital Network) [2].

ЦВЗ можна також використовувати для виявлення потенційних піратів: під час продажу в зображення вбудовують інформацію про час продажу та інформацію про покупця. Ключовою відмінністю ЦВЗ від звичайного приховання інформації є наявність активного противника. Наприклад, використовуючи ЦВЗ для захисту авторського права, активний противник намагатиметься видалити чи змінити вбудовані ЦВЗ. Тому основною вимогою є стійкість вбудованих даних до атак. Таємність не є настільки важливою, як у прихованій комунікації.

Зазвичай методи стиснення спричиняють втрати і тому відновлене зображення не збігається з оригіналом. Приховану інформацію майже завжди можна знищити, якщо метод має масове поширення. Незнищенних цифрових знаків поки не існує. Нові методи перевіряють, як правило, на стандартні атаки, однак для кожного з них завжди знаходиться спеціальна атака [3].

Список літератури

1. Генне О.В. Основные положения стеганографии. – 2000. – № 3. – 10 с.
2. Грибунин В.Г. Цифровая стеганография /В.Г.Грибунин, И.Н.Оков, И.В.Туринцев, - М: Солон-Пресс, 2009.-с264.
3. Канахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф.Канахович, А.Ю.Пузиренко,- МК-Прес,2006.-с.288.

УДК 004.056

Ф.И. Василенко, студент
Кировоградский национальный технический университет,
fedir.vasylenko@mail.ru

СОВРЕМЕННЫЕ ТЕХНИЧЕСКИЕ СРЕДСТАВ БОРЬБЫ С КОМПЬЮТЕРНЫМИ ВИРУСАМИ

Необходимо отметить, что компьютерные вирусы (КВ), или, как более правильно, программные вирусы (ПВ), являются в настоящее время наиболее эффективным средством доставки и внедрения различных разведывательных программ.

Цикл жизни вируса обычно включает следующие периоды: внедрение, инкубационный, репликация (саморазмножение) и проявление. В течение инкубационного периода вирус пассивен, что усложняет задачу его поиска и нейтрализации. На этапе проявления вирус выполняет свойственные ему целевые функции, например необратимую коррекцию информации на магнитных носителях (жестких либо гибких).

Наиболее распространенным средством нейтрализации вирусов являются программные антивирусы. Антивирусы, исходя из реализованного в них подхода к выявлению и нейтрализации вирусов, принято делить на следующие группы: детекторы, фаги, вакцины, прививки, ревизоры, мониторы

Таблица 1: Перечень существующих вирусов.

Класс вируса	Виды вируса	Характер воздействия
Не повреждающие файловую структуру	Размножающийся В ОЗУ Раздражающие оператора Сетевые	Имитация неисправности Процессора, НМД, принтера, портов дисплея, клавиатуры. Формирование на терминале текстовых и графических сообщений. Синтез речи, формирование мелодии и звуковых спецэффектов. Переключение режимов настройки клавиатуры, дисплея, принтера, портов.
Повреждающие файловую структуру	Повреждающие пользовательские программы и данные. Разрушающие системную Информацию (в том числе криптовирусы)	Разрушение исходных текстов программ, библиотек компиляторов, искажение баз данных, текстовых документов. Разрушение логической системы диска, искажение структуры заполнения носителя, форматирование носителей, повреждение файлов ОС
Действующие на аппаратуру и оператора	Выводящие из строя аппаратуру, действующие на оператора	Выжигание люминоформа, повреждение микросхем, магнитных дисков, принтера.

Как видно из таблицы 1, наибольший вред с точки зрения утечки информации могут нанести криптовирусы, поскольку они в состоянии пробить брешь даже в таком мощном средстве обороны, как криптозащита. Например, в момент проставления электронной подписи криптовирусы могут перехватить секретные ключи и скопировать их в заданное место.

Таблица 2: Перечень антивирусных систем

Средство защиты	Назначение	Программы	Принцип действия
Детектор	Обнаружение зараженных вирусом файлов	ViruScan NetScan Aidstest	Поиск участка кода, принадлежащего известному вирусу
Фильтр	Перехват «подозрительных» обращений в ОС и сообщение о них пользователю	FluShot Plus Anti4Us Floserum Disk Monitor Vshield	Контроль действий, характерных для вируса
Доктор (фаг)	Лечение зараженных программ или дисков	Clear-Up, M-Disk, Aidstest Dr.Web	Уничтожение тела вируса
Ревизор	Постоянная ревизия целостности файлов	Validate	Запоминание сведений о состоянии программ и системных областей дисков, сравнение их состояния с исходным
Доктор-ревизор	Обнаружение и «лечение» зараженных файлов	Dr.Veb, Nod32, и другие	Обнаружение изменений в файлах и дисках и возврат их в исходное состояние

Анализ современных антивирусных программ показывает, что в последнее время наметилась явно выраженная тенденция к интеграции различных видов программ в единое программное средство с функциями детектора–ревизора–доктора, что делает это средство удобным для пользователя. Однако приходится констатировать, что в настоящее время абсолютной защиты от неизвестных вирусов не существует, поэтому антивирусные программы постоянно обновляются, как правило, не реже одного раза в месяц.

Список літератури

1. Торокин А.А. Инженерно – техническая защита информации. – М.: Гелиос АРВ, 2005.
2. Титаренко Г.А., Брага В.В., Вдовенко Л.А. и др. (под ред. Г. Титаренко). Информационные технологии управления. Учебник для вузов. – М.: ЮНИТИ-ДАНА, 2005.
3. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение. – М.: Солон-Пресс, 2004.
4. Гринберг А.С., Горбачев Н.Н., Теплякова А.А. Защита информационных ресурсов государственного управления. Учебник для вузов. –М.: ЮНИТИ, 2003.

УДК 004.056

Васьков Д.О., студент
Кіровоградський національний технічний університет
kavabangaa27@gmail.com

ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ. Під інформаційною безпекою розуміється захищеність інформації і підтримуючої інфраструктури від будь-яких випадкових або навмисних неправомірних дій, результатом яких може з'явитися нанесення збитку самій інформації, її власникам або підтримуючої інфраструктури.

Основна частина.Самими поширеними способами несанкціонованого отримання конфіденційної інформації:

- прослуховування приміщень за допомогою технічних засобів;
- спостереження (у т. ч. фотографування та відеозйомка);
- перехоплення інформації з використанням засобів радіомоніторингу інформативних побічних випромінювань технічних засобів;
- читання залишкової інформації в запам'ятовуючих пристроях системи після виконання санкціонованих запиту, копіювання носіїв інформації;
- несанкціоноване використання терміналів зареєстрованих користувачів за допомогою розкрадання паролів;
- внесення змін, дезінформація, фізичні та програмні методи руйнування (знищення) інформації.

Попередження витоку інформації по акустичних каналах зводиться до пасивних і активних способів захисту. Відповідно, всі пристосування захисту інформації можна сміливо розділити на два великих класи – пасивні і активні. Пасивні – вимірюють, визначають, локалізують канали витоку, нічого не вносячи при цьому в зовнішнє середовище. Активні – «зашумлюють», «випалюють», «розгойдують» і знищують всілякі спецзасобів негласного отримання інформації.

Пасивний технічний засіб захисту – пристрій, що забезпечує приховування об'єкта захисту від технічних засобів розвідки шляхом поглинання, відбиття або розсіювання його випромінювань. До пасивних технічним засобам захисту ставляться екрануючі пристрої та споруди, маски різного призначення, розділові пристрою в мережах електропостачання, захисні фільтри і т. д. Мета пасивного способу – максимально послабити акустичний сигнал від джерела звуку, наприклад, за рахунок обробки стін звукопоглинаючими матеріалами.

Активний технічний засіб захисту – пристрій, що забезпечує створення маскують активних перешкод (або імітують їх) для засобів технічної розвідки або порушують нормальне функціонування засобів негласного знімання інформації.

Висновки. Для побудови надійної системи захисту інформації необхідно виявити всі можливі загрози безпеки, оцінити їх наслідки, визначити необхідні заходи і засоби захисту, оцінити їх ефективність.

Список літератури

1. Конявскій В.А. Управління захистом інформації на базі СЗІ НСД "Акорд"/ В.А. Конявскій - М: Радіо і зв'язок, 1999. – 323 с.
2. Стрільців А.А. Забезпечення інформаційної безпеки / Під ред. В.А. Садовничого і В.П. Шерстюка - М. МЦНМО, 2002. – 296 с.
3. Зегжда Д.П. Основы безопасности информационных систем / Зегжда Д.П., Ивашко А.М.. - М.: Горячая Линия - Телеком, 2000. - 452 с.

УДК 004.056

А.В.Панська, студентка
Кіровоградський національний технічний університет,
annapanskaya@mail.ru

ЗАХИСТ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу (НСД) і захисту інформації від витоку технічними каналами. Під НСД звичайно мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали сторонніх електромагнітних випромінювань і наведень (ПЕМІН), акустичні канали, оптичні канали й ін.

ТОВ «УЛІС Сістемс» має ліцензію на розробку, виробництво, впровадження, дослідження ефективності, супровід засобів і комплексів інформаційних технологій із захистом інформації від НСД, надання консультаційних послуг. Для рішення всього комплексу завдань з технічного захисту інформації ми співробітничаємо із провідними підприємствами й організаціями, що працюють в області захисту інформації (у тому числі, із Службою безпеки України).

Захист від НСД може здійснюватися в різних складових інформаційної системи:

- прикладне й системне ПЗ;
- апаратна частина серверів і робочих станцій;
- комунікаційне устаткування й канали зв'язку;
- периметр інформаційної системи.

Для захисту інформації на рівні прикладного й системного ПЗ нами використовуються:

- системи розмежування доступу до інформації;
- системи ідентифікації й аутентифікации;
- системи аудита й моніторингу;
- системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

- апаратні ключі;
- системи сигналізації;
- засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовуються наступні засоби мереженого захисту інформації:

- міжмережеві екрани (Firewall) – для блокування атак із зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway і Alteon Switched Firewall від компанії Nortel Networks). Вони управляють проходженням мереженого трафіка відповідно до правил (policies) безпеки. Як правило, міжмережеві екрани встановлюються на вході мережі й розділяють внутрішні (частки) і зовнішні (загального доступу) мережі;
- системи виявлення вторгнень (IDS - Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу "відмова в обслуговуванні" (Cisco Secure IDS, Intruder Alert і NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки й витрати на підтримку працездатності мережі;
- засоби створення віртуальних приватних мереж (VPN - Virtual Private Network) – для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її дінамічного шифрування;

- засоби аналізу захищеності - для аналізу захищеності корпоративної мережі й виявлення можливих каналів реалізації погроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon).

Їхнє застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Для захисту периметра інформаційної системи створюються:

- системи охоронної й пожежної сигналізації;
- системи цифрового відеоспостереження;
- системи контролю й керування доступом (СККД).

Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами й заходами:

- використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях;
- установкою на лініях зв'язку високочастотних фільтрів;
- побудовою екранованих приміщень ("капсул");
- використанням екранованого устаткування;
- установкою активних систем зашумлення.

З метою оцінки стану технічного захисту інформації, що обробляється або циркулює в автоматизованих системах, комп'ютерних мережах, системах зв'язку, і підготовки обґрунтованих виводів для прийняття відповідних рішень звичайно проводиться експертиза в сфері технічного захисту інформації.

На основі наведених засобів і заходів ТОВ «УЛІС Сістемс» пропонує наступні рішення:

- побудова комплексних систем захисту інформації локальних, глобальних і корпоративних обчислювальних мереж;
- розробка політики безпеки організації;
- сприяння в організації експертиз по ТЗІ;
- інтеграція устаткування й програмного забезпечення технічного захисту інформації в існуючу інформаційну систему організації;
- установка систем захисту периметру.

Список літератури

1. Хорошко В.А., Чекатов А.А. Методы и средства защиты информации. – К. : ЮНИОР, 2003. – 504 с.
2. Максименко Г.А., Хорошко В.А. Методы выявления, обработки и идентификции сигналов радиозакладных устройств. – К. : ПолиграфКонсалтинг, 2004. – 317 с.

УДК 004.7.56

А.В. Сахарова, студентка
Кіровоградський національний технічний університет,
lightsayder@mail.ru

ЗАХИСТ ІНФОРМАЦІЇ В ПРИСТРОЯХ МІКРО-ЕОМ

На даний час важливим питання стало саме процедура забезпечення цілісності та захисту даних від зовнішніх та внутрішніх факторів, що можуть нашкодити роботі підприємства чи приватної особи.

В пристроях мікро-ЕОМ процес захисту інформації має свої особливості, так як дані, що фіксуються та передаються пристроєм досить різноманітні та специфічні.

В мікро-ЕОМ необхідно ряд заходів для захист таких даних як:

- звукові сигнали, оскільки вони можуть бути змінені зовнішніми фактора, навмисними чи ненавмисними звуковими сигналами, що порушили б цілісність звукового ряду переданої інформації;
- електроживлення пристрою, зовнішні засоби можуть внести порушення в функціональність роботи пристрою та порушити передачу/отримання/зберігання даних;
- технічні канали, через які можлива передача чи отримання даних з пристрою;
- технічні засоби, що можуть бути порушені від ненавмисних та навмисних імпульсних завад у мережі живлення;
- інформації, що обробляється засобами обчислювальної техніки від витоку, викликаною побічним електромагнітним випромінюванням та наводками.

В мікро-ЕОМ реалізовані такі вимоги з технічного захисту інформації:

- аутентифікація користувачів шляхом системи паролів;
- аутентифікація користувачів шляхом персональних ідентифікаційних пластикових карток;
- протоколювання режиму експлуатації ЕОМ зареєстрованими користувачами з веденням журналу роботи в енергонезалежній пам'яті контролера захисту даних;
- кодування інформації, що зберігається на ЖМД, за допомогою апаратних засобів контролера захисту даних з використанням ключа довжиною не менше 512 байт;
- забезпечення рівня захищеності від витоку інформації за рахунок побічних випромінювань та наведень відповідно II категорії.

У зв'язку з необхідністю захисту і збереження цілісності даних було вжито заходів розробки та використання методів захисту інформації в приладах мікро-ЕОМ.

Список літератури

1. Гребешков А.Ю. «Микропроцессорные системы и программное обеспечение в средствах связи », ПГУТИ Самара , 2009. (надається в електронному) Стр. 90-100. 2.
2. Голицина О.Л., Партіка Т.Л. «Програмное обеспечение », 2-ое издание , Москва, 2008. (надається в електронному вигляді). Стор. 12-15.
3. http://glossary.starbasic.net/index.php?title=%D0%95%D0%9E%D0%9C
4. http://tmb.org.ua/new/index.php/i-i/4-/216-2012-12-17-09-40-16.html
5. http://www.dut.edu.ua/uploads/l_1220_70404765.pdf

УДК 004.056

О.А. Філіппов, студент
Кіровоградський національний технічний університет,
alex.fil25@yahoo.com

ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ЧЕРЕЗ КАНАЛИ ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ

Аналіз стану справ в області захисту інформації показує, що в промислово розвинених країнах світу в основному сформувалася інфраструктура захисту інформації (ЗІ) в системах обробки даних. Проте, кількість фактів зловмисних дій над інформацією не лише не зменшується, але й має достатньо стійку тенденцію до зростання [1]. В цьому сенсі Україна та інші країни СНД не є, на жаль, винятком.

Серед всіх можливих каналів просочування інформації найбільшу небезпеку в Україні найближчим часом, представлятимуть технічні канали [1]. Таке припущення ґрунтується на наступних фактах: наявності в Україні великого числа технічно грамотних фахівців, знання і навички яких не використані внаслідок важкого економічного стану; виходу на український ринок західних фірм - виробників апаратури для технічного шпіонажу; недостатньої уваги, а найчастіше просто ігнорування проблем безпеки інформації з боку українського бізнесу, що зароджується; стрімкий ріст кількості обчислювальної техніки.

Детально розглянуті можливі канали просочування інформації, яка обробляється технічними засобами прийому, обробки, зберігання і передачі даних. Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх розповсюдження і способів перехоплення, зазначені канали діляться на електромагнітні, електричні, параметричні й вібраційні [2].

Викладено основні особливості методів запобігання просочування інформації через побічні електромагнітні випромінювання і наведення персонального комп'ютера, а саме [3]:

- доопрацювання пристроїв обчислювальної техніки з метою мінімізації рівня випромінювання (внесення конструктивних змін, екранування, введення додаткових модулів). В свою чергу щодо екранування пристроїв розглянуто види і суть електромагнітного екранування, електростатичне екранування, магнітостатичне екранування, електромагнітне екранування, а також розглянуто екран, як об'ємний резонатор;
- електромагнітне екранування приміщень, в яких розташована обчислювальна техніка (розглянуті загальні положення відповідної методики, в тому числі, щодо захисту інформації від витоку по ланцюгах заземлення та електроживлення);
- активне радіотехнічне маскування (енергетичне та неенергетичне).

В заключній частині проведено аналіз методів запобігання просочування інформації, наведені характеристики каналів витоку і сформульовані критерії захищеності засобів обчислювальної техніки [4].

Список літератури

1. Домарев В.В. Защита информации и безопасность комп’ютерных систем. К.: Диасофт, 2003 г. – 480 с.
2. Полонский Н.Б. Конструирование электромагнитных экранов для радиоэлектронной аппаратуры. М.: Наука, 1999 г.
3. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997 г.
4. Алин Б.Ю. Защита компьютерной информации. СПб.: БХВ, 2000 г.

УДК 004.01/.08

M. V. Zinchenko, computer engineering student
Tavria State Agrotechnological University
marinka-vfhbyf@mail.ru

ROBOTS APPLICATION IN MEDICINE: POSSIBILITIES, ADVANTAGES, PROSPECTS

At present computer technology and robotics actively developed and implemented in different areas of life and sectors of science. Medicine is one of the important applications of robots. Using of the robots during surgery significantly reduces the errors of human factor, ensuring the accuracy of movements. The rate of introduction of medical robots is comparable to the rate of implementation of the first computers.

The aim of the article is to study areas of robots use in modern medicine, to recognize the main benefits and to consider the prospects for the application of medical robots.

Robotic surgery began to develop in the 1980s. The da Vinci surgical system is the first robot in the field of robotic surgery. The da Vinci Surgical System consists of three components: surgical console, patient cart and vision cart. The system provides the following advantages to the surgeons: three-dimension visualization, control of endoscopic instrument, and control of the camera [1].

Currently there are two fields in which surgical robots are designed and tested. One of them is the minimally invasive surgery. It is the surgery which is performed without making large incisions. The other field is the telerobotics that allows a doctor to do the surgery at a distance.

Robotic surgery is used for a large variety of medical procedures including renal transplant, nephrectomy, removal of the gallbladder, coronary artery bypass, gastric bypass, appendectomy, hip replacement.

There are also robots used in general medicine: rehabilitation robots, biorobots, pharmacy automation, disinfection robot, robots in hospitals.

Rehabilitation robots are robots that support people's lives with a dysfunction of the body parts that affect movement.

Pharmacy Automation is used for receiving the goods dispensing medication mixing powders and liquids.

Disinfection robot is applied for disinfection of premises. It generally uses pulsed ultraviolet light. For example, these robots are used to fight Ebola disease.

The main task of the robots in the hospital is finding the right way to the hospital in order to move things or to show the way for a person [2].

In comparison with open surgery, medical robots allow surgeons to perform difficult tasks through tiny incisions. 3D camera mounted on a robot, improves the visualization of the human body. This gives improved accuracy and improved agility.

Telerobotics solves the problem of shortage of specialists and increasing the number of facilities where you can do the operation. Thanks robotized surgery doctors less tired than during open surgery.

During surgery reduces the risk of blood poisoning, decreases blood loss and reduces injury the body. As a result, patients stay in hospital less.

The most perspective area of medical robotics is nanorobots.

Nanotechnology will allow scientists to create nanorobots that can move into a body and to transport necessary molecules to manipulate microscopic objects and communicate with doctors.

The convergence of nanotechnology, molecular biology, and medicine will open new possibilities for detecting and manipulating atoms and molecules using nanodevices, with the potential for a wide variety of medical applications at the cellular level. Today, the amount of research in biomedical science and engineering at the molecular level is growing exponentially due to the availability of new analytical tools based on nanotechnology [3].

Doctors plan to use this technology for emergency delivery of drugs directly into the cells and for the destruction of cancer cells and infections. Nanorobots can penetrate the body tissues and

destroy any disease instantly. Also, medical nanorobots are designed for the accurate diagnosis of diseases and collecting data about the human body [4].

Next promising sector of science is bionic prosthetics.

Most prostheses are purely mechanical. There are also robotic prostheses, which are equipped with motors, sensors and a processor.

The beautiful dream is that one day will be created arms and legs, which will as well functional as the natural limbs. Bionic prostheses are prostheses which are controlled by the brain. These prostheses are equipped with sensors of mechanical loads and electrodes that receive nerve impulses. It provides a quick control and natural movement and excellent coordination. Now the creators of the prosthesis are working on reducing the number of software flaws. The companies that work in this area are Ossur and Otto Bock [2].

Using robots in medicine is one of the most promising areas of robotics. Robots can replace doctors performing the operation. The main advantages of the robots application in medicine are reduced pain, faster recovery, reducing the risk of infection, high accuracy and large visualization. In the near future mini robots will be able to perform diagnostics and treatment in the human body, nanorobots could selectively affect even individual cells.

References

1. Changqing Gao. Robotic Cardiac Surgery. New York: Springer, 2014
2. Medical robots today and tomorrow, Available at: http://www.allonrobots.com/medical-robots.html
3. Tuan Vo-Dinh. Nanotechnology in biology and medicine: methods, devices, and applications. Boca Raton: CRC Press, 2006.
4. Prospects for Medical Robots, Available at: http://www.azonano.com/article.aspx?ArticleID=2035 (accessed 13 November 2007)

УДК 004.91

В.В. Вернигора, студент
Кіровоградський національний технічний університет,
vlad261094@gmail.com

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ ОСВІТИ

Сучасний період розвитку суспільства характеризується сильним впливом на нього комп'ютерних технологій, які проникають в усі сфери людської діяльності, забезпечують поширення інформаційних потоків в суспільстві, утворюючи глобальний інформаційний простір. Невід'ємною і важливою частиною цих процесів є комп'ютеризація освіти.

Відомі численні і цілком переконливі приклади, що підтверджують ефективність використання комп'ютерів на всіх стадіях педагогічного процесу:

1. на етапі пред'явлення навчальної інформації навчаються;
2. на етапі засвоєння навчального матеріалу в процесі інтерактивної взаємодії з комп'ютером;
3. на етапі повторення і закріплення засвоєних знань (навичок, умінь);
4. на етапі проміжного і підсумкового контролю та самоконтролю досягнутих результатів навчання;
5. на етапі корекції і самого процесу навчання, і його результатів шляхом вдосконалення дозування навчального матеріалу, його класифікації, систематизації.

Дистанційне навчання у вигляді заочного навчання зародилося на початку 20-го сторіччя. Сьогодні заочно можна отримати вищу освіту, вивчити іноземну мову, підготуватися до вступу до вузу і т.д. Однак у зв'язку з погано налагодженою взаємодією між викладачами та студентами і відсутністю контролю над навчальною діяльністю студентів-заочників в періоди між екзаменаційними сесіями якість подібного навчання виявляється гірше того, що можна отримати при очному навчанні.

При здійсненні дистанційного навчання інформаційні технології повинні забезпечувати:

1. доставку учнем основного обсягу досліджуваного матеріалу;
2. інтерактивну взаємодію учнів і викладачів в процесі навчання;
3. надання студентам можливості самостійної роботи по засвоєнню досліджуваного матеріалу;
4. оцінку їх знань і навичок, отриманих ними в процесі навчання.

Для досягнення цих цілей застосовуються такі інформаційні технології:

1. надання підручників і іншого друкованого матеріалу;
2. пересилка вивчаються, по комп'ютерних телекомунікаціях;
3. дискусії та семінари, що проводяться через комп'ютерні телекомунікації;
4. відеоплівки;
5. трансляція навчальних програм з національної та регіональним телевізійним і радіостанціям;
6. кабельне телебачення;
7. голосова пошта;
8. двосторонні відеотелеконференції;
9. одностороння відеотрансляція із зворотним зв'язком по телефону;
10. електронні (комп'ютерні) освітні ресурси.

Список літератури

1. «Информационные и коммуникационные технологии в образовании: монография» / Под.редакцией: Бадарча Дендева – М. : ИИТО ЮНЕСКО, 2013.

УДК 004.056.53

Е.І. Гришикашвілі, студентка
Одеський національний політехнічний університет
helentunik@gmail.com
К.О. Трифонова, ст. викладач
Одеський національний політехнічний університет
katikkatik@gmail.com

РЕАЛІЗАЦІЯ ПАРАМЕТРИЗАЦІЇ РАЙДУЖНОЇ ОБОЛОНКИ ОКА ДЛЯ МОБІЛЬНОЇ СИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ЛЮДИНИ

В сучасних умовах забезпечення безпеки інформаційних ресурсів представляє собою надзвичайно актуальну задачу. Останнім часом все більше поширення набувають біометричні системи ідентифікації. На відміну від традиційних, біометричні системи ґрунтуються на унікальних біологічних характеристиках людини, які важко підробити і які однозначно визначають конкретну людину.

Система ідентифікації за райдужною оболонкою ока вважається одною з найбільш точних та надійних способів ідентифікації людини.

Загальна схема системи складається з наступних етапів: локалізація райдужної оболонки ока [1], нормалізація радужної оболонки ока, параметризація та виділення коду, порівняння кодів райдужної оболонки. Параметризація представляє собою виділення інформативних ознак цифрового зображення райдужної оболонки ока. Ці ознаки повинні задовольняти наступним властивостям: незалежність від умов реєстрації зображення, тобто незалежність від умов зйомки та змін райдужної оболонки ока; незмінність при повторних реєстраціях однієї персони, повторні реєстрації можуть виконуватись протягом багатьох років; відміну для різних осіб.

Згідно дослідженням окулістів, форма та забарвлення райдужної оболонки ока можуть змінюватись зазвичай внаслідок зміни стану організму людини. Однак, кількість елементів текстури райдужної оболонки настільки велика, що при порівнянні двох еталонів досить збігу лише частини параметрів, щоб вважати, що еталони належать одній людині. Тому основними інформативними ознаками райдужної оболонки ока є ознаки текстури цифрового зображення. Різні автори пропонують використовувати різноманітні способи параметризації райдужної оболонки ока, що відображена в прямокутне цифрове зображення: двовимірні вейвлети Габора – автор J. Daugman; дискретне косинусне перетворення – автор D. Monro; одновимірні вейвлети різних масштабів – автор W. Boles; двовимірні вейвлети Хаара – автор S. Lim; піраміда Лапласа – автор R. Wildes.

В даній роботі досліджено та реалізовано підхід J. Daugman. Основні інформативні ознаки райдужної оболонки ока, тобто ознаки текстури цифрового зображення, визначено в результаті фільтрації цифрового зображення ядром Габора. Програмна реалізація проведена для мобільної платформи Android з використанням засобів мови програмування високого рівня Java. Подальша робота спрямована на завершення реалізації біометричної системи ідентифікації людини для мобільного пристрою.

Список літератури

1. Трифонова, К.О. Визначення контурів райдужної оболонки ока для системи біометричної ідентифікації людини / К.О. Трифонова, Е.І. Гришикашвілі, А.Р. Агаджанян // Научный и производственно-практический сборник. Труды Одесского политехнического университета. – Вып.1(45). – 2015. – С.107–112.

УДК 004.4

Н.А. Дроговоз, викладач
Кіровоградський державний педагогічний університет,
dna2011@ukr.net
І.М. Куліков, студент
Кіровоградський державний педагогічний університет,
vanekulykov31@gmail.com
Д.С. Харченко, студентка
Кіровоградський державний педагогічний університет

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДОВСЛІДЖЕННЯ ПСИХОЛОГО-ПЕДАГОГІЧНОЇ ХАРАКТЕРИСТИКИ УЧНІВ

Сучасна освіта висуває нові вимоги до організації роботи класного керівника. Вчитель повинен вміти визначати реальний рівень розвитку учнів класу, прогнозувати результат своєї діяльності, застосовувати виховні технології, які б забезпечили особистісне зростання вихованців. Він зобов'язаний перебувати в епіцентрі освітніх інновацій. Тому інформаційні комп'ютерні технології (ІКТ) стали невід'ємною частиною роботи сучасних класних керівників. Наприклад, створення характеристики учнів без використання ІКТ вимагає великих часових затрат. Це творчий процес. Вчителям під час складання характеристики доводиться писати її за шаблоном (певною структурою). Тому є необхідність автоматизації цього процесу. Для полегшення роботи вчителя можна скористатися інструментарієм на шкільних порталах.

Проведене дослідження програмного забезпечення документообігу сучасної школи виявило ряд недоліків. Зокрема, для створення характеристик учнів не використовуються електронні таблиці з результатами психологічних тестувань учнів, спрямованих на вивчення їхнього типу темпераменту, окремих рис характеру, становища в групі, інтересів та мислення тощо.

Таким чином при створенні програмного забезпечення для оформлення характеристики учнів необхідно було передбачити можливість:

- опитування класних керівників;
- формування характеристики за результатами тесту Айзенка (як для усього класу, так і для одного учня);
- редагування даних;
- подання даних в графічній формі.

Для коректної роботи даного програмного продукту потрібно оформлювати результати тесту Айзенка в середовищі MS Excel. Таблиця заповнюється за наступним шаблоном:

	A	B	C	D	E	F	G
1	ФИО ученика	Экстраверсия-интроверсия	Нейротизм	Ложь	Направления профессиональной деятельности, к которым есть интерес	Тип мышления	Тип темперамента
2	Бойко А. Р.	20	8	3	Физика и математика	Наглядно - действенное	Флегматик

В результаті обробки даних окрім створення характеристик є можливість побудувати діаграми для порівняння рівнів нейротизму, екстраверсії, інтроверсії учнів тощо.

Отже, розроблене програмне забезпечення дозволить оптимізувати роботу класних керівників у сучасній школі.

УДК 528.029

Н.В. Еременко, м.н.с.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»,
khai302@ukr.net
Е.В. Коновалова, м.н.с.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»,
smile_xai@mail.ru

ОРГАНИЗАЦИЯ СИСТЕМЫ РАСПРЕДЕЛЕННОГО ПРОИЗВОДСТВА

В настоящее время многие мировые компании постепенно перекладывают часть своих функций – от производства до обслуживания клиентов – на плечи подрядчиков, в качестве которых часто выступают филиалы или бизнес-партнеры, расположенные в других регионах, где такой аутсорсинг оправдан. Эта тенденция усилилась в условиях нынешнего экономического спада, когда компании все больше расширяют географию своей деятельности, стремясь сократить затраты и повысить доходность. Подобная глобализация привела к рассредоточению таких операций, как снабжение, производство и распределение товаров, а также обслуживание клиентов, среди множества организаций во всем мире. В связи с этим актуальной становится задача организации эффективной системы распределенного производства, в которой различные производственные операции, являющиеся частью единого технологического процесса, осуществляются отдельными самостоятельными участниками.

Организация распределенного производства позволяет полностью изменить создание и распространение любой продукции. В традиционном производстве сырье доставляется к месту, где сосредоточены все мощности, откуда после изготовления продукция поставляется потребителям. В распределенном производстве сырье и технологические мощности децентрализованы, благодаря чему конечный продукт находится в непосредственной близости от потребителя.

Преимуществом системы распределенного производства является повышение загруженности производственных мощностей, а, следовательно, и увеличение объема прибыли предприятия. Кроме того, важным преимуществом системы распределенного производства является снижение инвестиционных и производственных рисков, что автоматически сказывается на стоимости инвестиционных ресурсов.

Организация эффективной системы распределенного производства требует решения следующих задач:

1) разработать модель управления производственного процесса, отражающую механизм его организации, особенностью которого является структура производственной цепочки, ее финансирование и координация, распределение прав собственности на производственные фонды, диверсификация рисков и ряд других;

2) разработать метод выбора транзакционных предприятий с оценкой реализуемых проектов;

3) разработать метод согласования реализуемых производственных процессов с целью интеграции их в единый процесс создания продукта;

4) разработать информационную технологию поддержки процессов планирования, организации и оперативного управления системой распределенного производства.

Список литературы

1. Георасределенные производственные системы. Часть 1. Анализ, моделирование, проектирование: моногр. / В.М. Илюшко, О.Е. Федорович, О.Н. Замирец, Л.Д. Греков. – Х.: Нац. аэрокосм. ун-т «Харьк. авиац. ин-т», 2011. – 250 с.

2. Георасределенные производственные системы. Часть 1. Размещение на земной поверхности, оптимизация магистральных систем, космический мониторинг: моногр. / Л.Д. Греков, В.М. Илюшко, О.Е. Федорович. – К.: Издательство Сергея Пантюка, 2014. – 206 с.

УДК 004.738.5

К.В. Молодецька, канд. техн. наук
Житомирський національний агроекологічний університет,
kmolodetska@gmail.com

УПРАВЛІННЯ КОНТЕНТОМ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ ПРИ ПРОГНОЗУВАННІ СИНЕРГЕТИЧНИХ ЕФЕКТІВ

Одним із основних сучасних засобів комунікації суспільства є соціальні інтернет-сервіси (СІС), які реалізують обмін інформацією, зберігання посилань і мультимедійних документів, створення та редагування публікацій тощо. СІС застосовуються користувачами, яких називають агентами СІС для реалізації особистісних і групових інтересів їх представників у віртуальному просторі. Сьогодні віртуальні спільноти і зокрема агенти СІС, є об'єктами деструктивних інформаційних впливів з метою поширення контенту заданого змісту та впливу на суспільну думку [1, 2]. В результаті синергетичних ефектів у СІС породжуються нехарактерні властивості, які називають емерджентними. Своєчасне встановлення сутності і змісту синергетичних ефектів у СІС, їх завчасне виявлення та прогнозування, є актуальною проблемою забезпечення інформаційної безпеки людини, суспільства та держави.

З динамічної теорії хаосу відомо, що задана поведінка системи досягається шляхом придушення в ній хаотичної динаміки нелінійних періодично збурюваних динамічних систем. Для цього синтезуються управляючі впливи, недоліком яких є привнесення в систему, що управляється, суттєвих змін в її динаміку в цілому і в саму систему зокрема. При вивченні нелінійних динамічних систем встановлено, що задана поведінка досягається за рахунок її самоорганізації, однією з необхідних умов виникнення якої є підтримання стану нерівноваги [2, 3]. Завдяки процесам самоорганізації – теоретичній основі синергетики, можна виділити відносно невелику кількість параметрів порядку чи характеристик середовища, які визначають динаміку системи в цілому. Таким чином, наявність хаотичного атрактора забезпечує досягнення стійкого стану системи за незначних збурень системних параметрів.

В основу досліджень було покладено концепцію синергетичного управління процесами взаємодії агентів у СІС, що узагальнює відомі підходи до управління процесами взаємодії агентів та розвиває їх на клас нелінійних систем, які описуються на основі положень динамічної теорії хаосу [3]. Вирішення проблеми синтезу синергетичного управління, що забезпечить виникнення процесів керованої самоорганізації агентів у СІС для досягнення заданого стану інформаційної безпеки віртуального співтовариства є актуальною [4].

Метою досліджень є підвищення стійкості віртуальних спільнот в СІС до деструктивних інформаційних впливів за рахунок синтезу синергетичного управління попитом агентів на відповідний контент.

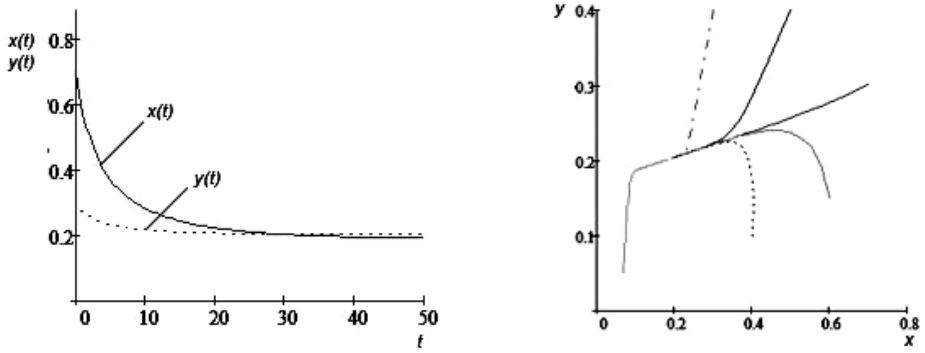
На першому етапі було виконано формалізацію взаємодії агентів у СІС як системи нелінійних диференціальних рівнянь, що описують попит на відповідний контент для досліджуваної віртуальної спільноти і пропозицію з надання відповідного контенту. З метою протидії інформаційним впливам шляхом штучного підтримання в агентів СІС заданого рівня зацікавленості до відповідного контенту виконаємо синтез управляючої дії, що реалізується через зворотний зв'язок. Закон управління синтезуємо на основі заданого параметра порядку, що ґарантує протікання процесів самоорганізації в системі і появу бажаних синергетичних ефектів.

В структуру системи введено динамічні інваріанти – атрактори, які враховують природні особливості СІС. Підтримання заданого рівня попиту агентів СІС і зміна цінності інформації, що становить інтерес, повинні змінюватись відповідно до логістичного рівняння. Після підстановки макрозмінної в рівняння, що описує протікання всіх перехідних процесів за визначений час, і враховуючи початкову систему диференціальних рівнянь, отримаємо синергетичне управління.

Синтезоване синергетичне управління переводить зображуючу точку синтезованої системи нелінійних диференціальних рівнянь на стабілізуючий інваріант. Із цього рівняння отримаємо значення точок сплеску синергетичного ефекту для попиту на контент агентів СІС і пропозиції, в яких система досягає бажаного стану на фазовій площині. Встановлено, що в синтезованій замкненій системі з урахуванням синергетичного управління пропозиція контенту у СІС не залежить від показника зміни швидкості пропозиції з надання агентам взаємодії в СІС відповідного контенту.

Синергетичне управління попитом на контент агентів СІС досягається варіюванням значень параметрів синтезованої системи нелінійних диференціальних рівнянь. Контроль рівня пропозиції контенту в СІС реалізується зміною граничної ємності інформаційного середовища шляхом обмеження поширення інформації заданого змісту у віртуальних спільнотах і врахуванням природної властивості зменшення цінності інформації в часі

Візуалізація результатів розрахунків для синтезованої замкнутої системи нелінійних диференціальних рівнянь подана на рис. 1.



а) б)

Рис. 1 – Керована система управління взаємодією агентів у СІС: а) графік зміни попиту і пропозиції контенту в СІС; б) фазовий портрет системи

Отже, зміна попиту агентів СІС на контент досягається варіюванням значень граничної ємності інформаційного середовища. Аналіз фазового портрету (рис. 1, б) показує, що система переходить від хаосу до керованого стану і фазові траєкторії синтезованої системи організовано прямують до обраного параметра порядку. На цьому інваріантному різноманітті міститься точка сплеску синергетичного ефекту із заданими фазовими координатами, в якій досягається обмеження попиту агентів на відповідний контент у СІС.

Вказаний синергетичний ефект досягається за рахунок запуску процесів самоорганізації агентів у СІС. Точка сплеску синергетичного ефекту є притягуючим атрактором системи, на якому реалізується редукція ступенів свободи вихідної системи нелінійних диференціальних рівнянь і забезпечується спрощення процесу досягнення поставлених завдань взаємодії агентів у СІС. Ефективне управління взаємодією агентів здійснює синергетично керований перехід до заданого стану інформаційної безпеки віртуального співтовариства. Подальші дослідження будуть направлені на визначення необхідних і достатніх умов реалізації синергетичного управління, що забезпечать стійкість досягнутого системою стану інформаційної безпеки.

Список літератури

1. Castells, Manuel. The Network Society : From Knowledge to Policy / Manuel Castells, Gustavo Cardoso. – Washington, DC : Johns Hopkins Center for Transatlantic Relations, 2005. – 434 p.
2. Молодецька К. В. Управління попитом агентів на контент у соціальних інтернет-сервісах / К. В. Молодецька // Міжнар. наук.-практ. конф. [«Актуальні проблеми автоматизації та управління»] (Луцьк, 27 трав. 2015 р.). – Л. : ЛНТУ, 2015. – Вип. 3. – С. 56–62.
3. Колесников А. А. Синергетическое методы управления сложными системами : теория системного синтеза / А. А. Колесников. – М. : Едиторал УРСС, 2005. – 228 с.
4. Бурячок В. Л. Політика інформаційної безпеки [Текст] : підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко; під заг. ред. проф. В. О. Хорошка. – К. : ПВП «Задруга», 2014. – 222 с.

УДК 65.012.123

Ю.И. Сергеева, младший научный сотрудник
Национальный аэрокосмический университет им Н.Е. Жуковского «ХАИ»,
bulgakova@ukr.net
С.В. Сергеев, научный сотрудник
Белгородский государственный национальный исследовательский университет НИУ БелГУ
sergeyev72@gmail.com

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ КОМПОНЕНТНО-ОРИЕНТИРОВАНОГО ПОДХОДА К УПРАВЛЕНИЮ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ

Основное внимание уделено имплементации компонентно-ориентированных решений в среду PLM, а именно в части MPM-систем. Для решения этой задачи необходимо корректно сформулировать условия информационного обмена между подсистемами.

Учитывая, что разрабатываемая подсистема взаимодействует с системами CAD/CAE и CAPP/CAM, а также принимая во внимание, что данные этих подсистем традиционно хранятся в среде PDM в виде базы данных под управлением SQL-сервера, и то, что проектируемые технологические процессы обычно создаются с использованием собственной базы данных систем CAPP, возникает необходимость в двустороннем обмене данными между этими системами с использованием возможностей проектируемой MPM-системы. А также MPM-система должна обеспечивать взаимодействие с подсистемами ERP, FRP, MRP и MES на различных этапах жизненного цикла изделия.

Анализируя классические модели PLM-систем, можно утверждать, что как правило, модули CAD/CAM/CAE/CAPP не имеют прямых связей с подсистемами ERP/FRP/MRP/MES, наблюдается существенный функциональный и информационный разрыв между ними [1]. Создание модели единого информационного пространства (ЕИП), способного в полной мере использовать преимущества концепции PLM, обеспечивается за счет установления функциональных связей между структурными элементами всей системы, анализа информационных потоков и принципов взаимодействия между структурными подразделениями участвующих в проекте исполнителей.

Следовательно, на основе такого функционального подхода единое информационное пространство должно иметь общую серверную платформу, состоящую из собственно баз данных, средств их администрирования, а также скриптов запросов доступа к данным, реализованных в классическом либо объектном представлении.

Однако сравнительно простое решение данной проблемы все же возможно, при условии, что различные подсистемы в составе PLM базируются на общей серверной платформе. В этом случае становится возможной интеграция разрозненных баз данных с обеспечением целостности данных и их непрерывной актуальности. При этом приоритет в выборе информационной платформы очевидно, будет определяться платформой PDM-сервера, поскольку именно эта подсистема способна хранить конструкторскую и технологическую документацию независимо от формата представления данных. При правильной организации доступа к техническим данным проекта не представляет принципиальной сложности налаживание двустороннего обмена данными между подсистемами, использующимися на различных стадиях жизненного цикла изделия, что в свою очередь позволит обеспечить получение данных по изделию и по каждой его структурной составляющей для подбора оптимального по технологическим, конструктивным и производственным признакам компонент (прямой поток данных), и внесении изменений в технологию и конструкцию изделия с более поздних стадий ЖЦ (обратный поток данных).

Список литературы

1. Кульга К.С. Модели и методы создания интегрированной информационной системы для автоматизации технической подготовки и управления авиационным и машиностроительный производством: моногр. / К.С. Кульга, И.А. Кривошеев. – М.: Машиностроение, 2011. – 377с.

УДК 627.01:004

О.Е. Федорович, д-р техн. наук,
Национальный аэрокосмический университет им. Н.Е. Жуковского
«Харьковский авиационный институт»
Ю.А. Лещенко, м.н.с.,
Национальный аэрокосмический университет им. Н.Е. Жуковского
«Харьковский авиационный институт»
Т.С. Писклова, м.н.с.,
Национальный аэрокосмический университет им. Н.Е. Жуковского
«Харьковский авиационный институт»
k302@d3.khai.edu

УПРАВЛЕНИЕ КАЧЕСТВОМ В УСЛОВИЯХ ОГРАНИЧЕННОСТИ РЕСУРСОВ ПРЕДПРИЯТИЯ

Переход на европейские рынки распространения продукции машиностроения требует повышения качества выпускаемых изделий отечественными предприятиями. Ограниченность ресурсов предприятий не позволяет комплексно и в сжатые сроки реформировать отечественные предприятия. Поэтому актуальна тема предлагаемого доклада, в котором ставится и решается задача последовательного улучшения качества с учетом ограниченных возможностей предприятия.

На первом этапе определяется множество мероприятий, которые необходимо провести для улучшения качества выпускаемой продукции. С использованием полного факторного эксперимента (ПФЭ) [1] и прогнозных оценок экспертов определяется наиболее важные (существенные) мероприятия, позволяющие улучшить качество продукции.

На втором этапе определяется структура системы управления качеством и места контроля «продукта» с помощью булевого программирования.

На третьем этапе с использованием целочисленного линейного программирования [2] определяется глубина контроля в отдельных точках контроля качества. На последнем этапе проводится имитационное моделирование процесса управления качеством с учетом сбора информации с точек контроля.

Построена агентная имитационная модель, которая позволяет адекватно отобразить основные составляющие процесса управления качеством в виде агентов: диспетчер, агент брака, агент контроля качества, агент технологических процессов, агент сбора статистики, агент результатов моделирования [3, 4].

Предложенный подход целесообразно использовать в задачах, связанных с обеспечением и улучшением качества, которое планируется при диверсификации производства с выходом на зарубежные рынки потребителей.

Список литературы

1. Монтгомери, Д. К. Планирование эксперимента и анализ данных [Текст] : пер. с англ. / Д. К. Монтгомери. – Л. : Судостроение, 1980. – 384 с.
2. Юдин, Д. Б. Линейное программирование. Теория, методы и приложения [Текст] / Д. Б Юдин, Е. Г. Гольштейн. – М. : Наука, 1969. – 318 с.
3. Федорович, О. Е. Стратегия последовательного улучшения качества в логистической цепи аэрокосмического производства [Текст] / О. Е Федорович, Ю. А. Лещенко // Авиационно-космическая техника и технология. – 2014. – № 5 (112). – С. 109 – 112.
4. Прохоров, А. В. Агентное имитационное моделирование процессов управления предприятиями нефтепродуктообеспечения [Текст] / А. В. Прохоров, Амен Соуд Абдалазез Мохаммед // Радіоелектронні і комп'ютерні системи. – 2011. – № 3 (51). – С. 37 – 43.

УДК 004.896, 004.855.5, 004.932, 004.048, 004.942

І.В. Ізонін, аспірант,
ivanizonin@gmail.com.
Р.О. Ткаченко, д-р техн. наук, професор,
roman.tkachenko@gmail.com.
К.Ю. Грицик, Р.О. Титик студенти,
Національний університет «Львівська політехніка»

ДО МЕТОДУ ЗБІЛЬШЕННЯ РОЗДІЛЬНОЇ ЗДАТНОСТІ ЗОБРАЖЕНЬ НА ОСНОВІ ШНМ МОДЕЛІ ГЕОМЕТРИЧНИХ ПЕРЕТВОРЕНЬ

У [1] описано розроблений метод надроздільності [2, 6] зображень на основі машинного навчання. Згідно методу, процес збільшення роздільної здатності зображень базується на використанні штучної нейронної мережі моделі геометричних перетворень (ШНМ МГП) [3, 4]. Даний тип нейромережі (рис.1) дозволяє розв'язувати поставлену задачу в автоматичному режимі, а також забезпечує високу швидкість роботи в режимах навчання та тестування, що зумовлює можливість практичного застосування методу в інтелектуальних системах реального часу. Запропонований метод надроздільності зображень для навчання використовує пару зображень низької та високої роздільної здатності, які розбиваються на однакову кількість фреймів *i* квадратної форми. Сукупність векторів v_i, утворених відповідними фреймами із зображень низької/високої роздільної здатності розмірностями *l* та *h* при коефіцієнті збільшення *k* складають вхідні дані ШНМ МГП в режимі навчання.

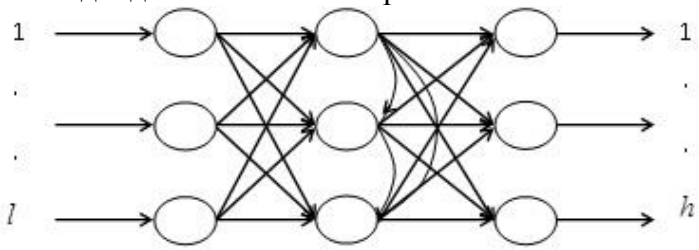


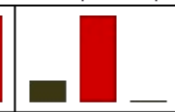
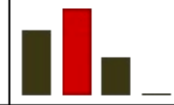
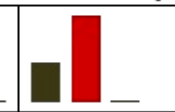
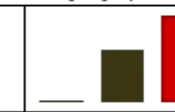
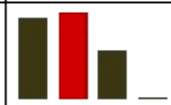
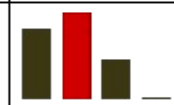
Рис. 1 Топологія ШНМ МГП для розв'язання поставленої задачі.

У [1] досліджувався вплив степеня нелінійності синаптичних зв'язків в режимі навчання на якість отриманих методом зображення. Експериментально встановлено, що лінійний синапс повністю задовольняє значеням показників якості синтезованих методом зображень. Метою даної роботи є дослідження залежності показників якості синтезованих зображень від розмірності фреймів на які розбивається зображення при різних коефіцієнтах збільшення роздільної здатності. Практичні експерименти проводилися на основі програмного рішення funk*net [3, 4] для 10 зображень роздільною здатністю $256\times256, 128\times128, 64\times64$ пікселів відповідно при коефіцієнтах збільшення зображень *k* = 2, 4, 8. Навчання ШНМ МГП відбувалося на основі пари зображень №1 (подано лише зображення низької роздільної здатності) із рис 2. Тестування роботи методу відбувалося на 10 зразках, 4 з яких подано на рис. 2., при *k* = 2, 4, 8.

Рис. 2 Зразки зображень

Розміри фреймів ($l \times l$), що формували навчальну та тестову вибірки для зображення низької роздільності становили: при k = 2, 4; l = 2, 4, 8, 16; при k = 8; l = 2, 4, 8. Розміри фреймів виходу ШНМ в режимі навчання ($h \times h$) (для зображення високої роздільності) формувалися згідно виразу: $h = l * k$. Якість синтезованих зображень оцінювалася на основі пікового співвідношення сигнал/шум [6] та індексу структурної подібності [5], які обчислювалися для кожного синтезованого зображення та відповідного йому еталону. Результати експериментальних досліджень для чотирьох зображень (рис.2) подано в таблиці 1.

Таблиця – Залежність показників якості синтезованих зображень від розміру фрейму зображення низької роздільності.

№ зображення	Коефіцієнт збільшення роздільної здатності зображення					
	2	4	8	2	4	8
	Індекс структурної подібності (SSIM)			Співвідношення сигналу до шуму (PSNR)		
1.						
2.						
3.						
4.						
Розмір фрейму (пікселі)	2*2 4*4 8*8 16*16	2*2 4*4 8*8 16*16	2*2 4*4 8*8	2*2 4*4 8*8 16*16	2*2 4*4 8*8 16*16	2*2 4*4 8*8

З таблиці видно, що здатність до генералізації ШНМ МГП падає зі збільшенням розміру фреймів зображення. Метрики PSNR та SSIM для першого зображення не враховуємо, оскільки навчання ШНМ відбувалося саме на цьому зразку. Найкращі результати для усіх 10 синтезованих зображень з коефіцієнтами збільшення k = 2, 4 ми отримали при розбиванні вхідного зображення на фрейми розміром l = 4. При збільшенні роздільної здатності зображень у 8 разів найкращі результати для більшості зразків видно для фреймів, розміром l = 2. Це можна пояснити високим коефіцієнтом збільшення роздільності, а також дуже маленькими вхідними зразками низької роздільності - 64×64 пікселі. Несуттєвою різницею в показниках для експериментів k = 8, l = 2, 4 в сторону l = 2 , яка майже не впливає на якість синтезованого зображення можна знехтувати, і при подальшому застосуванні методу використовуватимемо розбиття зображення на фрейми розміром l = 4.

Список літератури

1. Ізонін І.В. Метод надвисокої роздільної здатності зображень на основі моделі геометричних перетворень / І.В. Ізонін, Р.О. Ткаченко, Д.Д. Пелешко, Д.А. Батюк // Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту. Матеріали міжнародної наукової конференції – Херсон: ХНТУ, 2015. - 284-286 с.
2. Пелешко Д. Д. Аналіз основних методів збільшення роздільної здатності зображень на основі технології super resolution. / Д.Д. Пелешко, І.В. Ізонін, Ю.М. Пелех // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова. - 2013. - Вип. 67. - С. 162-169.
3. Рашкевич Ю.М. Нейроподібні методи, алгоритми та структури обробки сигналів і зображень у реальному часі. / Ю.М. Рашкевич, Р.О. Ткаченко, І.Г. Цмоць, Д.Д. Пелешко: Монографія – Львів: 2014. – 256с.
4. Ткаченко Р. О. Засоби штучного інтелекту. Навчальний посібник / Р. О. Ткаченко, Н. О. Кустра, О. М. Павлюк, У. В. Поліщук. Львів: Видавництво Львівської політехніки, 2014. 204 с.
5. Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Transactions on Image Processing, 2004, vol. 13, no. 4, pp. 600-612.
6. Premitha Premnath K Learning based face hallucination techniques: A survey TechS Vidya e-Journal of Research Vol. 3 (2014-15) pp. 37-45.

УДК 621.396.253

И.А. Лысенко, аспирант
Кировоградский национальный технический университет,
i1978@inbox.ru
А.А. Смирнов, доктор техн. наук, профессор
Кировоградский национальный технический университет,
assa_s@mail.ru

РАЗРАБОТКА АЛГОРИТМА ПРЕОБРАЗОВАНИЯ УПОРЯДОЧЕННОЙ КАСКАДНОЙ ТАБЛИЦЫ РЕШЕНИЙ

Для преобразования упорядоченной каскадной таблицы решений (УКТР) в граф потока управления сценария некоторого случая использования допустимы только обобщенные методы дерева решений, так как может оказаться, что проверку некоторого условия нельзя выполнять до выполнения какого-либо действия или проверки другого условия. С другой стороны, получение оптимального по любому критерию граф потока управления столь же трудная задача, как и в случае обычной таблицы решений (ТР). Поэтому алгоритм преобразования УКТР в граф потока управления случая использования целесообразно разрабатывать на основе алгоритмов получения близких к оптимальным деревьям решений.

Применительно к УКТР любой из алгоритмов построения дерева решений должен быть модифицирован таким образом, чтобы учитывалась дополнительная информация, заданная в матрице следования. Построим и обозначим на множестве T (составленном из множества условий C и множества действий A) несколько вспомогательных подмножеств. Безусловной ТР будем считать ТР, в которой либо нет условий, либо все условия несущественны. Безусловно выполнимым действием будем считать действие, которое задано во всех правилах ТР. Множество безусловно выполнимых действий обозначим $\dot{A}$. Очевидно, что $\dot{A} \subseteq A$, причем равенство имеет место только для безусловной ТР.

Обозначим $C = \{C | \exists(j)(t \rho C)\}$ подмножество связанных условий, а $\overline{C} = \{C | \neg\exists(j)(t \rho C)\}$ или $\overline{C} = C \setminus C$ подмножество несвязанных условий.

Аналогично обозначим $A = \{a | \exists(j)(t \rho a)\}$ подмножество связанных действий, а $A = \{a | \neg\exists(j)(t \rho a)\}$ или $\overline{A} = A \setminus A$ подмножество несвязанных действий.

В соответствии с приведенными определениями основные этапы алгоритма получения дерева по УКТР можно представить в виде следующей последовательности действий:

1.Сформировать для ТР множества $C, C, \overline{C}, A, A, A, \overline{A}$.

2. Пока $A \cap \overline{A} \neq 0$ и если $a \in A \cap \overline{A}$ то:

- построить вершину дерева соответствующую a;
- удалить из матрицы следования i - ю строку и i - й столбец;
- переформировать множества $A, A, A, \overline{A}, C, \overline{C}$;
- если $A \neq 0$, то завершить выполнение алгоритма.

3. Если ТР безусловна, то:

- если $A \neq A$, то выдать сообщение об ошибке в исходных данных;
- иначе завершить выполнение алгоритма.

4. Если $C = C$, то:

- выдать сообщение об ошибке в исходных данных;
- завершить выполнение алгоритма.

5. Выбрать $c \in \overline{C}$, удовлетворяющее заданному критерию оптимальности.

6. Построить вершину дерева, соответствующую c.

7. Удалить из матрицы следования j - строку и j - столбец.

8. Образовать из ТР для каждого значения c свою подтаблицу.

9. Рекурсивно применить этот же алгоритм для каждой подтаблицы и матрицы следования.

10. Завершить выполнение алгоритма.

На рисунке 1 показан пример преобразования УКТР на основе обобщенного метода дерева решений. Нулевые элементы в матрице следования опущены. В качестве критерия оптимальности алгоритма взят минимум количества вершин на дереве решений, а порядок выбора условий для очередной проверки соответствует алгоритму [1].

Таким образом, с помощью одной УКТР можно описывать случаи использования с сценариями, соответствующими классическим алгоритмам решений, т.е более широкий класс описываемых случав использования, чем в случае использования обычной ТР.

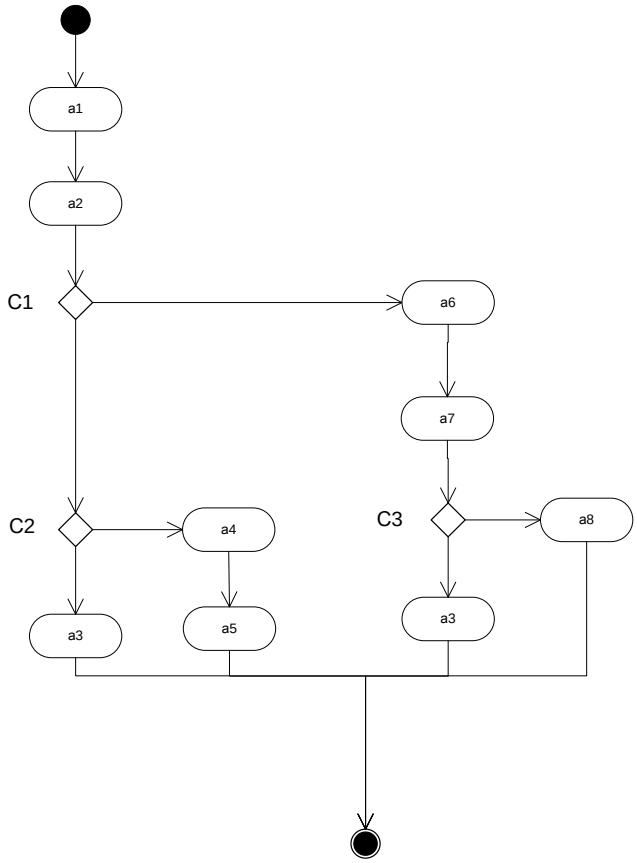


Рис. 1 - Пример преобразования УКТР на основе обобщенного метода дерева решений

Список литературы

1. 1. Pollack S.L. Conversion of Limited Entry Decision Tables to Computer Programs.-Comm. Of the ACM, 1965, v.8, №11,p.516-520.

УДК 621.396

С.А. Суржик, студент
Кировоградский национальный технический университет,
ssurzhik@gmail.com

СЕТЬ ПЕРЕДАЧИ ДАННЫХ КАК ОБЪЕКТ УПРАВЛЕНИЯ

Рассматривается такая задача как управления сетью передачи данных (СПД) как сложенная распределительная система из задержками доставки пользовательской, сигнальной и управляющей информации.

В теории управления [1] рассматривается совокупность — объект управления – управляющее устройство (рис.1).

В отличие от стандартных классических управляемых систем, любая сеть – это многосвязная система с немалым количеством сетевых и терминальных узлов, которые в свою очередь следует рассматривать как элементарные объекты управления (рис. 2).

Рис. 1 Абстрактная система управления

Рис. 2 Сеть как управляемая система

Другим одним из важным отличием задач управления СПД является его специфика управляющих воздействий, которые, представляют собой дискретные команды управления. Необходимо также учитывать внимание на задержки управляющей информации и ограничения информационного ресурса на решение задач управления сетью.

Для достижения глобальной цели – обеспечения требуемого качества сервиса QoS [2] необходим учет колебаний нагрузки а так же отказов и перегрузок отдельных сетевых узлов и других возмущающих воздействий на сеть.

Разработана математическая модель сетевых и терминальных узлов. Проведены анализы результатов управляющих информационных воздействий на эти узлы, взаимного влияния изменений их состояния.

Проанализирована устойчивость СПД как объекта управления и устойчивость системы управления сетью. В рамках информационной теории идентификации СПД рассмотрены задачи настройки эталонной модели сети и прогнозируемых изменений параметров и состояния сети.

Список литературы

1. Справочник по теории автоматического управления. Под ред. А.А. Красовского. – М.: Наука, 1987. – 711 с.
2. Таненбаум Э. Компьютерные сети. 4-е изд. – СПб.: Питер, 2003. – 922 с.

УДК 681.312

Е.В. Загуменная, канд. техн. наук
Харьковский национальный технический университет сельского хозяйства
ya_yaska@mail.ru

МЕТОДЫ РЕАЛИЗАЦИИ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

В позиционной системе счисления выполнение арифметических операций осуществляется путем последовательной обработки разрядов операндов по правилам данной операции и не может быть закончена до тех пор, пока не будет определен результат последовательной обработки всех разрядов с учетом межразрядных связей между ними. Таким образом ПСС обладает существенным недостатком - наличием межразрядных связей, которые накладывают свой отпечаток на получение достоверности вычислений реализации арифметических операций.

Поэтому в данном докладе рассматривается одна из непозиционных систем счисления, основанная на применении теории чисел - система остаточных классов. Существуют четыре метода реализации арифметических операций в системе остаточных классов (СОК): сумматорный, табличный, метод основанный на использовании кольцевых сдвигающих регистров, прямой логический метод реализации арифметических операций

Сумматорный метод состоит в том, что двоичные сумматоры снабжаются дополнительными логическими цепями, обеспечивающее возможность сложения вычетов по выбранным основаниям, при этом все арифметические операции выполняются за некоторое число сложений. Время реализации арифметических операций определяется временем выполнения модульной операции по наибольшему по величине модуля в СОК.

При прямом логическом методе реализации модульные операции описываются на уровне системы переключательных функций, посредством которых формируются значения двоичных разрядов результирующих вычетов.

Метод, основанный на использовании кольцевых сдвигающих регистров, особенностью которого заключается в том, что результат арифметических операций $(\alpha_i + \beta_i) \bmod m_i$ по произвольному модулю СОК, заданной совокупностью $\{m_j\}$, $j = \overline{1,n}$ оснований, определяется только за счет последовательных циклических сдвигов заданной цифровой структуры. Время выполнения модульных арифметических операций определяется временем выполнения модульной операции по наибольшему по величине m_n модуля в СОК.

Табличный метод реализуется в виде комбинационных схем, которые непосредственно реализуют таблицы соответствующих операций в двоичном или в унитарном коде. Табличный метод позволяет реализовывать арифметические операции с наиболее высоким быстродействием.

Таким образом в данном докладе были рассмотрены четыре принципа реализации арифметических операций в СОК. Любая операция в СОК всегда сводится к последовательности операций над малоразрядными вычетами.

Список литературы

1. Жихарев В. Я. Методы и средства обработки информации в непозиционной системе счисления в остаточных классах / В. Я. Жихарев, Я. В. Илюшко, Л. Г. Кравец, В. А. Краснобаев. // Издательство «Волынь», 2005. - 219

УДК 681.3.06

О.С.Котляр, студент
Кіровоградський національний технічний університет,
gazmyano@mail.ru

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Системна програма - це програма, яка призначена для підтримки працездатності СОІ або підвищення ефективності її використання.

Прикладна програма - це програма, яка призначена для розв'язання задачі або класу задач у певній галузі застосування СОІ.

Відповідно до термінології, системне програмування - це процес розробки системних програм (у тому числі керуючих та обслуговуючих).

З іншого боку, система - єдине ціле, що складається з множини компонентів та множини зв'язків між ними. Тоді системне програмування - це розробка програм складної структури.

Зафіксований у державному стандарті поділ програмного забезпечення на системне та прикладне є деякою мірою застарілим. Сьогоднішній поділ передбачає щонайменше три градації програмного забезпечення:

- системне;
- проміжне;
- прикладне.

Проміжне програмне забезпечення (middleware) визначається як сукупність програм, що виконують керування вторинними (такими, що сконструйовані самим програмним забезпеченням) ресурсами, орієнтованими на розв'язання певного (широкого) класу задач. До такого програмного забезпечення відносяться менеджери транзакцій, сервери баз даних (БД), сервери комунікацій та інші програмні сервери. З точки зору інструментальних засобів розробки проміжне програмне забезпечення ближче до прикладного, оскільки не працює прямо з первинними ресурсами, а використовує для цього сервісні програми. З точки зору алгоритмів і технологій розробки проміжне програмне забезпечення ближче до системного програмного забезпечення, оскільки завжди є складним програмним виробом багаторазового та багатоцільового використання і в ньому застосовуються ті ж або схожі алгоритми, що і в системному програмному забезпеченні.

Сучасні тенденції розвитку програмного забезпечення полягають у зниженні обсягу як системного, так і прикладного програмування. Основна частина роботи програмістів виконується у проміжному програмному забезпеченні. Зниження обсягу системного програмування визначене сучасними концепціями операційних систем, об'єктно-орієнтованою архітектурою та архітектурою мікроядра, відповідно до яких більша частина функцій системи виноситься в утиліти, які можна віднести і до проміжного програмного забезпечення. Зниження обсягу прикладного програмування обумовлене тим, що сучасні продукти проміжного програмного забезпечення пропонують усе більший набір інструментальних засобів та шаблонів для розв'язання задач свого класу.

Значна частина системного і практично все прикладне програмне забезпечення пишеться мовами високого рівня, що забезпечує скорочення витрат на їх розробку або модифікацію та здатність до перенесення.

Список літератури

1. Коноваленко І. В., Федорів П. С. Системне програмування у Windows з прикладами на Delphi, Т:ТНТУ.- 2012.
2. Харт Джонсон М. Системное программирование в среде Windows / Джонсон М. Харт ; пер. с англ. – М. : Издательский дом «Вильямс», 2005.

УДК 004.353.2

В.Г. Ладоня, студент
Кіровоградський національний технічний університет,
vadymvl@gmail.com

ПРИНЦИП РОБОТИ ДИСПЛЕЇВ ТЕХНОЛОГІЇ E-INK

Все більш широкого поширення зазнають електронні книги. Вони відомі своєю зручністю читання (відсутність постійного оновлення і підсвітки як у LCD-дисплеїв робить їх схожими на звичайний папір) і низьким споживанням заряду акумулятора, якщо зображення на екрані не змінюється. Тобто, енергія споживається тільки при оновленні зображення, наприклад, при перегортанні сторінки. Енергоспоживання дисплея електронної книги в середньому у 100 разів менше, ніж LCD-екрану. Це можливо завдяки використанню технології E-Ink (електронних чорнил). В чому ж полягає принцип їх роботи?

Основою екрана є скляна або пластикова пластина, товщиною трохи менше половини міліметра. На ній розташовуються нижні електроди, над якими розташований шар спеціальних прозорих мікрокапсул. Діаметр кожної з мікрокапсул приблизно дорівнює діаметру людської волосини. Мікрокапсула це і є мінімально можлива точка на e-ink екрані.

Принцип роботи таких дисплеїв полягає у ефекті електрофорезу – здатністю заряджених частинок переміщатися в рідині від одного електрода до іншого. Якщо на піксель матриці екрану (що являє собою капсула) подається негативний заряд, то білі частинки, заряджені позитивно, притягуються до нього і піднімаються на поверхню капсули (рис. 1). В результаті читач бачить чорну крапку на екрані.

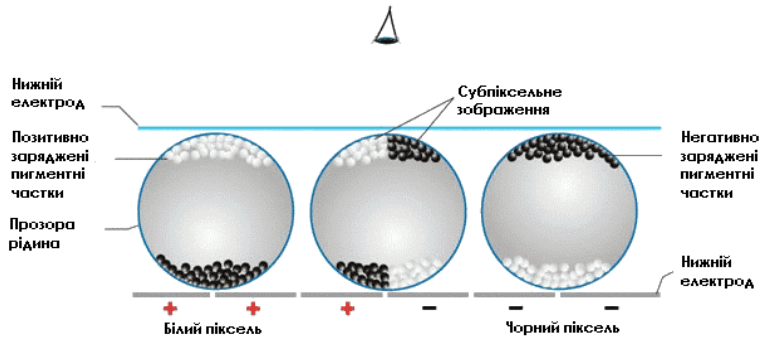


Рис. 1 – Принцип роботи електрофоретичного дисплею

До недоліків такої технології, слід віднести дуже низьку частоту оновлення зображення. Це перешкоджає розробникам реалізовувати інтерактивні додатки (з використанням анімації та прокрутки), як ті, що можливі на LCD дисплеях, що використовуютья у смарфонах.

Проте з широким поширенням, технологія E-ink стрімко розвивається і удосконалюється. Недоліки технології поступово зменшуються, та додаються нові можливості - вже доступні на ринку кольорові дисплеї з використанням електронних чорнил.

Список літератури

1. Хамула О.Г. Перспективи використання технології електронного паперу (e-ink) / О. Г. Хамула, Н. В. Сорока / «Комп’ютерні технології друкарства». Збірник наукових праць - Львів: УАД, 2014. № 31, С. 116-123.
2. Принципы работы современных дисплеев [Электронний ресурс]:[сайт]: – Режим доступу: http://www.upweek.ru/principy-raboty-sovremennyx-displeev.html.

УДК 004.421

В.С. Білий, студент
Кіровоградський національний технічний університет,
viktor_belyi@mail.ru

АНАЛІЗ СПОСОБІВ ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ АЛГОРИТМІВ

Не дивлячись на те, що поняття алгоритму було відоме ще вченим стародавніх цивілізацій, різноманітні формалізації цього терміну почали з'являтись лише в 30-х роках XX століття, що було спричинено утворенням і стрімким розвитком сучасної теорії алгоритмів.

Нагальні потреби в аналізі алгоритмів та їх систематизації, що виникли в середині минулого століття, тобто одночасно зі створенням та поширенням обчислювальних машин, дали потужний поштовх для розвитку теорії складності обчислень.

Найбільш зручним та ефективним методом порівняння швидкодії та результативності алгоритмів, як свідчать наукові знання та напрацювання в цій області, є поняття асимптотичної складності.

Перш за все слід з'ясувати та встановити обчислювальну модель, що буде використовуватись для конструювання алгоритму.

Якщо при оцінюванні алгоритму, ми звертатимемо увагу лише на число виконаних команд, то з'ясуємо лише однорідні міри складності. Тоді як доцільнішим буде також врахувати розмір операндів у бітах при виконанні кожної команди, що дасть нам визначити різноманітні логарифмічні міри складності.

Зазвичай, для того, аби дати характеристику складності алгоритмів, як основні обчислювальні ресурси, розглядають час, який було витрачено алгоритмом на операції обчислення та використану пам'ять.

Складність однорідного алгоритму є цілочисельною функцією цілого аргументу *t(n)*, що дорівнює часу його роботи для вхідних даних розмірності *n*. Однак визначення складності неоднорідного алгоритму, як функції $t(R_1 \dots R_m)$ від всього масиву вхідних даних є невдалим, тому що ця функція містить багато зайвої інформації і погано обчислюється.

Саме тому для визначення складності на практиці, потрібно розглянути складність алгоритму в найгіршому випадку.

Поліноміальний алгоритм - це алгоритм, складність якого в найгіршому випадку *t(n)* обмежена зверху деяким поліномом від n. Поліноміальні алгоритми прирівнюються до експоненціальних, тобто таких алгоритмів, для яких $t(n)>2^{n^k}$ для деякої константи $k \geq 1i$ майже всіх *n*.

Результатом проведеної роботи є огляд та порівняння відомих типів алгоритмів та методів визначення їх складності. Було з'ясовано, що для різних типів алгоритмів доцільні різні способи визначення складності.

Вивчення і розробка алгоритмів та способів оцінки складності з використанням теоретико-ймовірнісних методів в наші дні безперестанно розвивається

Список літератури

1. Ахо А., Хопкрофт Дж., Ульман Дж. Постороение и анализ вычислительных алгоритмов. М.: Мир, 1979. – 535 с.
2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. – 416 с.

УДК 519.681.5

В.В.Вернигора, студент
Кіровоградський національний технічний університет,
vlad261094@gmail.com

ПРИНЦИПИ ПОБУДОВИ ПАРАЛЕЛЬНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

Розподілені обчислення - спосіб вирішення трудомістких обчислювальних завдань з використанням декількох комп'ютерів, найчастіше об'єднаних в паралельну обчислювальну систему. Розподілені обчислення застосовні також у розподілених системах управління.

Загальна класифікація архітектур ЕОМ за ознаками наявності паралелізму в потоках команд і даних була запропонована Майклом Флінном в 1966 році і розширена в 1972 році. Все розмаїття архітектур ЕОМ в цій таксономії зводиться до чотирьох класів:

1. ОКОД - Обчислювальна система з одиночним потоком команд і одиночним потоком даних (SISD).
2. ОКМД - Обчислювальна система з одиночним потоком команд і множинним потоком даних (SIMD).
3. МКОД - Обчислювальна система з множинним потоком команд і одиночним потоком даних (MISD).
4. МКМД - Обчислювальна система з множинним потоком команд і множинним потоком даних (MIMD).

Слід зазначити, що хоча систематика Флінна широко використовується при конкретизації типів комп'ютерних систем, така класифікація призводить до того, що практично всі види паралельних систем виявляються віднесені до однієї групи MIMD. Як результат, багатьма дослідниками робилися неодноразові спроби деталізації систематики Флінна.

У загальному плані під паралельними обчисленнями розуміються процеси обробки даних, в яких одночасно можуть виконуватися декількох машинних операцій. Досягнення паралелізму можливо тільки при здійсненності таких вимог до архітектурних принципам побудови обчислювальної системи:

1. незалежність функціонування окремих пристроїв ЕОМ - дана вимога стосується однаковою мірою до всіх основних компонентів обчислювальної системи - до пристроїв введення-виведення, до оброблювальним процесорам і до пристроїв пам'яті;
2. надмірність елементів обчислювальної системи - організація надмірності може здійснюватися в наступних основних формах:

- використання спеціалізованих пристроїв таких, наприклад, як окремих процесорів для целочисленной і речової арифметики, пристроїв багаторівневої пам'яті (регістри, кеш);
- дублювання пристроїв ЕОМ шляхом використання, наприклад, кількох однотипних обробних процесорів або декількох пристроїв оперативної пам'яті.

Додатковою формою забезпечення паралелізму може служити конвеєрна реалізація обробних пристроїв, при якій виконання операцій в пристроях представляється у вигляді виконання послідовності складових операцію підкоманду. Як результат, при обчисленнях на таких пристроях на різних стадіях обробки можуть знаходитися одночасно декілька різних елементів даних.

Список літератури

1. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. – 416 с.

УДК.519.681

Д. И. Савеленко, студент
Кировоградский национальный технический университет,
decky1994@gmail.com

ОСОБЕННОСТИ ПРОГРАММИРОВАНИЯ МНОГОПОТОЧНЫХ ПРИЛОЖЕНИЙ НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ PYTHON

На сегодняшний день прогресс вычислительной техники тесно связан с развитием вычислительных платформ с параллельной архитектурой.

Для того чтобы приложения выполняло несколько задач одновременно используют потоки Потоки позволяют приложениям выполнять в одно и то же время множество задач. Многопоточность (multi-threading) важна во множестве приложений, от примитивных серверов до современных сложных и ресурсоёмких игр.

Потоки в Python реализуются с помощью нескольких модулей, которые есть в составе стандартной поставки Python. Как правило в группу модулей входит низкоуровневый механизм из модуля thread и механизм более высокого уровня из модуля threading. Именно последний модуль чаще всего имеется в виду при обсуждении реализации потоков в Python.

Минус модуля thread является то, что из-за отсутствия мощных средств синхронизации, для того, чтобы дождаться окончания дочерних потоков, пользователь вынужден создавать искусственные конструкции, типа контейнера. В отличии от thread модуль threading предоставляет гораздо больше возможностей и примитивов синхронизации (Lock, RLock, Condition, Semaphore, Event, Queue).

В связи с тем, что код приложения должен выполняться внутри виртуальной машины интерпретатора Python, потоки не могут быть реализованы с использованием механизмов операционной системы. Интерпретатор Python сам переключает потоки в исполняемом коде, но может делать это только после завершения очередного оператора исполняемого байт-кода.

Также, в Python имеется возможность использовать глобальную блокировку интерпретатора(GIL - Global Interpreter Lock). GIL з захватывается на время выполнения очередного потока, что делает невозможным активацию другого потока, пока эта блокировка не будет освобождена.

В заключении можно сказать что язык программирования Python имеет все необходимые инструменты для создания многопоточных приложений, еще одним плюсом является то что Python это кроссплатформенный ЯП. Минусом же такого вида программирования на Python есть относительно малая скорость вычислений по сравнению с тем же C.

Список литературы

1. Марк Лутц. Изучаем Python, 4-е издание. – Перевод с английского. – СПб.: Символ-Плюс, 2010. – 1280 с
2. Дэвид М. Бизли. Python. Подробный справочник, 4-е издание. – Перевод с английского. – СПб.: Символ-Плюс, 2010. – 864 с
3. Марк Саммерфилд. Программирование на Python 3. Подробное руководство. – Перевод с английского. – СПб.: Символ-Плюс, 2009. – 608 с

УДК.519.681

Д.В. Тасенко, студент
Кіровоградсикий національний технічний університет,
askarion98@gmail.com@gmail.com

ІСТОРІЯ ПАРАЛЕЛЬНИХ ТА РОЗПОДІЛЕНИХ ОБЧИСЛЕНЬ

Необхідність розділяти обчислювальні завдання і виконувати їх одночасно (паралельно) виникла задовго до появи перших обчислювальних машин.

Наприкінці XVIII століття у Франції під керівництвом Гаспара де Проні було розпочато роботу по уточненню логарифмічних і тригонометричних таблиць у зв'язку з переходом на метричну систему. Для її виконання був необхідний величезний на ті часи обсяг обчислень. Виконавці проекту були розбиті на три рівні:

- кваліфіковані фахівці-обчислювачі, від яких потрібна акуратність при проведенні обчислень;
- організатори розподілу завдань і обробки отриманих результатів;
- організатори підготовки математичного забезпечення та узагальнення отриманих результатів (вищий рівень, до складу якого входили Адрієн Лежандр і Лазар Карно).

Робота не була завершена через революційних подій 1799 року, однак ідеї де Проні підштовхнули Чарльза Беббіджа до створення аналітичної машини.

Рішення для моделі атомної бомби в США було отримано колективом учених, які користувалися обчислювальними машинами.

У 1962 році Е.В.Евреіновим (лауреатом Ленінської премії, 1957) спільно з Ю.Г.Косаревим в ІМ СО РАН запропонована модель колективних обчислювачів і обґрунтована можливість побудови суперкомп'ютерів на принципах паралельного виконання операцій, змінної логічної структури і конструктивної однорідності.

У 1973 році Джон Шох і Джон Хапп з каліфорнійського науково-дослідного центру Xerox PARC написали програму, яка ночами запускалася в локальну мережу PARC і примушувала працюючі комп'ютери виконувати обчислення.

У 1977 році в НГТУ (Новосибірськ) на кафедрі обчислювальної техніки під керівництвом В.І.Жіраткова була розроблена розподілена обчислювальна система з трьох ЕОМ "Мінськ-32" з оригінальним апаратним та програмним забезпеченням, що підтримує протоколи фізичного, канального і мережевого рівнів, і забезпечує виконання паралельних завдань. Одна машина перебувала на ВЦ НГТУ, а дві інші - на ВЦ Інституту Математики СО РАН. Зв'язок між НГТУ і ІМ СО РАН забезпечувалася по радіоканалу з використанням спрямованих антен. Система тестувалася при вирішенні оптимізаційних задач в області економіки з використанням крупноблочного розпаралелювання.

У 1978 році радянський математик В. М. Глушков працював над проблемою макроконвеєрних, розподілених обчислень. Він запропонував ряд принципів розподілу роботи між процесорами. На базі цих принципів їм була розроблена ЕОМ ЄС-2701.

У 1988 році Арьєн Ленстра і Марк Менес написали програму для факторизації довгих чисел. Для прискорення процесу програма могла запускатися на декількох машинах, кожна з яких обробляла свій невеликий фрагмент. Нові блоки завдань розсилалися на комп'ютери учасників з центрального сервера проекту по електронній пошті. Для успішного розкладання на множники числа завдовжки в сто знаків цій спільноті було потрібно два роки і кілька сотень персональних комп'ютерів.

З появою і бурхливим розвитком інтернету все більшу популярність стала отримувати ідея добровільного використання для розподілених обчислень комп'ютерів простих користувачів, з'єднаних через інтернет.

У січні 1996 року стартував проект GIMPS з пошуку простих чисел Мерсенна, використовуючи комп'ютери простих користувачів як добровільну обчислювальна мережа.

28 січня 1997 стартував конкурс RSA Data Security на вирішення завдання злому методом простого перебору 56-бітного ключа шифрування інформації RC5. Завдяки хорошій технічній

і організаційній підготовці проект, організований некомерційним співтовариством distributed.net, швидко здобув широку популярність.

17 травня 1999 на базі платформи BOINC запущений проект SETI@home, який займається пошуком позаземного розуму шляхом аналізу даних з радіотелескопів, використовуючи добровільну обчислювальна мережа на базі Grid.

Такі проекти розподілених обчислень в інтернеті, як SETI@Home і Folding@Home мають не меншу обчислювальну потужність, ніж найсучасніші суперкомп'ютери. Інтегральна продуктивність проектів на платформі BOINC за даними на 16 травня 2010 становить 5,2 петафлопс. Продуктивність мережі Bitcoin до 6 жовтня 2013 досягла 17000 петафлопс. Для порівняння, пікова продуктивність найпотужнішого суперкомп'ютера («K computer», Японія) - 8,16 петафлопс. До середини 2011 року найпотужнішим суперкомп'ютером був Тяньхе-1A з продуктивністю «всього» 2,57 петафлопс. Проект відзначений в Книзі рекордів Гіннеса як найбільше обчислення.

Список літератури

1. Воеводин В.В., Воеводин Вл.В. Параллельные вычисления. – СПб: БХВ-Петербург, 2002.
2. Ортега Дж. Введение в параллельные и векторные методы решения линейных систем. М.:Мир, 1991.
3. Программирование на параллельных вычислительных системах: Пер с англ./Под ред. Р.Бэбба.М.:Мир, 1991.
4. Бройнль Т. Паралельне програмування: Початковий курс: Навчальний посібник. – К.:Вища школа.,1997.
5. Воеводин В.В. Математические основы параллельных вычислений.- М.: Изд-во МГУ, 1991.
6. Векторизация программ: теория, методы, реализация: Пер. с англ. и нем. /Под ред. Г.Д.Чинина. - М:. Мир, 1991.
7. Корнеев В.В. Параллельные вычислительные системы. М.: Нолидж, 1999
8. С. Немнюгин, О.Стесик Параллельное программирование для многопроцессорных вычислительных систем. – СПб: БХВ-Петербург, 2002.
9. Pacheco P. Parallel Programming With MPI (див. www.parallel.ru).
10. Gropp W., Lusk E., Skjellum A. Using MPI (див. www.parallel.ru).

УДК 004.451.2

В.Г. Ладоня, студент
Кіровоградський національний технічний університет,
vadymvl@gmail.com

РЕАЛІЗАЦІЯ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ ЗА ДОПОМОГОЮ OPENMP

У наш час багатоядерні процесори зазнають досить швидкого розвитку. Якщо Закон Мура не втратить своєї сили, протягом 5 років середній комп'ютер матиме 16, або навіть 32 ядра на одному чіпі. Проте лише 30 % існуючого програмного забезпечення враховує багатоядерність процесорів при своїй роботі, і тому їх ефективне використання потребує загального переходу з послідовних програм на паралельні. Навіть спроби розпаралелювати потоки за допомогою операційної системи далеко не у всіх випадках призводять до позитивного результату. Існують дві основних моделі побудови паралельних програм. Це модель паралелізму по керуванню та модель загальної пам’яті. На разі одним з найбільш популярних засобів паралельного програмування на багатоядерних комп’ютерах із загальною пам’яттю є програмний засіб OpenMP (Open Multi-Processing), за допомогою якого можна розпаралелити окремі частини програми, які будуть виконуватися на ядрах комп’ютера окремими потоками.

Стандарт OpenMP – це набір директив компілятора, бібліотечних процедур і змінних оточення, які призначені для програмування багатопотокових додатків на багатопроцесорних системах з єдиною пам’яттю на мовах Сі, C++ і Fortran. Спочатку малося на увазі, що програма з OpenMP виконуватиметься на комп’ютері з декількома процесорами, причому кількість процесорів може не збігатися з кількістю потоків, на які розпаралелюється програма. Якщо кількість потоків більше кількості ядер або процесорів, то потоки можуть перемикатися при виконанні або «чекати» поки звільниться процесор. Якщо при ініціалізації багатопотоковій системі забороняється змінювати кількість потоків, то потоки виконуватимуться по черзі. Засоби, описані стандартом OpenMP, дають змогу маніпулювати потоками: видаляти, блокувати, перенаправляти, робити критичні секції, зупиняти і припиняти потоки і т.д. На однопроцесорних комп’ютерах паралельна програма виконуватиметься в одному потоці. Для подання послідовної програми у паралельному вигляді здебільшого використовують методи «інкрементного» програмування. Його суть полягає в тому, що програміст, проглядаючи програму, спочатку відшукує блоки, які можуть бути розпаралелені, а потім за допомогою спеціальних засобів OpenMP «розпаралелює» їх, тим самим зменшуючи кількість лінійного коду, і підвищуючи продуктивність програмного продукту або системи в цілому. Використання підходу «інкрементного» програмування полегшує модернізацію раніше написаного програмного забезпечення.

Таким чином, використання OpenMP на не тільки підвищує ефективність програмного забезпечення, але також дає можливість краще зрозуміти суть паралельного програмування.

Список літератури

1. Антонов А. С. Параллельное программирование с использованием технологии OpenMP / А. С. Антонов. – МГУ, 2009. – С. 78.
2. Левин М. П. Параллельное программирование с использованием OpenMP: учеб. пособие. – М. :Интернет университет информационных технологий; БИНОМ. Лаборатория знаний, 2008. – С. 118.
3. Векторизация программ: теория, методы, реализация: Пер. с англ. и нем. /Под ред. Г.Д.Чинина. - М:. Мир, 1991.
4. Корнеев В.В. Параллельные вычислительные системы. М.: Нолидж, 1999
5. С. Немнюгин, О.Стесик Параллельное программирование для многопроцессорных вычислительных систем. – СПб: БХВ-Петербург, 2002.

УДК 004.92

В.Г. Андрієнко, студент
Кіровоградський національний технічний університет,
avg94-13@mail.ru

ВЕКТОРНА ГРАФІКА ДЛЯ ОПИСУ ОБ'ЄКТІВ

Векторна графіка, на відміну від растрової графіки, визначає опис зображення на вигляді ліній і постатей, можливо, з зафарбованими областями, заповнюваними суцільним чи градієнтним кольором.

Хоча це може бути складнішим, ніж використання растрових масивів, але багатьом видів зображень використання математичних описів є у простий спосіб.

У векторної графіці для описи об'єктів використовуються комбінації комп'ютерних команд і математичних формул для описи об'єктів. Це дозволяє різним пристроям комп'ютера, таких як монітор і принтер, при малюванні цих об'єктів обраховувати, де необхідно поміщати реальні точки.

Векторну графіку часто називають об'єктно-орієнтованої чи креслярської графікою. Маємо низку найпростіших об'єктів, чи примітивів, наприклад: еліпс, прямокутник, лінія. Ці примітиви і їхні комбінації йдуть на створення складніших зображень.

Якщо зміст файлу векторної графіки, можна знайти схожість із програмою. Він може містити команди, схожі на свої слова, і такі в коді ASCII, тому векторний файл можна відредагувати з допомогою текстового редактора.

Векторна графіка має такі переваги:

– простота масштабування зображення без погіршення його якості;

– незалежність обсягу пам'яті, необхідної для зберігання зображення, від обраної колірної моделі.

Недоліком векторних зображень був частиною їхнього деяка штучність, яка полягає у цьому, що будь-який зображення необхідно розбити на кінцеве безліч складових його примітивів.

Векторні зображення, у яких розмір будь-якого елемента може бути змінений аж «до нескінченності». Але таку картинку неможливо отримати шляхом сканування, оскільки кожний її елемент будується з допомогою математичних описів об’єктів (так званих примітивів), в якості яких можуть виступати лінії, дуги, кола і тому подібне.

Також для кожного примітива існує ряд параметрів, які визначають колір, товщину лінії і тому подібне. Векторна графіка створюється за допомогою спеціальних програмних засобів типу CorelDRAW, Adobe Illustrator.

Також такий формат зображення використовується в усіх програмах Системи Автоматичного Проектування, P-CAD, Auto-CAD і тому подібне.

Фактично векторне зображення існує у вигляді набору математичних формул, які описують елементи, нарешті, векторна графіка не залежить від продуктивності апаратних засобів, яка дозволяє легко змінювати розміри статичних зображень без втрати загальної кількості елементів зображення, ясності і чіткості їхніх меж при виведенні на екран монітору або при друці.

Список літератури

1. Яхонтов В.М. Комп'ютерна графіка. - М.: ТИСБИ, 2003.
2. Маценко В.Г. Комп’ютерна графіка: Навчальний посібник. – Чернівці: Рута, 2009 – 343 с.

УДК 004.92

Р.В. Гребінка, студент
Кіровоградський національний технічний університет
1995roman12@I.ua

ПРОГРАМНІ ЗАСОБИ ДЛЯ РОБОТИ З КОМП'ЮТЕРНОЮ ГРАФІКОЮ

Вступ. Робота з комп'ютерною графікою – один з найпопулярніших напрямків використання персонального комп'ютера, до того ж займаються цією роботою не тільки професійні художники і дизайнери. На будь-яких підприємствах час від часу виникає необхідність в подачі рекламних оголошень в газетах і журналах або просто у випуску рекламної листівки або буклету.

Без комп'ютерної графіки не обходиться жодна сучасна мультимедійна програма. Робота над графікою займає до 90 % робочого часу програмістських колективів, які випускають програми масового примінення.

Не дивлячись на те, що для роботи з комп'ютерною графікою існує маса класів програмного забезпечення, розрізняють усього 3 види комп'ютерної графіки. Це растрова графіка, векторна графіка і фрактальна графіка. Вони відрізняються принципами формування зображення при відображенні на екрані монітора або при друці на папері.

Растрову графіку приміняють при розробці електронних (мультимедійних) і поліграфічних видань. Ілюстрації, виконані засобами растрової графіки, рідко створюють вручну за допомогою комп'ютерних програм. Частіше для цієї мети використовують скановані ілюстрації, підготовлені художником на папері, або фотографії. В останній час для вводу растрових зображень в комп'ютер широко використовують цифрові фото- і відеокамери.

Відповідно, більшість графічних редакторів, які призначені для роботи з растровими ілюстраціями, орієнтовані не стільки на створення зображення, скільки на їх обробку. В Інтернеті поки що приміняють тільки растрові ілюстрації.

Програмні засоби для роботи з векторною графікою**,** навпаки, призначені, в першу чергу, для створення ілюстрацій і в меншій мірі для їх обробки. Такі засоби широко використовують в рекламних агентствах, дизайнерських бюро, редакціях і виданнях. Оформлювальні роботи, основані на застосуванні шрифтів і простих геометричних елементів, вирішуються засобами векторної графіки набагато простіше. Існують приклади високохудожніх творів, створених засобами векторної графіки, але вони скоріше виключення, ніж правило, оскільки художня підготовка ілюстрацій засобами векторної графіки надзвичайно складна.

Програмні засоби для роботи з фрактальною графікою призначені для автоматичної генерації зображення шляхом математичних розрахунків. Створення фрактальної художньої композиції полягає не в рисуванні чи оформленні, а в програмуванні. Фрактальну графіку рідко приміняють для створення друкованих або електронних документів, але її часто використовують у розважальних програмах.

Висновок: Комп'ютерна графіка охоплює всі види та форми представлення зображень, як на екрані монітора, так і на зовнішньому носії (папір, плівка, тощо). Комп'ютерна графіка застосовується для візуалізації даних у різних сферах людської діяльності:

- медицина - комп'ютерна томографія;
- наука - склад речовин, векторні поля графіки процесів;
- дизайн - реклама, поліграфія, моделювання**.**

Список літератури

1. Пічугін М.Ф. Комп'ютерна графіка / М.Ф.Пічугін. І.О.Канкін, В.В.Воротніков Центр учбової літератури. 2013. - 346 с.

УДК 004.92

В.Г. Ладоня, студент
Кіровоградський національний технічний університет,
vadymvl@gmail.com

ОГЛЯД ОСОБЛИВОСТЕЙ OPENGL

OpenGL (Open Graphics Library) – відкритий програмний графічний інтерфейс, він підтримується багатьма операційними системами і придатний для реалізації на різних апаратних платформах – від персональних комп'ютерів до смартфонів.

Інтерфейс OpenGL реалізований у вигляді бібліотеки функцій, які програміст використовує при написанні інтерактивних програм для створення різних графічних об'єктів, операцій над ними і відображення їх на екрані.

Цей інтерфейс розроблений у 1992 р. дев'ятьма провідними фірмами з розробки програмного забезпечення, серед яких були Digital, Hewlet Packard, IBM, Intel, Silicon, Microsoft. В основу стандарту покладена бібліотека IRIS GL, розроблена фірмою Silicon Graphics.

Процедури OpenGL працюють як із растровою, так і з векторною графікою і з легкістю дозволяють програмісту:

1) створювати 2D- та 3D-вимірні об'єкти довільної форми на основі геометричних та растрових примітивів;
2) задавати сплайнові лінії та поверхні, що визначаються опорними точками;
3) розміщувати об'єкти в просторі, вибирати спосіб і параметри проектування, задавати розміщення камери;
4) виконувати роботу з кольором об'єктів. Колір може бути заданий як явно (в режимі RGBA та індексному режимі) так і обчислюватися з урахуванням джерел світла, параметрів освітлення. Для об'єктів може задаватися матеріал, накладатися текстура тощо;
5) проводити математичні перетворення над об'єктами зображення, наприклад видові та модельні перетворення, виконувати усунення невидимих ліній і поверхонь;
6) пересувати джерела світла і камеру за заданими траєкторіями;
7) додавати спеціальні ефекти туману, диму, прозорості тощо.

Команди OpenGL реалізовані як модель "клієнт-сервер". Додаток виступає в ролі клієнта – він виробляє команди, а сервер OpenGL інтерпретує і виконує їх. Сам сервер може знаходитися як на тому ж комп'ютері, що й клієнт, так і на іншому.

До характерних особливостей OpenGL, що забезпечили його поширення і розвиток, можна віднести:

1) стабільність (доповнення і зміни в стандарті реалізуються в такий спосіб, щоб зберегти сумісність із розробленим раніше програмним забезпеченням, тобто нова версія OpenGL відбувається тільки за рахунок розширення);
2) надійність і переносимість (додатки гарантують однаковий візуальний результат незалежно від конкретної апаратної і програмної платформи, типу використовуваної операційної системи);
3) легкість і простота застосування (OpenGL має продуману структуру, інтуїтивно зрозумілий інтерфейс, що дозволяє з меншими затратами створювати ефективні додатки, які містять менше рядків коду в порівнянні з використанням інших графічних бібліотек).

Важливим фактором є також підтримка інтерфейсу OpenGL виробниками графічних прискорювачів. Оскільки OpenGL відкритий стандарт, то виробники графічних прискорювачів самостійно можуть добавляти до OpenGL нові можливості, що підтримуються їхніми графічними процесорами (нові можливості зразу стають доступними програмісту). Апаратна реалізація всіх базових функцій OpenGL забезпечує швидкодію графічних програм, які використовують OpenGL. Ця швидкодія істотно залежить від відеоадаптера.

У наш час більшість відеоадаптерів містять спеціальний графічний процесор для підтримки графічних функцій. Відеоадаптер апаратно виконує всі базові функції OpenGL:

перетворення координат, розрахування освітленості, накладання текстур, відсікання, виведення полігонів тощо. Тому OpenGL дозволяє достатньо просто створювати швидкодіючі програми і широко використовується на практиці (наприклад, при розробці комп'ютерних ігор).

OpenGL надає користувачу достатньо потужний низькорівневий набір команд, а всі операції високого рівня виконуються в термінах цих команд.

Але хоча бібліотека OpenGL має практично необмежені можливості для моделювання і відтворення тривимірних сцен, деякі графічні функції в OpenGL безпосередньо відсутні, наприклад для камери необхідно розраховувати проекційну матрицю, що вимагає додаткових обчислень.

Тому для полегшення роботи разом з OpenGL постачаються бібліотеки додаткових команд. На даний момент реалізація Microsoft OpenGL містить кілька бібліотек:

- OpenGL – набір базових функцій (бібліотека opengl32.dll) для створення об'єктів та управління їх відображенням на екрані. Тобто OpenGL надає користувачу потужний набір функцій низького рівня, а всі інші операції високого рівня повинні задаватися в термінах цих команд. Імена базових команд починаються з префікса gl, а всі константи – з префікса GL. Кожне слово, що входить в ім'я функції, починається з великої літери, наприклад glPolygonMode;
- Glu-бібліотеку (бібліотека утиліт). Glu-бібліотека є невід'ємною частиною стандарту і поставляється разом з головною бібліотекою OpenGL (вона входить у поставку Windows – це бібліотека glu32.dll). Команди цієї бібліотеки доповнюють базові функції OpenGL і полегшують роботу програміста.
- До складу бібліотеки Glu увійшла множина більш складних функцій, таких як реалізація куба, кулі, циліндра, диска, сплайнових кривих і поверхонь, реалізація додаткових операцій над матрицями тощо. Усі вони реалізовані через базові функції OpenGL. Імена команд бібліотеки утиліт починаються з префікса glu;
- Glaux-бібліотеку. OpenGL безпосередньо не підтримує роботу з пристроями введення (миша, клавіатура), оскільки бібліотека платформо-незалежна. Але можна задіяти функції конкретної операційної системи, під яку пишеться програма, або скористатися надбудовами над OpenGL, таким як бібліотека Glut (для Unix) і Glaux (для Windows). Команди бібліотеки Glaux починаються з префікса aux.

Бібліотеки діють через драйвери пристроїв. Це дозволяє ефективно працювати з графічними прискорювачами, не прив'язуючись до їх конкретних особливостей. Одна і та ж сама програма буде успішно працювати на різних прискорювачах без модифікації вихідного коду.

Список літератури

1. Эйнджел Э. Интерактивная компьютерная графика. Вводний курс на базе OpenGL. – М.: Вильямс, 2001. – 592 с.
2. Херн Д., Бейкер М. Компьютерная графика и стандарт OpenGL. – М.: Вильямс, 2005. – 1158 с.

УДК 004.925

О.А. Філіппов, студент
Кіровоградський національний технічний університет,
alex.fil25@yahoo.com

ФРАКТАЛЬНА ГРАФІКА НА ПРИКЛАДІ БЕЗЛІЧІ МАНДЕЛЬБРОТА

Серед усіх зображень, які може створювати комп'ютер, лише деякі можуть посперечатися з фрактальними зображеннями, коли йде мова про справжню красу. У більшості з нас слово "фрактал" викликає в пам'яті кольорові завитки, що формують складний, тонкий і складовою візерунок. Але насправді цей термін має набагато більш широкий зміст. Фрактал - об'єкт, що володіє нескінченною складністю, що дозволяє розглянути стільки ж своїх предметів поблизу, як і здалеку. Земля - класичний приклад фрактального об'єкта. З космосу вона виглядає як сфера. Якщо наближатися до неї, ми побачимо океани, континенти, узбережжя і ланцюги гір. Будемо розглядати гори ближче - стануть видні ще більш дрібні деталі: шматочок землі на поверхні гори у своєму масштабі настільки ж складний і нерівний, як сама гора. І навіть ще більш сильне збільшення покаже крихітні частинки грунту, кожна з яких сама є фрактальним об'єктом [1].

Комп'ютери дають можливість будувати моделі таких нескінченно деталізованих структур. Є багато методів створення фрактальних зображень на комп'ютері. Фрактальні зображення з кольоровими завитушками відносяться звичайно до розряду так званих фракталів з тимчасовим порогом, які зображуються точками на комплексній площині з квітами, що відбивають час, необхідний для того, щоб орбіта даної точки перейшла певну межу [1].

Найбільш відомий фрактал, безліч Мандельброта - фрактал з тимчасовим порогом. Для кожної точки на екрані комп'ютер вважає координати серії точок, що визначають уявний шлях, званий орбітою. Точки, чиї орбіти ніколи не виходять за межі уявного циліндра, розташованого на початку координат комплексної площині, вважаються елементами множини Мандельброта і зазвичай зафарбовуються чорним. Точки, чиї орбіти виходять за межі циліндра, розфарбовуються відповідно до швидкістю "тікання": піксель, чия орбіта залишає циліндр, наприклад, на шостий ітерації, можна розфарбувати блакитним, а той - орбіті якого потрібно для цього сім ітерацій - червоним. У результаті на зображенні отримаємо безліч Мандельброта і його оточення з "нестабільними" областями фрактала - областями, для яких малізміни формули ведуть до великої різниці в орбітальному поведінці. Це характеризується густотою зафарбовування малюнка. Змінюючи формулу для підрахунку орбіт, отримаємо інші, такі ж екзотичні фрактали з тимчасовим порогом. Нескінченно деталізована структура множини Мандельброта стає "ясною", коли ви збільшуєте довільну область. Неважливо, наскільки маленьку ділянку ви розглядаєте: малюнок, який ви побачите, буде однаково складним. Чому? Тому що в двовимірної площині, на якій будується безліч Мандельброта, будь-яка область містить нескінченну кількість точок. Коли ви вибираєте область для відображення, комп'ютер точкам з області ставить у відповідність точки на екрані. І кожна точка, вибрана як завгодно близько до іншої, має свою характеристичну орбіту, породжує відповідний кольоровій візерунок [2].

Список літератури

1. Джеф Проузіс. Як працює комп'ютерна графіка. - СПб.: Питер, 2008. - 654 с.
2. Жвалевський А., Гурська І, Гурський Ю. Комп'ютерна графіка: Photoshop CS3, CorelDRAW X3, Illustrator CS3. Трюки й ефекти. - СПб.: Пітер, 2008. - 992 с.

УДК 004.77, 004.451

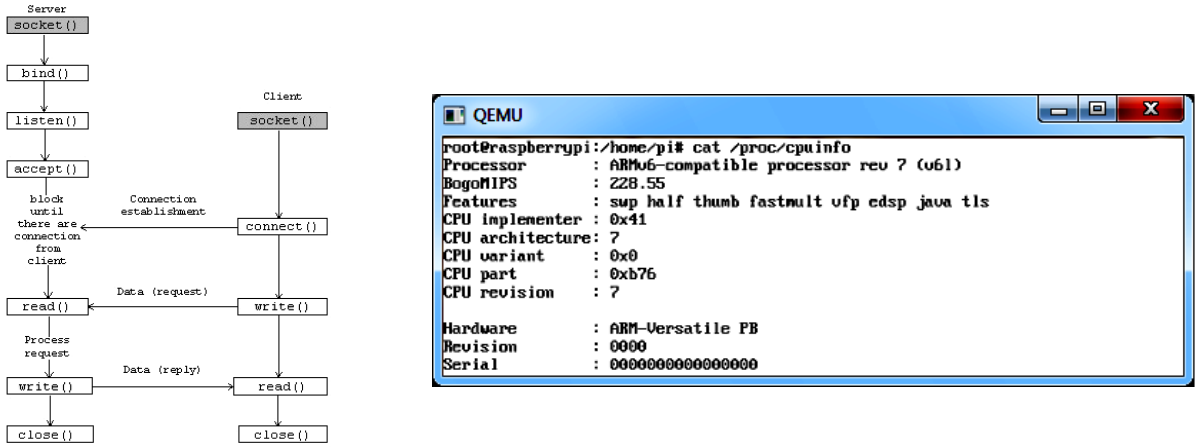
І.С.Бурлаченко, викладач
Чорноморський державний університет ім. Петра Могили,
ivan.burlachenko2010@gmail.com

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ МЕРЕЖЕВИХ ДОДАТКІВ В ПРОЦЕСІ ВІРТУАЛЬНОЇ ЕМУЛЯЦІЇ ВУЗЛІВ БЕЗДРОТОВИХ МЕРЕЖ

Актуальність ринку технологій віртуалізації за останні кілька років виникла завдяки збільшенню потужностей апаратного забезпечення, що дозволило створювати по-справжньому ефективні платформи віртуалізації комп'ютерних систем. Технології віртуалізації дозволяють запускати на одному фізичному хості кілька віртуальних екземплярів ОС з метою забезпечення їх незалежності від апаратної платформи. Виникає можливість запуску декількох віртуальних машин на одному фізичному хості [1].

Передача потоку відео між розподіленими вузлами сенсорної мережі є важливою задачею в процесі моніторингу промислових територій. Модуль відеокамери для Raspberry Pi забезпечує наступні характеристики: розширення: 5Мп, 2592 x 1944; розмір матриці: 1/4 дюйми; формат відео: 1080p (30fps), 720p (60fps), VGA (60-90fps).

Були досліджені можливості вузлів розподіленої сенсорної мережі в процесі емуляції архітектури Raspberry Pi с допомогою системи віртуалізації QEMU (рис. 1б). QEMU - вільна програма з відкритим вихідним кодом для емуляції апаратного забезпечення різних платформ, яка може працювати і без використання KVM, але використання апаратної віртуалізації значно прискорює роботу гостьових систем, тому використання KVM в QEMU (-enable-kvm) є кращим варіантом. KVM (або Kernel-based Virtual Machine) - це програмне рішення, що забезпечує віртуалізацію в середовищі Linux, яке підтримує апаратну віртуалізацію на базі Intel VT (Virtualization Technology) або AMD SVM (Secure Virtual Machine).



а) б)

Рис. 1 – а) Архітектура мережевого додатку (Sockets) б) Архітектура емулятора QEMU

За допомогою OpenSSH, як набору мережевих інструментів, що використовуються для захищеного доступу до віддалених комп'ютерів, було реалізовано SSH безпечне туннелирование і перенаправлення довільних TCP / IP з'єднань між віртуальними машинами Raspberry Pi. OpenSSH шифрує весь трафік, ефективно запобігаючи крадіжку даних, перехоплення з'єднання та інші мережеві атаки. Було вироблено конфігурація OpenSSH сервера на віртуальній машині QEMU. Запуск віртуальної машини з параметрами виглядає наступним чином:

qemu-system-arm.exe -M versatilepb -cpu arm1176 -hda 2012-07-15-wheezy-raspbian.img -kernel kernel-qemu -m 192 -append "root=/dev/sda2" -redir tcp:2222::22 (1)

За допомогою утиліти PSCP стало доступним розміщення модулів програмного забезпечення на віртуальних машинах для проведення подальших досліджень.

Архітектура мережевого додатку (рис. 1а) орієнтована на підвищення продуктивності передачі даних, тому використовує концепцію сокетів на відміну від передачі даних через http протокол. Завдання серверного сокетного з'єднання полягає в тому, що за один сеанс зв'язку необхідно прийняти дані від клієнта і відразу ж передати клієнту відповідь ефективно використовуючи потоки вводу/виводу як на сервері, так і на клієнті. Серверна частина додатку представлена в таблиці 1

Таблиця 1 – Ініціалізація сокетів серверної частини мережевого додатку

Python (Sockets)	Java (Sockets)

import socket
import sys
 	
HOST = None # Symbolic name meaning all available interfaces
PORT = 2222 # Arbitrary non-privileged port
s = None
for res in socket.getaddrinfo(HOST, PORT, socket.AF_UNSPEC,
socket.SOCK_STREAM, 0,
socket.AI_PASSIVE):
af, socktype, proto, canonname, sa = res
s = socket.socket(af, socktype, proto)
s.bind(sa)
s.listen(1)
	import java.net.*;
	import java.io.*;
	
	String hostName = args[0];
	int portNumber = Integer.parseInt(args[1]);
	try {
	Socket echoSocket = new Socket(hostName, portNumber);
	PrintWriter out =
	new PrintWriter(echoSocket.getOutputStream(), true);
	BufferedReader in =
	new BufferedReader(
	new InputStreamReader(echoSocket.getInputStream()));
	BufferedReader stdIn =
	new BufferedReader(
	new InputStreamReader(System.in))
	}

Живлення вузла бездротової мережі є критичною проблемою [2], тому що здійснюється від батареї, заряд якої є обмеженим. Тому був досліджений відносно суттєвий показник продуктивності мережі, що виражений класичним середнім арифметичним значенням сумарного завантаження процесорів U_i з урахуванням ролей $NetR_i$ всіх вузлів під час передачі відео потоку:

$$AvrCPUusage = \frac{1}{N}\sum_{i=1}^{N} U_i \cdot NetR_i \ . \qquad (2)$$

Таким чином процес емуляції мережі з 20 віртуальних Raspberry Pi демонструє низьке завантаження в випадку реалізації мережевого ПЗ з використанням стеку Java технологій. Результати експерименту представлені у таблиці 2.

Таблиця 2 – Середнє завантаження CPU вузлів мережі

Формат відео / Реалізація серверу	*AvrCPUusage*	
	60fps (720p)	30fps (1080p)
Java 7	47%	31%
Python 3.4	53%	38%

Список литературы

1. Robert Warnke and Thomas Ritzau., Qemu-kvm & libvirt // ISBN 978-3-8370-0876-0, Books on Demand GmbH, Norderstedt, 2010. - 4-th Edition. 276 p.

2. Мусиенко М. П. Модели диспетчеризатора заданий в распределенных компьютерных системах с ограниченным питанием удаленных модулей / М. П. Мусиенко, В. Ю. Савинов // Вісник Черкаського державного технологічного університету. Сер.: Технічні науки. - 2014. - № 2. - С. 44-47.

УДК 004.94

В.С. Білий, студент
Кіровоградський національний технічний університет,
viktor_belyi@mail.ru

МОДЕЛЮВАННЯ ОБ'ЄКТІВ ЗА ДОПОМОГОЮ ЗАСОБІВ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Проектування є найважливішим етапом життєвого циклу будь-якого об'єкта при його створенні, від виконання якого залежить якість реалізованого об'єкта. Моделювання є одним із методів проектування, який в наш час продовжує бурхливо розвиватись.

Сьогодні в таких сферах, як машинобудування, дизайн, архітектура і навіть медицина широке розповсюдження отримало створення 3D-моделей в якості випробувальних зразків, які підлягають різноманітним дослідженням перед перенесенням на реальний матеріал. Однак, потрібно зауважити, що побудова 3D-моделей потребує спеціальних знань та вмінь від інженерів, дизайнерів та медиків, які не завжди володіють ними, хоча і є експертами у своїй галузі.

Слід також додати, що побудова складних 3D-моделей потребує значних ресурсів, таких, як час та зусилля що, як наслідок, може значно збільшити вартість проекту.

Для того, аби вирішити подібну проблему, можна застосувати нестандартний підхід, використавши таку сучасну технологію, як розширена, або, як її ще називають, доповнена реальність.

Даний термін має відношення до всіх проектів, які спрямовані на доповнення реальності будь-якими віртуальними елементами. До нього входять: додавання віртуальних об'єктів до відео-зображення в режимі реального часу, накладення допоміжної інформації на зображення об'єктів і навколишнього простору і багато іншого з того, що входить у концепцію доповнення реальності.

Концепція, за якою працюють сьогоднішні технології, складається з двох кроків: зчитування зображення навколишньої дійсності за допомогою камер та розуміння його за допомогою алгоритмів розпізнавання образів.

Для вирішення нашої проблеми, ми можемо використовувати доповнену реальність як допоміжний засіб для створення попереднього передпроектного рішення.

Маючи в своєму розпорядженні певний невеликий об'єкт та його зображення на площині, ми можемо зчитати його камерою і обробити за необхідними алгоритмами, після чого отримати його на екрані в об'ємі, не прикладаючи до цього абсолютно ніяких зусиль.

Варто додати, що такий варіант буде для нас дуже корисний при виборі варіанту дизайну того чи іншого об'єкта, коли ми суттєво скорочуємо час до проектування одного остаточного варіанту для розробки, а не всього набору, з якого все одно буде обраний єдиний.

Список літератури

1. TheEndofHardware: AugmentedRealityandBeyond - Rolf R. Hainich, Booksurge, 416 p.

УДК 004.8

Васьков Д.О., студент
Кіровоградський національний технічний університет,
kavabangaa27@gmail.com

СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

Вступ. На сьогоднішній день штучний інтелект залишається одним із найбільш перспективних і нерозкритих напрямків розвитку інформаційних управляючих систем та технологій. До складу понять штучного інтелекту сьогодні відносять нейронні мережі, нечітку логіку, експертні системи, ЕОМ п'ятого покоління, системи моделювання мислення.

Основна частина. На сьогодні компанія Numenta приступила до розповсюдження дослідної версії обчислювальної платформи NuPIC (Numenta Platform for Intelligent Computing), з допомогою якої користувач може самостійно будувати системи, які реалізують принцип передбачувальної пам' яті, і використовувати їх для розв'язання задач, пов'язаних з аналізом та екстраполяцією різноманітних даних.

Інсталяційний пакет пакет програми NuPIC поширюється у двох версіях: для операційних систем Linux та Mac OS. Для користувачів ОС Microsoft Windows пропонується запускати на виконання Linux-версію NuPIC з допомогою спеціальної програми фільтра-емулятора.

Програмний пакет містить інструменти для створення і виконання додатків, модельованих кортексоподібними структурами, згідно з термінологією Numenta - НТМ-системами, а також вихідні коди на C++ та Python, документацію та приклади.

Для роботи системи штучного інтелекту бажано використовувати кілька процесорів, оскільки при використанні лише одного комп’ютера швидкість роботи помітно падає. Популярні нині нейро-експертні системи – це особливі системи штучного інтелекту, основою яких є величезна база знань. У ній зберігаються численні відомості та методи, необхідні для вирішення поставлених завдань.

Дуже важливим компонентом експертної системи є її інтерфейс. Завдяки йому людина може наповнювати базу новими даними, отримувати логічні висновки і т.д. Застосовуючи накопичені знання, ці системи можуть знаходити вірне рішення для тих завдань, які занадто складні для людських можливостей.

Нещодавно стало відомо, що корпорація Google має намір до 2029 року надати обробку пошукових запитів новому штучному інтелекту .

Висновки Однозначної відповіді, що ж таке «штучний інтелект» на даний момент не існує. Кожен автор має свою думку з цього приводу.

Деякі вважають, що штучний інтелект може бути створений на основі однієї з методик перерахованих вище, інші вважають, що створення штучного інтелекту неможливо саме на поточному етапі розвитку людства, треті - взагалі в принципі заперечують можливість створення штучного інтелекту.

Список літератури

1. Балабанов О. Комп’ютерний інтелект: можливість і реальність / О.Балабанов // Вісн. НАН України. – 1997. – № 9–10. – С. 16–21.

УДК 004

Н.А. Дроговоз, викладач
Кіровоградський державний педагогічний університет,
dna2011@ukr.net

ВИКОРИСТАННЯ МЕТОДУ ПРОЕКТІВ ПРИ ВИВЧЕННІ ДИСЦИПЛІНИ «ПРОГРАМУВАННЯ ЗАСОБАМИ DELPHI»

Знання і компетентність займають центральне місце у сучасному інформаційному суспільстві. Інформатизація більшості сфер виробництва вже зараз вимагає від спеціалістів уміння творчо мислити, вміти працювати в команді й визначати пріоритети, планувати конкретні результати й нести особисту відповідальність за їх реалізацію, ефективно використовувати знання в реальному житті.

Для вирішення цих завдань доцільно використовувати проектну методику. Суть цієї методики полягає в стимулюванні інтересу студентів до навчання через проектну діяльність, в демонстрації практичного застосування набутих знань, виконання самостійної (індивідуальної або групової) дослідницької діяльності.

Під навчальним проектом розуміють організаційну форму роботи, яка орієнтована на засвоєння навчальної теми або навчального розділу і становить частину однієї або декількох дисциплін [1].

Метод проектів можна успішно застосовувати для більш глибокого вивчення дисципліни «Програмування засобами Delphi».

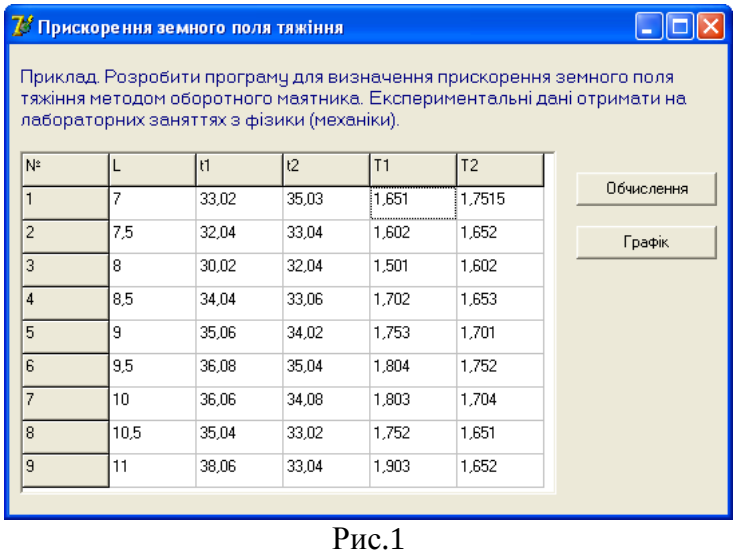
Розглянемо наступний приклад: розробити програму для визначення прискорення земного поля тяжіння методом оборотного маятника. Експериментальні дані отримати на лабораторних заняттях з фізики (механіки) [2].

Основною задачею проекту буде сформувати знання та навички створення багатовіконних проектів засобами Delphi. Кінцевим продуктом діяльності студентів у проекті буде нове знання, вміння і навички, необхідні для ефективного використання Delphi при розробці прикладного програмного забезпечення.

Розглянемо детальніше розробку проекту програми запропонованого прикладу. Роботу над проектом бажано розбити на декілька етапів, кожен з який присвячений вивченню певної теми курсу «Програмування засобами Delphi».

І етап. Вивчаючи тему «Введення та відображення текстової інформації», студентам можна запропонувати наступний план дій:

1. Визначити вхідні та вихідні дані, залежності між даними.
2. Створити новий проект. Визначити структуру та параметри головної форми проекту, зокрема, розміри, колір, назву.
3. Добавити компоненти для введення та виведення даних (рис.1).



№	L	t1	t2	T1	T2
1	7	33,02	35,03	1,651	1,7515
2	7,5	32,04	33,04	1,602	1,652
3	8	30,02	32,04	1,501	1,602
4	8,5	34,04	33,06	1,702	1,653
5	9	35,06	34,02	1,753	1,701
6	9,5	36,08	35,04	1,804	1,752
7	10	36,06	34,08	1,803	1,704
8	10,5	35,04	33,02	1,752	1,651
9	11	38,06	33,04	1,903	1,652

Рис.1

4. Розташувати на головній формі кнопку для розрахунку періоду власних коливань. Слід звернути увагу студентів на необхідність перетворення текстових даних у числові.

5. Забезпечити коректність введення даних. Студентам можна запропонувати наступні способи вирішення цієї проблеми:

– обмеження введення;

– обробка виключних ситуацій.

ІІ етап. Тема: «Компоненти відображення графічної та мультимедійної інформації».

На даному етапі задача ускладнюється необхідністю побудови графіків залежності періодів коливань від положення зовнішньої чечевиці. Для удосконалення проекту студентам слід виконати наступні кроки.

1. Додати в проект компоненти, що забезпечуватимуть можливість побудови графіків, їх редагування (рис. 2).

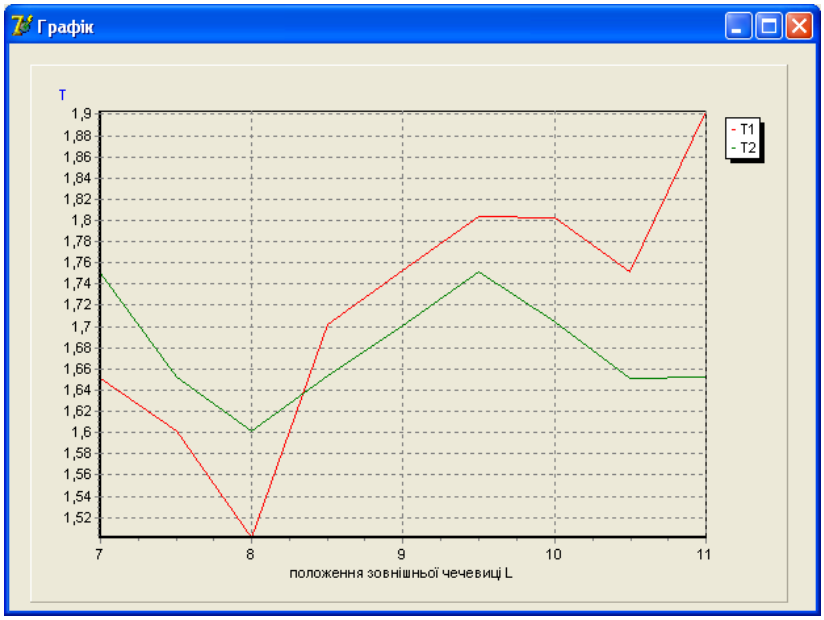


Рис. 2

2. Добавити в проект графічну імітацію коливного руху.

3. Забезпечити можливість збереження даних в різних форматах.

При виконанні подібних завдань у студентів розширюються уявлення про можливості використання об’єктно-орієнтованого програмування для створення і дослідження комп’ютерних моделей різних фізичних процесів.

Отже, у результаті організації навчально-пізнавальної діяльності на заняттях за допомогою метода навчальних проектів студенти набувають не тільки визначені програмою знання, уміння та навички, а ще починають самостійно вирішувати різноманітні проблеми; формувати навички критичного та творчого мислення, навчаються ставити перед собою практичні завдання.

Список літератури

1. Копотій В.В. Використання методу навчальних проектів у класах природничо-математичного профілю // Науковий часопис НПУ імені М.П. Драгоманова Серія №2. Комп’ютерно-орієнтовані системи навчання: Зб. наук. праць / Редкол. – К.: НПУ ім. М.П. Драгоманова. – № 3 (10) – 2005. – С. 84–102.

2. Дроговоз Н.А. Присяжнюк О.В., Рєзіна О.В. Досвід нівчання елементів комп’ютерного моделювання майбутніх учителів фізики // Наукові записки. – Випуск 5. – Серія: Проблеми методики фізико-математичної і технологічної освіти. Частина 2. – Кіровоград: РВВ КДПУ ім. В.Винниченка. – 2014. – С. 84–89.

НАУКОВЕ ВИДАННЯ

«Комп'ютерні технології та інформаційна безпека»

Збірник тез доповідей міжнародної науково-практичної конференції 2-3 липня 2015 року (електронне видання), м.Кіровоград

Відповідальний редактор	В.В.Смірнов
Комп’ютерна верстка і макетування	Н.В.Смірнова
Відповідальний секретар конференції	В.В.Смірнов

Матеріали збірника публікуються у авторській редакції.

Підписано до друку 28.06.2015
Ум друк.арк. 5.06. Тираж 100 прим.

Тел. 390-449