МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

УДК 681.518.54

Тези доповідей

ІІ Міжнародної науково-практичної конференції

“Інформаційна безпека та інформаційні технології”
“Information Security and Information Technologies”

2– 3 квітня 2020 р.

Кропивницький 2020

УДК 681.518.54

Матеріали II Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології”: тези доповідей, 2 – 3 квітня 2020 р. – Кропивницький: ЦНТУ, 2020. – 105 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несе автор.

© Центральноукраїнський національний технічний університет, 2020

СЕКЦІЯ 1
ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

УДК 681.03

И. Н. Вдовиченко

vivin2015@knu.edu.ua

Криворожский национальный университет, Кривой Рог

О МНОГОКРИТЕРИАЛЬНОМ ЭКСПЕРТНОМ ОЦЕНИВАНИИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Быстрое развитие информационных систем и создание новейших технологий упрощает нарушение конфиденциальности, целостности и доступности информации, и приводят к большим финансовым потерям.

Необходимость снижать риски преодоления систем защиты компьютерных системах на сегодняшний день, является актуальным вопросом. Для выполнения мероприятий по снижению риска необходимо выполнить оценку риска, его расчет, получение количественного значения. Это надо для сравнения и выявления критических значений риска. На сегодняшний день недостаточно описаны модели систем защиты, в которых формализован процесс оценки рисков информационной безопасности.

Изучая литературу по данной тематике выяснили, что основное внимание в работах уделяется обработке рисков, принятию решений по снижению рисков, уклонению, передаче или принятию рисков, управлению рисками, формированию плана по мерам воздействия на риски. Мы рассмотрим вопросы вычисления рисков информационной безопасности, получения их количественного значения, на основании которого можно строить сравнительный анализ.

Целью исследования является многокритериальный экспертный метод определения риска безопасности систем. Для реализации данной цели необходимо решить следующие задачи: 1. Выполнить анализ основных способов расчета риска безопасности компьютерных систем; 2. Разработать модель критериев риска; 3. Сформировать новый подход к определению рисков безопасности систем.

Анализ риска современных компьютерных систем представляет собой сложную комплексную задачу системного анализа. В общем случае аудит безопасности, не зависимо от формы его проведения, состоит из пяти основных этапов, на каждом из которых выполняется конкретный объем работ. Существует множество схем расчета рисков. Одна из самых простых та, в которой риск является произведением "возможного ущерба от атаки" на "вероятность такой атаки". В работе рассмотрены наиболее популярные в мировой практике методики оценки рисков информационной безопасности: CRAMM, OCTAVE, FRAP. Основными критериями в данных методиках являются финансовый ущерб и стоимость восстановления. Многие другие критерии, оказывающие влияние на основные, следовательно, в не малой степени определяющие значение риска, игнорируются. В результате сравнительного анализа методов оценки рисков информационной безопасности обнаружено, что оптимальным является комбинированный подход, при сочетании экспертного и аналитического анализа. Следовательно, для объективности расчетов надо учитывать дополнительные критерии и находить значение интегрального риска. Оценка рисков проводилась в два этапа. На первом этапе, в качестве критериев, предложенных экспертам для оценки, взяты следующие: причины (источники) возникновения угроз; объекты воздействия угроз; используемые методы и средства реализации угроз; текущие уязвимостей систем; направленность реализации угроз; характер и масштабы негативных последствий; временные характеристики воздействия; каналы проникновения в компьютерную систему. На втором этапе для вычисления интегрального значения риска предлагается использовать критерии описания уязвимостей. Далее выполняется нормирование коэффициентов. Полученная информация подвергается качественному, количественному и комплексному оцениванию, предполагающему шкалирование данных, их анализ (агрегирование, “весовым” оценкам, в целях принятия решения о правильности расчета риска. В качестве весов критериев будем использовать коэффициент критичности. По своей значимости в общей оценке риска определенные критерии всегда имеют различный удельный вес, который предлагаем устанавливать экспертным путем. Использование весов позволяет создать модель расчета риска близкую к реальности. Результатом предложенного подхода к расчету риска безопасности является комплексная модель расчета, которая позволяет обеспечить более объективное определение риска. В исследовании используются методы экспертных оценок, математической статистики, системного анализа, структурного анализа, сравнительного анализа. Полученный алгоритм для интегрального риска безопасности систем позволяет оценить систему защиты в целом. Дальнейшие исследования позволят снизить вероятность проведения атак и убытки от них.

УДК 681.3.06

А.А. Гаврилова, Р.М. Королев

alla.gavrylova@hneu.net, korolevrv01@ukr.net

Харьковский национальный экономический университет имени Семена Кузнеца, Харьков

АНАЛИЗ УЯЗВИМОСТЕЙ ТЕХНОЛОГИИ БЛОКЧЕЙН ПРИ РАБОТЕ С КРИПТОВАЛЮТАМИ

На сегодня использование блокчейн технологии имеет двойственный характер являясь одновременно перспективным многообещающим направлением и таящим в себе опасности как уже известные, так неизвестные. Самым популярным приложением данной технологии является работа с криптовалютой, что предполагает необходимость повышенного внимания к вопросам безопасности проходящих транзакций. Поэтому в работе рассмотрены возможные угрозы и риски, которые могут влиять на проведение процессов майнинга биткоина.

Во время майнинга биткоина решается огромное количество математических задач, которые приводят к зарабатыванию криптовалюты. При этом все прошлые совершенные операции сохраняются в общем доступе. Добытчики биткоина подбирают нужный хеш из различных комбинаций, который дает доступ к секретным ключам и к новым операциям. Весь этот сложный математический процесс требует наличия мощного специального устройства, которое поможет в минимальные сроки подобрать нужный хеш. Этим обосновывается положительная тенденция хешрейта [1] биткоина, которая наблюдалась с 2018 года и на конец 2019 года показал рост на 140% [2], свидетельствует также о достаточно высокой степени защищенности блокчейна от взлома [3]. Существует мнение, что транзакции криптовалют защищены, а схемы шифрования с открытым ключом почти невозможно взломать, но есть ряд уязвимостей, методы решения для которых приведены в табл. 1.

Таблица 1

Уязвимости и методы их решения

№ п/п	Уязвимость	Решения
1	хранения ключей	Использовать решения на основе Public Key Infrastructure (PKI): доверенный платформенный мо дуль (TPM); физически неклони руемые функции (PUF)
2	хищения ключей при помощи ме-тодов социа-льной инженерии	Совершенствовать процедуры конт роля, развитие критичности мыш ления, психологической устойчи вости, проницательности [4]
3	среды разработки	Использовать средства стати-ческого тестирования защищен-ности приложений (SAST)
4	в IT-архитектуре системы	Избавляться от неактуального программного обеспечения; Регуля рно устанавливать обновления на ПО; контролировать ИТ-инфрастру ктуру на предмет открытых портов, наличия мер защиты, регулярно менять пароли, контролировать полномочия пользователей
5	появления квантовых компьютеров	Использование математической модели, основанной на схеме Мак-Элиса гибридных модифицирован-ных эллиптических ко-дах (MEC) для кодирования и декодирования информации с использованием модифицированного алгоритма UMAC при передаче и получении открытого сообщения по каналам связи [5]
6	опасной “атаки-51”	Повышение хеш мощности биткоина

Отдельного внимания заслуживает уязвимость, связанная с применением полномасштабных квантовых компьютеров. В связи с этим в будущем будет возрастать возможность взлома используемых ныне относительно криптостойких алгоритмов SHA-класса (SHA-1, SHA-2, SHA-3) а также алгоритма RIPEMD, который используется в биткоинах и других криптовалютах на основе биткоинов. В процессе реализации предлагаемой модели предусмотрена двойная верификация, которая позволяет обеспечить высокий уровень целостности и достоверности передаваемого сообщения, а также высокий уровень быстродействия и криптостойкости хеш-кода в условиях пост-квантовой криптографии.

Список литературы

[1] Blockchain. Com [Online]. Available: https://www. Bloc kchain.com/ru/charts/hash-rate. Accessed on: Febr. 29, 2020.

[2] Лола Степанова, Вычислительная мощность сети биткоина достигла исторического максимума 74,5 млн. терра-хеш/сек. [Электронный ресурс]. Доступно: https:// hashtelegraph.com /vychislitelnaja-moshhnost-seti-bitkoina-dostiglastoricheskogo -maksimuma-745-mln-teraheshsek/. Дата обращения: Febr. 29, 2020.

[3] Биткоин: сетевая активность опережает рост цены [Электронный ресурс]. Доступно: https://altstake.io/news/ bitkoinsetevaya-aktivnostyopereghaet-rost-ceny. Дата обраще ния: Mar. 01, 2020.

[4] Константин Ценцура, Три убийственных проблемы блокчейна. [Электронный ресурс]. Доступно: https: //nv.ua/ techno/techno blogstri-ubiystvennyh-problemy-blokchejna-246 5554.html Дата обращения: Apr. 21, 2018.

[5] Alla A. Havrylova, Olha H. Korol, Stanyslav V. Milevskyi, and Lala R. Bakirova, "Mathematical model of authentication of a transmitted message based on a McEliece scheme on shorted and extended modified elliptic codes using UMAC modified algorithm", Кібербезпека: освіта, наука, техніка, No 1(5), p. 40 – 51, 2019.

УДК 004.056, 004.056.55, 004.91

І. Д. Горбенко, Ю. О. Кондря

uliakondria@gmail.com

Харківський національний університет імені В. Н. Каразіна, Харків

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ НА ОСНОВІ ЗАДАЧ ТЕОРІЇ РЕШІТОК ТА БАГАТОВИМІРНИХ КВАДРАТИЧНИХ СИСТЕМ

Поява квантового комп'ютера спричинить за собою необхідність багаторазового збільшення довжини ключів для симетричного шифрування, а для хеш-функцій – багаторазового збільшення довжини хешу. Такі довжини стають неприйнятними для практичного використання симетричних алгоритмів і існуючих хеш-функцій.

Метою роботи є аналіз і порівняльні дослідження схем електронного цифрового підпису (ЕЦП) постквантового періоду для виявлення найбільш перспективної схеми.

В результаті аналізу постквантових підходів були обрані перспективні кандидати: на основі задач теорії решіток (Lattices) та багатовимірних завадостійких кодів (Multivariate), що привертають увагу завдяки своєї швидкості та довжині ключів (табл. 1).

Таблиця 1

Порівняння постквантових підходів

Постквантовий підхід	Теорія решіток	Багатовимірні квадратичні системи
Обґрунтування складності	Розв'язання задач теорії решіток в особливих решітках. Знаходження «гарного» базису решіток	Вирішення систем багатовимірних квадратичних рівнянь
Швидкодія	Добре реалізується на спеціальному програмному забезпеченні	Добре реалізується на апаратних засобах
Переваги	Безліч сфер застосування. Обґрунтування складності в найгіршому випадку	Швидкість. Невелика довжина ключів
Недоліки	Відсутність точного методу	Неспроможність обґрунтування безпеки. Підвищена довжина відкритого ключа

Розглянемо параметри схем ЕЦП четвертого та п’ятого рівнів безпеки NIST (National Institute of Standards and Technology), тобто "ймовірно, надмірних по стійкості алгоритмів" (рис. 1).

Постквантовий підхід	Алгоритм	Конкретна реалізація	Закритий ключ, байт	Відкритий ключ, байт	Довжина підпису, байт
Теорія решіток	Falcon	falcon1024	8 193	1 793	1 330
	qTesla	qTesla_256	8 256	8 224	6 176
Багатовимірні квадратичні системи	LUOV	luov-64-68-330	32	19 973	3 184
		luov-80-86-399	32	40 248	4 850
		luov-8-117-404	32	100 989	521
		luov-8-90-351	32	46 101	441
	MQDSS	mqdss-64	48	88	67 800

Рис. 1. Параметри схем ЕЦП

Перший рівень безпеки забезпечують тільки схеми на решітках. Багатовимірні квадратичні схеми мають більш високі рівні безпеки. Якщо брати до уваги тактові витрати, то найцікавішою є схема qTesla_128. Що стосується параметрів, то явно виграє Falcon512.

Серед схем другого та третього рівнів найбільшою швидкодією володіє CRYSTALS-Dilithium, а MQDSS – найменшою. MQDSS-48 має короткі ключі, але занадто велику довжину підпису, що абсолютно неприйнятно для гібридних систем. Якщо порівнювати параметри, то знову явну перевагу мають схеми на решітках, зокрема, схема Falcon768.

На четвертому та на п'ятому рівнях безпеки багатовимірні квадратичні схеми LUOV мають занадто великі довжини відкритих ключів, а схема mqdss-64 – велику довжину підпису.

В результаті проведеного порівняльного аналізу існуючих постквантових підходів були знайдені переваги та недоліки цих підходів, було показано перевагу криптоперетворень ЕЦП над іншими алгоритмами за застосованими критеріями порівняння та було визначено найбільш перспективного кандидата – схему FALCON (у всіх трьох конкретних реалізаціях), яка на всіх рівнях безпеки забезпечувала найменшу довжину ключів і підпису з усіх представлених алгоритмів.

УДК 004.056, 004.75

В.М. Гребенюк[1], А.О. Корченко[2], Ю.О. Дрейс[1,2]

icaocentre@nau.edu.ua

[1] *Національна академія Служби безпеки України, Київ*
[2] *Національний авіаційний університет, Київ*

УЗАГАЛЬНЕНИЙ ПЕРЕЛІК ГРУП КРИТЕРІЇВ КРИТИЧНОСТІ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Основними проблемами у сфері захисту обєктів критичної інфраструктури (ОКІ) наразі є: відсутність класифікації ОКІ держави (ОКІД), не сформовано повний перелік інформаційно-телекомунікаційних систем (ІТС) ОКІД як об'єктів критичної інформаційної інфраструктури (ОКІІ), а також відсутні критерії оцінювання негативних наслідків до яких може призвести кібератака на ОКІІ. Тому, проведення аналізу та формування узагальненого переліку критеріїв критичності об'єктів інфраструктури держави як ОКІД з метою чіткого визначення повноти та меж усіх ОКІІ суб'єктами забезпечення її кіберзахисту є *актуальним* науковим завданням.

Виходячи з викладеного, *метою роботи* є формування узагальнених критеріїв критичності обєктів інфраструктури держави для формування їх переліку та подальшого забезпечення кіберзахисту.

Відповідно до законодавства України критерії та порядок віднесення об'єктів до ОКІ, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України (КМУ). Окремим проектом Постанови КМУ передбачається віднесення підприємств, установ, організацій незалежно від форми власності до ОКІ, які: провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах, у сферах життєзабезпечення населення, зокрема, у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, охорони здоров'я; є аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об'єктами, що підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду; є об'єктами потенційно небезпечних технологій і виробництв. Але, віднесення таких об'єктів до ОКІ відбувається лише за сукупністю критеріїв, що визначають їх важливість для реалізації життєво-важливих функцій та надання життєво-важливих послуг, свідчать про існування ризиків і загроз для них, можливість виникнення кризових ситуацій через втручання в їх функціонування, припинення функціонування, людський чинник чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму. Такий принцип застосування "сукупності критеріїв" у цілому є проблемним щодо їх визначення та сумнівнім у практичній реалізації.

Для вирішення цих проблем та протиріч, провівши аналіз і наукових праць та нормативно-правових документів, пропонується узагальнений перелік груп критеріїв критичності об'єктів інфраструктури держави [1]:

1) за сферою діяльності та надання послуг у секторі критичної інфраструктури;
2) за категорією об'єктів яким регламентуються особливі умови забезпечення їх захисту та функціонування;
3) за критеріями включення до переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями на підставі договорів про надання охоронних послуг;
4) за сукупністю критеріїв, що визначають їх важливість для реалізації життєво-важливих функцій та надання життєво-важливих послуг;
5) за наслідками порушення сталого функціонування ОКІ, які можуть спричинити кібератаки;
6) за методикою ідентифікації потенційно небезпечних об'єктів (критичних елементів);
7) за категорією критичності об'єкта;
8) за наявністю ОКІІ;
9) за класами наслідків (відповідальності) від категорії складності об'єкта;
10) за ознаками ідентифікації об'єктів підвищеної небезпеки;
11) за видом інформації, що обробляється.

За результатами проведеного аналізу сформовано узагальнений перелік груп критеріїв критичності обєктів інфраструктури держави, який може бути представлений у вигляді базової теоретико-множинної моделі.

Список літератури

[1] Korchenko, V. Hrebenuik, Y. Dreis, A. Hrebenuik, and O. Gavrylenko, "Criteria for assigning objects to critical infrastructure of Ukraine", Przetwarzanie, transmisja i bezpieczenstwo informacij: monografia, т. 2, Bielsku-Bialej, Poland: Akademia Techniczno-Humanistyczna w Bielsku-Bialej, с. 189 – 196, 2019.

УДК 004.056

Т.О. Гріненко, М.О. Кочанов

sir.cochanov1998@ukr.net

Харківський національний університет радіоелектроніки, Харків

МЕТОДОЛОГІЯ АНАЛІЗУ СУКУПНОГО РИЗИКУ БЕЗПЕКИ МОБІЛЬНИХ ДОДАТКІВ

Зловмисники можуть завдати збитків вашому бізнесу або організації, використовуючи вашу програму. Існує багато способів реалізації атак на ваш додаток, які треба мати на увазі, та прийняти дії щодо протидії цим атакам. У разі невеликого розміру організації та обмеженості ресурсів необхідно обирати ті погрози, які можуть найбільш імовірно нанести збитки вашій організації. З метою аналізу погроз для організацій була розроблена методологія аналізу сукупного ризику.

Суть методології полягає у тому, що для визначення ризиків для організації треба оцінити ймовірності, пов'язані з джерелами загроз, векторами атак і недоліками безпеки, а потім об'єднати їх з оцінкою технічної і репутаційної шкоди для організації. Сума цих факторів визначає сукупний ризик. Розроблена методологія оцінки сукупного ризику заснована на методиці оцінки загроз OWASP. У цій методиці для кожної категорії загроз оцінюються характерні для стандартного додатку недоліки, виходячи з факторів їх ймовірності і ризику. Потім загрози групуються за ступенем небезпеки для додатків.

Розроблена на базі OWASP методологія аналізу сукупного ризику визначає три фактори ймовірності наявності уразливості (поширеність, складність виявлення і складність експлуатації) і один фактор її небезпеки (технічні наслідки). Рівень критичності кожного фактору класифікується від 1 (низький) до 3 (високий) і визначається спеціальними термінами. Поширеність, як правило, не вимагає розрахунку. Потім ці дані об’єднуються з двома іншими факторами ймовірності (складність виявлення і складність експлуатації) для розрахунку ймовірності наявності кожної уразливості. Отримане значення множиться на середнє значення тяжкості технічних наслідків для визначення сукупної небезпеки кожного пункту роботи (чим вище результат, тим більша небезпека). Складність виявлення і експлуатації, а також наслідки розраховувалися на основі CVE. При цьому даний підхід не враховує джерела загроз, а також технічні особливості окремих додатків. Будь-який з цих факторів може в значній мірі вплинути на загальну ймовірність виявлення і експлуатації зловмисником уразливості.

Для прикладу реалізації аналізу загроз безпеки мобільного додатку за розробленою методикою скористаємося табл. 1 для візуалізації розробленої методології та табл. 2 для відображення отриманих у ході аналізу даних та результатів.

Таблиця 1

Методика оцінки сукупного ризику

Джерело загрози	Залежить від додатку
Складність експлуатації (F)	Просто: 3
	Середньо: 2
	Складно: 1
Поширеність уразливості (A)	Дуже поширена :3
	Поширена: 2
	Рідкісна: 1
Складність виявлення (C)	Просто: 3
	Середньо: 2
	Складно: 1
Технічні наслідки (X)	Важкі: 3
	Помірні: 2
	Незначні: 1
Сукупний ризик	$(F+A+C)\cdot X$

Таблиця 2

Приклад реалізації методики оцінки сукупного ризику

	Джерело загрози	Розробники
Небезпечне зберігання даних	Складність експлуатації (F)	Просто: 3
	Поширеність уразливості (A)	Поширена: 2
	Складність виявлення (C)	Середньо: 2
	Технічні наслідки (X)	Важкі: 3
	Сукупний ризик	21
Низька якість коду	Джерело загрози	Розробники
	Складність експлуатації (F)	Складно: 1
	Поширеність уразливості (A)	Поширена: 2
	Складність виявлення (C)	Складно: 1
	Технічні наслідки (X)	Помірні: 2
	Сукупний ризик	8

Отже, проаналізувавши дві загрози за розробленою методологію оцінки сукупного ризику,можна зробити висновок, що при одному й тому ж самому джерелі, загроза небезпечного зберігання даних має майже втричі більший сукупний ризик для безпеки мобільного додатку. Зважаючи на цей факт та у разі відсутності загроз з більшим рівнем сукупного ризику, організація, вклавши ресурси у реалізацію захищених сховищ даних, матиме найвищий показник безпеки для свого мобільного додатку.

УДК 004.056

В.Б Дудикевич, Г.В Микитин, М.О. Галунець

vdudykev@polynet.lviv.ua, cosmos-zirka@ukr.net, skyzhero50@gmail.com

Національний університет "Львівська політехніка", Львів

ДО ПИТАННЯ БЕЗПЕКИ "РОЗУМНИХ МІСТ"

Актуальність проблеми безпеки "розумних міст" в Україні. З метою інтеграції у світовий простір 4.0 Україна представила стратегію Індустрії 4.0, в якій одним з напрямів є – повномасштабне оцифрування (диджиталізація) ключових секторів промисловості, енергетики та інфраструктури, зокрема у контексті розвитку "розумного міста", як структури "сенсорна мережа – центральна платформа даних – мобільні додатки" та забезпечення її безпеки за профілями.

Інформаційна модель "розумного міста". Модель "розумного міста" є дворівневою. Перший рівень – функціональний, що забезпечує роботоздатність складових розумного міста згідно інформаційної структури "відбирання – оброблення – передавання/приймання – управління". Другий – безпековий, який представляє технології безпечного функціонування цих складових за профілями захисту інформації: конфіденційність – цілісність – доступність. Безпечний збір даних від сенсорів "розумних об'єктів" та обмін інформації в системі "розумне місто" відповідно здійснюють інтернет речей і хмарні технології. Інструментарій платформи даних забезпечує зберігання, аналіз, візуалізацію даних, прогнозування і, на цій основі, управління ситуаціями в режимі реального часу.

Система "Розумний будинок" – один з сегментів розвитку "розумного міста" засобами автоматизації управління станом безпечного функціонування систем: клімат-контролю, газо- та водопостачання, освітлення, пожежної сигналізації та сповіщення, контролю доступу і відеоспостереження, провідного і безпровідного зв'язку т. і. Частинний проект показано на рис. 1.

Рис. 1. Структура "розумного будинку"

На рис. 1: 1 – автоматизація системи опалення; 2 – управління освітленням; 3 – система управління вікнами; 4 – система відеоспостереження; 5 – імітація присутності господарів; 6 – кондиціонування та вентиляція; 7 – давачі протікання; 8 – автоматизована система очищення води в басейні.

Безпечний обмін інформацією на основі шифрування. Обмін інформацією в "розумному місті", як і у його сегменті – "розумному будинку", здійснюється сенсорними мережами, наприклад ZigBee, Wi-Fi, Bluetooth. З метою захисту інформації від перехоплення в безпровідних каналах зв'язку використовують шифрування/дешифрування даних. Серед криптографічних методів захисту інформації на практиці використовують алгоритм шифрування AES – симетричний блоковий шифр (NIST, 2002 р.).

Основні принципи алгоритму: загальне число бітів ключів в раундах дорівнює довжині блока, помноженій на число раундів, плюс один; ключ шифрування перетворюється в розширений ключ; раундові ключі генеруються з розширеного ключа: перший ключ раунду містить перші X слів, другий – наступні X слів і т. д. Схема функції шифрування AES наведена на рис. 2.

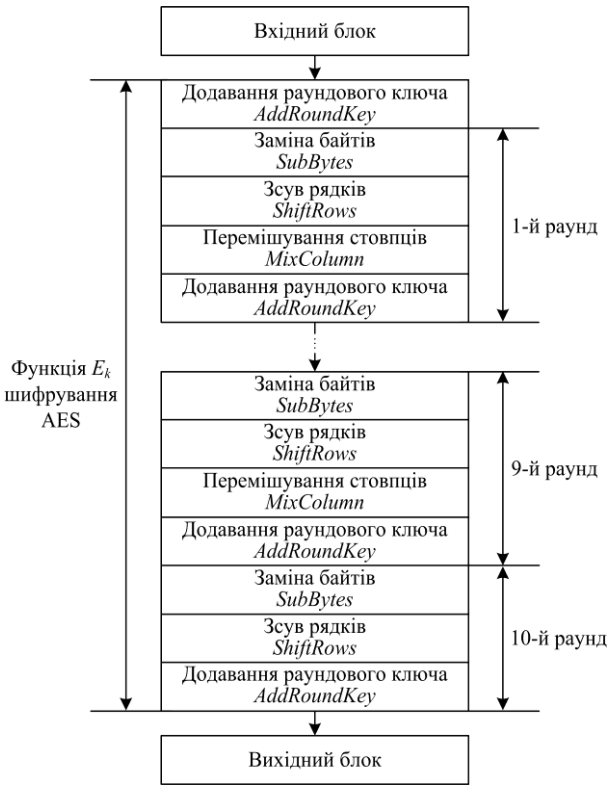


Рис. 2. Схема функції шифрування AES

УДК 004.056, 004.75

О.В. Желтухін, Р.В. Гордієнко

r.hordiienko@student.csn.khai.edu

Національний аерокосмічний університет ім. М. Є. Жуковського "ХАІ", Харків

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ АВТОМОБІЛЯ НА ДОРОЗІ

Вивчається система автопілоту або система курсової стійкості автомобіля, аналізується література та сучасні системи, а також випадки, де вона є незамінною. Розглядаються існуючі установки та варіанти конструкторських рішень таких систем, у яких були виявлені недоліки, а також як позбавити дану систему від цих недоліків.. Пропонується варіант організації системи, яка була б надійною, а також мала можливість своєчасно попередити ймовірність ДТП з боку даної системи.

Актуальність дослідження полягає в тому, що в даний час на дорогах збільшується кількість автомобілів, а це призводить до того, що підвищується кількість автомобільних катастроф. Тому, потрібне сучасне вирішення таких проблем, як створення систем автопілоту або системи курсової стійкості автомобіля.

Автопілот – пристрій або програмно-апаратний комплекс, що керує транспортним засобом за певною, заданою йому траєкторією.

Система курсової стійкості – це система, яка призначена для збереження стійкості і керованості автомобіля за рахунок завчасного визначення та усунення критичної ситуації на дорозі.

Безпілотний автомобіль є головною новиною, але він вже знайшов своє практичне застосування. Безпілотні транспортні засоби можуть з часом стати більш ефективними і більш безпечними. Вони також можуть зменшити число заторів і кількість шкідливих викидів у повітря.

Мета – проаналізувати існуючи системи керування автомобілем і виявити їхні недоліки і запропонувати способи їх вирішення.

Після комплексного аналізу літератури та вивчення ринку існуючих систем мною була обрана система автопілоту Tesla. Дана система зарекомендувала себе з боку трансформації системи допомоги водієві, відому як "2-ий рівень", в повністю автономну систему, яка могла б працювати без людського контролю, "рівень 4-5", і показати своє вміння аналізувати ситуацію на дорозі Таким чином, є деякі винятки для систем такого роду. Наприклад, системи автопілоту, часто спецтехнікою не виявляються, це є дуже важливим фактором, у всіх інших випадках рух триває по правилам. Покращення даного виду систем можна зробити наступним способом – транспортним засобам треба дати можливість "спілкуватися" між собою: передача швидкості і місця призначення, прогнозування шляху, будь-якою інформацією про дорогу або проблеми безпеки, також "маячки" для спецтехніки.

На даний момент розробляються системи, технології яких за рамками нашого уявлення. Повноцінне впровадження таких систем в сучасні автомобілі стає все більш реальним. Таке впровадження, дозволить транспортному засобу набирати необхідну швидкість, уникати аварійних ситуацій і здійснювати маневри без керування людиною. В цілому, на сьогодні такі системи, звичайно, допомагають при водінні, але не варто забувати про те, що це електроніка, і скласти програму на всі випадки життя неможливо, але це не означає, що нею стоїть нехтувати, навпаки, вона ніколи не розгубиться, не переплутає педалі і взагалі зробить те, що потрібно. Собі можна лише уявити, що по шляху проходження не пропустиш потрібний поворот, не буде штрафів за порушення правил ПДД, а також найголовніше такі системи зможуть врятувати не одне, а навіть кілька людських життів.

Після проведених досліджень були запропоновані заходи щодо поліпшення таких типів систем: для спецтехніки треба додати "маячки", бо автоматика сприймає її, як звичайний транспортний засіб. Припустимо, такі системи досягли "успіху", що бачать спецтехніку за версту. Це все дуже відмінно, складається питання – а чи буде влада наполягати на тому, щоб у такої техніки була можливість дистанційно зупинятися або сповільнювати свою швидкість. Думаю, що це є ще одною функцією, за якою слід стояти у черзі. Так, можна уявити, що є виклик, пожежа, прокладається маршрут і всі автомобілі на шляху проходження спецтехніки розуміють, що потрібно поступитися і йдуть в сторону, і пожежники потрапляють на місце пожежі за 3 хвилини. Для звичайної техніки – визначати швидкість зближення, обчислювати безпечні траєкторії, передавати будь-яку інформацію іншому автомобілю, тощо.

Підбиваючи підсумки, можна стверджувати, що розглянуті системи є дуже складними, вони поступово розвиваються і входять в наше життя, це дозволяє ефективно вирішувати завдання безпеки автотранспортних засобів, зниження числа пробок на дорогах, ДТП, травм та смертей, та й підвищення комфортабельності пасажирів.

УДК 343.3/.7:004

О.С. Кульчицький, О.А. Ладигіна

Tigger100500@gmail.com, ladyginaoa@ukr.net

Центральноукраїнський національний технічний університет, Кропивницький

ІНФОРМАЦІЙНА БЕЗПЕКА КОМП'ЮТЕРНОЇ СИСТЕМИ ТА МЕРЕЖІ ВІД ВНУТРІШНІХ ТА ЗОВНІШНІХ АТАК

Моделі надійності функціонування комп'ютерних мереж та систем розроблені давно і детально вивчені, а моделі безпеки тільки розробляються. Важливість та актуальність проблеми забезпечення інформаційної безпеки обумовлені тим, що сучасні рівні розвитку засобів інформаційної безпеки значно відстають від рівнів розвитку інформаційних технологій та розширення впровадження комп'ютерних та мережевих технологій у різноманітні сфери людської діяльності. Крім цього, стрімкий розвиток інформаційних технологій відкрив нові можливості для бізнесу, що призвело до появи нових загроз [1].

Моделі безпеки відіграють важливу роль у процесах розробки і дослідження захищених комп'ютерних систем, вирішують такі задачі [2]:

- вибір і обґрунтування базових принципів архітектури захищених комп'ютерних систем, що визначають механізми реалізації засобів і методів захисту інформації;
- підтвердження властивостей захищених систем шляхом формального дотримання політики безпеки;
- складання формальної специфікації політики безпеки, як найважливішої складової частини організаційного та документаційного забезпечення розроблюваних захищених комп'ютерних систем.

Основні загрози для комп'ютерних мереж та систем грунтуються в області конфіденційності, цілісності та доступності [3].

Відповідно до цього завдання інформаційної безпеки в комп'ютерних мережах полягають у [4]:

- аутентифікації одного або декількох взаємодіючих об'єктів;
- контролі доступу та захисту від несанкціонованого використання ресурсів мережі;
- маскуванні інформаційного потоку у мережі;
- захисту від можливих відмов відправки/ прийому змісту відправлених/ прийнятих даних.

Більшість підходів до формування моделі безпеки лише частково відображають компоненти та процеси захисту інформації та інформаційних ресурсів і є односторонніми.

Наприклад, у структурі моделі не відображають процес захисту інформації та інформаційних ресурсів; опис послідовності процесу формування моделі не враховує особливості побудови бізнес-процесів; формалізація моделі безпеки не враховує її адитивні властивості. А також велика концентрація захисних засобів в інформаційній системі може привести до того, що система виявиться дуже дорогою та можна отримати її перевантаження і зниження продуктивності.

Тому, головне при формуванні моделі безпеки комп'ютерної системи − це кваліфіковано визначити межі розумної безпеки і витрат на засоби захисту з одного боку і підтримки системи в працездатному стані і прийнятного ризику з іншого.

Передбачається, що модель безпеки в рамках комплексного підходу є функцією з множини області значень складових системи інформаційної безпеки. Тобто залежить від суб'єктів інформаційних процесів, завдань захисту інформації, загроз безпеки, рівнів вразливості комп'ютерних мереж та систем.

Умовами функціонування моделі є автономність, реагування та застосування мінімальних обчислювальних ресурсів.

Постійне зростання потреби в інформації обумовлює необхідність підвищення ефективності використання інформаційних ресурсів з інтеграцією різних підсистем забезпечення безпеки, підсистем зв'язку у єдину інтегральну систему з загальними технічними засобами та подальшого вдосконалення моделі інформаційної безпеки за рахунок вагових коефіцієнтів різних видів атак, і захищеності компонентів комп'ютерних мереж та систем від внутрішніх та зовнішніх атак.

Список літератури

[1] П. В. Кучернюк, "Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні)", Мікросистеми, Електроніка та Акустика, т. 22, № 6(101), с. 64 – 70, 2018.

[2] Д. Б. Мехед, "Захист інформації в комп'ютерних мережах, Технічні науки та технології", № 2, с. 140 – 141, 2015.

[3] О. С. Кульчицький, та О. А. Ладигіна, "Аналіз роботи захисту інформації в комп'ютерних системах та мережах", на Міжнародній науково-практичній конференції "Інформаційна безпека та інформаційні технології" 24 – 25 квітня 2019 р., Харків, 2019, с. 14.

[4] О. С. Кульчицький, та О. А. Ладигіна, "Особливості надійності та захисту інформації в комп'ютерних системах і мережах", Інформаційні технології і автоматизація – 2019, на XII Міжнар. наук.-практ. конф; Одеса, 17-18 жовтня 2019 р., Одеса, 2019, ч. 1, с. 19 – 21.

УДК 004.056.52

М. К. Левіна, М. В. Єсіна

Levina.mariya98@gmail.com , m.v.yesina@karazin.ua

Харківський національний університет імені В.Н. Каразіна, Харків

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПЕРСПЕКТИВНИХ ЕЛЕКТРОНИХ ПІДПИСІВ НА ОСНОВІ АЛГЕРБРАЇЧНИХ РЕШІТОК ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ

Метою цієї доповіді є розгляд сутності та властивостей алгоритмів електронного підпису на основі алгебраїчних решіток та проведення порівняльного аналізу алгоритмів електронного підпису на алгебраїчних решітках, що вийшли до другого етапу конкурсу NIST США.

Визнаючи, що існують суттєві невизначеності в оцінці безпеки алгоритмів постквантового кандидата, NIST визначив п’ять категорій безпеки, щоб можна було краще порівняти рівень безпеки, що надається в публікаціях. Відправникам було запропоновано надати попередню класифікацію відповідно до визначень, наданих у NISTIR 8240, з акцентом на задоволення вимог до категорій безпеки, продуктивності та/або алгоритму та реалізації [1].

Було вирішено порівняти підписи за трьома параметрами [1]:

1) безпека/стійкість,

2) техніко-експлуатаційні вимоги,

3) захищеність від атак.

Безпечність/Стійкість: Істинна вибірка Гауса використовується всередині, що гарантує незначний витік інформації про секретний ключі до практично нескінченного числа підписів (понад 264). Falcon пропонує дуже хороші показники продуктивності. Основна новизна – швидкість: використання швидкої вибірки Фур’є дозволяє дуже швидкі реалізації, в тисячі підписів на секунду на звичайному комп’ютері; перевірка у п’ять-десять разів швидше.

Техніко-експлуатаційні вимоги: Ця структура вимагає двох складових: Клас криптографічних решіток – обрано клас решіток NTRU. Зразок лазівки – покладаються на нову техніку, яка називаються швидкою вибіркою Фур’є. Схему підпису Falcon коротко можна описати таким чином: Falcon = GPV рамка + решітки NTRU + Швидка вибірка Фур’є.

Захищеність від атак: Зразок лазівки – покладаються на нову техніку, яка називаються швидкою вибіркою Фур’є. Схему підпису Falcon коротко можна описати таким чином: Falcon = GPV рамка + решітки NTRU + Швидка вибірка Фур’є. Потрібно більше роботи, щоб алгоритм був захищений від атак бічними каналами.

Найвідоміші атаки проти Falcon ґрунтуються на скороченні бази решітки, без істотного використання спеціальної структури решітки NTRU.

Безпечність/Стійкість: Схема підписів є доказово EUF-CMA-безпечною: надається зменшення безпеки від складності проблеми кільцевого навчання з помилками до EUF-CMA-безпечної схеми. Зменшення (рівня) безпеки надано у квантовій випадковій моделі оракула, тобто квантовому зловмиснику дозволено звернутися до випадкового оракула в суперпозиції. Зменшення безпеки ґрунтується на варіанті схеми над стандартними решітками. Для приведення
зменшення, використовується евристичний аргумент.
Зменшення безпеки є явним, тобто можна явно визначити зв’язок між ймовірностями успіху вирішення проблеми кільцевого навчання з помилками (ring learning with errors) (R-LWE) та підробки підписів qTESLA. Зменшення безпеки є суттєвим (щільним), що є бажаною властивістю, тому що при виборі параметрів схеми відповідно до зменшень безпеки, суттєве (щільне) скорочення призводить до менших параметрів і, отже, до підвищення продуктивності.

Техніко-експлуатаційні вимоги: Ця схема супроводжується несуттєвим скороченням випадкової моделі оракула та жорстким зменшенням квантової випадкової моделі оракула з R-LWE (ring learning with errors).

Захищеність від атак: Було помічено, що помилка в доказі безпеки вимагає коригування параметрів (що знижує ефективність схеми).

Однією з переваг qTESLA є те, що Гаусова вибірка вимагається лише під час генерації ключів до зразку *s* та *e*. Тим не менш, для деяких додатків може знадобитися ефективна і безпечна реалізація генерації ключів і, зокрема, захищеність від атак часу та кешу.

Falcon хороший тим, що справжня вибірка Гауса гарантує мінімальний витік інформації. Але алгоритм все ще вразливий для атак бічними каналами, зі скороченням бази решітки. Основною перевагою методу qTesla є те, що Гаусова вибірка використовується тільки під час генерації ключів, що робить алгоритм простіше і допомагає уникнути помилок. Але було помічено, що помилка в доказі безпеки потребує корегування параметрів (що знижує ефективність схеми).

Список літератури

[1] Lily Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone, Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT). [Online]. Available: http://csrc.nist.gov /publications/drafts/nistir-8105/ nistir_8105_draft.pdf. Accessed on: Febr. 20, 2020.

УДК 81

И. В. Лысенко

i.lysenko@csn.khai.edu

Национальный аэрокосиический университет имени Н.Е. Жуковского "ХАИ", Хаьрков

ИНФОРМАЦИОННО-ЛИНГВИСТИЧЕСКАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ

За последнее время значительно увеличилось количество исследований по проблеме информационно-психологической и, как частного случая, информационно-лингвистической безопасности личности и влияния информационных технологий на сознание людей. Тем не менее, как для зарубежных учёных, так и отечественных этот вопрос остаётся открытым для изучения.

В процессе коммуникации язык используется не только для передачи информации, но и для воздействия на адресата. Воздействующая сила языка и речи является предметом изучения современной лингвистики и ее разновидностей: прагмалингвистики, психолингвистики, социолингвистики, медиалин-гвистики.

О воздействующей силе языка, слова много писали поэты и писатели. Например, Ф.И. Тютчев писал:

Нам не дано предугадать, как слово наше отзовётся,

И нам сочувствие даётся, как нам даётся благодать.

А вот мысль В. Шефнера из его стихотворения "Слова":

Словом можно убить, словом можно спасти,

Словом можно полки за собой повести.

Словесная информация в текстовом виде, как и информация в целом, – универсальный инструмент прогресса человечества, главный ресурс развития современного общества. Но, став мощным средством познания и преобразования мира и самого человека, информационные технологии в то же время превратились для него в существенную угрозу. В качестве источников угроз информационно-лингвистической безопасности рассматриваются прежде всего печатные издания.

Стоит отметить, что современный человек часто всему открыт, он воспринимает все как знаковую поверхность, не пытаясь даже проникнуть в глубину вещей, в значение знаков.

Так, например, в медиатекстах для усиления воздействия используются различные средства выразительности – эпитеты, метафоры, сравнения, риторические вопросы, повторы, а также ирония, антитеза, инверсия, языковая игра и др. Они оказывают сильное воздействие на адресата, привлекают читательское внимание, активизируют ассоциативное и образное мышление. Вместе с тем эти языковые единицы имеют второй план – переносное значение. Поэтому с их помощью в текст закладывается имплицитный смысл. Этим свойством пользуются манипуляторы. А для искажения информации могут использоваться такие лексические средств языка, как эвфемизмы и дисфемизмы.

Кроме того, в медиатексте помимо информации о событии могут содержаться дополнительные оценочные смыслы, которые внедряются в сознание адресата. Многообразные оттенки эмоционально-экспрессивной окраски принято делить на два больших разряда: с положительной и с отрицательной характеристикой. Так, негативная характеристика выражается словами с неодобрительным, презрительным, укоризненным, ироническим, пренебрежительным, бранным оттенком. Особая речевая организация текста способствует возникновению заблуждений в сознании адресата. Медиатексты усложняются намеками, прецедентными феноменами, иронией, подтекстом. Разговорные слова и конструкции, жаргонизмы, просторечные, грубые слова повышают эмоциональность и выразительность текста. Искусный подбор слов позволяет актуализировать в сообщении те или иные оттенки их значений, в результате чего слова несут в тексте двойную смысловую нагрузку и незаметно искажают реальную действительность в представлениях адресата. Обладающий знаниями человек может самостоятельно создать самый первый и простой механизм психолого-лингвистической защиты в виде психологического барьера недоверия ко многим информационным потокам обработки сознания населения, сформировать установку на необходимость использования анализа и внимательного отношения к поступающей информации в виде печатных изданий. Очевидно, что человек не должен воспринимать получаемую информацию как истину в конечной инстанции, но не должен и отгораживаться от нее. Важно научиться интерпретировать информацию, понимать ее суть, принимать личностную позицию по отношению к скрытому смыслу, находить требуемую информацию в различных источниках, систематизировать ее, находить ошибки в получаемой информации, воспринимать альтернативные точки зрения, вычленять главное в информационном сообщении, а также научиться распознавать манипулятивные приёмы, используемые в текстовой информации.

.

УДК 004.056, 004.75

А.О. Макаренко, С.П. Євсеев, А.А. Юрченко

makarenkoanton5@gmail.com, serhii.yevseiev@hneu.net, yurchenko.anastasi@gmail.com

Харківський національний економічний університет імені Семена Кузнеця, Харків

АНАЛІЗ ОЦІНКИ ПОТОЧНОГО СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ SIEM-СИСТЕМ

SIEM-системи дозволяють здійснювати моніторинг інформаційних систем і систем безпеки, аналізувати події в них в режимі реального часу.

Функції SIEM-систем зводяться до наступного:

Агрегація даних.

Кореляція. SIEM-системи виробляють пошук загальних значень і атрибутів і пов'язують між собою надходять події.

Оповіщення. Після того як система справила аналіз схожих між собою подій, вона сповіщає адміністратора безпеки про існуючі проблеми в інфраструктурі.

Сумісність. SIEM-системи впроваджуються в існуючу в компанії інфраструктуру і дозволяють автоматично збирати інформацію про події, формувати звіти для зібраних даних і застосовувати їх з метою управління безпекою та проведення аудиту [1].

Зберігання подій.

Експертний аналіз. SIEM-системи дозволяють проводити пошук по збереженим подій інформаційної безпеки.

Перша платформа – класифікації загроз за складовими безпеки БОР ОБС: інформаційна безпека, безпека інформації, кібербезпека. Введемо такі визначення.

Визначення 1. Безпека контуру бізнес-процесів – стан захищеності бізнес-процесів і їх інформаційних ресурсів, що характеризується можливістю виконавців, технічних засобів і інформаційних технологій забезпечити конфіденційність, цілісність справжність і доступність ресурсів, необхідних для реалізації бізнес-процесів в контурі відповідного рівня [2].

Визначення 2. Ресурсна безпеку контуру бізнес-процесів – стан захищеності ресурсної середовища КБП.

Визначення 3. Кібербезпека контуру бізнес-процесів – набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і технологій.

Друга платформа – класифікація загроз за характером спрямованості: нормативно правовий, організаційний, інженерно-технічний.

Третя платформа – класифікація загроз відповідно до основними особливостями інформації: конфіденційність, цілісність, доступність, автентичність [3].

Четверта платформа – класифікація загроз за рівнями ієрархії інфраструктури контуру бізнес-процесів: FL – фізичний рівень, NL – мережевий рівень, OSL – рівень операційних систем, DBL – рівень систем управління базами даних, BL – рівень технологічних додатків і сервісів. [4]

Ефективність запропонованої моделі оцінювання економічних витрат залежить від точності формулювання ймовірності успіху захисту і визначення цінності БІР.

Запропонована модель дозволяє визначити найбільш ймовірні загрози, спрямовані на порушення безпеки інформаційних ресурсів і як результат – економічно обґрунтувати розподіл обмежених коштів між різними інформаційними ресурсами, які вимагають захисту [5].

Розроблено практичну методику для оцінювання рівня захищеності банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника, моделі оцінки захищеності банківських інформаційних ресурсів та моделі інфраструктури автоматизованих банківських систем, що дозволяє оптимізувати витрати коштів на побудову системи безпеки банківських інформаційних ресурсів.

Список літератури

[1] R. Hryshchuk, and S. Yevseiev, "The synergetic approach for providing bank information security: the problem formulation", Науково-технічний журнал "Безпека інформації", № 22 (1), с. 64 – 74, 2016.

[2] Р. В. Грищук, та Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника, Основи кібербезпеки, Житомир, Україна: ЖНАЕУ, 2016.

[3] L. Sun, R. P. Srivastava, and T. J. Mock, "An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions", Journal of Management Information Systems, Vol. 22, p.3 – 28, 2006.

[4] А. В. Потий, и Д. Ю. Пилипенко, "Концепция стратегического управления информационной безопасностью", Радіоелектронні і комп'ютерні системи, № 6 (47), с. 53 – 58, 2010.

[5] А. В. Потий, и Д. Ю. Пилипенко, "Классификация показателей безопасности информации", Системи обробки інформації, Вип. 3(84), с.53 –56, 2010.

УДК 004.56

В.І. Малінніков, М.Г.Амеліна

zahar.marchuc@gmail.com, tokar_marina@ukr.net

Кропивницький інженерний коледж Центральноукраїнського національного технічного університету, Кропивницький

ОГЛЯД ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX З УРАХУВАННЯМ ЗАСОБІВ ЗАХИСТУ

Поняття “операційна система” нерозривно пов’язане з сьогоденням. Усім відомо, що операційна система – це так званий інтерфейс, який забезпечує процес спілкування» користувача з його гаджетом/пристроєм.

Вибір операційної системи – цілком індивідуальний вибір кожного, оскільки ґрунтується на потребах та вимогах до того набору програмного забезпечення, яке операційна система дає змогу використовувати.

Операційна система Linux – це сімейство на базі ядра Linux, яке містить відповідний набір утиліт і програм проекту GNU та, за вимогою, інших програмних компонентів. Також Linux цікава ще й тим, що до неї часто відносять і програми, що доповнюють цю операційну систему, і прикладні програми, які роблять її, відповідно до потреб користувача, багатофункціональною.

Для цього дана операційна система забезпечується великою кількістю надлаштувань, так званих дистрибутивів, у яких програми GNU з’єднуються з ядром Linux та іншими програмами.

Розробником ядра Linux є Лінус Торвальд, який почав створювати її на MINIX. Але пізніше, коли Linux досягла певної зрілості, з’явилась можливість продовжити розробку вже на базі самого ядра Linux. Згодом розробники вирішили здійснити заміну операційної системи MINIX на GNU. Поштовхом до цього став той факт, що код знаходився у вільному доступі та був більш зручний для вживання в операційній системі.

На сьогоднішній день Linux – подібні операційні системи є найбільш популярними серед системних адміністраторів.

Хоча Linux спочатку була розроблена для персональних комп’ютерів, пізніше, завдяки таким компаніям, як Hp, IBM, Sun Microsystems, Novel та інших, набула великої популярності серед системних адміністраторів як серверна операційна система. Та найчастіше Linux використовують для надання веб-хостингу.

Важко переоцінити важливість серверів у роботі системних адміністраторів та користувачів операційних систем. Тому дуже важливою проблемою є здатність та можливість забезпечення збереження даних від різних видів несанкціонованих впливів.

У даних тезах ітиме мова про захист Linux – подібних операційних систем від несанкціонованих втручань.

Перш за все, слід зазначити, що для операційної системи Linux на данний час є три найпоширеніші проблеми:

1) переповнення стекового буфера (CVE-2018-16864);

2) виділення пам’яті без меж (CVE-2018-16865);

3) помилка читання понад допустимі межі (CVE-2018-16866)

Слід зазначити, що перша з вказаних загроз може використовуватися локально, друга підходить для мережевих атак, а третя може призвести до несанкціонованих витоків інформації.

Характерним є те, що всі ці експлойти не потребують будь-яких дій від користувача комп’ютера.

Також існує багато шкідливих програм, які можуть зашкодити системі та отримати доступ до даних користувача або інформації, яка зберігається на сервері.

Великою небезпекою для операційних систем є руткіти. Руткіт - це програма або набір програм для приховування слідів присутності зловмисника чи шкідливої програми в системі. Тобто, для зламу операційної системи Linux створюється спеціальний модуль ядра, який зловмисник завантажує в систему, яку планує зламати відразу після отримання прав суперкористувача.

Для менш складних і шкідливих руткітів видалення може бути здійснено за допомогою програми-антивірусу, а вже боротися з більш складними руткітами можна за допомогою спеціальних програм, наприклад, TDSSkiller, що створена для боротьби з руткітом TDSS. У випадку, коли системні файли вже пошкоджені дуже глибоко, доводиться знову інсталювати операційну систему.

У доповіді будуть проаналізовані загрози, які впливають на роботу операційної системи Linux та проведено огляд заходів, які можуть бути використані для її захисту від шкідливого програмного забезпечення.

УДК 614.8.01

К. М. Марченко, О. В. Оришака

k_marchenko@i.ua, oryhsaka@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА ЛЮДИНИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Одною із рис інформаційного суспільства є значні обсяги інформації, що зберігається та обробляється різноманітними пристроями за участю людини. За останні п'ять років людством було вироблено інформації більше, ніж за всю попередню історію.

Інформація не може існувати без суб'єкта, який їх сприймає та фіксує. Уся існуюча інформація пройшла через свідомість людей, які її зафіксували. Отже, при зростанні кількості інформації рівень її впливу на людину зростає у межах від суттєвого до критичного та травмуючого. Сучасна людина, яка хоче реалізувати себе в інформаційному суспільстві, не може відокремитися від інформації та інформаційних ресурсів.

Таким чином, актуальною задачею є вивчення механізмів впливу інформації різних типів на людину та розробка мір, що запобігають психічним розладам, захворюванням, та небезпеці для людини. За цих обставин можна анонсувати появу нового розділу безпеки життєдіяльності – інформаційної безпеки.

Різні види інформації по різному впливають на людину, але всі вони обумовлюють її здоров'я та якість життя, а також можливості. Можна сказати, що інформація сьогодні є найбільш впливовим чинником життєдіяльності людини, а інформаційні ресурси стають найважливішою запорукою успіху та конкурентної спроможності країн, суспільних та виробничих груп.

Існує багато видів та класифікацій інформації, але з точки зору безпеки життєдіяльності ні одна з них не відображає впливу інформації на людину.

Людина сама є складною інформаційною системою і в той же час носієм та виробником інформації. Інформаційна система людини багаторівнева: тіло росте та оновлюється за інформаційним шаблоном на рівні генів та ДНК, хімічні та фізіологічні процеси відбуваються за чіткими програмами, органи почуттів безперервно сприймають інформацію від навколишнього оточення, інтелект займається інтерпретацією та класифікацією сприйнятої інформації, у свідомості людина на основі наявної інформації робить вибір, приймає те чи інше рішення, у тому числі по відношенню до отриманої інформації. Рівні ці не ізольовані: наприклад [1], інформація, сприйнята органами почуттів, викликає психічні реакції, емоції, які впливають на вироблення певних гормонів, зміни хімії крові тощо.

За характером, механізмами та рівнем впливу на людину, інформацію можна поділити на такі групи: генетичну; біологічну та бактеріологічну; хімічну; гносеологічну; соціальну; виробничу та професійну; споживацьку; політичну; культурну та мистецьку; релігійну; духовну.

Найбільш небезпечною для людини є інформація, яка змінює генетику організму, стан здоров'я, психічний стан, пригнічує або спонукає до агресії. Відомо [2], що інформація може як шкодити здоров'ю людини, так і поліпшувати його. Інформація може бути спеціально підготовленою та спрямованою на окрему особу, а частіше на певні соціальні групи та етнічні спільноти з метою досягнення переваг та вигод, що розглядається як психологічний вплив або інформаційна війна [3].

Метою подальших досліджень у галузі інформаційної безпеки життєдіяльності є розробка заходів та норм, які забезпечують безпеку людини при роботі з інформацією.

Задачами досліджень є:

1) визначення гранично допустимих навантажень при роботі з інформацією у різних галузях суспільного виробництва;

2) розробка правил та норм інформаційної гігієни та інформаційної культури;

3) вивчення способів та механізмів спрямованого інформаційного впливу та засобів захисту від них [4, 5];

4) вивчення впливу неорганічних та органічних речовин, продуктів споживання на інформаційну систему людини та розробка рекомендацій із їх застосування;

5) розробка методів аудиту людиною власної інформаційної системи.

Список літератури

[1] К. Н. Марченко., В. М. Пестунов, Л. П. Свяцкая, и Т. К. Марченко, "Влияние информации на состояние злоровья человека", Наукові записки, вип. 10, ч. 2, с. 224 – 229, 2010.

[2] П. П. Гаряев, Лингвистико-волновой геном: теория и практика, Киев, Украина: Институт квантовой генетики, 2009.

[3] Г. Грачев, и И. Мельник, Манипулирование личностью: Организация, способы и технологии информационно-психологического воздействия, Москва, Россия: Алгоритм. 2002.

[4] К. Н. Марченко, "Составляющие информационно-психологической безопасности человека", Наукові записки, вип. 23, с. 181 – 191, 2018.

[5] К. М. Марченко, "Інформаційна безпека життєдіяльності людини", Наукові записки, вип. 26, с. 178 – 183, 2019.

УДК 681.32:007.5

А. В. Милов, С. В. Милевский

oleksandr.milov@hneu.net, milevskiysv@gmail.com

Харьковский национальный экономический университет имени Семена Кузнеца, Харьков

СРАВНЕНИЕ МЕТОДОЛОГИЙ МОДЕЛИРОВАНИЯ ПОВЕДЕНИЯ АГЕНТОВ СИСТЕМ БЕЗОПАСНОСТИ

Для обоснования выбора методологии моделирования поведения агентов систем безопасности было выполнено сравнение наиболее распространенных методологий, используемыми для аналогичных целей. Сравнение проводилось по следующим шести критериям.

Время и усилия, необходимые для применения той методологии методологию для проектирования актуальной модели с участием будущих пользователей. Требования пользователей. Объем технических знаний и уровень подготовки, необходимые пользователю для понимания и практического использования модели. Время обучения. Время и усилия для типичного пользователя для изучения спроектированной модели и правил ее использования. Гибкость модели. Простота, с которой разработчик может изменить модель для включения новой переменной или изменения используемых переменных. Количество существующих моделей-аналогов с функциями, которые можно адаптировать для использования в качестве части модели поведения агентов систем безопасности. Прозрачность. Простота, с которой пользователь может обнаружить в модели все, что может повлиять на результаты моделирования.

Результаты сравнения различных методологий представлены в табл. 1. Следует отметить, что первые три критерия должны быть низкими, а последние три критерия должны быть высокими.

По совокупности критериев сравнения методологий моделирования поведения агентов выбор может быть сделан в пользу системной динамики. В пользу такого выбора говорят и преимущества системно-динамического моделирования. Методология системно-динамического моделирования позволяет:

1. Обнаружить эмерджентные свойства поведения исследуемой системы. Системно-динамические модели обеспечивают способ исследования формируемого поведения агентов, исходя из относительно простых правил поведения отдельного агента. Такой подход позволяет получить и в дальнейшем исследовать синергетические свойства антагонистических агентов в процессе киберконфликта.
2. Определить наиболее важные параметры в динамике системы: необходимо определить множество входных данных, чтобы понять их влияние на выходные данные. Системно-динамическая модель позволяет оценить влияние каждого входного параметра на результат функционирования системы и ранжировать их в зависимости от степени влияния, а последующий анализ чувствительности модели поддержит принятия решения о включении в модель либо исключения того или иного фактора.
3. Подготовить количественные оценки качественных идей: системные динамические модели позволяют пользователю преобразовать качественное понимание взаимодействия агентов в количественные оценки эффективности реализации того или иного сценария поведения в процессе киберконфликта.
4. Прогнозировать долгосрочные последствия решений для определенного контура бизнес-процессов.
5. Поддержать использование модели и предоставляет системным администраторам набор инструментов для организации обучения персонала принятию решений в сложных условиях киберконфликта. В частности, системная динамика – это метод улучшения обучения в сложных системах безопасности, особенно крупных инфраструктурных проектов.

Таблица 1

Соответствие методологий моделирования критериям сравнения

Методологии	Время создания модели	Пользовательские требования	Время изучения	Гибкость	Наличие библиотеки моделей	Прозрачность
Теория игр	Н	Н-В	Н-В	С	В	Н-В
Агентное моделирование	С-В	Н-С	Н-С	С-В	Н-С	С-В
Динамические системы	С	В	В	С	С	С
Системная динамика	Н	Н	Н	В	Н	В
Модели, управляемые данными	С	С	Н	С	С	В

Примечание: Н – низкий, С – средний, В- высокий.

УДК 004.9

В.В. Міхав, Є.В. Мелешко

mihaw.wolodymyr@gmail.com, elismeleshko@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

МЕТОД ОПТИМІЗАЦІЇ ШВИДКОДІЇ БІНАРНИХ ДІАГРАМ РІШЕНЬ ПРИ ПРЕДСТАВЛЕННІ ДАНИХ РЕКОМЕНДАЦІЙНОЇ СИСТЕМИ

На сьогоднішній день рекомендаційні системи (РС) мають широке застосування у соціальних мережах, системах Інтернет-торгівлі, поширенні медіа-контенту, реклами та ін. Ефективний спосіб представлення даних, необхідних для роботи такої системи, може зменшити кількість потрібних ресурсів та полегшити розробку і використання більш складних алгоритмів для формування списків рекомендацій.

Було проведено дослідження щодо можливості використання бінарних діаграм рішень для представлення даних рекомендаційної системи та розроблено метод оптимізації швидкодії операцій читання/запису при роботі з ними.

Бінарні діаграми рішень (БДР) – це економна форма представлення булевих функцій у вигляді орієнтованого ациклічного графу. Вершини графу представляють аргументи функції, листки – її двійкові значення. БДР дають можливість зберігати дані у стисненому вигляді та швидко отримувати значення функції за її параметрами, але редагування БДР вимагає складних обчислень.

В рамках даної роботи було внесено зміни до раніше розробленої бібліотеки для роботи з БДР для зменшення часу, необхідного на виконання типових для роботи РС операцій. Розробка ведеться мовою С, оскільки вона дає можливість точно та економно використовувати пам’ять. Для представлення вузлів БДР у пам’яті було використано сторінкову модель пам’яті, що дозволяло створювати та видаляти вузли за $O(1)$. Для доступу до вузла необхідно було за допомогою бітової маски розкласти номер вузла на номер сторінки та номер вузла сторінки. В подальшому було вирішено відмовилися від цієї моделі на користь монолітного блоку пам’яті, який динамічно розширюється відповідно до потреб системи. Таким чином вдалося значно зменшити час доступу до вузла, але при цьому зріс час створення нового вузла, а також тимчасово зростає кількість необхідної пам’яті. Логіка сторінкового виділення пам’яті була частково збережена за рахунок розширення блоку пам’яті на фіксовану кількість вузлів, завдяки чому амортизований час виділення вузла не змінився. Проте, оскільки усі вузли зберігаються у суцільній області пам’яті, подібне розширення іноді вимагає виділення нової області пам’яті, що тимчасово спричиняє подвоєне використання пам’яті. Спочатку, у попередніх роботах, було реалізовано редагування значень БДР, яке максимально ефективно використовує існуючі вузли, не створюючи ізоморфних підграфів. Цей підхід дуже ефективно використовує пам’ять, але вимагає повного огляду деяких рівнів БДР, що значно сповільнює процес редагування. У цій роботі було додано режим швидкого редагування, у якому у БДР не можна використовувати вузли повторно, а, при потребі, створюється нова гілка. Це прискорює процес редагування, але спричиняє виникнення продубльованих вузлів, через що необхідно періодично робити очистку БДР. Частота очищення залежить від бажаного співвідношення витрат пам’яті до часу роботи. Цей підхід має побічний ефект – очищення робить блок вузлів розрідженим, що спричиняє ріст промахів кешу і, як наслідок, сповільнення роботи програми. Тому, після закінчення секції інтенсивного запису даних до БДР, необхідно виконати ущільнення вузлів шляхом їхнього переміщення до нової області пам’яті. Для вибірки значень, збережених у БДР, було реалізовано пошук за частковим ключем. Завдяки цьому можна, напр., знайти усі об’єкти, пов’язані з іншим об’єктом. При цьому, на відміну від інших структур даних, пошук не залежить від того, яку частину ключа використовувати для пошуку, що дає можливість зберігати зв’язки довільної розмірності. Проте такий пошук вимагає повного обходу усіх вузлів, що робить його дуже повільним. Щоб пришвидшити роботу пошуку були застосовані такі оптимізації:

1.Пошук було розділено на дві фази. У першій фазі перевіряється, які вузли з тих, що описуються частковим ключем, досяжні з терміналів, які містять значення, що нас цікавлять. У другій фазі ці дані використовуються, щоб відвідувати лише ті гілки, які можуть привести до бажаного значення. Обхід здійсненюється у алфавітному порядку, щоб мінімізувати кількість необхідних для цього даних.

2.Перша фаза розділена на два етапи. На першому етапі перевіряється лише досяжність терміналів, оскільки здебільшого треба працювати з однією і тією ж множиною значень, тож дані можна застосувати повторно. Вузли всередині рівня сортуються, щоб забезпечити прискорений перегляд на наступному етапі. На другому етапі здійснюється додаткова фільтрація цих вузлів за відповідністю до часткового ключа, відсікаючи непотрібні гілки.

Завдяки цим оптимізаціям, у роботі вдалося досягти рівня продуктивності, достатнього для того, щоб мати змогу розглядати БДР як альтернативу для більш традиційних структур даних у РС.

УДК 004[056.53+413.4]

В.В. Мохор[1], В.В. Цуркан[2]

v.mokhor@gmail.com, v.v.tsurkan@gmail.com

[1]Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, Київ
[2]Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського", Київ

ПОВЕДІНКОВІ АСПЕКТИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Система управління інформаційною безпекою розробляється для збереження конфіденційності, цілісності та доступності інформації в організації. Це досягається впровадженням набору заходів забезпечення безпеки [1]. Вони обираються завдяки оцінюванню ризиків і, як наслідок, гарантується досягнення заданого рівня інформаційної безпеки та мети діяльності організації. Означеною діяльністю визначається поведінка системи управління інформаційною безпекою [2]. Така поведінка моделюється діаграмами варіантів використання, послідовності, діяльності та кінцевого автомату в графічній нотації SysML [1, 3].

Варіантами використання відображається межі функціональності, функціональна поведінка системи управління інформаційною безпекою [3]. Насамперед, сукупність дій для збереження конфіденційності, цілісності та доступності інформації. Як наслідок, надаються впевненості зацікавленим сторонам належного управління ризиком інформаційної безпеки. Окрема увага приділяється екторам (система управління організацією, користувачам (вище керівництво, персонал), зацікавленим сторонам), а також встановленню відношень між ними і варіантами використання. Прикладами варіантів використання є [1, 2]: управління інформаційною безпекою, управління ризиком, оцінювання, аналізування, атестування і обробляння ризику.

Послідовністю відображаються особливості поведінки системи управління інформаційною безпекою у часі [3]. Цим відображенням враховуються передавання і приймання повідомлень між її елементами. Повідомлення передаються (приймаються) стосовно ліній життя і представляють окрему взаємодію між лініями життя. Їх прикладами є [1]: персонал, вище керівництво, зацікавлені сторони, система управління організацією. Тому, по-перше, вище керівництво може взаємодіяти зі зацікавленими сторонами шляхом передавання їм повідомлень про належність управління ризиком інформаційної безпеки та отримання відповіді від них. По-друге, вищим керівництвом може ініціюватися розроблення системи управління інформаційною безпекою.

Діяльність відображається послідовність дій системою управління інформаційною безпекою [3], що направлені на збереження конфіденційності доступності та цілісності інформації. З огляду на це основою діяльності є послідовність дій управління інформаційною безпекою і умов їх виконання. Дія розглядається як елементарна одиниця діяльності, наприклад [1, 2]: визначення внутрішнього та зовнішнього контексту, ідентифікування ризику, визначення оцінок (якісних та/або кількісних) оцінок ризику. Крім цього можливе виокремлення вузлів діяльності [3]. Прикладом такого вузла може бути оцінювання ризику. Діяльність координується використання вузлів управління. Зокрема вузла рішення [1 – 3], для прийняття рішення про необхідність обробляння та зіставлення залишкового ризику зі заданою прийнятною оцінкою.

Кінцевим автоматом моделюється поведінка системи управління інформаційною безпекою шляхом послідовного проходження її станами [3]. Інваріантом стану визначається істинність умов для поточного стану. Ним можливе відображення як статичних, так і динамічних умов. Зміна одного стану на інший моделюється переходом, який спрацьовує при настанні визначених подій. Тоді як подією специфікуються умови змін станів. Наприклад [1, 2], перехід від оцінювання до обробляння ризику здійснюється за умови існування неприйнятних оцінок його величини порівняно зі заданим прийнятним значенням, прийняття залишкового ризику за результатами його обробляння.

Отже, поведінка системи управління інформаційною безпекою визначається діяльністю на основі оцінювання ризику. Використання графічної нотації SysML дозволяє визначити межі функціональності означеної системи. Відобразити особливості її поведінки зважаючи на послідовність дій з управління інформаційною безпекою і умов їх виконання. Визначити стани та умови переходу між станами системи управління інформаційною безпекою.

Список літератури

[1] ДП "УкрНДНЦ". (2015, Груд. 18). ДСТУ ISO/IEC 27001, Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). Київ, 2016.

[2] В. В. Мохор, В. В. Цуркан, та О. О. Бакалинський, "Архітектура системи управління інформаційною безпекою", на XX Ювілейної Міжнародної науково-практичної конференції Безпека інформації в інформаційно-телекомунікаційних системах, Київ, с. 38, 2018

[3] SysML Open Source Project. [Online]. Available: https://sysml.org/. Accessed on: Febr. 21, 2020.

УДК 004.67

В.А. Обач, Н.М. Якименко

ivanlayon2@gmail.com, yakimenko_n_m@ukr.net

Центральноукраїнський національний технічний університет, Кропивницький

СУЧАСНІ МЕТОДИ СТЕГАНОГРАФІЇ

Завдання захисту інформації від несанкціонованого доступу вирішувалося в усі часи протягом історії людства. Уже в стародавньому світі виділилося два основних напрямки вирішення цього завдання, існуючі і по сьогоднішній день: криптографія і стеганографія. Метою криптографії є приховування вмісту повідомлень за рахунок їх шифрування. На відміну від цього, при стеганографії ховається сам факт існування таємного повідомлення.

Комп'ютерна стеганографія – напрям класичної стеганографії, заснований на особливостях комп'ютерної платформи. Приклади – стеганографічна файлова система StegFS для Linux, приховування даних в невикористовуваних областях форматів файлів, підміна символів в назвах файлів, текстова стеганографія і т. д.

Цифрова стеганографія – напрям класичної стеганографії, заснований на захованні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення цих об'єктів.

Останнім часом набули популярності методи, коли прихована інформація передається через комп'ютерні мережі з використанням особливостей роботи протоколів передачі даних називається мережева стеганографія [1].

На сьогодні вченими розроблені і випробувані різні алгоритми і методи стеганографії, вони поділяються на наступні види:

LSB-стеганографія контейнера. Чим менше біт задіяно, тим менше артефактів отримує оригінальний контейнер після впровадження.

Метод, заснований на приховуванні даних в коефіцієнтах дискретного косинусного перетворення – різновид попереднього методу, який активно використовується, наприклад, при впровадженні повідомлення в контейнер формату JPEG. За інших обставин, такий контейнер має дещо меншу ємність ніж в попередньому методі, в тому числі за рахунок того, що коефіцієнти “0” і “1” залишаються незмінними – впровадження повідомлення в них неможливо.

Метод приховування інформації за допомогою молодших біт палітри- цей метод по суті є варіантом загального методу LSB, але інформація вбудовується не в найменш значущі біти контейнера, а в найменш значущі біти палітри, очевидний недолік такого методу – низька ємність контейнера.

Метод приховування інформації в службових полях формату – досить простий метод, заснований на використанні службових полів заголовка контейнера для зберігання повідомлення. Очевидні мінуси – низька ємність контейнера і можливість виявлення впроваджених даних за допомогою звичайних програм для перегляду зображення.

Метод вбудовування повідомлення – полягає в тому, що повідомлення вбудовується в контейнер, потім за допомогою схеми, відомої обом сторонам, витягується. Можна вбудувати кілька повідомлень в один контейнер, за умови, що способи їх впровадження ортогональні.

Широкосмугові методи, які поділяються на:

- метод псевдовипадкової послідовності: використовується секретний сигнал, який моделюється псевдовипадковим сигналом;

- метод стрибаючих частот: частота несучого сигналу змінюється за певним псевдовипадковим законом.

Метод накладення – по суті не є справжньою стеганографією, заснований на тому, що деякі формати містять в заголовку розмір даних, або ж обробник цих форматів буде читати файл до маркера кінця даних. Прикладом такого методу є добре відомий метод “rar-jpeg”, який заснований на конкатенації графічного файлу в форматі JREG і RAR-архіву. Програми для перегляду JPEG буде зчитувати інформацію до кордону, зазначеної в заголовку файлу, а RAR-архіватор відкине всі, що знаходиться до сигнатури RAR, яка позначає початок архіву. Таким чином, якщо такий файл відкрити у вікні перегляду графічних файлів – ми побачимо картинку, а якщо в RAR-архіватор – вміст RAR-архіву. Очевидні мінуси такого підходу полягають в тому, що оверлей, доданий до контейнера, легко виділяємо при візуальному дослідженні такого файлу [2].

Стеганографія – один з найбільш захоплюючих і ефективних методів приховування даних, які використовувалися за всю історію людства. Є дуже багато причин для використання стеганографії, але головна – це легкість в обігу і складність при виявленні.

Список літератури

[1] Стеганографія [Електронний ресурс]. Доступно: https://uk.wikipedia.org/wiki/Стеганографія/. Дата звернен-ня: Бер. 9, 2020.

[2] Стеганографія в сучасних кібератаках [Електронний ресурс]. Доступно: https://securelist.ru/ steganography-in-contemporary-cyberattacks/79090/. Дата звернення: Січ. 9, 2020.

УДК 519.1

В.І. Петренюк

petrenjukvi@i.ua

Центральноукраїнський національний технічний університет, Кропивницький

ПРО МІНІМАЛЬНІ ГРАФИ-МОДЕЛІ НЕОРІЄНТОВНОГО РОДУ

Задача вивчення структури всіх мінімальних незовнішньоплощинних проективних графів вирі шена шляхом перебору всіх різних варіантів видал ення однієї з вершин одного з 35-ти мінорів проект тивної площини та відбору неізоморфних графів неорієнтованого роду 1. Оскільки в D. Archdeacon, N. Hartsfield,C.H.C. Little, B. Mohar. Obstructions sets for outer-projective -planar graphs. Iternet source не наведені діаграми цих графів, то виникає потреба їхньої побудови. Задача має дві підзадачі: 1. Дослідити структуру проективно площинних графів, мінімальних відносно операції видалення чи стягнення в точку довільного ребра, із заданою множиною точок, що має число досяжності t, t=2, та є сама чи має підмножину мінімальну відносно видалення довільної точки, і навести їхні діаграми графів із зазначенням вказаних підмножин.2. Дослідити спосіб побудови непроективно площин них чи неклейново поверхневих графів як φ-образів (структуру графа-склейки деякого числа графів як елементів множини мінімальних відносно числа досяжності 2 для заданої поверхні Клейна чи проективної площини) кількох мінімальних проективно площинних чи клейново поверхневих графів із підмножинами точок, що мають число досяжності 2 та є мінімальними відносно числа досяжності при операції видалення довільної точки. Розв'язок підзадачі 1 полягає в побудові всіх мінімальних незовнішньоплощинних проективно-площинних графів розв'язана в (не наведені діаграми цих графів) шляхом перебору всіх різних варіантів видалення однієї з вершин графа мінора проективної площини та відбору неізоморфних гра фів неорієнтованого роду 1. Ідея побудови аналогі чна тому, як мінімально проективно неплощинні графи K_5 чи $K_{3,3}$ утворені із мінімальних незовніш ньо площинних графів K_4 чи $K_{2,3}$ шляхом приклею вання простої зірки St(v) до мінімальних за потуж ністю підмножин точок графів K_4 чи $K_{2,3}$ з числом досяжності 2. Підзадача 2 полягає у виявленні міні мальної підмножини точок у мінімальних непроекти вно площинних чи мінімальних неклейново площин них графів із заданим числом досяжності 2 та хара ктеру їх склеювання з метою іншої побудови непрое ктивно площин них чи побудови всіх неклейново поверхневих графів-мінорів. Подібна задача розв'яза на, де розглянуто покриття непроективно площин них чи неклейново поверхневих графів G обструк цій неорієнтованого роду $\gamma(G)$ (з числом вершин не більше 10) $\gamma(G)$ підграфами гомеоморфним K_5, чи $K_{3,3}$, які попарно утворюють підграфи гомеоморфні обструкціям неорієнтованого роду $\gamma(G)$ розв'язана в для неорієнтованих поверхонь роду не більше 5, причому для тора також має місце зазначене покрит тя, але наведено контр приклад для покриття більшо го графа. Є розв'язок аналогічної задачі побудови неклейново площинних графів методом релятивних компонент. *Теорема 1*. Для довільного мінімального вкладення f простого графа G до неорієнтованої поверхні N мають місце наступні співвідношення: *1.* Немає ребер $e, e', e=(a,b), e'=(b,a)$ на границі довільної клітки s, $s \in S_G(N,f)$, але можуть мати місце повторення деяких вершин; 2. Немає повторення двох пар вершин чи двох пар частин ребер e', $e, e=(a,b)$, $e'=(c,d)$, які на площині попарно розділяють одна одну та лежать на грани ці довільної клітки s, $s \in S_G(N,f)$; 3. Немає двох 2-кліток s_1, s_2, де $s_1, s_2 \in S_G(N,f)$, на границях яких розташовані повторення трьох виділених ребра із різним поряд ком слідування. *Твердження 1*. Для довільного графа – обструкції G до проективної площини мають місце співвідношення:1. Для кожної вершини v графа–обструкції G для проективної площини із множиною $M(v)$ всіх вершин інцидентних v та підграфом $G \setminus v$ неорієнтованого рода $\gamma(G \setminus v)$ виконуються наступні співвідношення: 1) якщо $\gamma(G \setminus v)=1$, то $t_{G\setminus v}(M(v),N_1)=2$ та кожне ребро підграфа $G \setminus v$ є, або суттєвим відносно роду $\gamma(G \setminus v)$ при операціях видалення ребра чи стискання в точку, або належить до границь двох кліток проективної площини, які містять множину $M(v)$ (реалізують число досяжності $t_{G\setminus v}(M(v),N_1)$);2) якщо $\gamma(G \setminus v)=0$, то $t_{G\setminus v}(M(v),N_1)=3$ та $\theta_{G\setminus v}(M(v),N_1)=1$, причому кожне ребро підграфа $G \setminus v$ є суттєвим відносно $t_{G\setminus v}(M(v),N_1)$ при операціях видалення ребра чи стискання його в точку. 2. Кожна граф–обструкція G неорієнтованого роду 2 покривається щонайбільше 4-ма (наприклад графи A_2,G_1) підграфами чи части нами гомеоморфним одному з наступних графів: $K_{2,3}$, K_4, $K_5\backslash e$, $K_{3,3}\backslash e$, K_5, $K_{3,3}$ та матиме відносно N_2 (поверхні Клейна) число досяжності 2 для множини вершин, причому для кожного видаленого ребра e граф $G \setminus e$ матиме на N_1 число досяжності 2 для множини вершин.

УДК 681.3.06

С.С. Погасий, В. О. Алексеев

Spogasiy1978@gmail.com, alexievvo@hneu.net

Харьковский национальный экономический университет имени Семена Кузнеца, Харьков

АНАЛИЗ УЯЗВИМОСТЕЙ ТЕХНОЛОГИИ 3D ПЕЧАТИ

Проблематика возникновения потенциальных рисков кибербезопасности при аддитивном производстве (AM) - это процесс, в котором управляемое компьютером устройство объединяет различные типы материалов вместе, чтобы создавать трехмерные объекты из CAD или 3D модели.

Есть много типов 3D-принтеров; от обычного моделирования методом послойного наплавления (FDM), до стереолитографических (SLA), использующих свет для отверждения специальных жидкостей в твердые вещества, до принтеров селективного лазерного спекания (SLS), в которых используется лазер для расплавить порошкообразный материал на объекты послойно [1]. 3D принтеры отличаются по используемому материалу, кинематике, способу печати, но все они имею и общие характеристики, которые делают их уязвимыми для кибератак, не в последнюю очередь из-за того, что они управляются компьютером. Однако существуют кибер риски, которые в ближайшем будущем будут серьезно влиять на индустрию 3D-печати.

1. Все встроенные компьютеры имеют программные уязвимости. Все 3D-принтеры, управляются компьютером. На этих компьютерах работает программное обеспечение, которое может быть подвержено ошибкам разработки, приводящим к уязвимостям безопасности. Например, автономный принтер, который печатает с SD-карты формата RepRap, используя прошивку с открытым исходным кодом Marlin, имеет значительную уязвимость переполнения буфера [2]. Теоретически, злоумышленники могут использовать этот тип уязвимости для загрузки вредоносного процесса или, возможно, установить какую-то “троянскую” прошивку.

2. Сетевые принтеры или хосты принтеров уязвимы. Подключая 3D-принтер к сети, он становится устройством Интернета вещей (IoT) и приобретает потенциальные недостатки программного обеспечения устройства IoT. При получении доступа к настройке Octoprint, он может удаленно запустить печать со вредоносным файлом, что приведет к возникновению этой ошибки и выполнению кода на принтере по сети. Любой сетевой доступ к принтеру, прямой или через промежуточное программное обеспечение, становится более уязвимым. Эта сетевая функция раскрывает собственные уязвимости принтера. Стоит учитывать, что современные принтеры снабжены WEB камерами для контроля процесса печати, что может являться дополнительным стимулом несанкционированного доступа с устройству

3 Файлы печати могут привести к физическому повреждению устройства. Для печати объектов 3D-принтерам нужны точные инструкции о том, как перемещать свои печатающие головки в 3D-пространстве или как выглядит каждый слой 3D-печати. Многие 3D-принтеры, особенно с открытым исходным кодом, используют файлы G-кода для предоставления этих инструкций. G-код – это, стандартизированный язык программирования, разработанный для того, чтобы печатающая головка(экструдер) правильно себя позиционировала, и наносила слои в соответствии с программой разработчика [3]. Проблема заключается в том, что многие из этих типов файлов 3D-печати не имеют встроенной функции шифрования или проверки целостности. Большинство 3D-моделей имеют внутреннюю структуру объекта, которая не видна в конечном изделии, но влияет на его физические характеристики. При наличии доступа к G-коду или файлам модели, злоумышленник может изменить параметры изделия, тем самым создавая слабые места, которые, могут проявиться только при использовании детали. На примере dr0wned – AM Cyber Attack – полная цепочку атак с использованием 3D-печати (AM), начиная с кибератак, чтобы скомпрометировать доброкачественный компонент AM, путем злонамеренной модификации чертежа изготовленного объекта, что приводит к производству саботированной функциональной части. Использована исправленная уязвимость WinRAR, чтобы продемонстрировать вектор атаки, открыт обратный туннель к ПК жертвы и скачан файлы дизайна, после манипулирования с файлами загружен их обратно. В качестве решения проблемы Файлы печати и модели, которые мы используем для 3D-печати, должны иметь стандартизированное шифрование и, что более важно, проверку целостности. Можно использовать обычные решения для контрольных сумм MD5 и SHA, чтобы добавить проверки целостности к файлам или зашифровать их с помощью сторонних инструментов.

4 3D-принтеры – новые преимущества для киберпреступников с ограниченными ресурсами становится намного проще создать устройство, которое подключается к считывающему устройству банкомата и выглядит достоверно как часть машины. Доступ к этой технологии даже помогает им дорабатывать и минимизировать свои конструкции, встраивая скимминговую электронику в саму деталь, создавая скиммер, который не выделяется.

Необходимо обеспечить соблюдение законов и привлечь к ответственности тех, кто печатает что-то, что они используют для преступления. Общественность должна быть осведомлена о том, как киберпреступники используют 3D-принтеры. Кроме того, 3D-принтеры являются очень чувствительным ресурсом, особенно в производственной среде. Они создают физические объекты, на которые придется положиться или являются конфиденциальном интеллектуальной разработкой. По мере совершенствования технологии 3D-принтеры могут перейти от устройств, которые ускоряют создание прототипов, к основной части конечного производства, поэтому реализация мер минимизации проникновения является на сегоднящний день даже более актуальной, чем непосредственно техническое усовершенствование 3D-принтеров.

Список литературы

[1] National vulnerability database. Information Technology Laboratory. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-1000537. Accessed on: Mar. 01, 2020.

[2] Smid, Peter (2010), CNC Control Setup for Milling and Turning, New York: Industrial Press [Online]. Available: https://en.wikipedia.org/wiki/G-code. Accessed on: Mar. 01, 2020.

[3] dr0wned – AM Cyber Attack. [Online]. Available: https://www.youtube.com/watch?v=zUnSpT6jSys. Accessed on: Mar. 01, 2020.

УДК: 004.62

В.В. Прокопов, Н.М. Якименко

prostoemail97@gmail.com, yakimenko_n_m@ukr.net

Центральноукраїнський національний технічний університет, Кропивницький

ОСОБЛИВОСТІ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ ПРИ ВИКОРИСТАННІ ХМАРНИХ ТЕХНОЛОГІЙ

Хмарні (розсіяні) технології – це набір технологій, що дозволяє використовувати ресурси віддалених систем, як нібито вони знаходяться зовсім поруч – вдома або в офісі. Насправді комп'ютери, які обслуговують хмари, знаходяться в датацентрі, який може знаходитися в сотнях і тисячах кілометрах від кінцевого користувача [1].

Серед загроз, спрямованих на автоматизовані робочі місця (АРМ) кінцевих користувачів, можна виділити компрометацію клієнтських пристроїв доступу в хмару і атаки на клієнтські браузери. Ці загрози актуальні внаслідок слабкого захисту АРМ кінцевих користувачів і відсутності контролю політики інформаційної безпеки (ІБ) на АРМ користувачів при доступі в хмари. Через гіпервізор (монітор віртуальних машин (ВМ)) реалізується така загроза віртуальної інфраструктури, як несанкціонований доступ (НСД) до середовища віртуалізації. Він можливий внаслідок порушення ізоляції середовища, наданої клієнту в рамках хмарної послуги. DDoS-атаки на мережеву інфраструктуру між хмарою і клієнтом можливі внаслідок розгортання погано захищених ВМ і відсутності в складі гіпервізора засобів захисту мережевої інфраструктури. Випадкове або навмисне стирання (спотворення) образів ВМ можливо внаслідок відсутності засобів розмежування доступу і контролю цілісності віртуального середовища. Деякі традиційні загрози віртуальній інфраструктурі реалізуються внаслідок вразливості фізичних серверів, на яких вона розгорнута. У їх числі мережеві атаки між віртуальними машинами в рамках одного хоста, підміна і/або перехоплення даних і оперативної пам'яті ВМ в процесі їх міграції засобами віртуального середовища, вірусне зараження ВМ і використання їх вразливостей. Застосування технологій віртуалізації вносить в мережеву архітектуру нові елементи, наприклад, гіпервізор і засоби управління віртуальною інфраструктурою, які також потрібно захищати, так як зміна інфраструктури відкриває можливості для нових методів атак. Комплексний і багаторівневий захист можуть забезпечити тільки спеціалізовані засоби [2].

Традиційні міжмережеві екрани не контролюють трафік усередині сервера віртуалізації, де можуть перебувати десятки гостьових машин, взаємодіючих між собою по мережі. Відхід від традиційного периметра до відсутності контрольованої зони, переміщення ВМ між фізичними серверами призводить до необхідності реалізації політик ІБ незалежно від фізичних кордонів. Складно знайти баланс між централізованими заходами забезпечення ІБ, реалізованими постачальником інфраструктурних послуг, і локальними, що забезпечуються клієнтом. Для захисту від несанкціонованого доступу робочих місць користувачів, хостової системи і системи зберігання даних пропонується використовувати традиційні сертифіковані засоби захисту від несанкціонованого доступу, такі як Dallas Lock компанії "Конфидент" і Secret Net компанії "Код безпеки". Для антивірусного захисту ВМ пропонується використовувати новаторський безагентний підхід, що забезпечує комплексну безпеку без установки агентського модуля в системі, що захищається. Наприклад, безагентний режим використовує рішення Deep Security компанії Trend Micro. Необхідно використовувати системи виявлення вторгнень і міжмережевого екранування. З появою віртуальних середовищ з'явилася нова проблема – неконтрольована мережева взаємодія між ВМ. Загальна рекомендація така: контролювати зовнішні підключення до середовища віртуалізації слід за допомогою апаратних рішень, а внутрішні – з допомогою програмних рішень, реалізуючи таким чином комбінований підхід. Компанія CheckPoint може запропонувати продукти VPN-1 VE (Virtual Edition) – віртуального пристрою, який забезпечує захист віртуальних середовищ від зовнішніх і внутрішніх загроз безпеки [3].

Крім традиційних засобів захисту інформації кінцевих користувачів, таких як засоби захисту від несанкціонованого доступу і антивірусних засобів, особливу важливість набувають контроль виконання політики ІБ кінцевими пристроями і надійна аутентифікація з застосуванням апаратних засобів і безпечного віддаленого доступу, для реалізації яких використовується, наприклад, StoneGate Virtual SSL VPN.

Список літератури

[1] Хмарні технології [Електронний ресурс]. Доступно: https://www.xelent.ru/blog/oblachnye-servisy-dlya-chaynikov. Дата звернення: Бер. 09, 2020.

[2] Загрози хмарних обчислень і методи їх захисту [Електронний ресурс]. Доступно: https://habr.com /ru/post/ 183168/. Дата звернення: Бер. 09, 2020.

[3] Забезпечення безпеки даних при використанні хмарних технологій [Електронний ресурс]. Доступно: http://www.lastmile.su/files/article_p/df/3/article_3823_334.pdf/. Дата звернення: Бер. 09, 2020.

УДК 004.8

М. Ю. Сорока[1], Н. А. Сало[1], О. Г. Матющенко[2]

s_mike@ukr.net, natal6ka9@gmail.com, mog28@ukr.net

[1]Льотна академія Національного авіаційного університету, Кропивницький
[2] Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків

ІНТЕЛЕКТУАЛЬНІ АГЕНТИ В НАВЧАЛЬНІЙ СИСТЕМІ ПІДГОТОВКИ ДИСПЕТЧЕРІВ УПРАВЛІННЯ ПОВІТРЯНИМ РУХОМ

Як показує аналіз літератури закордонних та вітчизняних науковців в галузі адаптивних тренажерах диспетчерів управління повітряним рухом (УПР) є необхідність у створенні інтелектуального навчального середовища (ІНС), що б дозволило зменшити терміни підготовки диспетчерів управління повітряним рухом та заощадити на фінансових витратах, уникаючи негативного впливу на якість їх підготовки та безпеку польотів.

Перспективним є створення інтелектуальних об'єктів у теорії мультиагентних систем з використанням методів планування спрямованих дій або планування поводження з метою забезпечення моделювання інтелектуального поведінки об'єктів, що входять у віртуальне середовище навчання [1–4].

У зв'язку з цим у доповіді запропоновано використовувати агентно–орієнтований підхід до побудови ІНС підготовки диспетчерів УПР. В основі реалізації інтелектуальної поведінки об’єктів у рамках даного підходу пропонується використовувати методи планування поведінки інтелектуальних агентів.

Підвищення ефективності ІНС підготовки диспетчерів УПР загалом можливо за рахунок удосконалення методів планування поведінки інтелектуальних агентів та розширення їх функціональних можливостей.

В доповіді запропоновано підхід удосконалення та розширення функціональних можливостей системи підготовки диспетчерів УПР за рахунок використання теорії мультиагентних систем з метою створення ІНС, що забезпечує правдоподібність та нелінійності поводження об’єктів, що імітуються в ІНС.

Визначені вимоги до побудови мультиагентного середовища інтелектуальної навчальної системи підготовки диспетчерів управління повітряним рухом, розроблені моделі такої системи.

Представлена модель мультиагентного середовища інтелектуальної навчальної системи, особливістю якої є взаємодія агента з зовнішнім середовищем, у тому числі з іншими агентами, що здійснюється через модель фізичного представлення об'єкта. Таким чином, досягається поділ моделювання інтелектуального поводження об'єктів у середовищі навчальної системи від їх фізичного представлення, у яке в тому числі можуть входити засоби комунікації. Запропонована структура допускає прямі керуючі впливи на поведінку агентів з автоматизованих робочих місць навчальної системи диспетчерів управління повітряним рухом з метою забезпечення можливості внесення корегувань у розвиток навчальної обстановки (середовища), а також доступ до бази знань агента за допомогою спеціального інтерфейсу.

Розроблена структура забезпечує ідентифікацію ситуації в підсистемі підготовки і прийняття рішень, що виконує передачу управління на відповідний рівень ієрархії системи поводження інтелектуального агента. Крім того, підсистема підготовки і прийняття рішень відслідковує інформацію, що надходять з рівнів поводження агентів, та у випадку виникнення суперечливих ситуацій забезпечує їх розв’язання. Запропонований підхід реалізує взаємодію рівнів через посередника як підсистеми підготовки і прийняття рішень.

Список літератури

[1] П. І. Федорук, Адаптивна система дистанційного навчання та контролю знань на базі інтелектуальних інформаційних технологій: автореферат дис … докт. техн. наук:05.13.06 НАН України, Інститут проблем математичних машин і систем, Київ, 2009.

[2] В. К. Фин, “Об интеллектуальном анализе данных”, Новости Искусственного интеллекта, № 3, с. 98 – 103, 2004.

[3] Н. К. Юрков, Машинный интеллект и обучение человека: монография, Пенза: ИИЦ ПензГУ, 2008.

[4] Railsback, and V. Grimm, “Agent-based and Individual-based Modeling: A Practical Introduction”, Princeton University Press, 2011.

УДК 004.056, 004.75

В. Сушков, В.І. Петренюк

petrenjukvi@i.ua

Центральноукраїнський національний технічний університет, Кропивницький

ЗЛАМУВАННЯ АНДРОЇД СИСТЕМИ ДЛЯ ВИЛУЧЕННЯ ІНФОРМАЦІЇ З ПРИСТРОЮ

Смартфони є найбільш вразливими пристроями і зв'язано це не через помилки виробників або через людський фактор. Саме через людський фактор відбувається 73% успішних хакерських атак. Знаючи лише саму соціальну інженерію можна отримати доступ до необхідної інформації, не використовуючи при цьому навички програмування. Отже, спробуємо зробити певний алгоритм злому на власному прикладі. У ході експерименту буде застосовано вже існуючий вірусний білдер SpyMax. Необхідно скомпілювати вірус. Зробити це можна власноруч або, як в нашому випадку, застосувати білдер SpyMax. Конструювати програму будемо під виглядом антивірусу "Avast".

Важлива деталь, при використанні програмного засобу SpyMax, з'явиться вікно з вашими портами. Для коректної роботи, необхідно їх відкрити.

Необхідно вказати свій IP та відкритий порт. Необхідно мати на ПК програмне забезпечення Java. У рядку де необхідно обрати шлях до папки bin вказуємо: C:\Program Files (x86)\Java\jre1.8.0_231\ bin. Далі необхідно обрати патч, який йде у комплекті з програмним засобом. Починається будування програмного засобу (рис. 1):

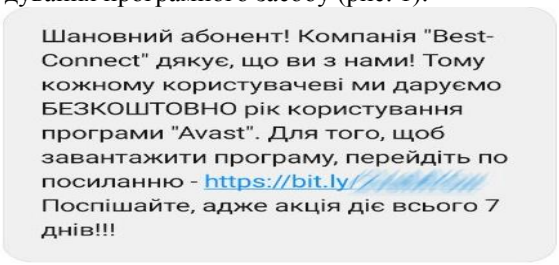


Рис. 1. Файл ready.apk , Фішинг через СМС

Далі з'являється файл "ready.apk". Його слід встановити у телефон жертви. Другим етапом буде спосіб встановлення на смартфон жертви. Є декілька варіантів цього:

- фізичний контакт з мобільним пристроєм. Цей спосіб передбачає, що у вас є можливість безпосередньо контактувати з пристроєм жертви. Необхідно під'єднати пристрій жертви до носія вірусу та передати його;

- фішинг. Цей водночас складний і дієвий спосіб. Базується він якраз таки на соціальній інженерії. Суть у тому, щоб змусити жертву саму встановити ваш програмний засіб (вірус). Якщо ви вже багато користуєтесь послугами оператора, то вам надсилають приблизно такі рекламні повідомлення: Оскільки ми отримали повідомлення, якби, від оператора, то у людини певним чином виникає довіра і він впевнений у тому, що ПЗ ліцензійне. Такі трюки як "безкоштовно" та "поспішайте, адже акція діє всього 7 днів", це база соціальної інженерії. Адже людина розуміє, що акція з обмеженим строком дії, а також за неї не треба платити і підсвідомо вона вже хоче встановити даний засіб. Також цікавий факт. Вбудований антивірус, не бачить вірусу, оскільки ПЗ є програмою склейкою. Після встановлення, необхідно згодитися на доступ до всіх можливостей смартфону, а саме камери, файлового менеджера, мікрофона, місцезнаходження, СМС, галереї і контактів (рис. 2).

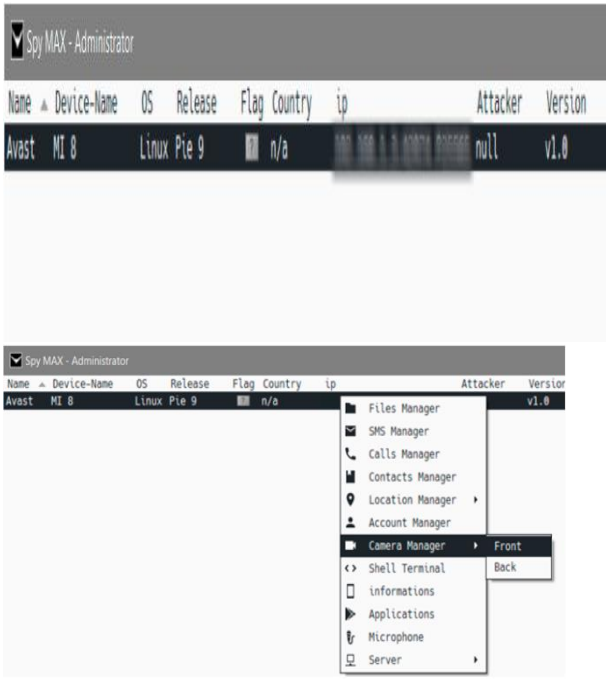


Рис. 2. Індикатор активності вірусу

З цим, як правило, проблем не буває, оскільки людина довіряє (повинна) даному ПЗ.

Висновок. Тепер є повний доступ до смартфона. Тож як можна захистити смартфон від таких нападів? По-перше, ніколи не переходьте на скороченні посилання такі, як "bit.ly" або "goo.gl", або переходьте з обережністю. Намагайтесь мати завжди нову версію андроїду, оскільки з кожним оновленням вигадують нові алгоритми захисту.

УДК 004.738.5

С. С. Федушко[1], Ю. О. Сєров[1], S. Syerov[2]

solomiia.s.fedushko@lpnu.ua, yurii.o.sierov@lpnu.ua, svyatsyerov@gmail.com

[1]*Національний університет «Львівська політехніка», Львів*
[2]*University of Illinois at Chicago, USA*

КЛАСТЕРНИЙ АНАЛІЗ МОВНИХ ІНДИКАТОРІВ ВІКУ ВЕБ-КОРИСТУВАЧІВ

З погляду мережевої та соціально-демографічної ідентичності веб-особистість аналізуємо як усвідомлення належності до соціальних груп веб-учасників. Складовими соціально-демографічної ідентичності є ґендерна, вікова та професійна ідентичність. Веб-ідентичність використовують для самовираження, отримання нового досвіду і як інструмент для маніпуляції іншими веб-користувачами. Віковий поділ вибрано на основі аналізу усіх можливих україномовних популярних веб-спільнот, для яких вік учасника є критичним: підліткові (University, Підліток, Просто чат), дитячі (Острів знань, Пустунчик); дорослі (Наш анектод з перцем, Пан+Пані, Український форум благодійників). Здійснено аналіз актуальних досліджень вікової онлайн-комунікації за такими напрямками: веб-комунікація підлітків (Arinze B., Ridings C., Gefen D., Turkle S.), соціолект підлітків (Боднар Р., Herring S.), засоби інтернет-комунікації підлітків (Calvert S., Wolf A., Witmer D., Lee M., Crystal D.), сучасний жаргон (Дзюбишина-Мельник Н.), мережевої етики (Аксак В., Смирнов Ф.), моделі комунікації підлітків (Schiano D., Isaacs E., Chen C.).

За вибраними чинниками вибірка “Age” поділена на два кластери – Кластер1 (дорослі особи) і Кластер 2 (підлітки). Вік учасників відомий, то проведено аналіз некоректності кластеризації. Результат кластеризації: тільки одного веб-учасник віднесено до Кластеру 1 (група дорослі), який в мережі Інтернет позиціонує себе підлітком. Цього веб-учасника в аналізі позначено – С5, вік –15 років. З огляду на адміністрування спільнотою є такі сценарії розвитку атомарної ситуації: учасник навмисно неправильно вказав вік у акаунті, щоб цілеспрямовано проникнути у веб-спільноту підлітків з прихованими намірами; учасник випадково помилився у вказанні віку; стиль спілкування веб-учасника не відповідає віку учасника. Графічно процедуру кластеризації зображено на дендрограмі (рис. 1).

Графічне зображення кластерів підтверджує ефективність проведеної класифікації. Матриця факторної структури отриманого результату також дозволяє оцінити вклад окремих факторів у класифікацію.

За результатами можна зробити висновок, що структура вихідних даних в основному обумовлена такими мовних індикаторами – AGE–B(1.3), AGE–E(1.4), AGE–B(1.4), AGE–D(1.3).

Порівняння індикаторів для отриманих кластерів вказує на істотну відмінність середніх значень таких індикаторів – AGE–B(1.3), AGE–D(1.3), AGE–E(1.4),

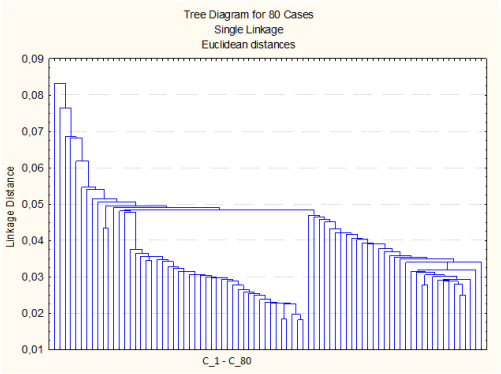


Рис. 1. Дендрограма кластеризації учасників веб-форумів за віком

AGE–C(1.3). Для групи підлітків (Кластер 2) характерне більше середнє значення в порівнянні з групою дорослих (Кластер 1), а саме: AGE–B(1.3) – середнє значення 0,032172 для підлітків проти 0,006376 для дорослих; AGE–D(1.3) – середнє значення 0,023031 для підлітків проти 0,004444 для дорослих; AGE–E(1.4) – середнє значення 0,019441 для підлітків проти 0,005059 для дорослих; AGE–C(1.3) – середнє значення 0,017359 для підлітків проти 0,005524 для дорослих. Вікову категорію веб-учасників вибрано для перевірки достовірності вказання віку у зв’язку з наявністю реальних он-лайн загроз (віком 6-17 років): розголос конфіденційних даних, доступ до вікового контенту, що негативно впливає на фізичне і психологічне здоров’я дитини, онлайн-насильство, інтернет-маркетингові злочини); необхідність відсіювання вікової групи дітей, які подали заявку чи вже стали веб-учасниками, призначеної тільки для дорослих користувачів. Характерними ознаками веб-ідентичності є самовираження, що характерно для підлітків. Проблема вікової диференціації веб-учасників постає гостро через збільшення випадків проникнень дітей у спільноти для дорослих. А неофіційна участь дорослої особи у веб-спільноті підлітків, може привести до кримінальної відповідальності адміністратора. Програмний засіб перевірки достовірності віку є затребуваним для запобігання випадкам педофілії та провокацій неповнолітніми особами у спільноти дорослих учасників.

Список літератури

[1] Yu. Syerov, S. Fedushko, and Z. Loboda. “Determination of Development Scenarios of the Educational”, on Web Forum. XIth International Scientific and Technical Conference (CSIT 2016). Lviv, p. 73 – 76, 2016.

УДК 004.7

Д. О. Фесенко, І. Д. Горбенко

dmytro.fesenko@nure.ua

Харківський національний університет радіоелектроніки, Харків

АТАКИ НА МЕРЕЖУ БЛОКЧЕЙН

Останнім часом в наше життя стрімко розвиваються децентралізовані технології, нові продукти впроваджуються настільки швидко, що фахівцям з інформаційної безпеки важко реагувати на проблеми, які вони несуть в собі, тому в цьому документі ми перевіряємо останні теми про технології. на основі блокчейна.

Ідеологія проектів, що застосовують технологію блокчейн – це можливість розмежованого використання доступу до інформації з унеможливленням зміни даних в реєстрі, що доступний усім користувачам мережі. Ця технологія стала відома коли вона була застосована для забезпечення появи електронних грошей, де здійснюються цифрові перекази грошей у розподілених системах. Через це блокчейн часто розглядається як пов'язаний з біткоїном або рішеннями в сфері електронної валюти в цілому. Незважаючи на це, технологія може бути використана більш широко для різних сфер застосування.

Кожен компонент можна просто описати та використовувати як структурний елемент, щоб зрозуміти більш складну систему.

В системі до старих даних додаються нові блоки, попередні блоки стає все важче модифікувати. Нові блоки додаються до всіх копій учасників реєстру в мережі та будь – які конфлікти вирішуються автоматично за допомогою встановлених правил.

Стосовно мережі блокчейн, порушники можуть бути зовнішніми або внутрішніми. Внутрішній порушник – це, здебільшого, розробник певного проекту або додаткового компоненту (модуля) проекту, що хоче порушити безпеку системи ще на етапі розробки або експлуатації, реалізує внутрішнє проникнення або віддалене, де використовується вже відома помилка у безпеці. Зовнішній – атакує мережу, як звичайний користувач або учасник мережі (вузол або нод мережі), реалізує віддалені атаки.

Мета порушника:

1) одержання можливості вносити зміни в мережу блокчейн згідно зі своїми намірами;

2) перешкоджати нормальній роботі мережі (перевантажувати вузли, блокувати доступ, отримати контроль над мережею тощо);

3) отримання матеріальної або іншої вигоди, шляхом крадіжки даних / грошових ресурсів.

Для того, щоб здійснити атаку, внутрішній порушник повинен:

1) мати доступ до редагування програмної частини мережі або створення та додавання до неї власних частин (бекдорів), що дадуть змогу використати мережу у своїх цілях;

2) володіти достатніми знаннями про роботу мережі та про її вразливі місця.

Зовнішній порушник повинен:

1) володіти достатньою кількістю обчислювальних та матеріальних ресурсів для здійснення своєї атаки;

2) володіти достатніми знаннями про роботу мережі та про її вразливі місця.

У ситуації для внутрішнього порушника, технічна оснащеність не є важливою тому, що використання бекдорів або заздалегідь створених каналів для несанкціонованого доступу є простою здачею для одного звичайного комп'ютера.

У ситуації для зовнішнього порушника, ресурси для атаки є вкрай важливими через те, що безпека багатьох сучасних блокчейн систем опирається на складність вирішення певних криптографічних задач. Успішність атаки залежить від кількості обчислювальних ресурсів/потужностей зловмисника,.

Кількість осіб, що здійснюють атаку, може бути різною і залежить лише від плану самої атаки. Для внутрішнього зловмисника достатньо і однієї людини. Атаку із необхідністю великої кількості ресурсів, одній людині буде виконати вже важче. Загалом, сучасні атаки на блокчейн або на користувачів мереж блокчейн, здійснюються підготовленою командою із продуманим планом дій на кожному етапі атаки.

Кожен учасник мережі повинен використовувати шифрування (здебільшого асиметричне). Заходи безпеки вбудовані в мережу і закладені у загальному протоколі, що забезпечує конфіденцій-ність і автентичність для користувачів.

При виконанні всіх рекомендацій з безпеки, використання перевірених та надійних криптографічних засобів можна легко побудувати гарно захищену систему на основі технології блокчейн.

УДК 004.056

Ю.І. Хлапонін, Д.Ю. Хлапонін

y.khlaponin@gmail.com, kmld.85@gmail.com

Київський національний університет будівництва і архітектури, Київ
Державний університет телекомунікацій, Київ

СЕРТИФІКАЦІЯ ПРИСТРОЇВ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Розвиток концепції Інтернету речей та її впровадження в різні сфери передбачає наявність десятків мільярдів автономних пристроїв. За даними порталу Statista в 2017 році їх вже налічується більше 20 млрд, а до 2025 року очікується не менше 75 млрд. Всі вони підключені до мережі Інтернет та передають через неї відповідні їх функціоналу дані. І дані, і функціонал є мішенню для зловмисників, а значить, повинні бути захищені.

Для IoT-пристроїв безпека полягає, перш за все, в цілісності коді, перевірці автентичності користувачів (пристроїв), встановлення прав володіння (включаючи дані, які ними генеруються), а також можливістю відображення віртуальних і фізичних атак. Але по факту, більшість з працюючих сьогодні IoT-пристроїв елементами захисту не забезпечені, мають доступні ззовні інтерфейси управління, дефолтні паролі, тобто, мають всі ознаки веб-уразливості.

Сьогодні питаннями сертифікації займаються і кілька приватних компаній. Зокрема, компанія Online Trust Alliance (OTA) вийшла з ініціативою вирішення проблеми безпеки IoT на рівні держав і виробників, випустивши IoT Trust Framework – перелік критеріїв для розробників, виробників пристроїв і постачальників послуг, який спрямований на поліпшення безпеки, конфіденційності та життєвого циклу їх IoT-продуктів. В першу чергу, він орієнтований на підключення домашні, офісні і мобільні пристрої і є таким собі рекомендаційним кодексом поведінки і основою для декількох програм сертифікації та оцінки ризиків.

У поточному році незалежним підрозділом компанії Verizon – ICSA Labs була запущена програма тестування безпеки і сертифікації IoT-пристроїв. Як стверджують її розробники, вона є однією з перших в своєму роді, і тестує такі складові, як повідомлення / протоколювання, криптографія, аутентифікація, зв'язок, фізична безпека і безпека платформи. Пристрої, які пройшли сертифікацію, будуть відзначені спеціальним знаком схвалення ICSA Labs, що вказує на те, що вони були тестовані, а виявлені вразливості були усунені. Також пристрої, що пройшли сертифікацію будуть перебувати під наглядом і періодично тестуватися на протязі всього їх життєвого циклу для збереження їх безпеки.

Безпека Інтернету речей стала однією з перших сфер використання блокчейн-технології. Завдяки технології розподіленого реєстру з'явилася можливість забезпечувати високий рівень безпеки IoT-пристроїв в мережі і усунути існуючі обмеження і ризики для IoT, пов'язані з централізацією.

Вона дозволяє швидко і безпечно зберігати протоколи обміну і результати взаємодії різних IoT-пристроїв в децентралізованій системі. Саме розподілена архітектура блокчейна гарантує досить високу безпеку всієї IoT-системи. Але якщо частина з пристроїв мережі все ж буде схильна до злому, в цілому, це не позначиться на загальній роботі системи. Згадане використання ботнетами «розумних» пристроїв, що працюють в IoT-системах, стало можливим внаслідок їх слабкої захищеності. Розподілений тип довірчих відносин дозволяє позбутися "зламаного" пристрою без відчутного збитку для всієї моделі взаємодії між "здоровими" об'єктами.

Найголовнішою проблемою на сьогоднішній день є відсутність стандартів в цій галузі, що ускладнює можливість інтеграції пропонованих на ринку рішень і багато в чому стримує появу нових. Необхідно впровадити механізми сертифікації пристроїв IoT як необхідну умову їх безпечного, безперебійного функціонування, що включають зменшення складності сертифікації, а процес сертифікації програмного та апаратного забезпечення, сертифікація зв'язку та захисту персональних даних має бути забезпечений відповідним органом.

Наявність величезної мережі, яка контролює весь навколишній світ, глобальна відкритість даних та інші особливості можуть мати і негативні наслідки.

IoT є динамічно зростаючою галуззю інтернет комунікацій, безумовно дана технологія приносить в життя людей безліч плюсів, таких як миттєві покупки товарів (Amazon Button), контроль якості повітря (Air Quality Egg), боротьба з незаконною вирубкою лісів (Invisible Tracck) і таких прикладів можна знайти сотні тисяч. Кожен IoT пристрій модернізує завдання будь-якого роду діяльності. У всьому є свої плюси і мінуси, в даному випадку мінусом є відсутність стандартизації випуску IoT продукту і відсутність надійних систем безпеки.

УДК 004.932

Д.Г. Чурсінов, Т.О. Гріненко

danylo.chursinov@nure.ua, tetiana.grinenko@nure.ua

Харківський національний університет радіоелектроніки, Харків

МЕТОДИ ОБРОБКИ ТА ПОРІВНЯННЯ ЗОБРАЖЕНЬ ДЛЯ ВЕРИФІКАЦІЇ ВІДБИТКІВ ПАЛЬЦІВ

Відбитки пальців є найбільш використовуваною біометричною технологією автентифікації. Актуальність використання відбитків пальця обумовлена широкою сферою застосування. Відбитки пальця використовуються для отримання доступу до мобільних телефонів, персональних комп'ютерів, оплати товарів і послуг та ін. Відбиток пальця є необхідним та застосовується у системах пропускного контролю на прикордонних постах та аеропортах.

Для алгоритма верифікації зображень відбитків пальців існує два основних етапи [1,2].

Перший етап – обробка вхідного зображення відбитка пальця. На сьогодні існує безліч методів для покращення якості зображення. Оскільки для багатьох задач програмної обробки зображень колір не грає важливої ролі, то можна виділити два основні методи для поставленої задачі, які було розглянуто у роботі – це бінаризація (порогова і адаптивна) та скелетизація (хвильовий метод, метод стоншення областей та шаблонний метод).

Другий етап – це вибір методу порівняння зображень відбитків пальців. В ході роботи розглянуто та проаналізовано основні алгоритми порівняння, які застосовуються на сьогодні, а саме: порівняння за візерунком, кореляційне порівняння, алгоритм порівняння шаблонів та порівняння на основі пошуку особливих точок.

В результаті дослідження у якості методу верифікації зображень відбитків пальців було обрано алгоритм порівняння відбитків на основі пошуку особливих точок. У ході порівняння алгоритмів верифікації зображень відбитків пальця було з'ясовано, що головною перевагою даного алгоритму є відносна швидкість його роботи. Алгоритм не потребує складних математичних розрахунків. В силу простоти реалізації і швидкості роботи алгоритми даного класу є найбільш поширеними на сьогодні. Недоліком даного методу порівняння зображень відбитків пальців за допомогою особливих точок є відносно високі вимоги до якості зображення, отримуваного при скануванні відбитка, тому даний метод потребує подальшої обробки отриманого зображення.

При подальшій обробці зображення на першому етапі здійснюється бінаризація зображення. Оскільки зображення на вході зазвичай є рівномірно освітленим та одразу у градаціях сірого кольору, то для його бінаризації було обрано пороговий метод. Даний метод добре працює з рівномірно освітленим зображенням та за часом роботи є більш швидким, ніж адаптивний метод.

Наступним етапом роботи є скелетизація зображення. При аналізі методів скелетизації, було зроблено висновок, що найбільш простим за своєю реалізацією є шаблонний метод скелетизації. У той же час, даний метод є найбільш швидким за часом роботи, оскільки він потребує лише одного обходу зображення, але для того, щоб знизити ймовірність утворення шумових пікселів рекомендується робити повторний обхід зображення за допомогою додаткових шаблонів.

Як результат роботи був розроблений найбільш оптимальний варіант алгоритму верифікації відбитка пальця для програмної реалізації (рис.1).

Рис. 1. Алгоритм верифікації відбитка пальця

В роботі розглянуті алгоритми порівняння та методи обробки зображень відбитків пальців. Наведено переваги та недоліки для найпоширеніших методів.

Список літератури

[1] В. Задорожный, "Идентификация по отпечаткам пальцев", PC Magazine/Russian Edition, № 2, 2004.

[2] J. L. Pfalz, and A. Rosenfeld, "Computer Representation of Planar Regions by their Skeletons", Communications of the Association for Computing Machinery, vol. 10, no. 2, p.119 – 125, 1967.

УДК 004.9

Д.В. Шингалов, В.В. Босько, Є.В. Мелешко

dimashingalov@gmail.com, victorvv2@ukr.net, elismeleshko@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ МОДЕЛЕЙ РЕПУТАЦІЇ КОРИСТУВАЧІВ СОЦІАЛЬНОЇ МЕРЕЖІ

При моделюванні соціальних мереж виникає необхідність врахування взаємного впливу їх членів, динаміки їх думок. Вплив – процес і результат зміни індивідом (суб'єктом впливу) поведінки іншого суб'єкта (індивідуального або колективного об'єкта впливу), його установок, намірів, уявлень і оцінок в ході взаємодії з ним. Можливості впливу одних членів соціальної мережі на інших її членів суттєво залежать від репутації перших. Репутація – це загальна думка про переваги чи недоліки кого-небудь, чого-небудь, або ж громадська оцінка. Репутацію можна розглядати, по – перше, як очікувану (управління в соціальних і економічних системах іншими агентами) норму діяльності агента, тобто якої поведінки від нього очікують інші. По – друге, як вагомість думки агента, яка визначається виправданістю його суджень і/або ефективністю його діяльності. Репутація виправдовується і, як правило, зростає, якщо вибір агента (його судження, дії і т.п.) збігається з тим, чого від нього очікують інші і/або з тим, що інші згодом вважають нормою.

Репутація може і знижуватися, наприклад, при порушенні суб'єктом прийнятих в співтоваристві норм поведінки, при прийнятті неефективних рішень і т.д. Треба зазначити, що репутація може бути як індивідуальною, так і колективною.

Оцінка показнику репутації індивідуального користувача заснована на наступних трьох компонентах:

– особисті атрибути, включаючи професію, рівень освіти, асоційовані групи, вибране, інтереси або політичну схильність, соціальну ідентичність;

– особисті заходи, що представляють якість та кількість взаємодій з іншими друзями через публікації, лайки, твіти, створення інтересів групи;

– характеристики, пов'язані з особами друзів із зазначенням кількості взаємодій з друзями та рівнем репутації друзів.

Перший компонент називається індивідуальними атрибутами, а інші два компоненти – реляційними атрибутами. Чим вище репутація агента, тим більше його можливості по впливу на підсумкову думку агентів в соціальній мережі. Поняття репутації тісно пов’язане з поняттям довіри. Довіра – це соціально-психологічний стан, що характеризується упевненістю більшої або значної частини агентів в сумлінності, щирості лідерів спільнот, правильності їх дій.

Для довіри характерні наступні властивості:

- Суб’єктивна: оскільки кожна людина має свою думку, засновану на власному суб'єктивному погляді, різні окремі особи можуть мати різні погляди на одну і ту ж ситуацію;

– Асиметрична: для двох суб'єктів, пов'язаних дружніми відносинами, довіра не обов'язково рівнонаправлена.

– Неперехідна: довіра не є повністю транзитивною або тою, що можна передати. Хоча довіра у спілкуванні в мережі раніше була перехідною за допомогою Інтернету, це вже не є актуальним для соціальних мережах, де суб'єкт є людиною і може мати різне суб'єктивне сприйняття чи пізнання при обробці інформації.

– Динамічна: довіра занепадає з часом без постійних взаємодій або змін за допомогою зміни контексту. У соціальних мережах коливання якості і кількість взаємодій перешкоджають безперервній еволюції довіри.

– Контекстно-залежна: довіра часто залежить від контексту. Наприклад, хоча ви можете довіритися механіку (в контексті кріплення автомобіля), ви б не довірили йому зробити операцію на вашому серці (в контексті медичної проблеми). Один загальний підхід до розгляду контексту передбачає створення окремого рейтингу довіри для кожного можливого контексту.

Дослідження моделей інформаційного впливу і репутації агентів, зокрема, дає можливість досліджувати залежність поведінки суб'єкта від його інформованості та, отже, від інформаційних впливів. Маючи модель репутації та/або інформаційного впливу, можна ставити і вирішувати завдання інформаційного управління: якими мають бути інформаційні впливи (з точки зору керуючого суб'єкта), щоб добитися необхідної поведінки від керованого суб'єкту. І, нарешті, вміючи вирішувати завдання інформаційного управління, можна моделювати інформаційне протиборство – взаємодію декількох суб'єктів, що володіють незбіжними інтересами і здійснюють інформаційні впливи на один і той же керований суб'єкт.

Список літератури

[1] J. Cho, A. Swami, and I. Chen, “A survey of trust management in mobile ad hoc networks”, IEEE Communications Surveys and Tutorials, vol. 13(4), 2016.

[2] T. Hossmann, F. Legendre, G. Nomikos, and T. Spyropoulos, “Stumbl: Using facebook to collect rich datasets for opportunistic networking research”, In Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks(WOWMOM), p. 1 – 6, 2011.

УДК 004.056.5

Д.В. Щербина, Т.О. Гріненко

dexxxed.app@gmail.com, tetiana.grinenko@nure.ua

Харківський національний університет радіоелектроніки, Харків

КВАНТОВІ АТАКИ НА ЦИФРОВІ ПІДПИСИ BITCOIN

Цифрові підписи в Bitcoin виконуються на основі алгоритму Elliptic Curve Digital Signature Algorithm (ECDSA) з використанням кривої secp256k1. Захищеність цієї системи ґрунтується на складності проблеми дискретного логарифмування у групі точок еліптичної кривої (ECDLP). Ця проблема вважається класично складною. Для вирішення цієї проблеми Шором був наданий ефективний квантовий алгоритм [1]. З використанням цього алгоритму квантовий комп'ютер зможе ефективно обчислити приватний ключ користувача, знаючи відкритий ключ (Bitcoin-адресу користувача), що робить схему цифрового підпису абсолютно незахищеною.

Основними вразливостями, які можуть бути використані при реалізації атаки на підписи в мережі Bitcoin, є:

1. Повторне використання адреси. Для того, щоб витратити Bitcoin з будь-якої адреси, необхідно дізнатися відкритий ключ, що пов'язаний з цією адресою. При знанні відкритого ключа і при наявності квантового комп'ютера, використання тієї ж адреси вже не є безпечним і тому ця адреса ніколи більше не повинна використовуватися. Хоча використання нової адреси – вже є класичною практикою в мережі Bitcoin, але на практиці цієї вимоги не завжди дотримуються. Будь-яка адреса, яка має певну кількість Bitcoin, і щодо якої відомий відкритий ключ, є абсолютно небезпечною.

2. Оброблені транзакції. Якщо транзакція робиться за адресою, з якої раніше не витрачувалися Bitcoin, і ця транзакція розміщується у блокчейні з кількома блоками, що слідують за нею, то ця транзакція є достатньо захищеною від квантових атак.

3. Неопрацьовані транзакції. Після трансляції транзакції в мережу, але до того, як вона буде розміщена у блокчейні, існує загроза квантової атаки. Якщо секретний ключ може бути отриманий з відкритого ключа за транзакцією, розміщеною в блокчейні, то зловмисник може використовувати цей секретний ключ для трансляції нової транзакції з тієї ж адреси на свою власну адресу. Якщо зловмиснику вдасться розмістити власну нав'язану транзакцію у блокчейні першою за пріоритетом, тоді він зможе ефективно викрасти весь Bitcoin за вихідною адресою.

В результаті аналізу можна зробити висновок, що атака, яка використовує неопрацьовані транзакції є найімовірнішою. Для визначення ймовірності цієї атаки необхідно точно оцінити час вирішення задачі ECDLP квантовим комп'ютером, і чи буде цей час близьким до часового інтервалу генерації блоків.

Для n бітного простого поля, використовуючи оптимізований алгоритм, квантовий комп'ютер може вирішити задачу ECDLP за допомогою $9n + 2\left\lceil \log_2(n) \right\rceil e + 10$ логічних кубітів та $\left(448\log_2(n) + 4090\right)n^2$ воріт Тофолі [2]. Bitcoin використовує n=256 бітові підписи, що в кількості воріт Тофолі дорівнює $1{,}28\text{x}10^{11}$, а при розпаралелюванні дорівнює $1{,}16\text{x}10^{11}$.

При майнінгу блоків домінуючий час споживається дистиляцією магічних станів для логічних $\mathbf{T}$ воріт. Час вирішення ECDLP на квантовому процесорі:

$$\tau = 1{,}28 \times 10^{11} \times c_\tau \left(p_g\right) / s,$$

де час накладних витрат c_τ залежить лише від швидкості помилки воріт, а s – тактова швидкість.

Кількість необхідних фізичних кубітів дорівнює:

$$n_q = 2334 \times c_{n_{ij}} \left(p_g\right),$$

де перший коефіцієнт – кількість логічних кубітів, включаючи 4 логічні кубіти асілла, а $c_{n_{ij}}$ – простір поля.

Із використанням так званого "surface code" зі швидкістю помилки фізичного затвора $p_q = 5 \times 10^{-4}$, коефіцієнтами c_τ =219,7 та $c_{n_{ij}}$ =735,3, час для вирішення задачі ECDLP на тактовій частоті 66 МГц буде становити 6,5 діб, із використанням $1{,}7\text{x}10^6$ фізичних кубітів. Для тактової частоти 10 ГГц та частоти помилок 10^{-5} підпис буде зламаним за 30 хвилин із використанням 485550 кубітів [3]. Враховуючи ці дані можна зробити висновок, що атака з використанням неопрацьованих транзакцій є цілком можливою, що робить систему Bitcoin небезпечною.

Список літератури

[1] P.W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Review, vol. 41, no. 2, p. 303-332, 1999.

[2] M. Roetteler, "Quantum resource estimates for computing elliptic curve discrete logarithms". [Online]. Available: arXiv:1706.06752. Accessed on: May 19, 2017.

[3] D. Aggarwal, "Quantum attacks on Bitcoin, and how to protect against them". [Online]. Available: arXiv:1710.10377. Accessed on: May 19, 2017.

СЕКЦІЯ 2
ПРОГРАМУВАННЯ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004. 056. 55

О. А. Борисенко, А. О. Горішняк, В. В. Сердюк, М. М. Яковлєв, М. С. Єрмаков

5352008@ukr.net, a.horishnyak@ias.sumdu.edu.ua

Сумський державний університет, Суми

ОЦІНКА ЗАВАДОСТІЙКОСТІ РІВНОВАЖНИХ КОДІВ

Засоби обчислювальної техніки знаходять все більше застосування в різних галузях промисловості та господарства. Рівень складності і значущості завдань, покладених на електронні та обчислювальні пристрої та системи, в ряді випадків вкрай високий. Наслідки в результаті відмов технічних засобів через вплив перешкод можуть становити суттєві матеріальні втрати, нести загрозу безпеці та життю користувача. Дослідження питань стійкості засобів обчислювальної техніки до завад є необхідним та актуальним аспектом розвитку сучасної техніки.

Робота спрямована на проведення оцінки ефективності рівноважних кодів для захисту двійково-десяткової числової інформації від завад. Вона дозволить перевірити ефективність роботи системи передачі числових, даних представленої у статті [1].

Рівноважний код – це двійковий код в якому комбінації містять k одиниць і n-k нулів, де n довжина коду. Особливістю рівноважних кодів є можливість швидко та ефективно знаходити помилки під час обробки інформації. Оскільки рівноважний код складається з двійкових чисел, які містять k одиниць і n-k нулів можна легко знайти помилку в процесі передачі даних. Ознакою помилки є перевищення числа n-k нулів або k одиниць. Так, наприклад в роботі [1] використовується завадостійкий код в основу якого покладені рівноважні коди, які складаються з 2 одиниць та 3 нулів. Вони допомагають зашифрувати двійково-десяткові цифри від 0 до 9. Тут ми маємо k = 2, n = 5 для кожної кодової комбінації. Наприклад, для цифри 0 була взята рівноважна комбінація 00011. Отже якщо кількість одиниць в комбінації буде перевищувати 2 – це буде ознакою її помилки.

Для оцінки завадостійкості рівноважних кодів були використані формули імовірностей переходів кодових комбінацій [2].

Для правильного переходу:

$$\prod = \sum_{i=1}^{M} P_i p_i^i \ ,$$

де P_i – імовірність генерування джерелом інформації і кодової комбінації;

p_i^i – імовірність правильного переходу і кодової комбінації в і-у.

Імовірність помилкових переходів кодових комбінацій, які не виявляються:

$$\bigcup = \sum_{i=1}^{M} P_i p_i^H \ ,$$

де $Z = \sum_{i=1}^{M} P_i p_i^o$ – імовірність помилкового переходу і-ї комбінації в клас комбінацій, які не виявляються, визначається за формулою:

$$p_i^H = \sum_{j=1, j=i}^{M} p_{i,j}^H \ ,$$

де $p_{i,j}^H$ – імовірність помилкового переходу і-ї комбінації, що передається, в j-у дозволену.

Імовірність помилкових переходів які можна виявити:

$$Z = \sum_{i=1}^{M} P_i p_i^o \ ,$$

де p_i^o – імовірність помилкового переходу і-ї комбінації, що передається, в клас комбінацій, які можна виявити. Її можна визначити за формулою:

$$p_i^o = \sum_{j=M+1}^{N} p_{i,j}^o \ ,$$

де $p_{i,j}^o$ – імовірність помилкового переходу для і-ї кодової комбінації.

Основними задачами дослідження є:

1) Аналіз методу захисту інформації від завад за допомогою рівноважних кодів.

2) Побудова програмної моделі досліджуваного методу.

3) Оцінка ефективності методу.

Отримані результати і рекомендації носять універсальний характер і можуть бути застосовані і використані для різних систем зв'язку і технічних пристроїв підприємств і установ.

Список літератури

[1] О. А. Борисенко, О. В. Бережна, А. І. Новгородцев, В. В. Сердюк, та М. М. Яковлев, “Система передачі та відображення інформації із захистом числових даних”, Системи обробки інформації, вип. 2, с. 103 – 108, 2019.

[2] А. А. Борисенко, О. В. Бережная, и И. А. Кулик, “Оценка помехоустойчивости системы передачи данных на основе равновесных кодов”, Вісник Сумського державного університету, №1(12), с. 79 – 82, 1999.

УДК 681.3

О.О. Гайша, В.А. Навроцький

oleksandrgaysha1982@gmail.com

Міжнародний класичний університет ім. Пилипа Орлика, Миколаїв

УРАХУВАННЯ ОСОБЛИВОСТЕЙ ЗДІЙСНЕННЯ ПОМИЛОК КОРИСТУВАЧЕМ ПРИ КОНТРОЛІ КЛАВІАТУРНОГО ПОЧЕРКУ В СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Як було встановлено у попередніх дослідженнях (див. напр. [1]), контроль особистості користувача системи дистанційного навчання (ДН) є важливою складовою всього комплексу засобів захисту інформації у ній. Доступним рішенням у галузі зведення систем контролю доступу (СКД) є використання біометричних поведінкових методів, таких як контроль клавіатурного почерку. Розробці відповідних засобів присвячено чимало досліджень, у яких найчастіше пропонується оцінювати час набору більш-менш поширених біграм, а трохи рідше – час утримання часто вживаних (або усіх) літер алфавіту. В той же час існують і інші, більш витончені показники, що також можуть використовуватися для клавіатурної автентифікації.

Пропонується у якості додаткової характеристики, що, як свідчать результати даного дослідження, покращує показники якості кінцевої СКД, використати особливості здійснення помилок користувачем при наборі тексту на клавіатурі ПК. А саме, за основний показник тут можна взяти інтенсивність здійснення друкарських помилок, тобто невірного набору. Так, загальновідомо, що будь-який оператор технічного пристрою (в т.ч. і звичайний пересічний користувач ПК) в процесі роботи може робити помилки, що, зокрема, залежить від його ступеня володіння ПК в цілому. Втім, іноді люди, що дуже повільно набирають текст, роблять це занадто ретельно, і практично не вносять помилок, правда, набираючи при цьому всього лише кілька букв за хвилину. Але і в цьому випадку інтенсивність виникнення помилок можна використовувати як елемент автентифікації, але важливо, щоби цей показник контролювався в комплексі з раніше згаданими, і тоді він може дати досить корисні результати у всій методиці оцінки.

При комп'ютерному наборі кількість помилок можна оцінювати за двома напрямками:

– помилки, які виникли в процесі набору, але були помічені і виправлені;

– помилки, які виникли в процесі набору і не були помічені або були помічені, але з якоїсь причини не були виправлені.

Помилки другого типу контролювати автоматично досить складно з алгоритмічної точки зору, тому у подальшому будемо говорити тільки про помилки першого типу: такі, що виправляються відразу ж під час набору тексту користувачем. Виправляти помилки можна по-різному, однак найпоширенішим при послідовному наборі тексту є натискання клавіші BackSpace кілька разів, щоб стерти останні, набрані невірно, символи і дістатися до помилки (кнопка Delete зазвичай розташована трохи менш зручно, і сам принцип її дії менше підходить для набору тексту: її краще використовувати при редагуванні раніше введених відомостей).

Отже, кількість виправлених помилок може бути оцінена по натисненням на кнопку Backspace. В цьому випадку потрібно враховувати тільки одне з декількох поспіль натискань кнопки повернення, що випливає з таких міркувань. Середній користувач набирає текст не по одному символу, а групами. Якщо в групі символів є хоча б одна помилка, користувач знайде її не відразу, а тільки після набору всієї групи, коли подивиться на екран. Як вже зазначалося раніше, зазвичай помилка виправляється відразу, шляхом натискання кілька разів клавіші Backspace для того, щоб повернутися до символу, який містить помилку. Таким чином, всі ці численні натискання викликані однією помилкою, і тому усі натискання Backspace, що ідуть поспіль, повинні асоціюватися з однією помилкою. Ще один варіант виправлення помилки – стрілками "вліво" – "вправо" на клавіатурі встановити курсор безпосередньо справа від неправильного символу і натиснути Backspace один раз. При цьому одній виправленій помилці відповідає одне натискання кнопки повернення.

Отже, без суттєвої втрати точності можна вважати, що одній помилці, допущеній при комп'ютерному наборі тексту, відповідає від 1 до M поспіль натискань на кнопку Backspace. Абсолютне число помилок E ділимо на загальне число набраних символів All, щоб перейти до відносного числа помилок, яке і можна порівнювати з еталоном:

$$R = \frac{E}{All}.$$

Додавання цього показника до тривалостей набору окремих біграм та утримання окремих клавіш показало покращення традиційних для СКД показників FAR та FRR на величину до 7%.

Список літератури

[1] О. О. Мочалов, О. О. Гайша, Є. С. Лєнков, та Л. О. Ряба, "Комплексне забезпечення безпеки систем дистанційної освіти", Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка, № 7, с. 128 – 131, 2007.

УДК 681.3

С.В. Герасимов[1], М.В. Грекуляк[2]

gsvnr@ukr.net, grekuliak@ukr.net

[1]Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків
[2]Льотна академія національного авіаційного університету, Кропивницький

МОДЕЛЬ ВЗАЄМОЗАЛЕЖНОСТІ МІЖ ЧУТЛИВІСТЮ ТА ТОЧНІСТЮ КОНТРОЛЮ ПАРАМЕТРІВ РАДІОЕЛЕКТРОННОГО ОБЛАДНАННЯ ЛІТАЛЬНИХ АПАРАТІВ

Процес контролю технічного стану радіоелектронного обладнання (РЕО) літальних апаратів (ЛА) полягає у дії на вхід їх складових блоків відомим вимірювальним (тестовим) сигналом $u(t)$, який формується генератором тестових сигналів і має певні характеристики [1]. Під впливом вхідного вимірювального сигналу $u(t)$ на виході зразка, що контролюється, утворюється вихідний сигнал (сигнал-відгук) $y(t)$, або реакція певної форми залежно від форми вхідного сигналу та параметрів контролю. Вхідний $u(t)$ і вихідний сигнали $y(t)$ подаються в аналізатор, за допомогою якого визначаються параметри контролю РЕО q_j, $j=\overline{1,n}$, де n – кількість параметрів контролю, або апостеріорні параметри z_i, $i=\overline{1,m}$, m – апостеріорна кількість параметрів контролю, значення яких дозволяють визначити технічний стан системи, що контролюється [1].

Розглянуто фізичну причину протиріччя між забезпеченням максимальної чутливості контролю та необхідною точністю визначення параметрів на прикладі, коли параметри РЕО q_j ортонормовані, параметри $z_i=\sum_{j=1}^{n}\alpha_{ij}q_j$ співпадають з ними, тобто матриця з елементами узгодження α_{ij} – одинична.

У цьому випадку чутливість контролю S' дорівнює сумі діагональних елементів кореляційної матриці $\tilde{R}_y : S' = \sum_{i,j=1}^{n}\left(\tilde{R}_y\right)_{ij}$, елементи матриці $\tilde{R}_y$ дорівнюють: $\left(\tilde{R}_y\right)_{ij}=\int_0^T a_i(t)a_j(t)dt+\sigma_\xi{}^2\xi_{ij}$, де $a_i(t)$ – коефіцієнти перетворення, $a_j(t,\{u\})=\frac{\partial\Delta y}{\partial q_j}$; $\xi_{ij},\sigma_\xi{}^2$ – перешкода, яка присутня при вимірюванні i-го і j-го параметрів, і її середньоквадратичне відхилення відповідно [2].

При значному часі контролю T перший член більше другого і $\left(\tilde{R}_y\right)_{ij}\approx\int_0^T a_i(t)a_j(t)dt$. Позначимо власні значення матриці $\tilde{R}_y$ через λ_j, $j=\overline{1,n}$. Тоді величина чутливості буде дорівнювати: $S'=\sum_{j=1}^{n}\lambda_j$. Точність визначення параметрів ε пропорційна в даному випадку сумі діагональних елементів матриці $\tilde{R}_y{}^{-1}$, тобто $\varepsilon=\sigma_\xi{}^2\sum_{j=1}^{n}\frac{1}{\lambda_j}$.

Нехай максимальна чутливість досягається при такому співвідношенні між власними значеннями λ_j, коли частина їх дуже мала, в той час як інші значні, так що сума $\sum_{j=1}^{n}\lambda_j$ максимальна. Тоді похибка ε стане дуже значною, а чутливість S – незначною. Якщо, наприклад, $\lambda_j\to 0$, то $\varepsilon\to\infty$, а $S\to-\infty$. Така ситуація буде виникати тоді, коли детермінант матриці $A_{ij}=\int_0^T a_i(t)a_j(t)dt$ дорівнює або прагне до нуля, так як при цьому добуток власних значень $\prod_{j=1}^{n}\lambda_j$ буде близьким до нуля, а деякі з власних значень будуть прагнути нулю.

Висновок. Оптимальний за чутливістю вимірювальний сигнал призводить до різкого зниження точності вимірювання параметрів при контролі РЕО ЛА. Такий випадок має місце, коли час контролю значно переважає час перехідного процесу. Для отримання достатньої точності при одночасному забезпеченні високої чутливості необхідно в даному випадку використовувати сигнал, який складається з гармонійних складових, кількість яких дорівнює половині параметрів контролю блоку РЕО ЛА.

Список літератури

[1] В. Н. Чинков, и С. В. Герасимов, “Комплексная методика оптимизации контролируемых параметров сложных технических объектов”, Украинский метрологический журнал, № 1, с. 11 – 15, 2003.

[2] В. М. Чинков, та С. В. Герасимов, “Варіаційний метод і методики синтезу оптимального вимірювального сигналу для контролю технічного стану САУ, Український метрологічний журнал, № 1, с. 59 – 64, 2014.

УДК 621.37/.39

І. Г. Гусарова, Р. В. Ревегук

iryna.husarova@nure.ua, roman.revehuk@nure.ua

Харківський національний університет радіоелектроніки, Харків

РЕЗУЛЬТАТИ ЧИСЕЛЬНОГО МОДЕЛЮВАННЯ НЕСТАЦІОНАРНИХ РЕЖИМІВ З ВИКОРИСТАННЯМ СПРОЩЕНОГО МЕТОДУ НЬЮТОНА

Однією з важливих задач, що виникають при експлуатації лінійних ділянок газотранспортної системи, є ефективне управління режимами транспорту газу в нештатних та аварійних ситуаціях. Режим течії газу в цих ситуаціях є нестаціонарним та неізотермічним.

Найпопулярнішим серед чисельних методів для розрахунку таких режимів є метод скінченних різниць з використанням неявних скінченно-різницевих схем. Підвищити ефективність даного методу можна, наприклад, за рахунок застосування ефективних чисельних методів на етапі вирішення нелінійної системи скінченно-різницевих рівнянь.

Мета роботи передбачає з'ясування можливості використання спрощеного методу Ньютону при розв'язанні системи нелінійних рівнянь (СНР), яка виникає на етапі розв'язання системи рівнянь математичної моделі нестаціонарних неізотермічних режимів течії газу (ННРТГ) по ділянці трубопроводу, з застосуванням методу скінченних різниць та використанням нерівномірної скінченно-різницевої сітки (НКРС). Для вирішення СНР можна використовувати метод Зейделя, різні модифікації методу Ньютона, метод Бройдена та інші. Зазвичай таку систему вирішують за допомогою методу Ньютона, який має квадратичну збіжність, спрощений метод Ньютона хоча і має тільки лінійну збіжність, але передбачає розрахунок матриці Якобі тільки на початковій ітерації.

У загальному випадку ННРТГ описуються квазілінійною системою диференціальних рівнянь гіперболічного типу з відомим початковими і граничними умовами (ПГУ). Ця система у загальному вигляді має вид [1]:

$$\frac{\partial \varphi}{\partial t} + B(x,t,\varphi)\frac{\partial \varphi}{\partial x} = F(x,t,\varphi), \quad (1)$$

де B, F – матриці, елементи яких задані неперервні та безперервно-диференційовані функції.

Щоб отримати чисельний розв'язок системи (1) з ПГУ використаємо НКРС [1]. Для цього розділимо відрізок $[0, L]$ на n відрізків, довжиною Δx, а потім перший і останній відрізки навпіл. Отримаємо $n+2$ відрізка. Перший, другий, останній і передостанній довжиною $\frac{\Delta x}{2}$, інші довжиною Δx, а також $n+3$ точки розбиття x_i, $i = \overline{0, n+2}$.

Підставляємо в дану систему (1) апроксимацію похідних і отримуємо систему нелінійних алгебраїчних рівнянь. Для проміжних точок рівняння мають вигляд

$$-\frac{1}{2\Delta x}B_i^k \varphi_{i-1}^k + \frac{1}{\Delta t}\varphi_i^k + \frac{1}{2\Delta x}B_i^k \varphi_{i+1}^k = F_i^k + \frac{1}{\Delta t}\varphi_i^{k-1},$$
$$i = \overline{3, n-1}.$$

Ці рівняння доповнюються рівняннями для 0-ї, 1-ї, 2-ї точок, а також рівняннями для n-ї, $(n+1)$-ї, $(n+2)$-ї точок розбиття.

Нелінійні системи будемо розв'язувати спрощеним методом Ньютона. На S-й ітерації отримуємо лінійну систему рівнянь, яка в загальному вигляді має вид:

$$\left[\frac{\partial \psi^k}{\partial \varphi^k}\right]_{\varphi^{k,0}} \delta\varphi^{k,s} = \psi^{k,s-1},\ s = 1, 2...,$$

де $\varphi^{k,s}$ – вектор розв'язку системи на s-й ітерації; $\left[\frac{\partial \psi^k}{\partial \varphi^k}\right]_{\phi^{k,0}}$ – матриця Якобі; $\psi^{k,s-1}$ – вектор нев'язок на (S-1)-й ітерації; $\delta\varphi^{k,s}$ – вектор поправок до невідомих на S-й ітерації, отже, $\varphi^{k,s} = \varphi^{k,s-1} - \delta\varphi^{k,s}$.

В результаті чисельного моделювання ННРТГ у математичному пакеті Mathematica 11.3 з використанням спрощеного методу Ньютона на етапі розв'язку системи нелінійних рівнянь був показаний задовільний результат.

Результати даного дослідження будуть корисні, зокрема, для повної автоматизації процесу постачання газу, і, як наслідок, зменшення кількості аварій.

Список літератури

[1] И. Г. Гусарова, и Д. В. Мелиневский, "Численное моделирование режимов течения газа методом конечных разностей", Системи Обробки Інформації: збірник наукових праць, №4(141), с. 23 – 27, 2016.

УДК 004.94

Г.М. Дрєєва, С.А. Смірнов, О.К. Конопліцька-Слободенюк

gannadreeva@gmail.com, smirnov.ser.81@gmail.com, ksuha80@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ ГЕНЕРАТОРА САМОПОДІБНОГО ТРАФІКУ НА ОСНОВІ ЛАНЦЮГА МАРКОВА ТА ЙОГО МУЛЬТИФРАКТАЛЬНИХ ВЛАСТИВОСТЕЙ

В даній роботі проведено дослідження фрактальної розмірності часового ряду, який отримано за допомогою генератора самоподібного трафіку на основі ланцюгів Маркова з керованою фрактальною розмірністю. Предметом вивчення у статті є фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова.

Для математичного опису телекомунікаційних процесів використовують математичні моделі самоподібного часового ряду. На графіках, де зображена завантаженість каналу комп'ютерної мережі самоподібність виражена наявністю викидів, кількість яких перевищує за передбачення класичної статистичної теорії, де на горизонтальній вісі показаний час в умовних одиницях, а по вертикалі завантаженість мережі відносно максимальної пропускної спроможності

Метою роботи є дослідження фрактальної розмірності часового ряду, який отримано за допомогою генератора самоподібного трафіку на основі ланцюгів Маркова з керованою фрактальною розмірністю.

Для цього у роботі були вирішені наступні задачі:

– на основі числових експериментів визначення фрактальної розмірності генерованих числових послідовностей, показано статистично значимі зміни фрактальних властивостей числової послідовності на різних масштабах;

– вказано на недостатній розвиток високопродуктивних алгоритмів отримання самоподібних числових послідовностей для імітаційного генерування трафіку в телекомунікаційних системах та мережах;

– запропоновано напрями подальших досліджень щодо керування явищем мультифрактальності в генераторах, які основані на ланцюгах Маркова.

В більшості випадків для самоподібного трафіку, передбачення параметрів за якістю обслуговування QoS, аналітичні вирази побудувати не вдається, або такі перетворення можливо побудувати для занадто специфічних ситуацій, тому переважно аналітичні викладки є недоцільними. З цієї причини для визначення основних показників якості обслуговування, таких як джитер, запізнення, середня кількість відмов, та інших, використовують імітаційне моделювання за допомогою генераторів самоподібного трафіку.

Це призводить до потреб в простих, з точки зору кількості обчислень, генераторів самоподібного трафіку з керованими фрактальними властивостями, які б давали числові послідовності з властивостями як можна ближчими до властивостей реального трафіку телекомунікаційної мережі, що досліджується.

З огляду актуальності виконання задачі керування фрактальними властивостями генерованого трафіку, робота присвячена визначенню залежності фрактальних властивостей моделі трафіку від використаного масштабування.

Результатом роботи є обґрунтування підвищення продуктивності імітаційного моделювання руху інформації в телекомунікаційних системах та комп'ютерних мережах за рахунок генератора самоподібного трафіку на ланцюгах Маркова.

Висновки:

– Генератори самоподібного трафіку на ланцюгах Маркова відрізняються від аналогів меншими вимогами до обчислювальної потужності систем моделювання, що дозволяє підвищити продуктивність імітаційного моделювання руху інформації в телекомунікаційних системах та комп'ютерних мережах, тому актуальним є подальший розвиток та вивчення таких систем.

– На основі спрощеної метрики $N(k\varepsilon)$ побудовано аналітичний вираз розрахування фрактальної розмірності результату генерування бінарного числового ряду на основі ланцюга Маркова.

– Відмічено залежність фрактальної розмірності від довжини проміжку, на якому проводиться розрахунок фрактальної розмірності, та зроблено припущення про повторення властивості мультифрактальності на класичних метриках, таких як рахування розмірності на основі R/S аналізу або розмірності Мінковського.

– З метою перевірки припущення було проведено чисельний експеримент, який з надійністю вищу за 99% підтвердив припущення про мультифрактальність числової послідовності, що отримана генераторами на ланцюгах Маркова.

– Робота може бути продовжена з метою розробки методів для керування параметрами мультифрактальності, або можливості усунення мультифрактальності в разі потреби.

УДК 004.4’233

О.С. Дробко, Д.А. Гахов

ms.alenas@gmail.com, danil@gahov.com

Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ ПЛАТФОРМИ ДЛЯ РОЗРОБКИ ДОДАТКІВ "FIREBASE", ЙОГО ПРАКТИЧНЕ ЗАСТОСУВАННЯ

Firebase – це інтегрована платформа Google для розробників, яка допоможе швидко створювати високоякісні додатки, розширювати базу зацікавлених користувачів і збільшувати прибутки. До платформи включено комплекс інтегрованих функцій, які можна поєднувати й суміщати, зокрема мобільний сервер, засоби аналітики, а також інструменти вдосконалення й монетизації для максимальної успішності додатків.

Підтримує iOS, Android, Unity, C++ та Web.

Щоб додати Firebase у додатки, необхідно виконати наступне:

1) зв’яжіть додатки із платформою Firebase;
2) інтегруйте SDK Firebase у свої додатки.

Основні служби Firebase:

– Firebase Analytics – рішення для оцінки застосунків, яке дає змогу ознайомитись із використанням застосунків та залученням користувачів.

– Firebase Cloud Messaging – це крос-платформове рішення для повідомлень і нотифікацій, які наразі можна використовувати безкоштовно.

– Firebase Auth – це служба, яка може аутентифікувати користувачів, використовуючи лише код на стороні клієнта. Він підтримує соціальні логін-провайдери Facebook, GitHub, Twitter, Google та Google Play Games. Крім того, вона включає в себе систему управління користувачами, за допомогою якої розробники можуть увімкнути автентифікацію користувача за допомогою входу з електронної пошти та пароля, що зберігаються в Firebase.

– Firebase Database – ця служба надає розробникам застосунків API, який дозволяє синхронізувати дані застосунків між клієнтами та зберігати їх у хмарі Firebase. База даних також доступна через REST API. Розробники, які використовують Realtime Database, можуть захищати свої дані за допомогою правил безпеки, що застосовуються на сервері.

– Firebase Storage – забезпечує надійне завантаження та вивантаження файлів для застосунків Firebase незалежно від якості мережі.

Розробник може використовувати його для зберігання зображень, аудіо-, відео- чи іншого вмісту, створеного користувачами. Зберігання Firebase підтримується Google Cloud Storage.

– Firebase Hosting&Functions – це статичний та динамічний веб-хостинг, який було запущено 13 травня 2014 року. Він підтримує хостинг статичних файлів.

Практичне використання

Слід зазначити те, що платформа дуже популярна серед розробників на ринку аутсорсу. Дійсно, як можна побачити, Firebase надає перелічені вище послуги, що є дуже зручним для швидкої та економної розробки програмного продукту.

В процесі роботи над доповіддю був обраний шлях практичного дослідження, а саме реалізації “demo”-проекту – невеликого мобільного додатку для обміну текстовими повідомленнями в режимі реального часу. Було створено одразу дві версії, для двох операційних систем: для Android і для iOS. Кожна з них будується виключно на вбудованих можливостях систем та засобах, що надають безкоштовні служб Firebase.

```
import UIKit
import Firebase
import GoogleSignIn
    func application(_ application: UIApplication,
        didFinishLaunchingWithOptions launchOptions:
        [UIApplication.LaunchOptionsKey: Any]?) -> Bool {
        FirebaseApp.configure()
        GIDSignIn.sharedInstance().clientID =
            FirebaseApp.app()?.options.clientID
        return true
    }
    func application(_ app: UIApplication, open url: URL,
        options: [UIApplication.OpenURLOptionsKey : Any]) ->
        Bool {
        return GIDSignIn.sharedInstance().handle(url,
            sourceApplication:options
            [UIApplication.OpenURLOptionsKey.sourceApplication]
            as? String, annotation: [:])
    }
```

Рис. 1. Інтеграція Firebase в додаток

УДК 004.7

Н. А. Єфременкова

n.efremenkova@gmail.com

Київський національний університет технологій та дизайну, ФРІІТ, Черкаси

ЧИННИКИ ЕФЕКТИВНОСТІ АДМІНІСТРУВАННЯ МЕРЕЖ

Однією із основних передумов інноваційного розвитку економіки України є розвиток ринку інжинірингу. Інжинірингові послуги щодо забезпечення ефективності діючого виробництва та реалізації виготовленої продукції включають не тільки роботи, спрямовані на оптимізацію процесів експлуатації, поліпшення функціонування технологічних ліній, поліпшення матеріально-технічного постачання, менеджменту та маркетингу, підбору і підготовки кадрів, рекомендації з фінансової політики. Значна доля успіху підприємства залежить від залучення до інформаційних систем

Основою для побудови сучасних інформаційних систем стали комп'ютерні мережі та мережеві технології обробки інформації. Локальні мережі останнім часом є обов'язковою приналежністю будь-якої компанії. В таких сферах як банківська справа, складські операції великих компаній, електронні архіви бібліотек просто неможливо обійтися без локальних мереж. В цих сферах кожна окремо взята робоча станція в принципі не може зберігати всієї інформації через занадто великий її обсяг. Фінансова, складська або бібліотечна інформація знаходиться в стані постійної зміни. В таких умовах підтримувати цілісність і точність декількох копій бази даних просто неможливо.

Створення та впровадження комп'ютерної мережі є складним комплексним завданням, яке вимагає узгодженого рішення та забезпечення можливості доступу користувачів до ресурсів загальної мережі. Забезпечити працездатність та безпеку комп'ютерної мережі здатне її адміністрування. Система адміністрування є сукупністю способів, засобів і технологій, що реалізують функції адміністрування мережі. Головною метою створення системи адміністрування є забезпечення виконання всіх функцій, передбачених переліком періодичних і епізодичних завдань адміністрування. Адміністратор мережі, який очолює службу адміністрування, повинен бути експертом з питань функціонування систем і мереж, вміти знаходити компроміс між вимогами користувачів та можливостями їх реалізації у системі. Правила, що розробляє системний адміністратор, повинні базуватися на трьох основних положеннях: максимальний доступ користувачів до власних ресурсів; максимальне обмеження доступу до ресурсів інших користувачів; відповідальність користувачів за збереження власних ресурсів. Для успішного адміністрування, особливо складними комп'ютерними мережами, необхідне застосування новітніх засобів і систем автоматизації цих процесів. Засоби адміністрування мереж є ефективним інструментом удосконалення управління роботи мережі, в тому числі в таких областях комп'ютерної мережі, як системне та мережеве адміністрування. Моніторинг мереж і сервісів є найбільш важливим інструментом підтримки безперебійної роботи підприємств. Зі збільшенням навантаження на мережу посилюються вимоги до швидкості обробки даних, роботи мережі, серверів, додатків і сховищ даних. Працездатність мереж можливо забезпечити в разі постійного контролю і аналізу роботи компонентів інфраструктури. Саме тому рішення моніторингу мережі, роботи додатків і серверів життєво необхідні для сучасного бізнесу. Гарантію максимально продуктивної роботи мережі забезпечить наявність точної схеми і документації мережі, поточної топологічної схеми ланцюга і докладної інформації про мережеве обладнання, його конфігурації, протоколи, IP-адреси, канали зв'язку WAN, сервери і сегменти для користувачів локальних мереж. Створення базової лінії дозволяє оцінювати роботу мережі в поточний момент. Важливо, щоб зміни в налаштуванні мережі були обґрунтовані та задокументовані. Простіша топологія сприяє зменшенню часу на пошук проблем, що виникають, сприяє підвищенню безпеки завдяки контролю за маршрутизаторами. Засобами оптимізації роботи мережі є сучасне обладнання і конфігурації програм. Джерелами покращення роботи мережі є достатня оперативна пам'ять серверів, потужність процесорів. Сегментація мережі також є важливим чинником, вона розбиває її на окремі функціональні ланки, підвищуючи тим самим загальну продуктивність, безпеку і надійність.

Ефективність функціонування комп'ютерних мереж суттєво залежить від обслуговуючого і управлінського персоналу, програмно-апаратних засобів і технологій системи адміністрування і умов використання системи адміністрування [1]. Обслуговуючий персонал, фахівці підтримують повну і постійну працездатність комп'ютерної мережі, її високу продуктивність, безпеку, діагностику і відновлення, управління користувачами і вирішення виробничих проблем. Служба адміністрування мережі, що функціонує в складі служби технічної підтримки, має вирішальну роль.

Список літератури

[1] Адиль Омер Юсиф Мохаммед, 'Математическое моделирование и алгоритм оценки эффективности системы администрирования локальной компьютерной сети', дис. канд. техн. наук, каф. открытых информ. систем Моск. гос. ун-та эконом, стат. и информ., Москва, 2007.

УДК 519.81:621.372

А.А. Засядько

sagitta@bigmir.net

Черкаський навчально-науковий інститут ДВНЗ "Університет банківської справи"

СПОСОБИ СПРОЩЕННЯ ЗАДАЧІ НЕЛІНІЙНОГО ПРОГРАМУВАННЯ НА ОСНОВІ КЛАСИФІКАЦІЇ ОБМЕЖЕНЬ

Важливою проблемою задач нелінійного програмування (ЗНП) є те, що вони можуть містити велику кількість обмежень. В процесі розв'язання ЗНП може виявитися, що частину з цих обмежень можна було б відкинути, що значно спростило б початкову постановку ЗНП, тим самим, зменшивши її обчислювальну складність. Крім того, ЗНП можуть мати проблему багатоекстремальності, яку не завжди можна вирішити звичайними програмними засобами, що реалізують чисельно пошук оптимуму.

Багатокритеріальні методи оптимізації дозволяють ефективно вирішувати задачі досить широкого класу. Особливе місце в цих методах займає нелінійна схема компромісів або згортка А. Н. Вороніна, уведена в [1]. Відомо, що, на відміну від інших скалярних критеріїв, нелінійна схема компромісів дозволяє знайти оптимальний по Парето розв'язок, а у випадку опуклих частинних критеріїв – унімодальний (єдиний) розв'язок. Також НСК має властивість безупинної адаптації до різних ситуацій, у яких потрібно прийняти багатокритеріальний розв'язок.

Мета даної роботи – розробити різні способи спрощення задачі нелінійного програмування на основі нелінійної схеми компромісів (НСК) Вороніна.

В роботі наведені різні способи спрощення задачі нелінійного програмування. В цих задачах серед множини обмежень на допустиму область розв'язків можуть бути суттєві і несуттєві обмеження, які можна відкинути, що призведе до спрощення початкової постановки ЗНП. Компоненти початкової ЗНП, тобто її цільова функція і система обмежень розглядаються як частинні критерії в багатокритеріальній постановці ЗНП. Розглянуті різні скалярні згортки частинних критеріїв і проаналізовані їх можливості в спрощенні ЗНП. Приділено увагу механізму взаємній компенсації конфліктних частинних критеріїв, яка відбувається між ними в процесі оптимізації скалярної згортки [2].

Була додатково спрощена вже існуюча багатокритеріальна модель ЗНП. Представлення ЗНП великої розмірності більш складною багатокритеріальною задачею виправдане зниженням обчислювальної складності задач ЗНП. Здійснюється редукція ЗНП великої розмірності в ЗНП меншої розмірності, яку можна розв'язувати звичайними оптимізаційними методами. На відміну від інших скалярних критеріїв, нелінійна схема компромісів дозволяє знайти неполіпшуваний або оптимальний по Парето розв'язок, а у випадку опуклих частинних критеріїв – унімодальний (єдиний) розв'язок. Складна задача представляється простішою моделлю, вираженою системою рівнянь невеликої розмірності.

В роботі наведений спосіб сортування обмежень ЗНП за значущістю за допомогою багатокритеріальної постановки ЗНП на основі вже розробленого способу сортування частинних критеріїв в багатокритеріальній постановці задачі [3].

В роботі також розроблений алгоритм сортування обмежень ЗНП за значущістю за допомогою НСК. В даному випадку спрощення – зниження розмірності за допомогою відкидання обмежень, від яких розв'язок знаходиться далеко.

Наведемо переваги алгоритму сортування обмежень ЗНП, що здійснюється на основі класифікатора НСК:

1. Обмеження ЗНП сортуються за ступенем конфліктності з їх поділом на напружені і спокійні.

2. Початкова ЗНП спрощується, бо містить тільки обмеження, що конфліктують з цільовою функцією, що і показано в наведених прикладах.

Таким чином, використання скалярної згортки у вигляді нелінійної схеми компромісів у якості класифікатора обмежень дозволяє звести розв'язування складної задачі нелінійного програмування до простішої, тим самим зменшивши обчислювальну складність. В цьому способі спрощення використання скалярної згортки у вигляді нелінійної схеми компромісів – це не спосіб розв'язання ЗНП, а спосіб спрощення ЗНП великої розмірності в ЗНП малої розмірності, яка вирішується відомими методами.

Список літератури

[1] А. Н. Воронин, Ю. К. Зиатдинов, О. И .Козлов, и В. С. Чабаню, Векторная оптимизация динамических систем, Київ, Україна: Техніка, 1999.

[2] А. А. Засядько, "Зниження обчислювальної складності в задачі нелінійного програмування великої розмірност", Вісник УБС, №2(23), с. 158 – 162, 2016.

[3] А. А. Засядько, "Два этапа методики гибкой адаптации в задачах многокритериальной оптимизации", Вісник ЧДТУ, №.2, с. 14 – 17, 2002.

УДК 631.347

Ю.В. Здоровець[1], М.В. Мінзар[2], А.П. Плахтєєв[1]

j.zdorovets@csn.khai.edu, minzukrarnik@ukr.net, a.plahteev@csn.khai.edu

[1]Національний аерокосмічний університет ім. М.Є. Жуковського "ХАІ", Харків
[2]ТОВ "ВаріантАгроБуд", Харків

СИСТЕМА ВІДДАЛЕНОГО КЕРУВАННЯ КРУГОВОЇ ДОЩУВАЛЬНОЇ МАШИНИ НА БАЗІ ТЕХНОЛОГІЇ IoT

Прогнозоване збільшення чисельності населення та потреби в продуктах харчування останнім часом мотивує прийняття рішень у галузі інформаційних технологій у рамках підходів до точного сільського господарства. Тому, сільське господарство поступово перетворюється на високотехнологічну галузь, а застосування всіх технологій в сукупності забезпечує істотне підвищення ефективності господарства шляхом реалізації так званих систем точного землеробства.

Однак, вітчизняні виробники сільськогосподарської продукції та продовольства, в силу різних причин, в тому числі через низький рівень забезпеченості сучасними цифровими технологіями і технічним оснащенням, відстають від виробників провідних країн в таких значущих показниках як продуктивність праці, собівартість продукції на одного працівника, врожайність з одного гектара ін., не завжди можуть собі дозволити застосування розумних рішень. Впровадження сучасних інформаційно-технологічних рішень дозволить значно скоротити витрати, підвищити продуктивність праці і якість продукції. Інтернет речей (IoT) відіграє вирішальну роль у розумному сільському господарстві. Розумне землеробство – це нова концепція, оскільки датчики IoT здатні надавати інформацію про свої галузі сільського господарства.

Серед розробників спеціалізованих IoT-платформ для сільського господарства поширені такі світові гравці: Farmmobile, OnFarm і Farmers Business Network, Monsanto Company, Libelium, CLAAS, John Deere, Horsch. Деякі з них, наприклад, OnFarm базуються на універсальних IoT-платформах.

Сьогодні інноваційні технології в сільському господарстві впроваджуються точково, а не комплексно в основному великими агрохолдингами, але для стабільного повсюдного розвитку сільського господарства дані технології повинні бути досить доступними та зрозумілими для використання приватними підприємцями, фермерами та колгоспами.

У рослинництві нові технологічні рішення пов'язані із селекційною роботою, генною інженерією, органічним землеробством, мікрозрошенням та ін. У зв'язку з тим, що кліматичні умови останніх років зумовлюють зниження здатності ґрунту забезпечувати сільськогосподарські рослини сприятливим температурним режимом та вологістю в оптимальній кількості. для створення умов росту і розвитку рослин виникає потреба в забезпеченні рослин вологою згідно їх біологічних потреб, для отримання максимальної кількості продукції.

Тому, важливим напрямком є наукове обґрунтування та розробка нової техніки для поливу з врахуванням світових тенденції розвитку меліорації.

Для поливу сільськогосподарських культур створені різні дощувальні установки, машини, агрегати та обладнання. Установки отримують воду під напором зрошувальної мережі та не мають пристроїв для пересування по поливні площі. Машини, які поливають від напору в мережі, але мають свій привід для пересування. Знання конструкції та можливостей даних дощувальних машин дозволяє визначити подальшого направлення їх удосконалення, який відповідає сучасному рівню розвитку сільського господарства.

Система віддаленого керування і віртуалізації дощувальної машини, яка відображає на панелі оператора інформацію про режим роботи, напрям та швидкість руху, режим руху, стан кінцевого водомету, положення машини відносно початкового положення, відображення тиску на вході машини, автореверс, показники відпрацьованих годин, а також інформацію про аварійну ситуацію: тиск на вході більше або менше норми, аварія насосу, порушення ланцюга безпеки, порушення параметрів електричної мережі є сучасною провідною системою на базі IoT. Дана система дозволяє оптимізувати штучне зволоження – максимізувати ефективність зрошення за допомогою подачі необхідної кількості води на локальні ділянки господарств, яка подолає дефіцит водоспоживання і дозволить рослинам повною мірою реалізувати свій генетичний потенціал.

Отже, перспективним напрямком є створення універсальних дощувальних машин з регульованими параметрами витрати води та параметрів штучного дощу з використанням новітніх технологій. Тому, що дощування ще тривали час залишатиметься незамінним способом зрошення.

УДК 621.391

В.Г. Иванов

vladimir-ivanov50@ukr.net

Национальный юридический университет имени Ярослава Мудрого, Харьков

СЖАТИЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ МЕТОДОВ ВЫДЕЛЕНИЯ И КОДИРОВАНИЯ ОБЛАСТЕЙ

Характерной особенностью изображения как сигнала с большой информационной избыточностью является наличие в нем геометрических образов, содержащих связные множества близких по значению (сильно коррелированных) отсчетов. Поэтому в связи с успехами в области изучения механизма зрения, распознавания образов и анализа сцен открывается еще одна возможность в описании и кодировании изображений на основе контурно-текстурной модели, которая сводится к сегментации изображения на отдельные области (текстуры), окруженные контурами так, чтобы эти контуры по возможности соответствовали контурам объектов на изображении. Контурная и текстурная информация затем кодируется по отдельности. Идеология этого направления была заложена М. Кунтом в 1985 году [1] и названа им “Методы кодирования изображений второго поколения”.

Базовой составляющей предложенного метода сжатия второго поколения является сегментация изображения, то есть разбиение его на однородные (в смысле некоторого критерия) области. Процедура сегментации находится на стыке задач обработки и распознавания изображений. В литературе методам сегментации посвящено очень большое количество публикаций, перечень которых заканчивается фундаментальными трудами Гонсалеса [2] и Форсайта [3].

На первом этапе предложенного метода кодирования изображений на основе выращивания областей элементы изображения разделяются на контурные и текстурные. Эта процедура разбивает изображение на множество смежных областей с тем условием, что изменения уровня яркости (речь идет о монохромных изображениях) внутри области не давали резких разрывов, то есть контуров. Сегментация изображения проводится в три этапа: предобработка, выращивание областей и устранение артефактов.

Предобработка предназначена для сокращения локальной зернистости исходного изображения и не должна нарушать его контуры. Она нужна для того, чтобы после выращивания не оказалось слишком много малых областей, так как эти малые области не соответствуют, как правило, реальным объектам исходного изображения и дают, таким образом, ложные контуры. Ключевая проблема предобработки состоит в том, чтобы решить две противоречащие друг другу задачи: удаление мелкой зернистости в изображении и сохранение контуров. Данная задача решается при помощи фильтров, частотные характеристики которых адекватны фильтрам нижних частот в областях свободных от контуров и фазовым фильтрам в областях высокого контраста. Для достижения более качественной предобработки требуется итерационное применение данной процедуры. Однако с целью экономии времени на проведение сегментации изображения, процедуру предобработки можно заменить процедурой объединения (выращивания) областей, на втором этапе сегментации. Имеется в виду следующее. Если область мала, то есть количество принадлежащих ей элементов меньше заданного параметра $L_{\min}$, то объединить эту область можно с той соседней областью, которая наиболее близка к ней по среднему значению уровня яркости, и повторять этот шаг пока не будут удалены все малые области.

Основной этап сегментации – выращивание областей, состоит в следующем. Области, подлежащие выделению, должны характеризоваться некоторым свойством. Этим свойством могут быть, например, уровень яркости для элемента изображения, вариации уровня яркости или энергии внутри заданной полосы частот. От выбора этого свойства во многом зависит сложность метода обработки и точность контуров, полученных после сегментации.

Список литературы

[1] М. Кунт, А. Икономопулос, и М. Кошер, Методы кодирования изображений второго поколения, ТИИЭР. т. 73, № 4, с. 59 – 86, 1985.

[2] Р. Гонсалес, и Р. Вудс, Цифровая обработка изображений. Издание 3-е, исправленное и дополненное, Москва, Россия: Техносфера, 2012.

[3] Д. Форсайт, и Д. Понс, Компьютерное зрение. Современный подход: пер. с англ., Москва, Россия: Вильямс, 2004.

УДК 004.424:681.5(06)

Є. О. Канарський, О. В. Желтухін,

y.kanarskiy@student.csn.khai.edu, a.zheltukhin@csn.khai.edu

Національний аерокосмічний університет ім. М.Є. Жуковського "ХАІ", Харків

АВТОМАТИЗОВАНА СИСТЕМА КЕРУВАННЯ ТЕПЛИЧНИМ ГОСПОДАРСТВОМ

Тепличне господарство – виробничий підрозділ сільськогосподарського підприємства, яке вирощує в теплицях переважно овочі і розсаду овочевих культур для відкритого грунта.

Автоматизована система управління дозволяє оптимізувати витрати на управління та утримання тепличного господарства.

В даному проекті була розроблена автоматизована система управління тепличним господарством, що складається з двох рівнів.

Нижній рівень являє собою мікроконтролер з підключеними до нього датчиками рівня освітленості, температури повітря, температури грунта, вологості повітря, концентрації CO_2. Мікроконтролер здійснює управління подачею добрива, поливом, нагріванням грунта і освітлення для створення необхідного мікроклімату в теплиці.

Основним джерелом енергії для росту рослин є світло, тому встановлення штучних джерел світла в тепличному приміщенні дозволяє пришвидшити зростання вирощуваних культур. При цьому штучне освітлення бажано використовувати лише в темний період доби, оскільки природне освітлення є більш сприятливим для рослин та дозволяє економити потрібну для забезпечення штучного освітлення електроенергію. Для того, щоб визначити, коли потрібно вмикати і вимикати освітлювальні прилади, використовується датчик рівня освітленості. Датчик освітленості передає на мікроконтролер поточне значення рівня світла. Коли рівень освітленості в теплиці досягає відповідного мінімуму, мікроконтролер за допомогою реле вмикає лампи в теплиці. При цьому рослини також потребують нічного спокою, тому лампи вимикаються в нічний час, і вмикаються знову через шість годин. Для того, щоб визначити, коли можна вимикати штучне освітлення, використовують другий датчик рівня освітлення ззовні теплиці.

Також для забезпечення процесу фотосинтезу рослинам потрібен вуглець (CO_2). Для регулювання рівня вуглекислого газу використовується датчик концентрації CO_2.

Кожна рослина містить певний рівень води, що поступово випаровується впродовж дня для охолодження. При високому рівні вологи в повітрі цей процес сповільнюється, що може призвести до деформації рослини та зниження загальної врожайності. Для контролю рівня вологи в повітрі теплиці використовується датчик рівня вологи.

При низьких температурах процес зростання урожаю може сповільнитись, а у зимовий період призвести до замерзання. А надто висока температура повітря і ґрунту може призвести до засихання врожаю. Для спостереження за температурою використовуються датчики температури повітря і температури ґрунту.

Добрива для рослин разом з водою подаються в окремий бак для змішування, звідки за допомогою крапельного поливу потрапляють у ґрунт. Полив відбувається автоматично двічі на добу згідно налаштованому розкладу.

Верхній рівень являє собою мікрокомп'ютер з встановленої серверної системою. На сервері розташована база даних, за допомогою якої відбувається налаштування параметрів теплиці. Зміни в базу даних вносяться через web-додаток, де можна встановити режим роботи для кожної теплиці, налаштувати режими роботи, керувати функціями тепличного господарства в ручному режимі і переглядати записи про проведені операції. Взаємодія верхнього і нижнього рівня теплиці здійснюється за допомогою модулів ZigBee.

ZigBee – стандарт для набору високорівневих протоколів зв'язку, заснований на стандарті IEEE 802.15.4-2006 для бездротових персональних мереж. Дозволяє створювати мережі, що самоорганізуються, з комірчастою топологією для широкого кола завдань, маючи при цьому малий час відгуку і низьке енергоспоживання.

При увімкненні системи, мікроконтролер виконує операцію самотестування для виявлення несправних або не підключених датчиків. В разі виявлення несправності посилається відповідне повідомлення на верхній рівень системи, а мікроконтролер переходить у автономний режим роботи, що забезпечує мінімальні умови для росту рослин. Якщо система справна, мікроконтролер посилає запит на отримання функціональних параметрів роботи теплиці з бази даних.

При реалізації даного проекту була розроблена система управління тепличним господарством. Розроблена система дозволяє реалізувати контроль і регулювання температури грунта і повітря, вимір вологості, управління поливом, управління освітленням, автоматизувати процес подачі добрив рослинам. Керування системою може здійснюватися автоматично або вручну за допомогою web-додатка. При виникненні несправності система може працювати автономно.

УДК 004.056.55

О.К. Конопліцька-Слободенюк, В.А. Бісюк

ksuha80@gmail.com, kntubisuk@ukr.net

Центральноукраїнський національний технічний університет, Кропивницький

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ КВАНТОВОЇ КРИПТОГРАФІЇ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Широке розповсюдження різного роду телекомунікаційних мереж привело до активного розвитку засобів зламу та підслуховування передачі інформації, що в свою чергу викликало інтенсивні розробки та дослідження різного роду систем захисту інформації. Квантова криптографія – стійкий та надійний метод захисту каналів зв'язку від підслуховування, який використовується при передачі інформації об'єктами квантової механіки (фотони в оптоволоконному кабелі або електрони в електричному кабелі). Захист інформації заснований на зміні фізичних властивостей об'єктів при спробі перехоплення сигналу .

Даний метод захисту комунікацій стає все більш актуальним через появу так званих квантових алгоритмів, які значно зменшують надійність класичних методів криптографії. Рішенням може стати саме спосіб квантової криптографії. Стверджується, що даний спосіб криптографії зламати неможливо. Пропонована система використовує ключі, створені оптичним чіпом, що не зберігаються і не передаються разом з повідомленням. В результаті їх неможливо відтворити або перехопити.

Один з факторів, які стримують практичне використання даного методу є складність апаратного забезпечення. На обох кінцях каналу повинно бути встановлена складна апаратура – джерела поодиноких фотонів, засоби управління поляризацією фотонів і чутливі детектори. При цьому для вимірювання кута поляризації фотонів необхідно точно знати, яке обладнання на обох кінцях каналу. Через це метод квантової криптографії не підходить для мобільних пристроїв.

Але в результаті досліджень проведених вченими Брістольського університету та дослідницького центру Nokia в Кембріджі було запропоновано систему квантової криптографії, при якій складне обладнання необхідно тільки одному учасникові переговорів. Другий лише модифікує стан фотонів, кодуючи цим інформацію, і відправляє їх назад. Все необхідне обладнання для цього можна розмістити на одиночному чипі в кишеньковому пристрої. Дослідники пропонують також вирішення проблеми орієнтації обладнання. Вимірювання проводяться в випадкових напрямках. Список напрямків може бути опублікований відкрито, але при розшифровці будуть враховуватися тільки напрямки, що збігаються. Автори називають метод "незалежним від системи відліку квантовим розподілом ключів" (англ. "reference frame independent quantum key distribution" або rfiQKD).

Всі складні обчислення по обміну ключами шифрування виконуються на одній стороні обміну даними. Простіше кажучи: сервер є джерелом фотонів, а мобільний пристрій буде лише модифікувати їх по заданому алгоритму. Такий метод значно спрощує процедуру квантового шифрування і вимоги до апаратного забезпечення, але надійність і стійкість до зламу залишається на високому рівні.

Алгоритм rfiQKD працює досить стабільно і надійно. Дослідники зробили порівняння алгоритму rfiQKD з алгоритмом BB84, стандартним алгоритмом, використовуваним в квантовій криптографії. Коли учені додали до передаваного сигналу шумовий сигнал, алгоритм BB84 негайно припиняв працювати. Новий алгоритм rfiQKD виявився більше завадозахищеним, він продовжував працювати навіть тоді, коли рівень шуму піднімався майже до половини значення рівня корисного сигналу. У тому випадку, коли квантовий зв'язок порушувався із – за шуму, після зниження рівня шуму знову до допустимого значення синхронізація роботи пристроїв відбувалася знову і працездатність усієї системи повністю відновлювалася.

В результаті своїх праць учені отримали систему, яка зможе стати основою технологій квантової криптографії, вбудованою в широкий ряд електронних пристроїв, надавши можливість користуватися безпечними комунікаціями кожній людині.

Хоча практичне використання квантової криптографії поки що обмежено, але цей напрямок вважається дуже перспективним, тому що квантові закони дозволяють вивести методи захисту інформації на якісно новий рівень. На сьогоднішній день вже існує досвід по створенню і апробації комп'ютерних мереж, захищених методом квантової криптографії – єдиним на даний час, який неможливо зламати.

УДК 004.627

И.А. Кулик, М.С. Шевченко

i.kulyk@ekt.sumdu.edu.ua, m.shevchenko@ekt.sumdu.edu.ua

Сумский государственный университет, Сумы

ПОСТРОЕНИЕ МОДЕЛИ АДАПТИВНОГО СЖАТИЯ НА ОСНОВЕ ДВОИЧНЫХ БИНОМИАЛЬНЫХ ЧИСЕЛ

С целью увеличения быстродействия методов сжатия и восстановления на основе двоичных биномиальных чисел, представленных в [1], предлагается ввести в модели процессов сжатия и восстановления процедуру выбора способов кодирования для исходной двоичной n-разрядной последовательности.

При сжатии $A_j \in A = \{0,1\}^n$ необходимо использовать функцию f_w, ставящую в соответствие исходной последовательности A_j выборку $\left(k, Y_j\right)$, где Y_j – равновесная комбинация, имеющая число k двоичных единиц, $Y_j \in Y\left[n,k\right]$ ($A_j = Y_j$). Если полученное значение k удовлетворяет системе неравенств вида:

$$\left(0 < k < \alpha_b\right) \vee \left(\beta_b < k < n\right),$$

то для кодирования комбинации Y_j используется кодирование f_b на основе двоичных биномиальных чисел $X_j \in X\left[n,k\right]$, где n и k – параметры соответствующей двоичной биномиальной системы счисления. Если для значения k выполняется неравенство $\alpha_b \le k \le \beta_b$, то реализуется метод векторного кодирования f_v, переводящую Y_j в саму себя. При этом в обоих случаях к кодируемым комбинациям для однозначного восстановления добавляется двоичное число $\mathrm{Bin}\, k$, т.е. выполняется дополнительное кодирование f_k. Значения границ α_b и β_b сжатия выводятся из условия, что длина сжатого образа должна быть меньше длины исходной A_j [2]. Если же

$$\left(k = 0\right) \vee \left(k = n\right),$$

то кодируемая результирующая комбинация будет состоять только из $\mathrm{Bin}\, k$, т.е. используется только метод кодирования f_k. Таким образом, рассматривается отображение вида $f_{bv} : A \to Z$, которое задается функцией $Z_j = f_{bv}\left(A_j\right)$, где $A_j = a_1 a_2 ... a_i ... a_n$, $A_j \in A$, а $Z_j \in Z$ может принимать вид $Z_j = \left(\mathrm{Bin}\, k, X_j\right)$, $Z_j = \left(\mathrm{Bin}\, k, A_j\right)$ или $Z_j = \mathrm{Bin}\, k$, $j = \overline{1, 2^n}$.

Модель процесса адаптивного сжатия f_{bv} двоичных последовательностей A_j на основе двоичных биномиальных чисел X_j состоит из следующих этапов.

Этап 1. Определяется количество s разрядов для двоичного представления $\mathrm{Bin}\, k$ числа k единиц, $0 \le k \le n$, исходной n-разрядной последовательности $A_j = a_1 a_2 ... a_i ... a_n$: $s = \left\lceil \log_2 \left(n+1\right) \right\rceil$.

Этап 2. Производится вычисление числа k двоичных единиц в исходной A_j, тем самым реализуя функцию $f_w\left(A_j\right)$ и определяя класс $Y\left[n,k\right]$ равновесных комбинаций, к которому относится $Y_j \in Y\left[n,k\right]$, $Y_j = A_j$.

Этап 3. Выполняется преобразование числа k единиц к его двоичному виду $\mathrm{Bin}\, k$, состоящему из s разрядов.

Этап 4. Если число k удовлетворяет системе равенств (2), то результирующей будет комбинация вида $Z_j = \mathrm{Bin}\, k$. В противном случае выполняется переход к следующему этапу.

Этап 5. Если число k удовлетворяет системе неравенств (1), то значения n и k представляют собой параметры двоичной $\left(n,k\right)$-биномиальной системы счисления и осуществляется реализация сжимающего кодирования вида $f_k\left(f_b\left(Y_j\right)\right) = Z_j$. В противном случае выполняется реализации кодирования вида $f_k\left(f_v\left(Y_j\right)\right) = Z_j$.

Такой адаптивный подход к выбору способов кодирования f_b или f_v позволяет увеличить степень сжатия, повысить скорость информационных преобразований и расширить область эффективного использования предлагаемого метода сжатия на основе двоичных биномиальных чисел.

Список литературы

[1] I. Kulyk, O. Berezhna, and M. Shevchenko, "Development of data compressing coding methods on basis of binary binomial numbers", Technology audit and production reserves, № 2/2(46), p. 12-18, 2019. doi: 10.15587/2312-8372-2019.169897.

[2] И. А. Кулик, А. И. Новгородцев, и М. С. Шевченко, "Метод оценки границ применения сжатия на основе двоичных биномиальных чисел", Системи обробки інформації, № 2(157), с. 57 – 62, 2019. doi: 10.30748/soi.2019.157.07.

УДК 004.9

Є.В. Мелешко, Г.М. Дрєєва, В.С. Гермак, В.А. Резніченко, О.О. Шевченко

elismeleshko@gmail.com, gannadreeva@gmail.com, germak_vs@ukr.net, upsbilly@meta.ua, shev4enos@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

МЕТОДИ ВИЗНАЧЕННЯ БОТІВ СЕРЕД КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕРЕЖ

Віртуальні соціальні мережі починають відігравати все більшу роль у суспільному житті звичайних людей, тому вони все частіше стають середовищем інформаційного впливу. Як правило, такий вплив реалізується через мережі ботів, що намагаються змінювати суспільну думку через поширення великої кількості схожих повідомлень, які містять інформаційно-психологічні посили потрібного змісту. Для знешкодження мереж ботів існують різні підходи: блокування акаунтів, спростування недостовірної інформації, поширення інформації з протилежним посилом, тощо. Переважно акаунти ботів блокують, або обмежують у можливостях. Але найперше, що треба здійснити для успішного застосування даних методів – ідентифікація ботів. Методи ідентифікації ботів слід шукати серед Data Mining методів, що включають в себе кластеризацію даних, нейронні мережі, еволюційні та генетичні алгоритми, статистичні методи, корреляційно-регресивний аналіз, тощо.

Які саме методи чи сукупність методів застосовувати, а також які статистичні показники враховувати, при виявлені ботів у соціальних мережах – значно залежить від особливостей та тематичного спрямування веб-ресурсу. Але можна говорити про певні загальні принципи.

Для ідентифікації акаунтів ботів можна аналізувати наступні характеристики їх профілів:

– швидкість здійснення дій – програми-боти, якщо розробники не використають моделювання часових затримок, будуть працювати швидше, ніж людина;

– зміст публікацій – найпростішим є аналіз текстових повідомлень інтелектуальними засобами (нейронними мережами, байесовськими класифікаторами, тощо) на наявність надмірного емоційного забарвлення, входження наборів підозрілих слів та словосполучень і т.д.;

– здійснені дії – боти можуть мати певні шаблони поведінки, напр., реагувати (ставити лайки/дизлайки, писати коментарі, репостити) тільки на певні публікації та коментарі, що мають цільові ключові слова чи цільову тему;

– список друзів – переважно буде містити тільки інших ботів та/або користувачів, що підтверджують майже всі заявки у друзі, напр., через свою публічність;

– подібність з іншими користувачами – акаунти, що входять до однієї мережі ботів, будуть мати значну схожість між собою, значно більшу, ніж можуть мати між собою звичайні користувачі, бо будуть здійснювати багато однакових дій (що можна оцінювати за допомогою коефіцієнтів кореляції).

Задачу виявлення профілів ботів можна розділити на наступні етапи:

1. Визначення можливих шаблонів поведінки ботів на основі можливих цільових об’єктів.
2. Збір статистичних даних про користувачів соціальної мережі та обчислення певних статистичних показників.
3. Порівняння зібраних даних з шуканими шаблонами поведінки та формування списків підозрілих користувачів.
5. Визначення коефіцієнтів кореляції між підозрілими користувачами та формування списків можливих мереж ботів.

Основні методи виявлення груп ботів передбачають розділення профілів користувачів на два кластери на основі їх коефіцієнтів подоби. Аналізуючи статистику кластерів, приймається рішення про наявність нападу, і якщо так, то який кластер містить профілі атаки. Вважається, що напад відбувся, якщо різниця в статистичних особливостях профілів для двох кластерів досить велика. Кластер з меншим стандартним відхиленням визначається як кластер ботів. Однак, особливо для невеликих розмірів атак, значна частина кластера ідентифікованого як кластер ботів може містити справжніх користувачів.

Крім автоматизованих методів виявлення ботів, веб-сайти часто надають користувачам можливість відмітити певний акаунт як підозрілий, і після того, як кількість скарг перевищуватиме деяке критичне число, акаунт буде ідентифіковано у системі як фейковий, або відправлено на перевірку.

Також існує ще один підхід для захисту від ботів на веб-ресурсах, яким переважно користуються дошки об’яв та маркетплейси – репутаційні системи.

Репутаційна система – це система, що дозволяє користувачам оцінювати один одного в онлайн-спільнотах, тим самим підвищуючи або знижуючи рівень довіри до оцінюваного.

Хоча репутаційні системи переважно використовуються для захисту від шахраїв серед продавців або покупців на веб-ресурсах електронної комерції, вони також можуть бути одним з інструментів захисту від ботів, так як їх можна побудувати таким чином, щоб боти одержували низьку репутацію і, як наслідок, мали низький вплив на учасників соціальної мережі.

УДК 004.92

Є. В. Мелешко, О. Д. Старкіна

arina.star2@gmail.com, elismeleshko@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

ОПТИМІЗАЦІЯ АЛГОРИТМУ ЗАЛИВКИ ДЛЯ ВИКОРИСТАННЯ У СИСТЕМІ ІГРОВОГО РУШІЯ ДЛЯ ПЛАТФОРМИ ANDROID

Визначення області, колір якої слід змінити, поширена задача у програмуванні графічних додатків, таких як ігрові рушії.

Оскільки на передньому плані завжди враження користувача, підтримка якості зображення стає надважливим завданням. Однією з проблем при розробці таких додатків є робота алгоритму заливки із зображеннями, що містять згладжування.

Метою даної роботи є оптимізація алгоритму заливки для ігрового фреймворку (рушія).

Ігровий фреймворк – основа для створення гри, містить у собі модулі графіки, звуку, користувацького вводу та ін. Містить один або декілька інтерфейсів, кожен з яких містить хоча б одну реалізацію.

Заливка – це алгоритм, що визначає область, “поєднану” з певним елементом у багатомірному масиві. Переважно застосовується у програмах для визначення області, яку треба заповнити певним кольором. Згладжування – технологія, що використовується в обробці зображень з метою зробити межі кривих ліній більш гладкими, прибираючи “зубці”, що виникають на краях об'єктів.

Заливка зображень зі згладжуванням.

Алгоритм заливки не маркує “згладжені" пікселі, як такі що потребують зміни кольору, в результаті після завершення роботи алгоритму колір цих пікселей не змінено, що утворює ефект не суцільної заливки. Для вирішення цієї проблеми було випробувано два підходи [1]:

1. Повторний прохід по неперевіреним пікселям і додаткова перевірка на те, чи не знаходяться вони поблизу "кордону" зафарбовування:

```
private fun antiAliasFloodFill() {
    for (y in 1 until height - 1) {
        var i = y * width + 1
        for (x in 1 until width - 1) {
// if pixel is not filled by neighbour is then
it's on the border
            if (!pixelsChecked[i] &&
(pixelsChecked[i - 1] || pixelsChecked[i + 1] ||
pixelsChecked[i - width - 1] || pixelsChecked[i -
width] || pixelsChecked[i - width + 1] ||
pixelsChecked[i + width - 1] || pixelsChecked[i +
width] || pixelsChecked[i + width + 1])) {
// fill pixel near border
                pixels!![width * y + x] =
antiAliasPixel(x, y)
            }
            i++
        }
    }
}
```

2. Встановлення чіткої умови визначення зафарбовувати піксель чи ні:

```
private fun checkPixel(px: Int): Boolean {
 return px != Color.BLACK
}
```

Перший підхід дозволяє зберегти згладжування, але погано опрацьовує гострі краї робочої області, а також потребує додаткового часу. Другий підхід визначає сто відсотків області, яку треба заповнити певним кольором, але повністю руйнує згладжування зображення. Обидва підходи не є ідеальним з точки зору кінцевого вигляду зображення, тож реалізація алгоритму потребує інших рішень [2]. Одним з можливих рішень є пошук основного кольору області і, враховуючи його, визначення значення згладжування (відтінку кольору) кожного оброблюваного пікселя, однак рішення не підходить для усіх варіантів випадків через те, що існують такі області зображень, де основний колір представлений одним пікселем, що робить неможливим програмне визначення його як основного. Іншим можливим шляхом оптимізації було розглянуто таку реалізацію алгоритму, в якій ведеться робота з двома зображеннями, чорно-білим, що виступає картою згладжування та робочим зображенням, на якому власне відбувається процес заливки. Ідея полягала в тому, що ми шукаємо координати області на базовому зображені, а заливку проводимо на його копії, таким чином ми точно можемо визначити, які пікселі потребують згладжування. Однак такий алгоритм дуже вимогливий до пам’яті, що робить його використання у мобільних пристроях, обмежених з точки зору ресурсів, неоптимальним рішенням.

Оскільки розробка ігрового рушія для мобільної системи вимагає балансу між швидкодією, ресурсами і результатом, задля подолання розглянутої проблеми було вирішено, в залежності від наявних на мобільному пристрої ресурсів, автоматично обирати використовувати або не використовувати згладжування у зображеннях. Для переважної більшості сучасних мобільних пристроїв від згладжування зображень слід відмовлятися на користь швидкодії додатку.

Список літератури

[1] Дж. Ди Марцио, Разработка игр под Android, СПб., Россия: Питер, 2014.

[2] М. Цехнер, Программирование игр под Android, СПб., Россия: Питер, 2013.

УДК 004.9

Є.В. Мелешко, В.Д. Хох

elismeleshko@gmail.com, vd.khokh@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ МОДЕЛЕЙ РЕКОМЕНДАЦІЙНИХ СИСТЕМ НА ОСНОВІ ПРИХОВАНИХ ФАКТОРІВ

На сьогоднішній день, при побудові рекомендаційних систем (РС) на основі колаборативної фільтрації, часто застосовують матричні факторизаційні моделі (МФМ) вподобань користувачів [1].

Факторизація – це процес декомпозиції об'єкту в набір інших об'єктів (факторів), добуток яких дає початковий об'єкт [2]. Факторизація дозволяє виділити ключові компоненти об'єкту факторизації. У РС факторизація застосовується до матриці рейтингів (ФМ) з метою виявляння прихованих факто-рів об'єктів, що впливають на оцінки користувачів.

Найбільш відомими МФМ є FunkSVD, SVD++, Asymmetric SVD, timeSVD [1, 3]. Усі вони містять у назві абревіатуру методу Singular value decomposition, бо засновані на спільній з ним ідеї – факторизувати матрицю на дві матриці, добуток яких дає матрицю наближену до початкової, де початково порожні комірки заповнені (для РС це дозволяє прогнозувати рейтинги для порожніх комірок матриці рейтингів).

Загальний алгоритм ФМ рейтингів:

1. Ініціалізуємо матрицю прихованих факторів користувачів F_u та матрицю прихованих факторів об'єктів F_i випадковими значеннями.

2. Перемножуємо F_u і F_i та порівнюємо результат зі справжніми рейтигами, обчислюємо помилки.

3. Мінімізуємо помилки за допомогою деякого алгоритму машинного навчання (напр., градієнтного спуску, методу найменших квадратів, тощо).

FunkSVD. Найперша модель рекомендаційних систем, що застосовує матричну факторизацію [3].

Дана модель полягає у наступному. Спочатку треба визначити базові предиктори (зміщення):

$$b_{u,i} = \mu + b_u + b_i .$$

Прогнозування оцінок здійснюється за формулою:

$$\hat{r}_{u,i} = \mu + b_u + b_i + q_i \cdot p_u ,$$

де q_i – вектор факторів об'єкту i; а p_u – вектор факторів користувача u; b_u – базові зміщення окремих користувачів; b_i – базові зміщення окремих об'єктів; μ – глобальний середній рейтинг об'єктів.

Спочатку обчислюється μ. Потім знаходяться найкращі предиктори та фактори, що дозволяють прогнозувати рейтинги з найменшою помилкою.

Для визначення помилки використовується сума квадратів відхилень, що оптимізується градієнтним спуском, також виконується регуляризація, щоб подолати проблему перенавчання системи:

$$b_*, q_*, p_* = \arg\min_{b,q,p} \sum_{(u,i)}^{n} (r_{u,i} - \mu - b_u - b_i - q_i \cdot p_u)^2 + \\ + \lambda \left(\sum_u b_u^2 + \sum_i b_i^2 + \|q_i\|^2 + \|p_u\|^2 \right),$$

де λ – параметр регуляризації.

Під час градієнтного спуску використовуються наступні правила для оптимізації змінних:

$$b_u = b_u + \gamma(e_{u,i} - \lambda b_u),$$
$$b_i = b_i + \gamma(e_{u,i} - \lambda b_i),$$
$$q_{i,k} = q_{i,k} + \gamma(e_{u,i} \cdot p_{u,k} - \lambda q_{i,k}),$$
$$p_{u,k} = p_{u,k} + \gamma(e_{u,i} \cdot q_{i,k} - \lambda p_{u,k}),$$

де $e_{u,i} = r_{u,i} - \hat{r}_{u,i}$ – помилка на наборі даних для навчання; γ - швидкість навчання.

SVD++. Відрізняється від FunkSVD тим, що крім рейтингів (явного зворотного зв'язку від користува-ча) використовує також неявну інформацію про вподобання користувачів, напр., перегляди об'єктів, написання коментарів, тощо [4]. TimeSVD++. Це факторизаційна модель з враху-ванням часу. Вподобання користувачів можуть залежати від часу, саме це враховує дана модель, трактуючи зміщення об'єкту b_i як функцію часу. Asymmetric SVD. Дозволяє додавати до моделі нових користувачів з декількома рейтингами, без необхідності перенавчати всю модель [1]. Отже, існує багато різних моделей РС, заснованих на ФМ. Усі вони успішно застосову-ються на різних існуючих веб-ресурсах. Перевагами МФМ є висока робастність до атак та висока точність прогнозування вподобань, недоліками – погана масштабованість, довгий час навчання, переважна більшість МФМ потребує при додаванні нових користувачів повного перенавчання усієї моделі.

Список літератури

[1] F. Ricci, L. Rokach, B. Shapira, and P. B. Kantor, "Recommender Systems Handbook", Editors, 1st edition, New York, NY, USA: Springer-Verlag New York, Inc., 2010. doi: 10.1007/978-0-387-85820-3.

[2] I. Krupnik, "Decomposition of a monic matrix polynomial into a product of linear factors", Linear Algebra Appl, p. 239 – 242, 1992.

[3] S. Funk, "Netflix Update: Try This at Home", [Online]. Available: https://sifter.org/~simon/journal/20061211.html. Accessed on: May 19, 2014.

[4] Ya Jia, "Users' brands preference based on SVD++ in recommender systems", IEEE Workshop on Ad-vanced Research and Technology in Industry Applications, p. 1175 – 1178, 2006. doi:10.1109/wartia.2014.6976489

УДК 004.056

М.А.Назаркевич, І.І. Лозовицька

mariia.a.nazarkevych@lpnu.ua,, lozira.2000@gmail.com

Національний університет *"Львівська політехніка", Львів*

РОЗРОБКА TELEGRAM-БОТА ДЛЯ КОПІЮВАЛЬНОГО ЦЕНТРУ

Все частіше для спілкування один з одним люди обирають програми на власних мобільних пристроях – месенджерах – Viber, Telegram, Skype, Facebook Messenger. Поєднання систем миттєвих повідомлень забезпечило появу ботів – програм для автоматизованого виконання простих та повторюваних завдань.

Для охоплення більшої аудиторії потенційних клієнтів та автоматизації процесу формування замовлення для копіювального центру було вирішено створити бота використовуючи платформу із можливостями створення індивідуальної клавіатури Telegram.

При розробці бота було враховано ймовірність того, що на кожному етапі користувач може пригадати чи захотіти ще якийсь товар, якого попередньо не було у кошику, тому створено можливість повернення до перегляду каталогу продукції а потім відновлення оформлення замовлення. Знайти бота поліграфії Printing&Publishing можна через пошук в Telegram, задля полегшення ідентифікації було додано короткий опис функцій робота та аватарку.

Каталог продукції складається із таких найменувань – бірки, блокноти, буклети, візитки, друк на пакетах, меню, календарі, конверти та флаєри, що відображаються в переписці як inline-кнопки. Кількість найменувань продукції можна змінювати.

При натисненні на будь-яку із них з'являються товари даного типу продукції – повідомлення із зображенням, назвою та короткою характеристикою (ціна, матеріал, кількість, наявність лакування, розмір), які пропонує виготовити копіювальний центр. Також Telegram – бот пропонує обрати товар для занесення в кошик шляхом натиснення на inline – кнопки із назвою продукції, опісля з'являється вікно із написом, що було додано до замовлення (рис. 1).

При визначенні платформи для розробки робота було виявлено, що хоча українці при виборі месенджерів надають перевагу Viber – 87%, Facebook Messenger – 48%, Telegram – 40%, найбільш перспективний для розробки зрозумілих та зручних у використанні ботів є останній. Визначено, що для підвищення рівня продаж та залучення клієнтів за допомогою мобільних телефонів для копіювального центру можна застосовувати ботів-месенджерів, які відповідають наступним критеріям – розроблений засіб не займає додаткової пам'яті на пристрої, не має унікального дизайну, який би заважав сприймати інформацію користувачу, легкість у використанні, цілодобова підтримка, простий спосіб комунікації.

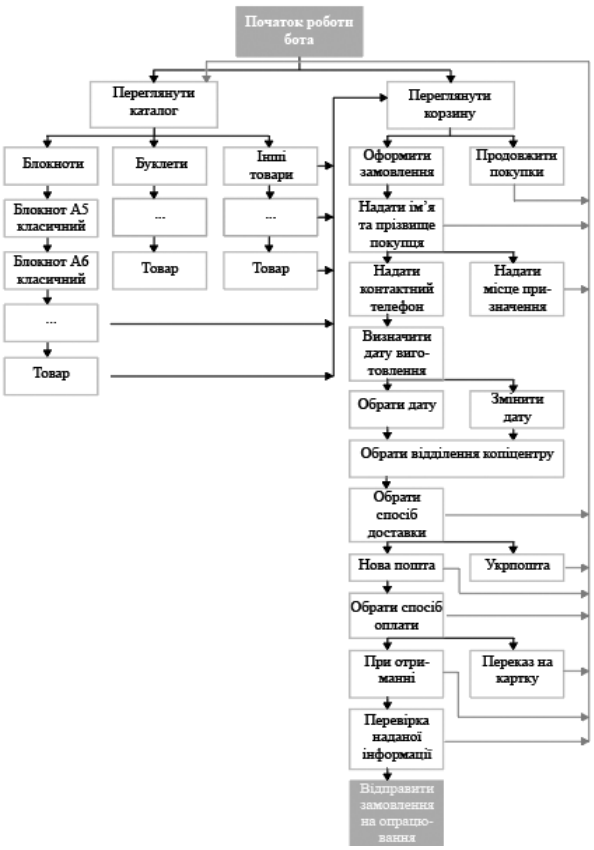


Рис. 1. Схема роботи бота

На Python було розроблено Telegram бота, що допомагає оформлювати замовлення онлайн: обирати продукцію через каталог, додавати в кошик товари, оформлювати замовлення, надавати контактні дані клієнта та обирати дату виготовлення та відділення копіювального центру, обрати спосіб доставки та оплати, надсилати деталі замовлення на електронну пошту. Для забезпечення користувачів службою підтримки було створено чат-бота на основі засобів розпізнавання людської писемності – Dialogflow. Чат-бота було протестовано, а на виявлених похибках здійснено тренування агента..

УДК 658.5.011

Е. В. Нестеряк, Р. М. Минайленко

egenchantments@gmail.com, aron70@ukr.net

Центральноукраїнський національний технічний університет, Кропивницький

ЕФЕКТИВНІСТЬ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Інтерес до системи підтримки прийняття рішень (СППР) як до інструментарію підвищення ефективності праці у сфері управління економікою постійно зростає.

За допомогою СППР, в яких сконцентровані потужні методи математичного моделювання, теорії управління, інформаційних технологій, може здійснюватися вибір рішень деяких неструктурованих і слабоструктурованих задач, у тому числі й багатокритеріальних. Тому СППР, як правило, є результатом міждисциплінарного дослідження, що включає теорії баз даних, штучного інтелекту, інтерактивних комп'ютерних систем, методів імітаційного моделювання тощо.

Дослідження ефективності використання СППР визначається необхідністю врахування великого об'єму даних, обробка яких без допомоги сучасного комп'ютингу практично неможлива [1].

СППР розв'язують дві основні задачі. По-перше, вибір найкращого рішення із багатьох можливих (оптимізація). По-друге, впорядкування можливих рішень по пріоритету (ранжування). В обох задачах першим і найбільш принциповим моментом являється вибір сукупності критеріїв, на основі яких надалі будуть оцінюватись і зіставлятись можливі рішення (альтернативи).

СППР являє собою комплекс програмних інструментальних засобів для аналізу даних, моделювання, прогнозування і прийняття управлінських рішень, які складаються з особистих розробок корпорації та придбаних програмних продуктів (Oracle, IBM, Cognos).

В широкій практиці давно використовуються такі системи, як EIS, GDSS, ODSS. Компанією Texas Instruments було створено Gate Assignment Display System для United Airlines. Це дозволило значно знизити збитки від польотів і відрегулювати управління різними аеропортами. Пізніше сфера можливостей СППР розширювалась за допомогою впровадження в роботу сховищ даних та інструментів OLAP [2].

Виділяють два основних фактори, що впливають на ефективність рішень: фактор якості рішення Q та фактор прийняття рішення людиною А. Ефективність рішення Е може бути виражена формулою: $E = Q \times A$.

За умов, що один із зазначених факторів прямує до мінімуму, ефективність рішення падає. Фактор якості рішення Q пов'язаний із вибором кращої альтернативи з тих, що зумовлює проблемна ситуація з урахуванням умов прийняття рішень та можливостей виконавців рішення.

Підвищення ефективності рішення головним чином слід спрямовувати на покращення фактору якості, а саме на вірний добір обмежень і критеріїв рішення, правильне формування множини допустимих альтернатив та на коректний вибір найкращого для умов задачі варіанту.

Так, ефективність розв'язання задачі розподілу ресурсів характеризує ступінь співвимірності цілей із витратами ресурсів на їх досягнення та визначається фактором якості рішення Q, який обумовлюється доброякісністю і глибиною виконання етапу постановки задачі та вибором методів і моделей для розв'язання задачі [3].

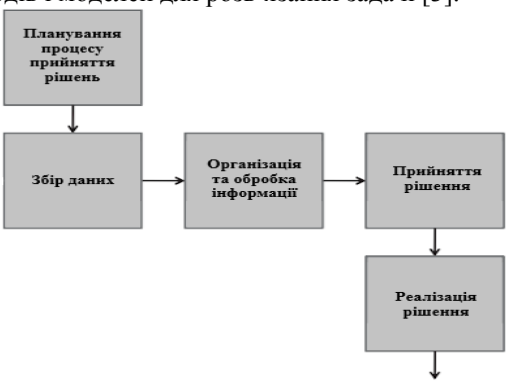


Рис.1. Процес прийняття рішень з СППР

СППР дозволяє полегшити роботу керівників підприємств та підвищити її ефективність, покращити контроль над діяльністю організації. Вона значно прискорює розв'язання проблем та завдяки їй відкриваються нові підходи до вирішення повсякденних та нестандартних задач.

Список літератури

[1] О. А. Клепікова, "Інформаційно-аналітичні системи прийняття рішень в управлінні підприємством", № 1 (62), с. 196 – 204, 2017. [Електронний ресурс]. Доступно: http://oaji.net/ articles/2019/2849-1576589397.pdf. Дата звернення: Лют. 28, 2020.

[2] О. І. Ларичев, та О. Б. Петровський, "Системи підтримки прийняття рішень", т. 21, с. 131 – 164, 1987. [Електронний ресурс]. Доступно: http://www.raai.org/library/papers/Larichev/Larichev_Petrovsky_1987.pdf . Дата звернення: Лют. 28, 2020.

[3] О. В. Мазурець, "Системи підтримки прийняття рішень", т. 12, с. 1 – 6, 2015. [Електронний ресурс]. Доступно: https://msn.khnu.km.ua/course/ view.php?id =4237. Дата звернення: Лют. 29, 2020.

.

UDC 681.3

M. Pavlenko[1], V. Larin[1], Ahmed Abdalla[2]

bpgpma@ukr.net, l_vv83@ukr.net, Ahmedalassam90@gmail.com

[1]*Ivan Kozhedub Kharkiv National Air Force University*
[2]*Flight Academy of the National Aviation University*

DRAWBACKS OF WIRELESS TELECOMMUNICATION SYSTEMS

An analysis of the current state of information applications regarding the demand for video information resources is carried out. It is shown that, as a result of the development of telecommunication technologies, there are also dangerous risks regarding interaction with an open and uncontrolled external information environment. It is substantiated that wireless telecommunication technologies have become widely used as information delivery systems. The shortcomings of wireless telecommunication systems are revealed. It is justified that for the image processing variant the probability of reliable interpretation is directly proportional to the value of the peak signal-to-noise ratio in case of unauthorized access. The shortcomings of existing cryptosystems are identified.

Recently, the usage of wireless telecommunication technologies has sharply increased as information delivery systems. Wireless telecommunications systems are divided into aerospace and ground-based technologies.

Geostationary spacecraft are the basic component for the organization of satellite communications. Advantages of satellite communication systems are the possibility of data transmission over considerable distances; relatively large bandwidth channels, unlimited space overlap, channels' high quality and reliability. Based on the low-orbit satellites and UAVs using, an aerospace monitoring system is being built. As practice shows in the course of remote strategic objects monitoring and in the emergency situations liquidation, more than 90% of all information has video images based on the aerospace means.

For wireless telecommunication systems, there are a number of characteristic drawbacks, namely:

1. Limited computing, power capabilities and significantly lower transmission speeds compared to wired technologies.

The main parameter affecting the execution time of any conversion is the computer system's performance (the processor clock speed). One of the approaches to computing the modern computing systems' performance is the peak computers' performance.

Peak performance is measured in teraflops (TFLOPS) and shows how many operations per second the given computing system performs (usually refers to operations on 64-bit floating numbers in the IEEE 754 format):

1 teraflops = 1 tril. oper. in seconds = 1000 billion oper. in seconds;

1 TFLOPS = 1012 FLOPS = 103 GFLOPS.

The actual modern computers' performance (based on the LINPACK test) is about 80 – 95% of the peak performance.

Despite the apparent unambiguity, in reality peak performance, calculated in flops, is not ideal, since its very definition is ambiguous. Very many factors not directly related to the performance of the computational module, such as: the communication channels' bandwidth with the processor environment, the main memory's performance, and the synchronization of cache operation at different levels. Therefore, the performance of the computer system for research purposes is proposed to be determined through the clock frequency. The transmission rates from the low-orbit spacecraft are from 15,3 M to 61 Mbps for the frequency range of the 8,2 GHz radio link and 665,4 Kbps for the 1,7 GHz band. The transmission speed for modern UAVs is within 500 Kbit / s.

2. Limited communication session. For UAV vehicles, this is due to the antennas' limited size. Communication is carried out within the line of sight. For low-orbit satellites, the limited communication session is caused by the limited territory of Ukraine, which allows one to create one control point.

3. Increased vulnerability of information security systems.

There are two main technical ways of accessing user data transmitted in cellular communication systems without decrypting information:

- unlimited access to the equipment of cellular operators and terrestrial data transmission channels;

- creation of a transit base station.

In cellular communication, data is encrypted only in the radio-frequency segment - from the subscriber's phone to the base station. And then they are transmitted in the terrestrial channel by wires in an unencrypted form, which enables the attacker to obtain data with unhindered access to the equipment of the mobile operator. This is the method used by law enforcement agencies.

Hypothetical creation of the transit base station will enable the attacker to encrypt and decrypt the data passing in the radio channel (in the zone of operation of this station) practically on the fly. As a result the transmission time of video data using wireless telecommunication technologies can reach several minutes. This reduces the ability to organize encryption of video data on-board aerospace monitoring.

References

[1] V. Larin, N. Yeromina, S. Petrov, A. Tantsiura, and M. Iasechko. "Formation of reference images and decision function in radiometric correlation-extremal navigation systems", Eastern-European Journal of Enterprise Technologies, vol. 4, iss. 9, p. 27 – 35, 2018.

УДК 004.056, 004.75

Н.О. Пунченко[1], О.В. Цира[2]

iioonn24@rambler.ru, aleksandra.tsyra@gmail.com

[1]Одеська державна академія технічного регулювання та якості, Одеса
[2]Одеська національна академія зв'язку ім. О.С. Попова, Одеса

МІСЦЕ І РОЛЬ Е-НАВІГАЦІЇ В ГЛОБАЛІЗАЦІЙНИХ ПРОЦЕСАХ ОРГАНІЗАЦІЇ БЕЗПЕКИ МОРСЬКИХ ПЕРЕВЕЗЕНЬ

Актуальність теми дослідження в тому, що концепція "е-навігація" діскуросмислівает інтеграцію "інформація на борту судна – інформація на березі" і є центральною для забезпечення навігаційної безпеки. Дана концепція інформаційної взаємодії систем свідчить не тільки про загально теоретичному сенсі постанови проблеми, а й її праксеологічні значення на користь безпечного судноплавства.

Становлення і розвиток інтеграційних систем як високорозумних, високотехнологічних, високоінтелектуальних е-систем, які при дослідженні проблеми безпечного судноплавства намагаються вдосконалити сегмент ринку, як судноводіння інноваційними технологіями. У зв'язку з цим е-системи розглядають трирівневу модель інформатизації:

1) медіатизацію – процес вдосконалення засобів і поширення інформації;

2) комп'ютеризацію – процес вдосконалення засобів пошуку та обробки інформації;

3) інтелектуалізація – процес розвитку здатності сприйняття і конструювання принципово нової соціально значимої інформації.

З вище зазначених обставин інтеграцію систем можна представити у вигляді процесу оволодіння інформацією, перетворюючи її в головний ресурс управління, за посередництвом інформаційно-технічних засобів, що підвищують ефективність позиціонування в рамках різних форм і порядків практики.

За таким сценарієм в процесі інформатизації відбувається прогресивно наростаюче використання в судноплавстві інформаційних технологій і їх інформації. Інформація розглядається не тільки як мета і засоби діяльності, а й як результат діяльності. На такій основі формуються принципово нові технології для підвищення безпеки судноводіння.

Для прискорення зростання судноплавної індустрії, на даний момент прийнято наступне визначення концепції e-Navigation: Концепція e-Navigation, впроваджувана Міжнародною морською організацією, має на увазі «узгоджені збір, інтеграцію, передачу, відтворення і аналіз інформації про ситуацію на морі, на борту судна і на берегових об'єктах з використанням електронних засобів з метою вдосконалення процесу плавання "від причалу до причалу" і функціонування відповідних служб для забезпечення надійності та безпеки мореплавання, а також захисту морського навколишнього середовища [1].

Щоб втілити в життя концепцію е-Навігація важлива присутність інформаційної інфраструктури, яка зможе передавати цілісну інформацію.

Першій була концепція, заснована на відпрацьованих хмарних технологіях інтернету, "Хмара моря". Далі "EfficienSea", EfficienSea в розробці якого брали участь вже 12 країн, в силу чого він перетворився з регіонального в європейський [2]. Також ACCSEAS. У 2018 році Норвегія, Нідерланди, Бельгія почали розробляти проект Hull-to-Hull, який фінансує ЄС, завершальна стадія цього проекту в 2020 році.

Функціональним ядром платформи морського зв'язку всіх проектів, які створюються на основі хмарних технологій, є одні і ті ж елементи, які визначили головне "хмара море", так що платформа морського зв'язку може стати не тільки базисом "Інтернету речей" на море, а й передумовою переходу е-Навігації з стадії тестових перевірок в аспект впровадження.

Функції спрямовані на вирішення проблем:

стандартизація та автоматизація процедур складання доповідей береговим і портовим властям;

комплексування і висновок на дисплеї інформації містка, одержуваної з використанням засобів зв'язку.

Ці проблеми є як судновими, так і береговими компонентами е-Навігації, які реалізовують фізичний зв'язок між абонентами і функціональну зв'язок з системою людино-машинного інтерфейсу.

Напрямок концепції е-Навігація, на практиці буде потурати: зниження навігаційних аварій, особливо в зоні охоплення системи управління рухом судна, підвищення рівня інформованості судноводія, в силу трансформації доступу до стандартизованих, найголовніше – надійним даними.

Список літератури

[1] e-Navigation сегодня: Определение, стратегия, цели, задачи, тестовые проекты и разработанные технологии, на ежегодной научно-практической конференции "Перспективы развития и применения комплексов с беспилотными летательными аппаратами", Коломна, 2016, с. 15.

[2] Б. С. Ривкин, е-Навигация на марше, на XIII Всероссийском совещании по проблемам управления ВСПУ-2019 17-20 июня, Москва, ИПУ РАН, 2019, с. 1323 – 1329.

УДК 004.042

О.Я. Різник

riznykoleg@gmail.com

Національний університет "Львівська політехніка", Львів

ЗАВАДОСТІЙКЕ ПЕРЕТВОРЕННЯ ДАНИХ

Метою цих тез є дослідження та удосконалення алгоритму синтезу завадостійких кодових послідовностей. Запропоновані завадостійкі кодові послідовності мають практичну цінність, так як одержувана кодова послідовність дозволяє знаходити до 50% та виправляти до 25% спотворених символів від довжини завадостійкої кодової послідовності.

Для вирішення цієї проблеми розглянемо нееквідистантні кодові послідовності, під якими будемо вважати послідовності, де дозволені кодові комбінації утворюють послідовності з різними відстанями між одиницями та нулями.

Ці нееквідистантні кодові послідовності мають деякі переваги перед іншими завадостійкими послідовностями щодо простоти знаходження і виправлення помилок на стороні прийому даних, бо поява символу "1" та/або символу "0 ", у вигляді завади говорить про помилку, так як змінилась кількість дозволених відстаней. Помилка не знаходиться тільки тоді, коли кількість хибних кодів рівна або більше кодової відстані. Задачу покращення завадостійких характеристик нееквідистантних кодових послідовностей варто вирішувати на основі застосування ідеальних кільцевих в'язанок (ІКВ).

Ідеальною числовою в'язанкою (ІКВ) будемо називати в'язанку, в якій множина всіх чисел вичерпує значення, які є пропорційні елементам натурального ряду з заданою кількістю повторів для кожного елементу цього ряду. Кожній числовій комбінації завадостійкій нееквідистантній кодовій послідовності відповідає набір одиниць та нулів, який будується за вагами ІКВ за наступним правилом: 1 це 1, 2 – 10, 3 – 100, 4 – 1000 і так далі.

Таким чином мінімальна кодова відстань будь-якої завадостійкої нееквідистантної кодової послідовності, що побудована за допомогою ІКВ буде визначена у вигляді співвідношення порядку та кратності ІКВ:

$$d_{\min} = 2(N\text{-}R)$$

Для збільшення кількості дозволених комбінацій нееквідистантних кодових послідовностей за допомогою ІКВ побудуємо дзеркальну завадостійку нееквідистантну кодову послідовність з вагами ІКВ, де поміняємо місцями одиниці і нулі при кодуванні.

Кількість дозволених комбінацій основної та дзеркальної завадостійких кодових послідовностей:

$$P = 2S_N^R$$

Кількість помилок t_1, які виявляються за допомогою завадостійкої кодової послідовності, визначається за допомогою мінімальної кодової відстані $d_{\min}$:

$$t_1 \le d_{\min} - 1.$$

Кількість помилок t_2, які виправляються за допомогою завадостійкої кодової послідовності, визначається кількістю помилок, що виявляються t1:

$$t_2 \le (t_1 - 1)/2$$

Визначимо залежність, що визначає кількість помилок, що можуть бути виявлені t_1 завадостійкою кодовою послідовністю:

$$t_1 \le 2(N - R) - 1.$$

Визначимо залежність, що визначає кількість помилок, що можуть бути виправлені t2 завадостійкою кодовою послідовністю:

$$t_2 \le N - R - 1.$$

Мінімальну кодова відстань для завадостійкої кодової послідовності визначимо як

$$d_{1,2} \le S_N - 2(N - R)$$

Знайдемо оптимальний взаємозв'язок між значеннями параметрів N і R з точки зору найкращої коригуючої здатність завадостійкої кодової послідовності. Завадостійкість цієї кодової послідовності зростає зі збільшенням значення різниці $L = N - R$. Найбільше значення L буде за умови:

$$S_N = 2N.$$

Наведемо взаємозв'язок між параметрами N і R, коли завадостійка кодова послідовність максимально виявляє та виправляє найбільшу кількість помилок:

$$L = \begin{cases} N/2, \ N - парне \\ (N-1)/2, \ N - непарне \end{cases}$$

Отримані на основі ідеальних кільцевих в'язанок завадостійкі кодові послідовності можуть знаходити до N-1 та виправляти до $N/2-1$ помилок за парними значеннями N, і знаходити до N та виправляти до $(N\text{-}1)/2$ помилок за непарними значеннями N за умови, що кількість дозволених комбінацій збільшується вдвічі за рахунок впровадження дзеркальних завадостійких кодових послідовностей.

Застосування алгоритму кодування і декодування даних на основі нееквідистантних завадостійких кодових послідовностей дає змогу суттєвого покращення завадостійкості.

УДК 004.738.5

Т.В. Смірнова, Л.І. Поліщук, О.М. Дрєєв

sm.tetyana@gmail.com, pli_80@ukr.net, drey.sanya@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

ЗАСТОСУВАННЯ СЕРВІСУ CAEaaS ЯК СИСТЕМИ ІНЖЕНЕРНИХ РОЗРАХУНКІВ З ВИКОРИСТАННЯМ ХМАРНИХ ТЕХНОЛОГІЙ

З метою визначення місця сервісу CAEaaS (англ. Computer Aided Engineering as a Service – комп'ютерні системи інженерного аналізу як сервіс), для базових умов, щодо подальших досліджень, у роботі проведений розширений аналіз хмарних обчислень як сервісів. Серед наведених сервісів виділено базові сервіси IaaS, SaaS, PaaS, які є основою для існування більш уніфікованих сервісів (CaaS, MCaaS, DaaS, FaaS, IPaaS, MBaaS, NaaS, SeCaaS, DBaaS, MaaS, GaaS, STaaS, TaaS, DRaaS), що збільшують область використання. Вказані можливі постачальники сервісів, в тому числі і українські. Визначено, що для того, щоб перенести роботу систем інженерних розрахунків та систем автоматизованого проектування (САПР) на хмарну платформу, з'явився досить новий перспективний сервіс CAEaaS.

Аналіз моделей – обслуговування хмарних сервісів показав, що основними сервісами, які призначенні для вирішення різних інженерних задач, розрахунків, аналізу і створення моделей фізичних процесів є PaaS і SaaS сервіси.

PaaS ідеально підходить для ефективного надання програмних середовищ та інструментів для розробників промисловим організаціям, які розробляють і тестують програмне забезпечення та застосунки для баз даних. Це забезпечує повне та централізоване середовище розвитку, яке доступне на вимогу.

При правильній реалізації SaaS може означати значну економію коштів від традиційного підходу до володіння програмним забезпеченням. Ця модель хмарної послуги пропонує мінімізовані витрати на налаштування устаткування та програмного забезпечення, навіть якщо вона забезпечує надмірність і високу доступність, що дозволяє обслуговувати запущені програми. Кінцеві користувачі звільняються від управління та контролю базової IT – інфраструктури. Ліцензії на безпеку, мережу, обчислення та всі ліцензії на програмне забезпечення вкладаються в щомісячну або щорічну плату, виключаючи або значно скорочуючи капітальні витрати. Натомість існує разова вартість доступу до будь-яких бажаних послуг. Організації платять за те, що вони використовують, і часто мають можливість додавати або видаляти послуги за потребою.

Деякі середовища, що базуються на хмарі, включають складні середовища моделювання для повного тестування проектних застосунків перед переміщенням їх у виробничу систему. Програми та застосунки для баз даних можуть бути спеціальними програмами, які промислові організації раніше використовували, але зараз розгортаються на віртуальних машинах у хмарі. Вони також можуть бути додатками, побудованими з нуля в хмарі за допомогою платформи та інструментів, наданих постачальником послуг автоматизації.

У деяких випадках те саме програмне забезпечення може використовуватися для програм SaaS і PaaS. Інженери з управління та процесів можуть використовувати модель PaaS для розробки програми та SaaS для їх виробничого середовища. Наприклад, автоматизація, керування процесами та програмне забезпечення SCADA, що традиційно пропонується лише на базі замовника, доступні як позапроцесорне середовище розробки та моделювання (Open VEP) або як програмне забезпечення SCADA, оптимізоване для забезпечення надійності та безпеки для моніторингу на рівні підприємства та контролю широкорозповсюджених активів.

Розміщення такого програмного забезпечення в центрі обробки даних з прямим високошвидкісним підключенням до телекомунікацій та Інтернету дає можливість швидкодіючого та надійного підключення до всіх віддалених пристроїв та візуалізації загального бізнесу.

В рамках даних сервісів з'являється досить новий перспективний сервіс CAEaaS – комп'ютерні системи інженерного аналізу як сервіс, який покликаний перенести роботу систем інженерних розрахунків та систем автоматизованого проектування (САПР) на хмарну платформу.

CAE або Computer-Aided Engineering – термін, що використовується для опису процедури всього процесу інженерії продукту, від проектування та віртуального тестування за допомогою складних аналітичних алгоритмів до планування виготовлення. Комп'ютерна інженерія є стандартною в майже будь – якій галузі, яка використовує якесь програмне забезпечення для розробки продуктів. CAE – це наступний крок не тільки розробки продукту, але й підтримки інженерного процесу, оскільки він дозволяє виконувати випробування та моделювання фізичних властивостей виробу без необхідності фізичного прототипу. У контексті CAE, найбільш часто використовуються типи моделювання аналізу, що включають аналіз кінцевих елементів, обчислювальну динаміку рідин, термічний аналіз, багатодіагностику та оптимізацію.

УДК 004.421.5

О.Г. Собінов

sagcob14@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

МОДЕЛЮВАННЯ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ХАОТИЧНИМ БІЛЬЯРДОМ СІНАЯ

Процес генерації випадкових чисел (ГВЧ) є невід'ємною частиною багатьох криптографічних операцій.

В даний час існує велика кількість методів генерації послідовностей з різним ступенем випадковості. Однак на практиці більшість цих генераторів виробляють послідовності, властивості яких не відповідають вимогам випадковості і є генераторами псевдовипадкових чисел (ГПВЧ).

Часто в числах, які згенеровані за допомогою таких ГПВЧ простежуються очевидні закономірності. Також, дуже часто генератори ГПВЧ є найбільш слабким місцем у системах шифрування. Справа в тому, що генератори програмного забезпечення повністю детерміновані. Вони використовують різні складні функції для обчислення псевдовипадкових чисел. Послідовності, отримані в результаті роботи таких генераторів, є передбачувані та відтворювані і не придатні для використання в криптографічних програмах.

Системи динамічного більярду виявили добре розвинену хаотична поведінку. Незважаючи на хороші характеристики, ці системи ще не застосовуються у криптографії. Головною причиною є складність вираження рівняння руху частинок в явній формі.

У 1976 році відомий математик Ю.Г. Сінай довів, що поведінка більярдної кулі у динамічному більярді, яка визначається визначеним детермінованим рівнянням, та поведінка більярдної кулі, яке керується процесом Маркова першого порядку, нерозрізнимі. Оскільки марковський процес першого порядку є імовірносним процесом, який залежить тільки від попереднього зіткнення з перепоною, то він є як недетермінованим, так і непередбачуваним.

Програма моделювання руху кулі у більярді Сіная базується на твердженнях, що рух кулі здійснюється без втрати швидкості(тертя відсутнє) та кут падіння дорівнює куту відбиття. Таким чином приймаємо, що рух кулі має швидкості по координатах $V_x=cos(á); V_y=sin(á)$. Звідси $V_x^2+V_y^2=1$.

Приймаємо для побудови алгоритму руху кулі наступні вхідні параметри:

– напрямок руху кулі – $V=\{V_x,V_y\}$,

– початкове положення кулі у більярді – $P=\{P_x, P_y\}$.

Алгоритм моделювання більярду Сіная наступний:

```
Begin
  Px := Value_Px; Py:=Value_Py;//Конкретні початкові координати початку руху кулі
  Vx := Value_Vx; Vy := Valye_Vy;//Конкретний напрямок руху відповідно по координатах x та y
  N := Value_N;//Конкретна кількість ітерацій циклів обчислення точок перетину
  for i:=1 to N do//Кількість зіткнень кулі
   x0 [0..3]:=[1, -1, -1, 1];//Коефіцієнти для векторів, які враховують квадрант знаходження
  y0[0..3]:=[1, 1, -1, -1];// кулі у площині більярду Сіная
  for i:=0 to 3 do//Цикл знаходження координат точок перетину траєкторії руху кулі
    Cx :=Px - x0[i]; Cy :=Py - y0[i];
    D :=(Vx * Cx + Vy * Cy)2 — (Cx 2 + Cy2 - 1);
    if (D > 0) then
    Begin
      t0 := - (Vx * Cx + Vy * Cy) - sqrt(D);
      t1 := - (Vx * Cx + Vy * Cy) + sqrt(D);
      if (t0 > 0) and (t1 > 0) then
      Begin
        t := min(t0 , t1);
        x0 := Vx * t + Px;
        y0 := Vy * t + Py;
        rx := x0 - x0[i];
        ry := y0 - y0[i];
        Vx* :=Vx * (ry2 - rx2) - 2 * Vy * rx * ry;
        Vy := Vy (rx2 - ry2) — 2 * Vx * rx * ry;
        Px* := x0; Py :=y0;
        Vx := Vx* Vy:=Vy*;
      End;
    End;
  End;
End.
```

УДК 621.397

В.І. Солодка[1], М.Ю.Левковська[2]

valyaonas@gmail.com, levkovskaja46@gmail.com

[1]Одеська національна академія зв'язку ім. О.С. Попова, Одеса
[2]Одеський національний медичний університет, Одеса

ФОРМУВАННЯ ТА ФІЛЬТРАЦІЯ СИГНАЛІВ ВЕЙВЛЕТ – ПЕРЕТВОРЕННЯ В ЗАДАЧІ ЦИФРОВОЙ ОБРОБЦІ СИГНАЛІВ

У теперішній час використовуються повсюдно вейвлети фільтрації, для таких завдань, як стискування зображень, завдань при обробці і синтезі різних сигналів, при аналізі зображень самої різної природи, при згортку (стисканні) великих обсягів інформації, та для захисту інформації.

Для формування скорочення цифрового потоку проблема поліпшення якості фільтрації цифрових перешкод на основі одновимірної ДВП була проаналізована з використанням різних порогових функцій та вибору основи вейвлетів. Зважаючи на значний інтерес до цієї проблеми та численні дослідження, пошук способів оптимізації придушення перешкод, наявних у сигналах та зображеннях, залишається актуальним та важливим. При реалізації алгоритмів швидкого розкладання сигналу в вейвлет-базисі довжина вибірки вибирається рівною мірою двійки $N = 2^j$, так як перехід від одного рівня декомпозиції до іншого (більш детальному) еквівалентно зменшенню вдвічі довжини вибірки. Затухаючі характеристики дискретного вейвлет перетворення при збільшенні M (де постійна M визначає довжину області завдання вейвлет-базису)відчуває деякі недоліки при вирішенні деякого ряду завдань. У зв'язку з цим вибір вейвлет-перетворення повинен задовольняти залежно від пріоритетів і вибору сигналів в цифровій обробці сигналів. Разом з цим, зі збільшенням M супроводжується призводить до істотного зростання коефіцієнтів фільтра, що призводить до суттєвих недоліків (підвищення часу обчислень).

У завданнях ЦОС, синтезу фільтрів, розпізнавання об'єктів і стиснення зображень в якості основних функцій для реалізації ДВП застосовують вейвлети Хаара, Добеши.

Для масштабування функції вейвлета Добеши при малих M коефіцієнти h_k можуть бути записані у вигляді точних виразів, наприклад, вейвлет D^4 задається коефіцієнтами:

$$h_0 = \frac{1}{4\sqrt{2}}(1+\sqrt{3}); \quad h_1 = \frac{1}{4\sqrt{2}}(3+\sqrt{3});$$

Для, приклада, наведемо набір коефіцієнтів ВЧ-фільтра, за допомогою якого визначається широко застосовуваний на практиці вейвлет D^8:

$$h_0 = -0{,}0757657, \quad h_1 = -0{,}0296355,$$
$$h_2 = 0{,}4976187, \quad h_3 = 0{,}8037388,$$
$$h_4 = 0{,}2978578, \quad h_5 = -0{,}0992195,$$
$$h_6 = -0{,}0126040, \quad h_7 = 0{,}0322231.$$

У практичних обчисленнях зазвичай використовуються коефіцієнти з точністю до 32-х або 64-х десяткових розрядів. Коефіцієнти розкладання по вейвлет $d_{j,k}$ відображають амплітудні характеристики аналізованих процесів на різних рівнях дозволу. Для фільтрації перешкод невеликі по абсолютній величині вейвлет-коефіцієнти на малих масштабах відкидають перед проведенням метод порогової фільтрації. При цьому якість фільтрації істотно залежить від вибору варіанта завдання порогової функції, на яку збільшуються відповідні коефіцієнти перед зворотним перетворенням і від вейвлет-базису. Відповідний вибір сприяє отриманню більш високої якості очищення сигналу або зображення від перешкод. Існують завдання, де важливіше зберегти регулярність сигналу, ніж точно відтворити його амплітуду. Прикладом служить фільтрація зображень від різних перешкод, де метод "м'якого" завдання порогової функції є широко використовуваним підходом. При аналізі сигналів збереження незмінною амплітуди також не завжди є обов'язковою вимогою.

Що стосується аналізу зображень процедура розкладання по вейвлет передбачає перехід до двовимірної реалізації дискретного вейвлет-перетворення двовимірного ДВП. Такий підхід, зокрема, використовується в комп'ютерній графіці в рамках формату JPEG2000. При практичної реалізації даного формату розглядається розширення одновимірного ДВП, при якому окремо аналізуються рядки і стовпці двовимірного зображення. У цьому випадку проводиться аналіз зображення по горизонталях, вертикалях і діагоналях з однаковим дозволом, і відповідні фільтри формуються на основі творів характеристик НЧ і ВЧ-фільтрів для одновимірного випадку.

Список літератури

[1] O. Gofaizen, O. Osharovska, M. Patlaenko, and V. Pyliavskyi, Complex Algorithm of Image Wavelet Compression: Distortion Evaluation in the Light of Trade of Contour Separation and Compression Ratio 2018, on 9-th International Conference on Ultrawideband and Ultrashort Impulse Signals. Conference Program. Book of Abstracts September 4-7, 2018, Odessa IEEE Kharkiv, 2018, p. 131 – 135.

UDC 681.3

O. Tymochko, S. Osiievskyi, O. Petrov

timochko.alex@gmail.com, stiv161272@gmail.com, ssz2007@ukr.net

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv

MODEL ANALYSIS AND METHODS DESCRIPTION OF INFORMATION – ANALYTICAL SYSTEM ARCHITECTURE

The term “architecture” secured a number of international standards. At the same time, there is a fairly large variety of definitions related term concepts, in addition, the simultaneous use of the terms “structure” and “architecture” indicate the need to harmonize the general concept of “system architecture” and the definition of classes for which this concept is basic.

A characteristic feature of modern projects of information of organizational management processes is their focus not on creating new systems from scratch, but on transformation – reengineering – of existing systems. This context defines the importance of the task of ensuring the effective transformation of the information system architecture. It is well known that architectural design of information systems is an important phase of the life cycle of the process of its development. It is the adequate architectural model and its consistent implementation in the process of information system development that ensures the logical integrity of the project, which ensures its success. The tendency of increasing complexity of information systems, especially distributed ones, has led to increasing requirements for the validity and quality of architectural solutions. This leads to increased requirements for architectural design in general.

Among the issues that are studied in the works devoted to the study of processes of architectural design of information systems, first of all, the following should be noted: definition of the concept of architecture of the information system, objectification of architectural elements and their classification, creation of a formal language for describing the architecture, finding out the relation between the terms “architectural style” and “architectural template”.

Based on the results of the analysis for organizational management information systems, it is established that systems of this type should be designed with the need for their multiple transformations, including at the architectural level. The purpose of transformation is to ensure that changes are adequately reflected in the information system, both in the environment in which the organization operates and in the organization itself as a management entity.

The standard model of information systems reengineering is the horseshoe model, which considers reengineering as a process of interaction of three subprocesses:

– rebuilding an architecture that is to analyze an existing system based on one or more of its logical descriptions;

– transformation of architecture – transformation of these logical descriptions into a new, improved logical description of the system;

– development based on a new architecture – development of a new system that meets the new logical descriptions of the system.

Comparative analysis of system architecture definitions showed that the difference between the architecture of a complex object from its structure may be only clearly established specificity facility components and / or specificity of their interaction. The international standards proposed a conceptual model describing the architecture description specifying components and software architecture rich systems and their relationships rather than components of the system with their attitude, that represent meta description for any architecture. One of the most famous is the Zachman architecture.

The main idea of this metamodel is a selection list of participants (stakeholders, with specific interests (concerns) in relation to the projected system (system of interest), which are issued in the form of viewpoints), which in turn, establish agreements necessary to further the creation, interpretation and use of architectural solutions (view) system.

In terms of systems theory, this means the basic idea being considered complex information – analytical system, where there are several subjects with a common object of activity. Different views of participants on the system sets correspond to certain types of models (model kind); the totality of these models reflects the integral representation (view) system (set its properties and relationships).

It should be noted the possibility of hierarchical (fractal) expansion of the conceptual model (meta) by considering a description of a system architecture components (embedded architecture).

However, in the standard the terms of various “partial” architectures, such as “technical architecture”. That is, in terms of the standard system architecture is a holistic concept, so instead of the terms proposed to use the term “technical representation”. Thus, locked proposed to use a standard metamodel for domains (subsystems domains) of the system. That is Present in the standard ISO / IEC / IEEE 42010: 2011 metamodel architecture requires a description of relevant concepts as additional elements describe the architecture.

УДК 654.02

П.С. Усік, О.А. Смірнов, Н.М. Якименко

mr.usik@ukr.net, dr.smirnovOA@gmail.com, yakimenko_n_m@ukr.net

Центральноукраїнський національний технічний університет, Кропивницький

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ МЕРЕЖЕВИХ ТЕХНОЛОГІЧНИХ РІШЕНЬ В 5G

Концепція 5G

5G це нове покоління радіосистем і мережевої архітектури, яке буде представляти з себе максимальний широкосмуговий доступ, ультра-надійність, малий час затримки підключення і масивні мережі для користувачів та Інтернет речей . 5G буде набагато більше, ніж просто нова технологія радіозв'язку. Вона буде поєднувати в собі існуючі технології радіодоступу з новими, оптимізованими для конкретних смуг частот і розгортання мережі, сценаріїв і варіантів використання. 5G також буде використовувати принципово нову мережеву архітектуру, засновану на технологіях Network Function Virtualization (NFV) і Software Defined Networking (SDN). Програмованість матиме ключове значення для досягнення гіпер-гнучкості, так як стільниковим операторам потрібно буде підтримувати нові вимоги зв'язку, що висуватимуться до них з широкого кола користувачів, пристроїв, компаній з різних галузей промисловості та інших організацій. Мережі 5G повинні бути програмованими, програмно забезпеченими і управлятися цілісно, щоб забезпечити різноманітний і вигідний спектр послуг.

Визначають п'ять ключових аспектів, які описують трансформацію сучасних комунікацій в епоху 5G.

– Можливості визначають нові вимоги, які повинна підтримувати технологія 5G і нові ресурси, які вона створить.

– Універсальна радіосистема досліджує різні технології радіодоступу, які в сукупності забезпечують ультра-гнучке підключення.

– Система систем визначає архітектуру мережі, яка буде необхідна, як вона буде підтримувати нові вимоги і забезпечувати великий досвід і надійний захист, які очікують користувачі та підприємства з різних галузей.

– Практичність пропонує основні етапи розвитку 5G і як оператори зв'язку зможуть розгорнути мережі в найбільш ефективний спосіб.

– Потенціал описує, як нова комунікаційна ера 5G змінить повсякденне життя людей, різні галузі промисловості і весь бізнес стане провайдером зв'язку.

Концепція SDN

Концепція SDN базується на наступних принципах:

– розділення control plane та data plane. В SDN відбувається розділення процесів передачі інформаційного трафіку та трафіку управління;

– єдиний, уніфікований, незалежний від постачальника інтерфейс між рівнем управління та рівнем передачі даних;

– логічно централізоване управління мережею, здійснюване за допомогою контролера;

– програмованість мережі. Метою програмованості є можливість застосовувати програмні додатки, що будуть впливати на всю мережу. Ці додатки можуть підвищити надійність мережі шляхом надання нових засобів безпеки, покращити маршрутизацію трафіку та процес надання пріоритетів, що призводить до кращої якості обслуговування;

– віртуалізація фізичних ресурсів мережі.

Концепція NFV

Network Functions Virtualization (NFV) – це архітектурна концепція, яка використовує технології віртуалізації на рівні мережі і мережевих функцій. Певною мірою NFV можна вважати розвитком концепції SDN (Software-Defined Networking), але більш правильним буде зворотне твердження про те, що NFV використовує SDN. SDN всередині NFV може застосовуватися на мережевому рівні як в інфраструктурі, так і в споживача сервісу. Контролер SDN може бути вбудований в систему менеджменту NFV, може бути реалізований як віртуальна або навіть апаратна сутність. Концептуальне поєднання архітектур NFV і SDN на якісному рівні описано в документі Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework Європейського інституту телекомунікаційних стандартів (ETSI).

Проведені в даній роботі дослідження надали змогу отримати наступні результати. Було проаналізовано ключові напрямки та рушійні сили розвитку стільникових мереж зв'язку п'ятого покоління. В даній роботі було проведено змістовний аналіз перспективних стільникових мереж 5G, визначено основні рушійні сили розвитку мобільного широкосмугового доступу. Також було проаналізовано узгоджену архітектуру стільникових мереж 5G. В даній архітектурі планується використання сучасних технологічних рішень, що нададуть змогу забезпечити критичні вимоги до сучасних стільникових мереж. До цих технологій відноситься віртуалізація мережевої архітектури (NFV), програмно-конфігуровані мережі (SDN) та MEC. В роботі були розглянуті перспективи використання кожного із запропонованих технологічних рішень, а також обмеження та недоліки їх використання.

УДК 004.67

О.О. Чабан, Н.М. Якименко

VisardValimar@gmail.com, Yakimenko_n_m@ukr.net

Центральноукраїнський національний технічний університет, Кропивницький

ВИКОРИСТАННЯ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ У СУЧАСНИХ ОБРОБНИКАХ СИГНАЛІВ

Сама суть сучасних персональних комп'ютерів робить їх залежними від систем числення і від правил, які визначають зв'язок між числами. Однак, залишкова система, або система залишкових класів, яка є темою цих тез, є досить відмінною від двійкової та десяткової систем числення. Внаслідок певних відмінностей залишкова арифметика, яка є маніпуляцією чисел, виражених в системі залишкових класів, пропонує незвичайний набір характеристик. Наприклад, залишкова арифметика забезпечує можливість додавати, віднімати або множити в один етап, незважаючи на протяжність чисел, не вдаючись до проміжних цифр перенесення або внутрішніх затримок. На жаль, залишкова арифметика також має атрибути, які є неприємними та збитковими настільки, що на практиці технологія використання не завжди можлива.

Розглянемо деякі властивості залишкової арифметики в порівнянні з традиційними системами числення. Для проведення порівняння розглянемо властивості десяткової системи. Введемо деякі відмінні властивості систем числення. Межа числової системи визначається як інтервал, над яким кожне ціле число може бути представлено системою через комбінацію двох чисел з одним і тим самим поданням. Очевидно, що десяткова система має невизначені межі, проте в практиці застосовуються усічені системи чисел. Так в комп'ютерах числова межа визначається точно становищем довжини слова і типом використовуваної системи числення. Подання числа називається унікальним, якщо кожне число в системі має тільки одне подання. Однак багато які зазвичай використовувані системи чисел не є чимось унікальним. Наприклад, десяткова система числення, розширена для входження від'ємних чисел, зазвичай має два подання для нуля: + 0 і - 0. Очевидно, що будь – яка система з поданням знаку і величини модуля також не унікальна. Існують деякі системи числення, які використовують змінні уявлення для всіх чисел. Система числення буде надлишковою, якщо існує менше чисел, ніж комбінацій цифр. Альтернативно різні комбінації можуть стосуватися одного і того ж числа. Очевидно, що не унікальність створює надмірність. Наприклад, двійкова система з парними цифрами, доданими в останню позицію цифр, має унікальне представлення для кожного числа, і так як половина комбінацій заборонені, це представлення є надмірним.

З вищесказаного випливає, що тільки дві системи числення знайшли спільне використання в комп'ютерних застосуваннях: двійкова система і двійково – десяткова система. Обом системам властиві такі важливі позитивні риси: проста апаратурна реалізація порівняння чисел; множення або ділення на степінь 2 і 10 можна виконати шляхом зміщення цифр в регістри зберігання; розширення меж системи числення легко реалізується шляхом додавання більшої кількості цифрових позицій; логіка, необхідна для виконання складання, є ідентичною для всіх цифрових позицій; простота виявлення надлишку; просте перетворення з цифрової форми в аналогову.

Ознаки, які ведуть до цих позитивних рис, накладають обмеження на швидкість, з якою можуть бути виконані арифметичні операції, оскільки через поширення перенесення неможлива паралельність операцій. Для всіх арифметичних операцій в цих обох системах числення, кожна цифра результату – це функція всіх цифр рівної або меншої значущості. Ця риса робить непрактичним впровадження паралельного додавання, віднімання, множення або ділення для чисел, що складаються з декількох цифр і, отже, накладає так зване фундаментальне обмеження на швидкість арифметичних операцій.

В системі залишкових класів арифметичні операції є вільними від перенесення, тобто кожна цифра результату – це функція тільки однієї цифри кожного операнда, вона незалежна від всіх інших цифр основ. За рахунок властивості вільного перенесення підвищується швидкість операцій, таких як додавання, віднімання і множення у комбінаторній логіці. Зокрема, для випадку множення, необхідність в часткових результатах виключена.

Виходячи з вищесказаного ми можемо зрозуміти особливості, які несе з собою система залишкових класів, та переваги її використання у приладах та процесах, де потребується прискорене обчислення отриманих результатів. Прикладом використання систем залишкових класів є радіолокація на кораблях, цифрових синтезаторах частот, та в окремих випадках дешифрування.

УДК 681.51

Д.А. Чопенко, К.С. Васюта

dmychop@gmail.com

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків

ВИРІШЕННЯ ЗАВДАНЬ УПРАВЛІННЯ СИЛАМИ ТА ЗАСОБАМИ ПУНКТУ УПРАВЛІННЯ ПОВІТРЯНИХ СИЛ В РЕАЛЬНОМУ МАСШТАБІ ЧАСУ

На сьогоднішній день формалізувати процес управління силами та засобами пункту управління (ПУ) Повітряних Сил (ПС) у повному обсязі не представляється можливим. Тому під управлінням будемо розуміти тільки процес, який пов'язаний з виробленням рішення та реалізацією розподілу сил та засобів ПУ у ході безпосередньої підготовки та ведення бойових дій.

Встановлені особливості управління силами та засобами ПУ ПС, а саме:

– бойові дії будуть виконуватися в умовах гострого дефіциту часу;

– значна кількість інформації, яка надається командиру й на основі якої він повинен приймати рішення;

– прийняття якісного рішення, тобто рішення яке найбільше відповідає ситуації, що склалася, важке через невизначену інформацію.

Слід мати на увазі, що для вироблення рішення на управління повітряними об'єктами ПС командир повинен мати, принаймні, хоча б один варіант дій підлеглих сил та засобів, що визначає розподіл їх по повітряним цілям. Проте в сучасних умовах кількість можливих варіантів дій значно збільшилося за рахунок можливостей, що з'явилися. Це призводить до того, що для вироблення більш обґрунтованого рішення необхідно синтезувати множину варіантів розподілу ресурсів ПУ ПС в конкретній ситуації з урахуванням заданих обмежень на кількість ресурсів, що використовуються, та на час виконання бойової задачі. Усі керуючі впливи на повітряні об'єкти (повітряного противника) здійснюються силами та засобами ПС за допомогою використання множини ресурсів. У загальному випадку система може володіти різними типами ресурсів. Тому в рамках використовуваного формально-логічного апарату структури цільових установок (СЦУ) необхідна розробка моделі використання ресурсів у відкритій експертній системі ПУ ПС. Використання СЦУ в якості апарату формалізації задач управління, що вирішуються на ПУ ПС, передбачає, що особливості предметної області, зокрема, знання про ресурси, описуються за допомогою деякої логічної моделі. Однак жорсткі обмеження, що пред'являються до часу вироблення рішення на ПУ ПС не дають можливості безпосередньо використовувати систему нелогічних аксіом для опису знань про ресурси. Тому існує необхідність в розробці методу формалізації, який би дозволив сформувати структуру знань, що забезпечує їх придатність для вирішення завдань управління ресурсами ПУ ПС в реальному масштабі часу. Проаналізовані порядок і правила використання ресурсів, зумовлені специфікою управління засобами вогневого та інформаційного придушення і інформаційними засобами ПУ ПС, для того, щоб сформулювати основні гіпотези, обмеження і припущення моделі ресурсів. Наведені порядок та основні правила використання множини ресурсів системи. Виходячи з аналізу особливостей даної предметної області, порядок використання ресурсу конкретного типу був представлений у вигляді графа станів. Використання ресурсів керованої системи здійснюється на основі сукупності правил, які сформульовані в нормативних документах (бойових статутах, директивах і розпорядженнях командирів і т.п.). Дані правила можна розділити на наступні групи: нормативні правила використання ресурсу, нормативні правила витрати і поповнення запасу впливів ресурсу і правила спільного використання ресурсів. Обґрунтовані та сформульовані на змістовному рівні такі основні гіпотези моделі ресурсів, які можуть бути використані при формалізації задач управління, що вирішуються на ПУ ПС. Встановлено, що при формалізації задач управління, що вирішуються на ПУ ПС з використанням апарату формалізації СЦУ безліч нелогічних аксіом, які характеризують особливості предметної області, необхідно доповнити сукупністю аксіом, які описують розглянуту модель ресурсів. Наведений вигляд таких даних нелогічних аксіом. Встановлено, що використання СЦУ для формалізації задач управління передбачає, що всі синтезовані варіанти досягнення множини цільових станів повинні задовольняти деякої сукупності ресурсно-часових обмежень. Тому при формалізації знань про правила використання ресурсів необхідно врахувати ці обмеження. Сформульовані ресурсно-часові обмеження, яким повинен задовольняти варіант рішення, що синтезується.

Використання апарату формалізації СЦУ для формалізації задач управління, що вирішуються на ПУ ПС, передбачає необхідність здійснення контролю коректності всіх її структурних елементів на етапах розробки та поповнення бази знань відкритої експертної системи. Знання про правила використання ресурсів і запасу їх впливів є одним з основних структурних елементів використовуваного апарату формалізації, і тому необхідна розробка відповідної процедури контролю їх коректності, що й буду напрямком подальших досліджень.

УДК 004.896

Я.П. Шуліка, Є.В Мелешко

syaroslav1997@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

НЕЙРОННА МЕРЕЖА ALPHASTAR

Зазвичай нейронні мережі доволі вузько направлені, тому створення могутнього навчального алгоритму загального призначення дуже актуальна мета. Один з шляхів такого покращення нейронних мереж це нейронні мережі від компанії DeepMind, які також дуже корисні для розуміння принципів роботи нейронних мереж та людського мозку.

Спочатку ця компанія розробила потужну нейронну мережу для гри в Го під назвою AlphaGo, що вважалася однієї з найскладніших настільних ігор, на даний момент ця мережа навчилася грати в го настільки добре, що майстри, що присвятили життя цій грі признають свою поразку. DeepMind вирішили одразу зробити величезний крок і вирішили розробити нейронну мережу для гри в StarCraft II, стратегію у реальному часі. Складності полягають у тому, що гравці виконують свої дії одночасно, вони володіють неповною інформацією, стратегії працюють у стилі камінь – ножиці – папір, а для перемоги треба планувати свої дії задовго наперед, окрім того у цій грі існує біля 10^26 можливих дій у одиницю часу. З компанією активно співпрацювали розробники гри, Blizzard Entertainment, що допомогли розробити API для взаємодії ШІ з грою, та надали записи ігор для початкового навчання. DeepMind вперше використали мультиагентну систему навчання, кожен агент мережі примітив щось особливе для себе при навчанні та покращував стратегію, що він бачив, таким чином нейронна система мала декілька агентів з різними стратегіями та різним рівнем гри.

Після цього почався мульти-агентний процес навчання, коли агенти почали грати один з одним, по типу як гравці грають один з одним та набиралися досвіду. Метод взяв деякі ідеї еволюційного методи. Він дозволяє реалізувати неперервний процес вивчення всього величезного стратегічного простору гри. І при цьому бути впевненими, що агенти можуть протистояти найскладнішим стратегіям, при цьому пам’ятаючи та не програючи старим. Поки проходив цей процес навчання було помітно як поступово змінюються найпопулярніші стратегії та методи агентів, від швидких стратегій до більш надійних, поступово вивчаючи одні з найефективніших, що використовуються чемпіонами гри. За 2 тижня агенти Alphastar пройшли шлях, що звичайні гравці проходили роками. Різні агенти мали різні власні цілі, від перемоги над певним або кількома опонентами, до перемоги використовуючи лише певні ресурси, із-за цього різні агенти навчалися по різному, а цілі змінювалися під час навчання. Із-за реалізації і неперервного навчання, кожен агент за 2 неділі отримав досвід, що можна порівняти з 200 років гри. Фінальна версія складає розподіл Неша всіх агентів, тобто найефективніше поєднання всіх стратегій, що були виявленні у ході навчання.

Один з важливих факторів у грі – кількість дій, що може виконати гравець за секунду, машинний інтерфейс має колосальні переваги у порівнянні з мишею, тому цей параметр та йому подібні були максимально приближені до рівня звичайного гравця, так щоб агент мав камеру та був змушений також керувати “економікою уваги”. Однак у перших версій це не було добре реалізовано і нейронна мережа мала величезні переваги, це стало причиною чому нейронна мережа показала неймовірний результат проти реальних гравців дивуючи усіх найефективнішим та неможливим для реальної людини мікро- та макро-менеджментом. При цьому інші навики теж були вражаючими, найкращі гравці бачили для себе нові варіанти використання знайомих стратегій, не дивлячись на свій величезний досвід у грі. Окрім найкращих стратегій агенти нейронної мережі також навчилися поганим звичкам, потрійне відправлення армії у одну й ту ж саму точку, та знищення каміння, яке нікому не заважало, можливо це збіг, що під час навчанні за записами звичайних гравців багато гравців діяли так із-за емоцій, або із-за того, що клікнули не туди. Після виправлення цих нюансів AlphaStar почав грати з реальними гравцями, приблизно за місяць, його рейтинг був більший ніж у 99,8% гравців. У матчах з найкращим гравцем нейронна мережа показала відмінний результат, 5 перемог та 0 поразок. Але треба відзначити, що чемпіон грав стандартними стратегіями у яких AlphaStar дійсно став кращим у багатьох аспектів гри, але щодо психологічного аспекту гри, коли кращі гравці знають, що чекати від інших кращих гравців, то нейронну мережу дуже легко подолати виконуючи дії, з якими вона скоріше за все ще не знайома. У деяких випадках вона навіть може на протязі усієї гри намагатися виконати одну й ту ж саму дію, так і не розуміючи, чому гра не дозволяє виконати мережі ту дію, що вона хоче.

Не дивлячись на те, що StarCraft лише гра – розробники впевнені, що використані при створенні техніки можуть бути корисні у інших сферах, наприклад моделювання великих послідовностей можливих дій, як при складанні прогнозу погоди, моделювання клімату, чи розуміння мови.

СЕКЦІЯ 3
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ, МЕДИЦИНІ ТА ОСВІТІ

UDC 628.35:661.5.63

L.A. Aliyeva

Azerbaijan State University of Oil and Industry, Azerbaijan, Baku

FEATURES OF ELECTRICAL CIRCULATIONS

This paper introduces power conversion principles and defines the terminology. The concepts of sources and switches are defined. From the basic laws of source interconnections, a generic method of power converter synthesis is presented. Finally, the notions of commutation cell and soft commutation are introduced and discussed. A switch is a device which is designed to interrupt the current flow in a circuit, in other words, it can make or break an electrical circuit. Every electrical and electronics application uses at least one switch to perform ON and OFF operation of the device.

So the switches are the part of a control system and without it, control operation cannot be achieved. A switch can perform two functions, namely fully ON (by closing its contacts) or fully OFF (by opening its contacts).

When the contacts of a switch are closed, the switch creates the closed path for current flow and hence load consumes the power from source. There are numerous switch applications found in wide variety fields such as home, automobiles, industrial, military, aerospace and so on. In some applications multi way switching is employed (like building wiring), in such cases two or more switches are interconnected to control an electrical load from more than one location. Switches can be of mechanical or electronic type, Mechanical switches must be activated physically, by moving, pressing, releasing, or touching its contacts.

Electronic switches do not require any physical contact in order to control a circuit. These are activated by semiconductor action.

The electronic switches are generally called as solid state switches because there are no physical moving parts and hence absence of physical contacts. Most of the appliances are controlled by semiconductor switches such as motor drives and HVAC equipments.

There are different types of solid state switches are available in today market with different sizes and ratings. Some of these solid state switches include transistors, SCRs, MOSFETs, TRIACs and IGBTs.

Switching circuits are the circuits used in all electrical units that produce, distribute, produce electricity, various devices and apparatus, as well as cables, wires, transformers, machines. As a rule, switching processes are accompanied by transient processes that result from the rapid redistribution of currents and currents in the electrical circuits [1].

The transition from one cycle to another is called the transition of dynamic processes. In this case, in the stationary mode, the constant current remains unchanged from the current and voltages in the circuit, while the alternating current changes as a rule. In the set mode, all parameters are completely dependent on the power source. Therefore, each energy source produces a constant and variable current that is relevant to it. Also, the frequency of the alternating current coincides with the source frequency. In any form, the switching processes occur when the electrical circuits change. Opening the circuit and changing the load can cause various accidents. All these links are called switching. From the physical point of view, all the processes in the energy state transition coincide with the previous and subsequent switching modes [2].

The process is very short – up to one nanosecond. In rare cases, these processes can take as few as ten seconds, if necessary. Transition processes are constantly being studied as they help to create switching circuits. The work of many devices, particularly industrial electronics, is based on these switching processes. In general, electrical circuits are provided by the presence of inductive and capacitive elements that can collect and transmit magnetic and electric fields. At the start of the process, the process of redistribution of electricity between all the elements in the circuit and external sources begins. In part, energy is unilaterally transformed into another type of energy [3].

We can use uninterrupted food sources – like the “black box” we use to protect your computers or protect your other equipment when the network is severed – without having to go deep into electronics. In addition to FQMs to combat power outages or to create uninterrupted power supply systems, voltage stabilizers, filters, diesel engines, etc. can also be used.

References

[1] Caratas, M.A.; Spatariu, E.C. Energy efficiency barriers-contemporary approaches for energetic auditors. J. Environ. Prot. Ecol. 2014, 15, 382–386.

[2] А. Д. Князев, Элементы теории и практики обеспечения электромагнитной совместимости радиоэлектронных средств, Москва, Россия: Радио и связь, 2010.

[3] И. С. Гурвич, Защита ЭВМ от внешних помех, Москва, Россия: Энергоатомиздат, 2008.

[4] Дж. Барнс, Электронное конструирование: методы с помехами, Москва, Россия: Мир, 2009.

[5] Г. В. Алешин, С. В. Панченко, та С. І. Приходько, Оптимізація цифрових систем передачі. Харків, Україна: Укр. держ. акад. залізн. трансп., 2018.

UDC 628.35:661.5.63

Allahverdiyeva Nurana

Azerbaijan State University of Oil and Industry, Baku

GASİFİCATİON BY GASEOUS ABSORPTİON TECHNOLOGİCAL PROCESS RESEARCH

Gasification has been around for more than 200 years. There are to be sure, many reasons, but the two most significant reasons are the continuing high price of natural gas and highway transportation fuels. Granted, over the past year and a half, these prices have moderated considerably. However over the past month, the price of gasoline has inched upward about 30 cents per gallon. The second significant reason is the need for energy independence. In other words, the use of domestic energy sources such as coal not only for electricity production but also for synthetic natural gas (SNG) and liquids for transportation is a must.

Gasification is a key fundamental baseline technology for converting coal to anything other than

electrons and can potentially be competitive even there [1]. For example, gasification it the key conversion step for converting coal to H_2, SNG, liquid fuels, and the capture of CO_2 for sequestration.

Gasification has excellent environmental performance such that some states' Public Utility Commissions have identified Integrated Gasification Combined Cycle (IGCC) plants for power generation as the best available control technology (BACT). In addition, the uncertainty of carbon management requirements and the potential suitability of IGCC for CO_2 controls make it an ideal choice for power.The absorption method is one of the most common methods for gasification of gases. The process is based on the absorption of various gas mixture components in liquids. Absorbent is used for distillation of gasoline, kerosene and saliva. The heavier the hydrocarbons, the greater their solubility in the absorbent [1].

The amount of soluble hydrocarbons increases with increasing pressure and temperature reduction (the amount of heat released during the absorption is equal to the hydrocarbon solubility temperature). The gas absorption facility by gas absorption is shown in (fig.1):

The most common absorbers are spread with narrow plates or hats. In both cases, a liquid layer is stored in the plate, the gas is released from the inside, and the absorption is carried out at relatively low temperatures (30 – 40ºC) and high pressure (10 – 50 atm). The associated gas passes through the regulator and enters the compressor receiver, where it is compressed in one and two stages and sent to the lower part of the absorbent, and the absorbent from above.

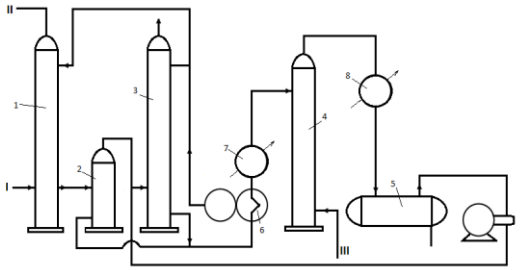


Fig.1. gas absorption facility by gas absorption is shown

The dried gas above the absorbent is sent to the operator after being cleaned in compressor oil.

Absorbent mainly absorbs small amounts of methane and ethane, starting with propane and higher hydrocarbons. The saturated absorbent substance is released from the bottom of the absorbent, and the air enters the absorber, where methane and ethanol are released due to lower pressure.

According to the written scheme, only 50% of propane can be separated from the original solution. An enhanced absorption column, which consists of two different diameters, is used to increase the emission rate of the compressed gases. The upper serves as a small-diameter absorber. From the top it is given a fresh absorbent, and from the bottom gas is injected.

Using an absorption method, 70 – 90% propane, 97 – 98% butane, all pentane and heavy components can be separated from the starting product.

References

[1] И. Л. Гуревич, Технология переработки нефти и газа, Москва, Россия: Химия, 1980.

[2] А. С. Клюев, Б. В Глазов, и А. Х. Дубровский, Проектирования систем автоматизации процессов: справ. пособ., Москва, Россия: Енергоавтомиздат, 1989.

[3] J. Huang, Y. Fang, H. Chen, and Y. Wang, Coal gasification characteristics in a PFB, Energy Fuels, 2003, № 17, p. 1474 – 1479.

[4] M. Mark, Delivering performance in Chinese operations. In Proceedings of the Gasification Technologies Conference, Colorado Springs, CO, USA, October 2009.

[5] Г. В. Алешин, С. В. Панченко, та С. І. Приходько, Оптимізація цифрових систем передачі. Харків, Україна: Укр. держ. акад. залізн. трансп., 2018.

УДК 681.396

Г.В. Альошин[1], О.В. Коломійцев[2], Г.В. Акулінін[3], С.І. Клівець[3]

Aloshingv@gmail.com, Alexus_k@ukr.net, Akuliningv@gmail.com, 1546.hnups@gmail.com

[1]*Українська державна академія залізничного транспорту, Харків*
[2]*Національний технічний університет "Харківський політехнічний інститут", Харків*
[3]*Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків*

ПАРАМЕТРИЧНИЙ ТА СТРУКТУРНИЙ ОПТИМАЛЬНИЙ СИНТЕЗ БАГАТОШКАЛЬНИХ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМ

На даний час існує класифікація методів вимірювання радіоелектронних вимірювачів (вимірювальних каналів інформаційно-вимірювальних систем (ІВС)) [2 – 5]: дискримінаторні (функціональні), панорамні (пошукові), багатоканальні, багатошкальні, багатоетапні та комбіновані. Кожний вимірювач (канал системи) реалізує свій метод вимірювання, відповідає своєму принципу дії і будується на множинах параметрів, сигналів і структур.

Панорамний метод – має простоту у реалізації, але йому присутні і недоліки: великий час на вимірювання та можливість пропуску об'єкту.

Багатоканальний – має мінімальний час на вимірювання, але – складний за кількістю і великою вартістю каналів, а також має багатозначність вимірювань при потужному сигналі. Багатоетапний – вміщує як точні етапи, так і ті, що вирішують багатозначність вимірювань. Багатоканальний метод, а тим більше дискримінаторний, є частковим випадком багатоетапного (комбінованого) методу вимірювання. У такому випадку, процедура порівняння структур вимірювачів спрощена тому, що число типів структур зменшується до трьох або чотирьох. При цьому, різноманіття структур вимірювачів може бути будь-яким. Воно визначається відношенням апріорної невизначеності й апостеріорної, числовими значеннями показників якості, у тому числі – показників ресурсів, тощо. Зокрема, оптимальним може виявитися n-етапний вимірювач, у якого структура кожного етапу може бути побудована будь-яким способом. Для дикримінаторних вимірювачів відома крива обміну, яка зв'язує між собою усі показники їх якостей: дисперсію похибки, апріорний діапазон та відношення потужностей сигналу до шуму. Із аналізу отриманих кривих обміну можливо стверджувати, що найменша дисперсія похибки може бути при малому апріорному діапазоні вимірювань і при малої смузі пропускання, тобто при фазових методах вимірювання, при гармонійних сигналах, що перекривають діапазон. А найбільша точність вимірювань – досягається на більшій частоті за рахунок крутизни фазових детекторів. Отже, фазові багатошкальні вимірювачі мають суттєву перевагу в економії потужності сигналу. Таким чином, існує проблема, яка викликана тим, що при великому апріорному діапазоні та при однозначних фазових вимірюваннях неможливо досягнути високої точності. Це пов'язано з потрібністю мати достатньо велику частоту шкал сигналу, яка забезпечує відповідно найбільшу крутизну шкал фазового детектору і точність. Але при застосуванні великої частоти самої точної потребується додаткове розкриття неоднозначності вимірювань. Отже, актуальна наукова проблема полягає у тому, що необхідно знайти оптимальний метод вимірювання, структуру вимірювача, сигнал і параметри за умовним критерієм максимуму ефективності при обмеженій вартості. В доповіді показана можливість постановки і вирішення задач оптимізації ІВС за критерієм максимуму точності вимірювань різних типів ІВС при обмеженнях на параметри і вартість, а також синтез їх вимірювальної структури і сигналів на трьох множені (структур, сигналів і параметрів).

Представлені методи отримання кривих обміну, аналітичні вирази для вибору методу вимірювання, структури і параметрів вимірювачів для ІВС з панорамним, багатоканальним, багатоетапним і багатошкальним методами вимірювання з одночасними шкалами, або з послідовними в часі шкалами.

Список літератури

[1] Л. С. Гуткин, Оптимизация радиоэлектронных устройств по совокупности показателей качества. Москва, Россия: Советское радио, 1974.

[2] Г. В. Алешин, и Ю. А. Богданов, Эффективность сложных радиотехнических систем. Киев, Украина: Наукова думка, 2008.

[3] Г. В. Алешин, Оцінка якості інформаційно-вимірювальних систем. Харків, Україна: Укр. держ. акад. залізн. трансп., 2009.

[4] Г. В. Алешин, Ефективність інформаційно-вимірювальних радіотехнічних систем. Харків, Україна: Укр. держ. акад. залізн. трансп., 2005.

[5] Г. В. Алешин, С. В. Панченко, та С. І. Приходько, Оптимізація цифрових систем передачі. Харків, Україна: Укр. держ. акад. залізн. трансп., 2018.

UDC 628.35:661.5.63

A. S. Asadzadeh

Azerbaijan State Oil and Industry University, Baky

THE USE OF DIGITAL TECHNOLOGY IN OIL REFINING

Smart manufacturing will transform the oil refining and petrochemical sector into a connected, informationdriven environment. Using real-time and high-value support systems, smart manufacturing enables a coordinated and performance-oriented manufacturing enterprise that responds quickly to customer demands and minimizes energy and material usage, while radically improving sustainability, productivity, innovation, and economic competitiveness. In this paper, several examples of the application of so-called "smart manufacturing" for the petrochemical sector are demonstrated, such as the fault detection of a catalytic cracking unit driven by big data, advanced optimization for the planning and scheduling of oil refinery sites, and more. Key scientific factors and challenges for the further smart manufacturing of chemical and petrochemical processes are identified.

Several different types of digital technology are used in oil refineries. Before you go to oil wells or in your office, you need to be able to use digital technology.

Seismic description. First technology – 3D seismic image technology. This method is used to create a three – dimensional method of geologic stratification of the voltage at the base of the longitudinal plane. The simplest method is to approach the volcanic, solitary and carbonate powders. MAZ, Multipurpose Azimuth This paper outlined the main opportunities and challenges regarding smart manufacturing for an oil refinery or petrochemical plant by demonstrating the progress in so-called "smart manufacturing". Although considerable progress has been made, there is still a long way to go to achieve true smart process manufacturing. PSE is expected to take a central role in guiding, and perhaps shortening, the new journey toward smart process manufacturing. From an academic perspective, it is best for the industry to provide the test beds; while from an industrial perspective, it is best for academia to offer a reliable and scalable platform that includes hardware and software to update the instrument technology level.

In fact, these two aspects complement each other. An industryuniversity research coalition is urgently needed for the future. (WAZ), WATS is used in 2000 oil wells, and in 2009 – 2010 years, with 150 million barrels of oil. The 4D seismic image is used in parallel with 3D images. This taxis compels mobile mobility and allows you to disconnect the edges in the field.

The Tube. "Intelligent or Intelligent Pipe" – a tube with sensors and valves inside. Operators need to disconnect the exhaust, heat and temperatures in the freezing pipe without the use of pipes or other pipes in the real time mode.

The system switches on and at the same type of valves: valve control valve – ICV and control valve (ICD). ICV sockets are the active valve, which translates into a controlled/open function. ICD has fixed overlays and a category of passive valves.

SCADA system. The SCADA Dispatch Control System (SCADA) system is turned on for monitoring of pipelines, process control, oil refining and multifunction. Easy to add, get rid of, and wait for processors. SCADA system is based on telephone lines. The SCADA system is based on WAN. The simplest meat system does not have a better control. The SCADA remote control system is based on the local network. The meat system SCADA uses several stations to get rid of all that. If you want to use a user – friendly protocol in a system, it is not possible to save it with an advanced machine. Developing a SCADA system with built – in architecture, web – based systems and standards. SCADA switches on: RTU (remote terminal), PLC, telemetry system, server integration data, HMI (shut – down machine interface), stationary control and control station. The SCADA system is a modern technology based on advanced technology.

SRM. Intelligent technology is embedded in software and hardware integration. The SRM model is used in smart oil refineries. Using SRM Plug – In Simulation Models Plugs New Roots, Moving Forwarding And Investing In Plastic Analysis. The SRM is used in a multi – layered simulation model collector, which translates into a real – time mode in real – time mode. The SRM simulates the visibility of the polynomial model with a high frequency. Used in all stages of development of oil deposits in the oil industry.

Manage peace and security:

– Implicit post-simulation model for all-oil saturation in real-time mode;

– Predictive modeling;

– nonlinear analysis;

– optimization in real time;

– The SRM model incorporates a digital simulation model in real-time mode.

References

[1] G. Stephanopoulos, and G. V. Reklaitis, Process systems engineering: From Solvay to modern bio- and nanotechnology. A history of development, successes and prospects for the future. Chem Eng Sci, 2011, № 66(19), p. 272–306.

[2] D. Li, "Perspective for smart factory in petrochemical industry", Comput Chem Eng., 2016, 91:136–48.

UDC 628.35:661.5.63

Rzayev Asif

Azerbaijan State Oil and Industry University, Baku

DEVELOPMENT OF SPEED CONVERTER CONSTRUCTION AND PREPARATION TECHNOLOGY

Design of a frequency converter from 50 Hz to 60 Hz – The power that this frequency converter can produce depends mainly on the values of C1 and C2; the larger they are, the greater the output. Transistors are great for low power applications and can handle more power, assuming they are installed in an adequate heating device and the control unit will not be affected at all. Since this circuit receives an output voltage of 110 V, it can be used as such a voltage converter if the device does not require 60 Hz and operates at 50 Hz, but in this case a transformer is really a better solution.

We can divide the frequency converter into three different parts. One is a 110V rectangular switch (inverter), the other is a switching control unit, and the third is a low-voltage power supply for the control unit. First, let's take a brief look at the different parts, starting with the switch inverter section.

C1 and C2 are connected from the single-phase 230 V mains to a total of 320 V from the diode bridge and are divided equally between the two. There is no power factor correction, so this design is only suitable for relatively small loads. Several resistors of equal value in parallel with C1 and C2 ensure that the voltage is evenly distributed between the two capacitors. I also added a protector to the inverter part not shown in the diagram at the entrance to the line. This is to prevent overload (fig. 1).

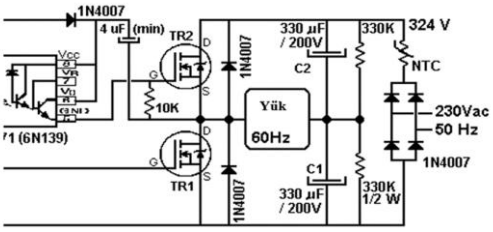


Figure 1. Design diagram of a frequency converter

The load is connected from one end to the midpoint of C1 and C2, the other end is alternately replaced by a half-bridge created by TR1 and TR2 between the high and low rails. The reverse side 1N4007 diodes are shown in parallel to each of TR1 and TR2. This is to protect against crossings due to inductive loads. In fact, I did not install them because the MOSFETs IRF830 are built into this diode. I installed two transistors on one radiator, although they hardly heat up with a reduced load, but by increasing the values of C1 and C2, the inverter circuit can be upgraded to have greater power, and the transistor temperature would not be a problem. This is a good thing to work at low frequencies such as 50 Hz and 60 Hz.

For the output to be peak, the output must be:

1/4 cycle = 0 V (both transistors are connected),

1/4 circuit = +160 V (conducts TR2),

1/4 cycle = 0 V (both transistors are connected),

1/4 cycle = = 160 V (TR1 conducts).

The design is quite simple and works well at 60 Hz, but is not suitable for high switching frequencies because there are delays in closing the TR2 and the circuit must be changed to turn it off faster (which is not difficult to do). This is because the door discharges from the capacitor instead of having a signal that forces it. Changing the value of the resistor speeds up the shutdown time, but requires a higher current when the transistor is turned on.

Now let's look at the control part of the frequency converter. A classic 555 oscilloscope with a speed of 960 Hz, a four-stage CD4029 meter (divided into 16) and three NOR elements are installed at the output. These waveforms explain themselves. T1 and T2 can be seen to be positive in 1/4 of the period. S2 is applied with an optocouple that changes the TR2 level.

Tap 1 of the 4029 meter, preloads the value set to Q1-Q4 at points 4, 12, 13, 3 when connected to voltage, and the meter is considered normal when connected to ground. This means that we can stop the output by pulling high. It will take a second to start working after the power is applied to the resistor and capacitor as shown. At first I used a frequency converter, but then I removed the capacitor to speed up my test and never replaced it. You can use it or not, or you can use a link according to your needs. In addition, it can be used to apply load protection with a high-carrying circuit when it detects excessive current at the output.

References

[1] A. M. Kopylov, I. V. Ivshin, A. R. Safin, R. Sh. Misbakhov, and R. R. Gibadullin, “Assessment, Calculation And Choice Of Design” Data For Reversible Reciprocating Electric Machine International Journal of Applied Engineering Research, 2015, № 12, c. 31449–31462.

UDC 628.35:661.5.63

Rzayev Asif

Azerbaijan State Oil and Industry University, Baku

DEVELOPMENT OF SPEED CONVERTER CONSTRUCTION TECHNOLOGY

All frequency converters work on the following basic principles: The alternating voltage, which is converted to a constant current of 50 Hz, is transferred directly from the internal circuit to the voltage medium and the energy is stored in the capacitor. The current converter inside the external circuit converter converts the middle circuit directly to voltage. In converters operating on this principle, the alternating current motor is suitable for use at different speeds.

Several attributes dictate how devices are used. Devices such as diodes conduct when a forward voltage is applied and have no external control of the start of conduction. Power devices such as silicon controlled rectifiers and thyristors (as well as the mercury valve and thyratron) allow control of the start of conduction, but rely on periodic reversal of current flow to turn them off. Devices such as gate turn-off thyristors, BJT and MOSFET transistors provide full switching control and can be turned on or off without regard to the current flow through them. Transistor devices also allow proportional amplification, but this is rarely used for systems rated more than a few hundred watts. The control input characteristics of a device also greatly affect design; sometimes the control input is at a very high voltage with respect to ground and must be driven by an isolated source. As efficiency is at a premium in a power electronic converter, the losses that a power electronic device generates should be as low as possible. Devices vary in switching speed. Some diodes and thyristors are suited for relatively slow speed and are useful for power frequency switching and control; certain thyristors are useful at a few kilohertz. Devices such as MOSFETS and BJTs can switch at tens of kilohertz up to a few megahertz in power applications, but with decreasing power levels. Vacuum tube devices dominate high power (hundreds of kilowatts) at very high frequency (hundreds or thousands of megahertz) applications. Faster switching devices minimize energy lost in the transitions from on to off and back, but may create problems with radiated electromagnetic interference. Gate drive (or equivalent) circuits must be designed to supply sufficient drive current to achieve the full switching speed possible with a device. A device without sufficient drive to switch rapidly may be destroyed by excess heating.

Practical devices have non-zero voltage drop and dissipate power when on, and take some time to pass through an active region until they reach the “on” or “off” state. These losses are a significant part of the total lost power in a converter.

A frequency converter or inverter must be used for a 3-phase induction motor to rotate at different speeds or at the same speed in all conditions. Controlling the speed of an induction motor with a frequency converter has several advantages. Large powerful engines will consume high energy. To prevent such high energy consumption and to ensure that the motors rotate at the desired speed, a frequency inverter has been developed that operates at any constant speed without exhausting the engine by producing variable frequencies.

The basic principle of a frequency converter:

The basic idea in nature is simple, the process of converting a stable power line into a frequency change is basically done in two steps:

1. The alternating current power source is rectified to a direct current source.

2. DC voltage is divided by the alternating voltage of the desired frequency.

The DC voltage of the inverter is obtained from a single phase. Three phases are derived from alternating current, and three-phase asynchronous motors operate on these three phases. With the feedback signal to be received from the motor shaft, the motor can be rotated at any constant period by changing the feed voltage and frequency value of the motor in proportion to the load changes connected to the motor shaft. It is desirable that the induction motor rotate at different speeds or at the same speed under all load conditions. A frequency converter or inverter must be used for this purpose. Various inverter applications have been developed to produce the right torque, reduce harmonics and increase engine efficiency.

References

[1] A. M. Kopylov, I. V. Ivshin, A. R. Safin, R. Sh. Misbakhov, and R. R. Gibadullin, “Assessment, Calculation And Choice Of Design Data For Reversible Reciprocating Electric Machine”, International Journal of Applied Engineering Research, 2015, № 12, c. 31449–31462.

[2] V. Gureich, "Electronic Devices on Discrete Components for Industrial and Power Engineering", CRC Press, New York, 2008, p. 418.

UDC 628.35:661.5.63

İmran Bayramov

Azerbaijan State University of Oil and Industry, Baku

ANALYSİS OF HARDWARE AND SOFTWARE ON ECOLOGICAL MONITORING

An information resource is individual documents and individual document arrays, documents and document arrays in information systems (libraries, archives, funds, data banks, other types of information systems. In the regulatory aspect, a document is defined as information recorded on a physical medium with details that allow it to be identified.

The documentation process turns information into information resources.

The processes that ensure the operation of an information system for any purpose can conditionally be represented as consisting of the following blocks:

1. input information from external or internal sources;
2. processing of input information and its presentation in a convenient form;
3. information output for presentation to consumers or transfer to another system;

feedback is information processed by people of a given organization to correct input information.

Information processes are implemented using information procedures that implement a particular mechanism for processing input information into a specific result.

The following types of information procedures are distinguished:

- Fully formalized, in the implementation of which the information processing algorithm remains unchanged and completely defined (search, accounting, storage, transmission of information, printing of documents, calculation on models).
- Unformalized information procedures, during which new unique information is created, and the algorithm for processing the initial information is unknown (the formation of a multitude of alternatives, the choice of one option from the resulting set).
- Poorly formalized information procedures during which the information processing algorithm may change and is not completely defined (planning task, evaluating the effectiveness of economic policy options).

Functions of information units creating and supporting information systems (administrator service): notification and processing of requests; maintaining the integrity and safety of information; periodic revision of information; automation of indexing information.

There are high requirements for the quality of the data stored in a particular system and the service results. These requirements are particularly difficult, for example, when they affect the safety of citizens at the end of the system. Therefore, control over system delivery and access by system users is a natural and appropriate way to ensure the quality of the systems and services provided. The quality of the information provided and the quality of the research here is determined by their attention, integrity and goodness. The certification and efficient investigation process is laborious and time consuming. Because the required documentation is always required, it is imperative to ensure interaction between businesses and users when completing and querying the database. Therefore, the patchwork process can take quite a long time (even a few days). When the data and the student are large enough, it is also recommended to maintain an alliance between the user and the user. To ensure that Alchemist works effectively, it is necessary to define the composition and leaders of the devices used [1].

As a data collection unit and a truly socialist independent structure, it should ensure that the following functional issues are addressed:

A Collection, processing and storage of various large-scale transmitters from various sources (may not have access to allied data);

High Compliance with high requirements for the quality of both incoming and outgoing data; This is achieved by applying additional measures to process incoming information;

The existence of various types of queries belonging to different users of the system; this requires a suitable application software.

It is important to note that socialists should be assigned to collect information about specific claims and access to surveys.

The jokes of the most popular algorithms also show that these algorithms require additional information about external infotainment systems and that these features can be distinguished from their existing infrastructure.

A special feature of the socialist, as mentioned above, is that it works in an integrated system to support communication with infrastructure systems. This modernist socialist has to do basic integration functions.

In the interpretation, it is necessary to collect appropriate information and methods for the collection of information and the follow-up of the most efficient procedures and maintenance of corridors.

As a result of the aneurysm, the structure of the alchemist and its compounds should be summarized.

References

[1] W. Stallings, Data and Computer Communications, Fifth Edition Upper Saddle River, NJ: Prentice Hall, 2007.

UDC 622.413.3

N.Y. Bayramzade

Azerbaijan State Oil and Industry University, Baku

OPERATION OF THE TEMPERATURE MEASUREMENT SYSTEM WITH COMPENSATION OF ENVIRONMENTAL

The international reference temperature used by the calibration community is 20 °C and CMMs and machine tools are normally calibrated with reference to this temperature. In a normal factory environment where precise temperature control is often not available, the machine will not be at this temperature. Because most machines expand or contract with temperature, this can cause an error in the calibration. To avoid this calibration error, the linear measurement software incorporates a mathematical correction called thermal expansion compensation or 'normalisation' which is applied to the linear laser readings.

The software normalises measurements using the coefficient of expansion of the machine, which must be entered manually, and a mean machine temperature measured using the XC compensator and material temperature sensor. The objective of this correction is to estimate the laser calibration results that would have been obtained if the machine calibration had been performed at 20 °C.

The thermal expansion coefficient of a machine is specified in parts per million per degree C (ppm/°C).

These coefficients specify the amount that the material will expand or contract for every degree rise or fall in material temperature. For example, suppose the coefficient of thermal expansion is +11 ppm/°C. This means that for every 1°C rise in material temperature, there will be a material expansion of 11 ppm, which is equivalent to 11 μm/m of material.

Incorrect compensation for material thermal expansion is one of the primary sources of error in laser linear distance measurements in non-temperature controlled environments. This is because the expansion coefficients of common engineering materials are relatively large compared to the coefficients associated with wavelength compensation errors and laser beam alignment errors.The principle of using glass fluid thermometers is based on the thermal expansion of fluids. With the change of temperature, the thermometric fluid changes and the state of the fluids changes in the direction of temperature measurement.

Manometric Thermometer – The principle of operation is based on changes in the volume of gas, liquid or saturated vapor, depending on the temperature and temperature. Structurally, a thermometer consists of a thermal lamp immersed in a controlled environment, a pressure gauge, and a capillary to measure pressure. Gas gauge thermometers are used to measure temperatures from -200 to 600°C. Used as a filler for helium (low temperature), nitrogen (medium temperature) or argon (high temperature). Thermocouple is made up of two different metals that form a voltage (expressed in millivolts) by changing the temperature in one piece. The two metal joints, called the junction, are connected to the extension cords. Both different metal can be used for a thermocouple. The working principle is as follows:

1) When two separate metals are joined together, a small tension occurs at the junction at the thermo junction. This is called the Peltier effect.

2) When the temperature of the coupling changes, it also causes variability and the electronic controller is measured by the input circuits. The output is proportional to the temperature difference between the joints and the open ends. This is called the Thompson effect.

3) Both of these effects can be combined to measure heat. By combining at a specific temperature (reference point) and measuring the voltage, the temperature at the sensing junction can be removed. The generated voltage is proportional to the heat difference. The combined effect is known as the thermo junction effect or Seebeck effect.

Resistance Temperature Detector is basically a long, small diameter metal wire, or a rod cipher on a substrate, like a high degree of voltage. Operation Principle – Resistance temperature detectors work on the principle that a metal's electrical resistance can change in a linear and repetitive way, with the change in temperature. The RTD has a positive temperature coefficient (resistance increases with temperature).

References

[1] H.H Plath, Checking Accuracy of 3D-CMMM by Use of Diffrent Types of Calibrated Artifacts – a Comparative Report ofIndustrial Experiences. Proceedings First International Work-shop on Coordinate Measuring Machine Calibration. Prague (Czech Republic), June 1 – 2, 1999, p.36 – 42.

[2] E. Ratajczyk, Methods of checking on the accuracy of coordinate measuring machine. Procedures and programs for determining the errors of length measurements by means of plate master, Part IV, Mechanik 11, 1999, p.757 – 765.

UDC 621.183.9

Fahri Nifdalızade

Azerbaijan State Oil and Industry University, Baku

ANALYSİS OF HARDWARE AND SOFTWARE ON ECOLOGICAL MONITORING

The term ecological monitoring refers to the system of monitoring, monitoring and evaluating, forecasting and information support system. The purpose of environmental monitoring is to provide environmental management and information management of environmental safety. The earth has been facing ecological pollution, especially in recent years. To solve the problem, it is necessary to measure the pollution level and take the necessary precautions. Sensors are installed at the area for monitor to degree of pollution. The data we receive from the sensors represent the degree of contamination.

An environmental monitoring system is the process that monitors the quality of the environment. The RMS software allows for a realtime monitoring of any parameter required. Rotronic offer solutions for relative humidity, temperature, dew and frost point, differential pressure, pressure, flow, lux and CO_2. For all other parameters, Rotronic offer an analogue to digital converter so that all analogue signals can be monitored. The RMS-Converter will allow you to integrate any digital product (with a LAN connection) into the RMS software giving you the highest flexibility possible.

The RMS hardware itself gives you the possibility to log down to 10s intervals and the data can be viewed via the RMS webpage if you choose the cloud solution, but also via your own server should you choose the server version.

The software offers charts and graphics, as well as an alarming function (EMail, SMS, Telephone call). The analysis tool will allow for you to establish daily, weekly, monthly or personalised reports with all of the statistical data required. The Rotronic hardware and software comply to the FDA CFR 21 Part 11 regulations and and designed based upon the GAMP5 guidelines.

- Monitor any parameter (Rotronic products, integration of 3rd party analogue and digital devices).
- Log between 10s and 15 minutes.
- World wide data access.
- Highest flexibility in terms of software setup.
- Cloud or server based solutions.
- FDA CFR 21 Part 11 compliant software.

A lot of researchers investigated this problem. Previous researches have attempted to establish network air quality monitoring and diagnostic systems. SensorScope [1] and CitySense [2] are examples of large – scale wireless environmental monitoring systems. SensorScope is designed for spatial and temporal observations in – situ throughout the landscape. CitySense supports the development and evaluation of city-wide wireless systems using more than 100 Wi – Fi enabled Linux based computers installed on buildings and on street lamps. SensorScope uses solar energy with a comprehensive radio circulation to prevent power outages, while CitySense uses wired power supplies. Another power intensive platform is N-SMARTS, a GPS – capable mobile phone or city – level environmental data collection system. The sensor module consists of carbon dioxide, carbon monoxide, triaxial accelerometer and temperature sensors. SensorMap is a network that monitors mobile air quality of sensors that can detect O3, NO2, and CO/VOC. The program focuses on data collection and presentation, but does not take into account gas sensors and energy management features. LaserSPECks are based on a laser spectroscopic trace gas sensor platform. By integrating quantum cascade laser technology, a wide range of detectable gases is provided, reducing both system size and cost. However, energy consumption is not taken into account.

The results of the environmental monitoring constitute the database (data bank) of the PoE (protection of environment), which enables the use of computers to collect, store, process and analyze information. The information provision of the PoE, in turn, is the basis for the management of nature protection activities and the implementation of resource protection policies. We must to build the sensor network for the monitoring and get the results from sensors. After the getting results send them to the database.

We put the air sensors to the electric poles which are located all the sides of city for the measure of air pollution. The data from these sensors be collected in a central database to check which areas of the city are likely to be contaminated.

References

[1] G. Barrenetxea, F. Ingelrest, G. Schaefer, M. Vetterli, O.Couach, and M. Parlange, "SensorScope: Out-of-the-Box Environmental Monitoring", In Proceedings of the 7th International Conference on Information Processing in Sensor Networks, St. Louis, MO, USA; IEEE Computer Society: St. Louis, MO, USA, 2008.

[2] R.N. Murty, G. Mainland, I. Rose, A.R. Chowdhury, A. Gosain, J. Bers, and M. Welsh, "CitySense: An Urban-Scale Wireless Sensor Network and Testbed", In Proceedings of the 8th IEEE Conference on Technologies for Homeland Security, Waltham, MA, USA; IEEE Computer Society: Waltham, MA, USA, 2008.

УДК 004.6

В.С. Гермак, В.А. Бісюк

germak_vs@ukr.net, kntubisuk@ukr.net

Центральноукраїнський національний технічний університет, Кропивницький

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ПОБУДОВИ РЕКОМЕНДАЦІЙНИХ СИСТЕМ

Рекомендаційні системи — це системи для фільтрації контенту, що намагаються передбачити, які продукти можуть зацікавити користувача.

Основними проблемами при побудові рекомендаційних систем є: розрідженість даних (багато користувачів та продуктів, мало оцінок); проблема холодного старту (нові для системи продукти або користувачі); масштабованість (ускладнення роботи системи зі збільшенням кількості користувачів і продуктів); синонімія (однакові по суті продукти або їх категорії мають різні назви); шахрайство (штучне збільшення рейтингу); забезпечення різноманітності (популярні товари можуть витісняти новачків на ринку і тим самим знижувати різноманітність рекомендацій); білі ворони (користувачі, інтереси яких протилежні до інтересів більшості). Щоб уникнути виникнення перелічених проблем, при розробці рекомендаційних систем застосовуються різні методи. Основними є методи колаборативної фільтрації, контентної фільтрації і метод експертних систем (метод, заснований на знаннях).

Системи колаборативної фільтрації рекомендують продукти в залежності від оцінок користувачів, розрізняють User-Based і Item-Based системи. В User-Based системі для прогнозування інтересів конкретного користувача треба знайти інших користувачів зі схожими смаками. При цьому є ряд проблем: смаки користувачів з часом змінюються і система може генерувати безліч неактуальних рекомендацій; чим більша кількість користувачів, тим більше часу йде на генерування рекомендації; система погано працює, коли продуктів багато, а оцінок мало; система уразлива для накрутки рейтингів, коли зловмисник необ'єктивно підвищує оцінку одних продуктів в порівнянні з іншими. В Item-Based системі схожість двох елементів розраховується по рейтингах, виставлених користувачем. Якщо певним користувачам одночасно сподобалися декілька продуктів, то можна зробити висновок, що більшості користувачів, які високо оцінили один з них, повинні сподобатися і інші. Частенько віддається перевага саме Item-Based системам, оскільки вони позбавлені усіх недоліків, властивих User-Based системам. По-перше, елементи в системі не змінюються з часом, тому рекомендації вийдуть більш релевантними. Крім того, продуктів зазвичай значно менше, ніж користувачів, тому обробка даних при такій фільтрації відбувається швидше. Зрештою, такі системи набагато складніше обдурити. Для колаборативної фільтрації в цілому властиві проблеми холодного старту, розрідженість матриці рейтингів, ресурсоємність обчислень, необхідність наявності великого обсягу даних для високої точності рекомендацій.

У контентних рекомендаційних системах рекомендації формуються на основі атрибутів, що привласнюються кожному елементу. Складніші системи в змозі виявляти співвідношення між множинними атрибутами і давати якісніші рекомендації. Цей метод не вимагає наявності великої групи користувачів для забезпечення точності результату, практично відсутня проблема холодного старту по продуктах (досить мати заповнені характеристики нового об'єкту). До недоліків можна віднести наявність проблеми холодного старту по нових користувачах, труднощі з побудовою рекомендацій при обмеженій інформації про продукти. Експертні рекомендаційні системи особливо корисні для роботи з продуктами, які придбаються нечасто, наприклад будинки або дорогі предмети розкоші. У цих системах рекомендації пропонуються не на основі рейтингів, а на основі схожості між вимогами користувача і описом продукту. Тому система такого типу виходить унікальною, адже вона дозволяє клієнтові явно вказати, чого він хоче. Перевагою є точніше визначення вимог користувача завдяки явній взаємодії з системою.

Гібридні рекомендаційні системи. У всіх розглянутих рекомендаційних систем є свої переваги і недоліки. Експертні системи найбільш ефективні в контекстах, де кількість доступних даних обмежена. Колаборативна фільтрація краще всього працює в середовищах, де є великі масиви даних. Часто можна скомбінувати рекомендації, отримані декількома способами, тим самим підвищивши якість системи в цілому. Існують такі прийоми комбінування рекомендацій: зважені, де рекомендаціям, отриманим різними методами, привласнюється різна вага, тобто деякі рекомендації вважаються прийнятнішими, ніж інші; змішані, тобто загальний набір рекомендацій, без явної переваги тим або іншим класам; доповнені, де рекомендації від однієї системи використовуються як вхідні дані для наступної; перемикання, або вибір випадкового методу. Плюс такої системи – висока точність, мінус – найвища складність розробки. Таким чином, можна дійти висновку, що за наявності можливостей завжди краще спиратися на сукупності алгоритмів, а не на єдиний алгоритм.

УДК 355.415

О.М. Гурін, Н.Є. Сальна, В.В. Старцев, І.О. Гурін

Goorin61@gmail.com

Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків

РОЗГЛЯД ПИТАНЬ ЩОДО УПРАВЛІННЯ ЗАПАСАМИ ДВОСТУПІНЧАСТОЇ ЕШЕЛОНОВАНОЇ СИСТЕМИ СКЛАДІВ

В розвинутих у військовому відношенні країнах світу логістика стає невід'ємною частиною операцій, оскільки від своєчасного, повного та безперервного забезпечення військ залежить їх успіх (ефективність), збереження людського та технічного ресурсу, а також швидкість його відновлення.

Управління запасами є однією з основних складових логістичного забезпечення, пов'язана зі значною обчислювальною складністю. Підготовка до застосуванням за призначенням пов'язана з прогнозом та необхідністю врахування невизначеності, підвищення оперативності прийняття рішень [1].

Логістичні системи планування запасів для Повітряні Сили (ПС) Збройних Сил (ЗС) України є ієрархічними, територіально розрізненими та ешелонованими, гнучкими за місцями розташування, з підвищеними ризиками втручання та втрат.

Планування запасів ПС ЗС України має лише йому притаманні особливості, які стосуються забезпечення бойових дій (БД) з'єднань та частин родів військ, що ведуть збройну боротьбу у бойових порядках майже на всій території України. Прикладом складності може бути організація забезпечення підрозділів радіотехнічних бригад (РТБР) ПС ЗС України, які розташовані у бойовому порядку на території 7–8 областей України. Питання забезпечення погіршується тим, що відстань від складів РТБР до окремих підрозділів складає від 100км до 600км [2].

Існуюча структура підрозділів забезпечення, обсяги запасів та їх ешелонування у тактичній ланці в основному відповідають завданням, які покладені на військові частини ПС ЗС України. В той же час, в зв'язку з обмеженою штатною наявністю засобів підвозу та значних відстанях від органів забезпечення, запасів матеріальних засобів вистачає на обмежений термін ведення БД, що потребує розробку моделей багато ешелонованої системи управління запасами [2].

Таким чином, застосування сучасних інформаційних технологій, розробки моделей та методів автоматизованого управління процесами логістичного забезпечення з урахуванням специфічних завдань та особливостей ведення операцій – є необхідністю сучасності.

В переважній більшості випадків зустрічаються більш складні для управління потоками матеріальних засобів види ешелонованих систем переміщення майна: розгалужені, комбіновані і двоспрямовані. Однак, нажаль ешелоновані системи підпорядковуються різним організаціям. В такому випадку об'єднані центри забезпечення, склади військових частин можуть бути різного підпорядкування. У такій системі кожна організація має можливість сама обирати стратегію функціонування складського господарства і управління запасами, що знаходяться в її підпорядкуванні [3 – 4].

Під час розгляду систем управління запасами більш логічно буде характеризувати складські системи на підставі організаційної приналежності того чи іншого ешелону до окремо взятої структури. Тому під ешелонованими системами розглядаємо структури, які включають в себе більше одного рівня ешелонів запасів.

Пропонується розгляд системи управління запасами для двоступінчастої ешелонованої системи складів і можливості трансформації існуючих логістичних концепцій для потреб ПС ЗС України.

На семінарі планується розглянути види складських систем та систем управління запасами, з визначенням можливих стратегій управління, що можуть бути застосовані в перспективній автоматизовані системі управління логістичним забезпеченням ПС ЗС України, з метою підвищення ефективності планування логістичного забезпечення.

Список літератури

[1] К. В. Орєхова, та І. В. Кучерявенко, "Логістичні концепції управління матеріальними потоками у Збройних Силах України", Інфраструктура ринку, Вип. 20, с. 23 – 28, 2018.

[2] О. М. Гурін, "Проведення аналізу шляхів формування обгрунтрваного раціонального варіанту тилового забезпечення бойових дій ПС ЗС України", Збірник наукових праць ХУПС, № 1 (46), с. 37 – 40, 2016.

[3] В. Я. Платов, С .Е. Золотарева, и О. В. Платова, Технология стратегического планирования и управления. Москва, Россия: Дело, 2012.

[4] V. Voinov, G. Kachurovski, A. Shevchenko, and O. Gurin, Creating a database of existing weapon system, Збірник наукових праць ХНУПС, вип. 3 (57), с. 38 – 42, 2018.

УДК 519.876.330.115

Эльнарэ Гусейнли

Азербайджанский Государственный Университет Нефти и Промышленности, Баку

МАК КАК СИСТЕМА МАССОВОГО ОБСЛУЖИВАНИЯ

Теория массового обслуживания обязана своим возникновением практическим задачам, связанным с реальными ситуациями, в которых имеется налицо выполнение последовательности однородных операций, случайных по длительности и времени начала. Первым важным предметом исследования теории массового обслуживания были телефонные системы, характеризующиеся случайным потоком вызовов абонентов, требующих случайного времени занятия телефонной линии. В этой ситуации возникает задача расчета объема телефонного коммутатора, при котором вероятность занятости коммутатора не выше заданного уровня.

Аналогичные задачи давно возникали при расчете нагрузок энергетических сетей, планировании предприятий массового обслуживания, исследовании скученности транспорта и во многих других прикладных вопросах.

Мультисервисный абонентский концентратор показано на рис. 1.

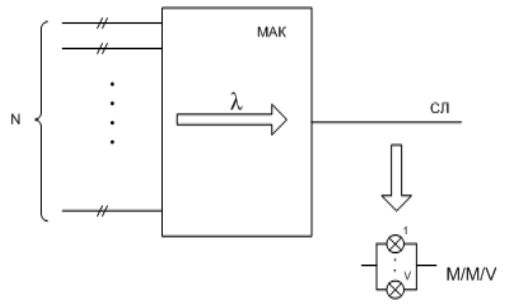


Рис. 1. Мультисервисный абонентский концентратор как система M/M/V

Включая в мультисервисный абонентский концентратор 570 аналоговых телефонных аппаратов, можно рассматривать, что количество источников N увеличивается. Потому, оно приближается к ∞.

Полностью доступный луч с линией υ ($1 \le \upsilon \le \infty$), поступающей в систему коммутации без повреждений, обслуживает простейший поток с параметром λ. При использовании системы коммутации срок службы вызова распределяется по экспоненциальному закону (F (t) = 1-e-t, β = 1).

Простейший параметр потока λ является постоянной величиной, независимой от состояния системы коммутации. Поэтому, согласно времени P_t, вызовы $P_в$ и вероятность потери относительно формул P_v-загрузки следующие:

$$P_t = P_v = P_в = \frac{\lambda^v / v!}{\sum_{j=0}^{v} (\lambda^j / j!)}$$

В формулах (1) предполагается, что средняя продолжительность курса равна единице; параметр длительности классов с экспоненциальным законом распределения β=1. Обычно при измерении продолжительности уроков в одной единице (β≠1) распределение Эрланга имеет следующий вид;

$$P_i = F_{i,v}(\lambda / \beta) = \frac{(\lambda / \beta)^i / i!}{\sum_{j=0}^{v} (\lambda / \beta)^j / j!}$$

Определяем вероятность того, что зависит P_i от интенсивности нагрузки:

$$y = \mu \ \bar{t} = \lambda / \beta = \mu / \beta :$$

где μ – интенсивность потока вызовов; $\bar{t}$ - Среднесрочный. μ=λ для самого простого и простого потока. Тогда есть форма распространения Эрланга:

$$P_i = F_{i,v}(y) = \frac{y^i / i!}{\sum_{j=0}^{v} (y^j / j!)}$$

в полнодоступном пучке все υ линий (i=υ), равна:

$$P_v = F_v(y) = \frac{y^v / v!}{\sum_{j=0}^{v} (y^j / j!)}$$

Список литературы

[1] Общие принципы модернизации местных сетей связи. Руководящий документ, Санкт-Петербург, Россия: НТЦ ПРОТЕЙ, 2003.

[2] Cordelio J. D. Unreliable Retrial Queues in a Random Environment. Dissertation, Ohio: Air Force Insti-tute of Technology, 2007.

UDC 628.35:661.5.63

S. F.Hasanli

Azerbaijan State Oil and İndustry University, Baku

APPLICATION OF ADSL AND HDSL TECHNOLOGY IN TELECOMMUNICATION'S NETWORKS

Term that encompasses the broad range of digital subscriber line (DSL) services, offers a low-cost, high-speed data transport option for both individuals and businesses, particularly in areas without access to cable internet.

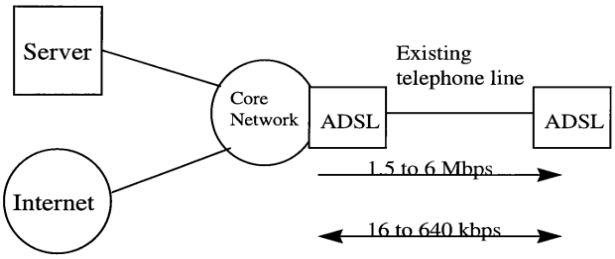
xDSL provides data transmission over copper lines, using the local loop, the existing outside-plant telephone cable network that runs right to your home or office. DSL technology is relatively cheap and reliable.

While the quality of the signals in all xDSL technologies deteriorates as distance increases, some types of DSL are more suitable than others to a specific distance and bandwidth demands.

ADSL is not a new technology, but it has been in the recent period of rejuvenation of youth, not only in the international market has been more widely used, but also by the attention of domestic operators, began to scale the network and put into commercial. China Telecom, China Unicom, Chinese railcom and so on have invested funds to build ADSL networks in varying degrees. At the same time, the relevant DSL technology, including VDSL, HDSL and other technologies are becoming increasingly active, and began to move to the market. In China's metropolitan area network construction Wave, Ethernet technology and DSL technology have been applied, but experts believe that for China's uneven development of the market, DSL technology to break the bandwidth bottleneck of fixed network will play a greater role. The Pragmatic broadband technology

ADSL technology can become the current mainstream broadband fixed access technology, there are several reasons. First of all, in recent years, the construction of telecom backbone network, especially the construction of optical fiber network, so that the transmission network has a very high bandwidth, telecommunications access to the limit of data speed bottlenecks, If the backbone network bandwidth is insufficient, even if the access section has very high bandwidth, it is difficult to meet people's demand for high-speed. Second, the Internet application market after several years of training has a large-scale user base. But most users in the country only dial-up access to the Internet, the access rate is limited to 100kbps, users of high-speed Internet has become a real demand.

Asymmetric Digital Subscriber Line (ADSL): provides high-speed communication to almost any home or business with a telephone line. ADSL supplies three line. Phone conversations are carried on one channel, while data from the service provider to the user is transferred on another line at speeds ranging from 16 kilobits-per-second (kbps) to 9 million – bits – per – second (Mbps). The third channel runs data upstream from the user to the service provider at speeds up to 64 kbps (fig. 1).



Fiq. 1. ADSL Architecture

High Bit Rate Digital Subscriber Line (HDSL): Using the existing copper infrastructure, High bit rate Digital Subscriber Line (HDSL) provides full duplex Tl (1.544 Mbps) or El (2.048 Mbps) data transmission across existing twisted pair copper without repeaters. Not only is HDSL the fastest and least costly solution for deploying Tl/El lines, it also provides transmission quality comparable to fiber (fig. 2).

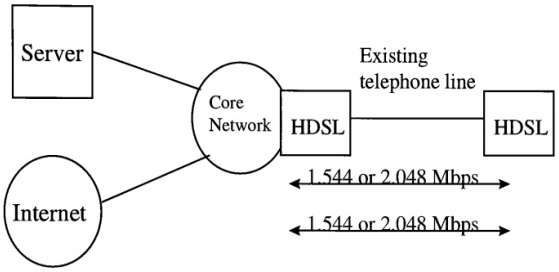


Fig. 2. HDSL Architecture

References

[1] Digital Subscriber Line Forum, "Symmetric DSL White Paper," Digital Subscriber Line Forum, Tech. Rep.1-14, 2002.

[2] D. Smith, "xDSL: The Solution for Todays Bandwidth Demands," New Telecom Quarterly- Technology Futures, vol. 5, pp. 33-37, 1997.

UDC 628.35:661.5.63

S. F.Hasanli

Azerbaijan State Oil and İndustry University, Baku

APPLICATION OF xDSL TECHNOLOGY IN TELECOMMUNICATIONS NETWORKS

Digital Subscriber Line (DSL) is a telecommunications technology for providing high-speed transmission to subscribers over the existing copper wire twisted-pair local loop between the customer premises and the telco's central office (CO).

DSL is not a specific digital line technology but rather a form of digital modem technology that defines the signaling processes for high-speed, end-to-end digital transmission over the existing copper twisted-pair wiring of the local loop. DSL accomplishes this by using advanced signal processing and digital modulation techniques. However, with DSL, the digital signals are not converted to analog or vice versa; instead, the signals remain digital for the complete communication path from the customer premises to the telco's CO.

Usually, a DSL modem and a signal splitter are installed at the customer premises to separate voice and data signals. DSL modems can use a variety of modulation methods, including carrierless amplitude and phase modulation (CAP) or discrete multitone (DMT) technology modulation, depending on the vendor's implementation. At the telco's CO, a Digital Subscriber Line Access Multiplexer (DSLAM) connects subscribers to a high-speed Asynchronous Transfer Mode (ATM) backbone.

Depending on the type of xDSL technology used, signal modulation by the DSL modem might use CAP, DMT, or some other modulation process. (CAP is currently the most popular implementation.)

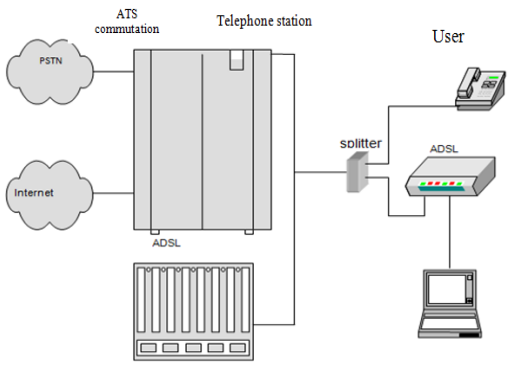
Currently digital broadcasting in the Republic's telecommunications network is in its development phase. The use and operation of classical equipment for high – speed Internet access does not justify itself economically. Most users use low-speed analog modems connected to a public telephone network to access the Internet. This connection is not only poor quality but also overloads the telephone network designed to transmit sound signals. Digital Subscriber Line equipment – digital subscriber network equipment that has recently started to play a major role in addressing these problems. xDSL technology uses a subscriber line that connects an end user's phone with ATS as an information environment. Let us illustrate the generalized scheme of data exchange using xDSL technologies in the example of ADSL2 + modems in (fig 1) below.

Generally, there are two variants of xDSL technologies:

1. Symmetric technologies.

2. Asymmetric technologies.

If the rate of transmission is the same in both broadcasting and reception, such technologies are symmetric, and if the speed of transmission and reception differs, such technologies are called asymmetric technologies.



Fiq. 1: Generalized data exchange scheme in xDSL technology.

Symmetric xDSL technologies include HDSL, SDSL, and RADSL. Other technologies are asymmetric technologies.

In modern times, copper subscriber telephone lines are in the process of moving from analogue networks designed to transmit voice signals to a broadband digital network that enables high-speed exchange of voice, video, and digital transmission. However, using modern xDSL technology developed for use in this network, it is possible to increase this speed by 100 times, as well as to use a subscriber line for telephone communication.

It is gratifying that xDSL is one of the most popular types of xDSL technology used in advanced telecommunication networks in the world. Both the quality and reasonable prices of this service are acceptable to users.

References

[1] Y. Hu, and V. O. K. Li, Satellite-Based Internet: A Tutorial, IEEE Communications Magazine, March 2001, p. 154 – 162.

[2] J. Modi, An Architectural Framework that supports Asynchronous RMI, Java Report, Vol. 6, N 3, March 2001, p.44 – 48.

[3] D. Fellows, DOCSIS Cable Modem Technology, IEEE Communications Magazine, March 2001, p.201 – 209.

UDC 681.32

E.A. Hasanov

Azerbaijan State Oil and Industry University, Baku

INFLUENCE OF QUALITY OF CABLE COMMUNICATION LINES ON THE DIAGNOSTICS PROCESSES OF FERROMAGNETIC DEVICES IN THE OIL INDUSTRY

Telecommunication is the exchange of signs, signals, messages, words, writings, images and sounds or information of any nature by wire, radio, optical or other electromagnetic systems. Telecommunication occurs when the exchange of information between communication participants includes the use of technology. It is transmitted through a transmission medium, such as over physical media, for example, over electrical cable, or via electromagnetic radiation through space such as radio or light. Such transmission paths are often divided into communication channels which afford the advantages of multiplexing. "channel" has two different meanings. In one meaning, a channel is the physical medium that carries a signal between the transmitter and the receiver. Examples of this include the atmosphere for sound communications, glass optical fibers for some kinds of optical communications, coaxial cables for communications by way of the voltages and electric currents in them, and free space for communications using visible light, infrared waves, ultraviolet light, and radio waves. Coaxial cable types are classified by RG type or "radio guide", terminology derived from World War II. The various RG designations are used to classify the specific signal transmission applications [79]. This last channel is called the "free space channel". The sending of radio waves from one place to another has nothing to do with the presence or absence of an atmosphere between the two. Radio waves travel through a perfect vacuum just as easily as they travel through air, fog, clouds, or any other kind of gas.

The other meaning of the term "channel" in telecommunications is seen in the phrase communications channel, which is a subdivision of a transmission medium so that it can be used to send multiple streams of information simultaneously. For example, one radio station can broadcast radio waves into free space at frequencies in the neighborhood of 94.5 MHz (megahertz) while another radio station can simultaneously broadcast radio waves at frequencies in the neighborhood of 96.1 MHz. Each radio station would transmit radio waves over a frequency bandwidth of about 180 kHz (kilohertz), centered at frequencies such as the above, which are called the "carrier frequencies". Each station in this example is separated from its adjacent stations by 200 kHz, and the difference between 200 kHz and 180 kHz (20 kHz) is an engineering allowance for the imperfections in the communication system.

Early means of communicating over a distance included visual signals, such as beacons, smoke signals, semaphore telegraphs, signal flags and optical heliographs. Other examples of pre-modern long-distance communication included audio messages such as coded drumbeats, lung-blown horns, and loud whistles. 20th- and 21st-century technologies for long-distance communication usually involve electrical and electromagnetic technologies, such as telegraph, telephone, and teleprinter, networks, radio, microwave transmission, optical fiber, and communications satellites. The oil industry employs a large number of different types of equipment.

Drilling rigs are made up of separate parts that must also be inspected by the inspector when preparing the unit. Because any problem that occurs in these parts will cause a major technological process to stop or crash. Non-destructive testing (NDT) methods are used for diagnostics of technical devices. Magnetic particle inspection is the most commonly used method of non-destructive testing.

This method is used for ferromagnetic materials.

The device we use for magnetic particle inspection consists of a connecting cable and windings inside. The magnetic particle inspection method is used to detect surface and subsurface defects in the material by applying a magnetic flux into the ferromagnetic material.

During the operation of the "Rigid Coil" magnetic particles are applied to the product being tested. If there are any defects in it, then magnetic particles accumulate in them. In order to make a correct diagnosis, it is important that the device be operated properly and in good quality.The unit must be able to generate sufficient magnetic field during operation.

In order to carry out the diagnostic process, the ability of the equipment is evaluated first. If the device is of good quality, it can be used for diagnostics. Otherwise the diagnostic results will not be correct. The quality of cable lines is essential for the diagnostic process. Defects in cable lines affect the quality of diagnostic results.

References

[1] F. Li, L. Ma, Y. Sun, & J. Mathew, "Group Maintenance Scheduling: A Case Study for a Pipeline Network", Engineering Asset Management, 2011, p. 163–177.

[2] G. E. Newell, "Oil analysis cost-effective machine condition monitoring technique", Industrial Lubrication and tribology, 51(3), p. 119–124, 1999.

UDC 628.35:661.5.63

Keyan Imamverdiev

Azerbaijan State Oil and İndustry University, Baku

CURRENT TRENDS IN THE AUTOMATION OF TECHNOLOGICAL PROCESSES

As a comprehensive technology, industrial automation is a general term for information processing and process control of measurement, manipulation, etc., without direct manual intervention, according to expected aim in machine equipment or production process. Through the application of computer, electronic equipment, control theory, and related process technologies, industrial automation produces the management functions of optimization, detection, control, and regulation of the whole industrial production process to realize the established objectives, achieving industrial production increase, energy saving, consumption reduction, and safe production.

The foundation of intelligent manufacturing is digitalization, networking, and integration. Correspondingly, industrial automation in the era of intelligence will transform centralized control into decentralized enhanced control under the original automation technology and architecture, so that the communication between sensors and the Internet can be seamlessly docked, establishing a highly flexible, personalized, and digital production mode that integrates products and services. In this mode, production automation technology can make equipment more intelligent through self-diagnosis, self-correction, and various functional software to better assist workers to complete production. Therefore, the communication and integration capabilities of automation equipment are required to be stronger, while the automation software needs to have a stronger ability of analysis and processing and data sharing with other software systems of enterprises.

Modern oil and gas enterprises and chemical plants combine complex objects (compressors, pumps, converters, tanks, etc.) scattered over large areas. At the same time, obtaining and processing information from various objects is difficult. These problems are solved by comprehensive automation of the production process. Typically, new technologies are used to ensure the intensification of production and improve the quality of products [1].

The effectiveness of automation largely depends on the goals of developing the system: either spend money for a year, solving the current problem, or identifying the most important problems of automation in advance. Unfortunately, the frequent restructuring of enterprises at oil and gas enterprises does not allow strategic planning for the development of automation systems. The result of this approach is the lack of a tangible economic effect and a violation of information technology. However, when creating any automation system, it must work harder to "fit" into an existing and effective system and open up opportunities for further development. This requires an integrated approach to industrial automation.

In most oil and gas companies, automation of enterprises occurs spontaneously, projects are financed from various sources, and work is carried out by unrelated firms. This leads to incompatibilities between operating systems, communications, application problems, storage and data management formats. As a result, the situation typical for the oil and gas industry today is:

– telemechanics and automation systems that collect and register primary information, support the specified process parameters and block at the level of supervisory control;

– power supply and electricity metering system;

– separate local automated workstations (PCs) and computer networks of stores;

– poorly connected with accounting systems of enterprises (companies) or usually there are independent automation subsystems. This in turn reduces the quality of management. These problems remain relevant for most production sites of oil and gas enterprises operating in the republic.

The way out of this situation is the effective use of modern information and communication technologies at the production sites of oil and gas enterprises. At the same time, modern automation systems should be based on the following principles of effective process control:

– Application of programmable logic controllers:

– Use of industrial tires.

– Real-time interference with technological data

References

[1] R. Grochowski, S. Strugholtz, H. El hor, S.J. Linz, and P. Waltzel, “Transport properties of granular matter on vibratory conveyors”, in Proceedings of the International Congress on Particle Technology (PARTEC 2004) in Nuremberg, 2004.

UDC 628.35:661.5.63

Imamverdiev Keyan

Azerbaijan State Oil and İndustry University, Baku

VIBRATION SEPERATOR FOR FEEDING MATERIAL

The authors have developed a method for cleaning liquids from particles of solid contaminants by acting on the flow of the liquid being cleaned by centrifugal, hydrodynamic and vibrational forces, which, in combination with traditional filtering methods through a porous partition, can significantly reduce the load on it, thereby increasing its service life, which means a service life filter [1]. The filter is named by the authors as a hydrodynamic vibration filter.

Filters of this type can be widely used in systems for cleaning large volumes of highly contaminated liquids with a high viscosity, the cleaning of which requires the use of filter baffles (Fb) of increased dirt capacity and high mechanical strength, which can withstand significant pressure drops on it, only through which manages to maintain high throughput. Fields of application: chemical and petrochemical industry, systems for the regeneration and restoration of the conditional properties of oil products, in particular various types of oils, in particular motor, transformer, turbine, etc. Advantages and disadvantages of the proposed types of filters, in particular their environmental advantages, as well as schemes and the mechanisms of separation of solid particles, and possible applications in purification systems are discussed in detail in [2, 3].

The introduction of filtering a new device into practice requires the development of a calculation technique that allows you to choose their design and operating parameters depending on the characteristics of the liquid being cleaned, the contamination present in it, as well as the required efficiency and fineness of cleaning and the life of the designed device.

In order to create a methodology for calculating and optimizing the operational and structural parameters of hydraulic gas turbine engines, it is necessary to create a theoretical model of the processes that take place in it, which would make it possible to identify features of the separation mechanisms and hydrodynamics of processes, determine the most significant parameters from the point of view of the effect on the final result, and create a basis for the development of engineering calculation methods.

Simultaneously, the process is triggered by the process control. The system of basic systems of control of material systems is not absorbed by toxicity and mass transfer, no automatic control and technological process control. Modern automated wires and separators get rid of unnecessary complexity of automated breakdowns.

Unmanageable Separator Separators for Controlled Feeding Granulated material is absorbed by ribbon separators. Prepare for the predicted content of material in the output. Buckwheat conveyor belt is determined by the screws

Let's integrate the mass materials into the conveyor belt, a simple integrated signal timer. The conveyor belt has a continuous scroll, integrated output and integrated screws. Use the vibration controller with the inertia and the steering wheel.

Disconnect on:

Vibration Electromagnetic Pit (VH), ribbon conveyor, tensor (m), controller SIEMENS S7-300; Panel Operator, Sensor Load Sensor (V), Sensor Sensor (SV) in Bunker;

Magnetic Converter (M); Sinamics S120 Converter.

The characteristic separator is fitted with a propellant (up to 300 t / h) and a dosage (: ± 0.5%).

Processes of technologically inclined hotspots to switch on objects (transmitters, engines, reservoirs, etc.), in subdivisions. Before or after the information and processing of information about the objects.

The essence of the theoretical approach to the development of an analytical model proposed by the authors of a new device for cleaning liquids from suspended particles of a solid fraction – a hydrodynamic vibration filter. The analytical model is the basis for creating engineering methods for calculating and optimizing the operational and design parameters of the new filter. Key words: filtration, solid phase separation, hydrodynamics, vibration filter, theoretical model.

References

[1] Fundamentals of Sustainable Drilling Engineering. M. Enamul Hossain, Abdulaziz Abdullah Al-Majed. 2015, p. 785.

[2] Drilling Fluids Processing Handbook. Asme. 2005, Elsevier Inc., Reference book 2017, Elsevier Inc., p. 729.

[3] Circulating system. Johannes Fink. 2015, Elsevier Inc., p. 817.

УДК 519.876.330.115

Т.М. Исаева, Е.С. Аллахвердиев

Азербайджанский Государственный Университет Нефти и Промышленности, Баку

ИСТОЧНИК БЕСПЕРЕБОЙНОГО ПИТАНИЯ С ВЫСОКИМ БЫСТРОДЕЙСТВИЕМ

Проблемы обеспечения электрического и электронного оборудования бесперебойной и качественной энергией является весьма актуальной. Особенную актуальность представляют вопросы обеспечения непрерывной энергией электронного оборудования, которая является уязвимым в смысле перерывов в электропитании. Эта задача может быть успешно решена применением источников бесперебойного питания (ИБП или UPS – Uninterruptable Power Supply) [1].

Существует множество разновидностей ИБП, отличающихся и по топологии, и по принципу действия, и по конструктивному исполнению. В соответствии с международным стандартом IEC 62040-3 [1] различают три основных типа ИБП:

1. резервный — Passive Standby, который ранее назывался Off-Line (IEC 62040-3.2.20);
2. линейно-интерактивный — Line-Interactive (IEC 62040-3.2.18);
3. с двойным преобразованием — Double Conversion, который ранее назывался On-Line (IEC 62040-3.2.16).

ИБП резервного типа (рис. 1) наиболее простой и дешевый. В нормальном режиме работы нагрузка получает питание прямо из сети. При пропадании напряжения в питающей сети нагрузка переключается на инвертор и батарею с помощью быстродействующего переключателя за время 3–10 мс при потере главного питания. То есть при использовании такого ИБП возможны кратковременные перерывы питания от нескольких миллисекунд до половины периода питающего напряжения. Это является одним из недостатков такого ИБП, хотя для большинства видов нагрузок такие провалы и не являются критическими. Еще одним недостатком ИБП такого типа является то, что в нормальном режиме работы в нагрузку из сети поступают все неблагоприятные воздействия, такие как искажения формы напряжения, импульсные перенапряжения, отклонения частоты и напряжения и т. д. Для частичной компенсации этих недостатков ИБП резервного типа снабжают дополнительными пассивными фильтрами гармоник, варисторами и т. д., включенными параллельно выходной цепи. Как правило, по такому принципу строятся самые дешевые и самые маломощные ИБП (до 1,5–2 кВт), например, бытовые ИБП для компьютеров, встроенные источники питания которых допускают кратковременные провалы напряжения.

Естественно, источники питания с синусоидальной формой выходного сигнала более надежные и качественные, обеспечивают надежную работу всех типов электронного и электрического оборудования, особенно нагрузок с нелинейным реактивным элементом в виде индуктивности. Однако, для большинства указанных выше оборудований наиболее критичным является характеристики и параметры быстродействия ИБП, которое выражается в способности источника питания переключаться из одного режима на другой, в частности, из дежурного режима в режим обеспечения оборудования при обесточивании электрической сети. Например, система управления полетом и регулирования движения самолетов в аэропортах, критичны к обесточиванию оборудования, так как промедления в процессе контроля и диспетчеризации могут привести к значительным потерям времени и средств, а также к авариям.

Быстродействие, которое для современных ИБП измеряется микросекундами, обеспечивается оптимальным выбором принципа построения источника, с учетом, всех его компонентов и параметров нагрузки, в частности, потребляемой мощности, требований к обесточиванию, к временным характеристикам, т.е. к изменениям подачи электроэнергии во времени и т.д.

Исходя из этого, рассмотрены принципы построения ИБП, проанализированы основные параметры, влияющие на выбор принципа функционирования источника питания. Проведен сравнительный анализ характеристик и современной элементной базы источников, показаны перспективные направления разработки ИБП с требуемыми характеристиками. При этом выявлено, что в настоящее время принцип двойного преобразования в онлайн режиме является наиболее подходящим для построения быстродействующего ИБП.

Список литературы

[1] T. F. Wu, H. S. Nien, C. L. Shen, and T. M. Chen, A Single-Phase Inverter System PV Power Injection and Active Power Filtering with Nonlinear Inductor Consideration, IEEE Transactions on Industry Applications, vol.41, №.4, 2005.

УДК 519.876.330.115

Т.М. Исаева, Дж.М. Гасанов

Азербайджанский Государственный Университет Нефти и Промышленности, Баку

ИЗМЕРИТЕЛЬ ГАРМОНИК В ЭЛЕКТРИЧЕСКОЙ СЕТИ

Наличие нелинейных элементов нагрузки в электрических сетях приводит к искажению сигналов переменного тока, к появлению гармонических составляющих тока и как следствие к потере мощности. Поэтому с целью повышения качества электроэнергии становится необходимым измерение компонентов мощности в электрической сети: активной, реактивной, полной мощностей, а также параметров соответствующих сигналов переменного тока. Таким образом, для определения качественных показателей электрической энергии необходимо измерить параметры гармонических составляющих тока.

Постоянно увеличивающиеся требования промышленности и народного хозяйства к стабильности, приспосабливаемости и точности контроля в электрическом оборудовании привело к появлению относительно дешевых силовых диодов, тиристоров, SCR (Silicon Controlled Rectifier) и других силовых полупроводников. Сейчас, широко используемые в выпрямительных цепях UPS полупроводники, статические преобразователи переменного напряжения в постоянное, устройства плавного пуска пришедшие на смену устаревшим устройствам изменили картину формы тока и напряжения в электросетях. Гармоники тока могут сильно влиять на энергоснабжающие сети, а также перегружать косинусные конденсаторы служащие для компенсации реактивной мощности (при увеличении частоты, снижается сопротивление конденсатора и растет ток через него). Мы сфокусировали наше внимание на таких источниках гармоник, как твердотельные элементы силовой электроники, однако существует много других источников гармонических токов. Силовое электронное оборудование: частотные привода переменного тока, привода постоянного тока, источники бесперебойного питания UPS, выпрямители (шестифазные, по схеме Ларионова), конвертеры, тиристорные системы, диодные мосты, плавильные печи высокой частоты. Насыщаемые устройства: Трансформаторы, двигатели, генераторы, и т.д. Гармонические амплитуды на этих устройствах являются обычно незначительна по сравнению с элементами силовой электроники и сварочным оборудованием, при условии, что насыщение не происходит.

Как показывают исследования, кроме основной гармоники с базовой частотой в сигнале присутствуют другие сигналы с меньшей амплитудой, частоты которых кратны базовой частоте. К таким сигналам, приводящим к искажению основного сигнала, можно отнести 3 – ю, 5 – ую, 7 – ую, 9 – ую и 11 – ую составляющую (гармонику) сигнала. Данный перечень гармоник обычно достаточно точно покрывает диапазон возможных отклонений формы сигнала переменного тока и позволяет достоверно оценить искажения сигнала.

С учетом приведенных выше раскладок и предположений выбрана оптимальная структура измерителя гармоник и разработана блок – модульная схема устройства. Проведены расчетно-имитационные компьютерные эксперименты с математической моделью измерителя. Представлены результаты моделирования и имитационного моделирования в среде МАТЛАБ Симулинк.

Анализ результатов компьютерных экспериментов с предварительно искаженным сигналом показал, что выбранная с учетом реализации на микроконтроллерах структура измерительного устройства, достаточно адекватно описывает процесс измерения гармоник и позволяет наглядно изучать поведение устройства во время измерений, автоматизировать процесс измерения и обработки результатов с последующей оценкой параметров гармонических составляющих, наиболее сильно влияющих на форму основного сигнала.

Список литературы

[1] А. П. Бурман, Управление потоками электроэнергии и повышение эффективности электроэнергетических систем: учеб. пособ., Москва, Россия: Издательский дом МЭИ, 2012.

[2] Z. Xiao-Ping, C. Rehtanz, and P. Bikash, Flexible Transmission Systems: Modelling and Control, Berlin: Springer, 2006.

УДК 681.396

В.В. Калачова[1], С.С. Ткачук[2], Є.О. Меленті[3], Д.В. Третяк[3]

vkadres@ukr.net

[1]Науковий центр Повітряних Сил Харківського національного університету Повітряних Сил, Харків
[2]Вінницький національний технічний університет, Вінниця
[3]Інститут підготовки юридичних кадрів для СБУ національного юридичного університету імені Ярослава Мудрого, Харків

БАГАТОКРИТЕРІАЛЬНИЙ СИНТЕЗ ОРГАНІЗАЦІЙНОЇ СТРУКТУРИ БІЛІНГОВОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МЕТОДОМ АНАЛІЗА ІЄРАРХІЙ

Білінгова система є автоматизованою системою розрахунків (АСР) фірми-постачальника товарів або послуг з клієнтами. Вона призначена для обчислення вартості товарів або послуг, виходячи з визначених у ній даних про ціни, тарифи та інші вартісні характеристики, організації різних способів обліку і обробки даних про клієнтів, товари, послуги, платежі та інші визначні місця та події, а також для виставлення рахунків клієнтам і організації інших форм звітності. Прототипи сучасних БС зародилися разом з виникненням перших обчислювальних пристроїв, проте в їх сучасному розумінні (і сам цей термін) з'явилися всього трохи більше десяти років тому.

Правильний вибір БС критичний для прибутковості підприємства сфери обслуговування. На певному етапі зростання компанії білінг перетворюється з надійного і швидкого помічника в зборі та обробці інформації в інструмент для розширення і вдосконалення сервісу на існуючій технічній базі, а значить, для залучення нових клієнтів. Від надійності та швидкості роботи БС залежить якість обслуговування клієнтів і можливості, які отримує фірма–постачальник, що, в кінцевому рахунку, впливає на прибутковість підприємства сфери обслуговування. В доповіді наведено багатокритеріальний синтез організаційної структури білінгової інформаційної системи методом аналізу ієрархій (МАІ).

Метод призначений для прийняття багатокритеріальних проектних рішень в умовах слабкої структурованості організаційно-технічних систем і невизначеності вихідної інформації, заданої набором кількісних і якісних залежностей. Обґрунтованість і достовірність прийнятих рішень багато в чому залежать від узгодженості експертних думок, які формалізовано виражаються через властивості зв'язності і транзитивності між експертними оцінками вихідного факторного простору.

Закладений в основу МАІ принцип декомпозиції складної проблеми сукупністю більш простих складових, дозволяє здійснити побудову найбільш оптимального варіанту організаційної структури білінгової інформаційної системи відповідного призначення. Результати виконаних розрахунків показують, що кращою альтернативою, рекомендованої до вибору, вважається та інформаційна білінгова система, яка має максимальне значення глобального пріоритету, незважаючи на її найвищу вартість[1–4].

Якщо у замовника є нестача фінансових коштів для придбання такої системи, то вибір більш дешевого варіанту системи здійснюється шляхом перерахунку всіх таблиць з урахуванням залучення додаткової інформації про нові вимоги до проекту, що розробляється і узгодженості експертних думок

Список літератури

[1] В. В. Калачева, В. Ф. Третяк, и Д. В. Сумцов, "Многокритериальный синтез логических систем методом анализа иерархии", Інформаційно-керуючі системи на залізничному транспорті, 2003, №2, с. 37 – 41,

[2] В. В. Калачева, С. В .Осієвський, и В. Ф. Третяк, "Моделирование логистических систем информационного обслуживания", 2003, Вып. 22, с. 196 – 199.

[3] Д. В. Сумцов, В. В Калачова, и В. Ф. Третяк, "Многокритериальный выбор проекта логистической информационной системы", Системи обробки інформації, 2004, Вып. 1, с. 97 – 100.

[4] В. С. Пономаренко, Д. Ю. Голубничий, та В. Ф. Третяк, Цілочисельне програмування в економіці, Харків, Україна: Вид. ХНУ, 2005.

УДК 004.09

Л.В. Константинова

liliyashel976@gmail.com

Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ МЕТОДІВ МОДЕЛЮВАННЯ СОЦІАЛЬНИХ СИСТЕМ

Сучасні канали соціальної комунікації використовуються для різних акцій інформаційно-психологічного впливу на особистість. Створення комплексу гнучких моделей соціальних процесів дозволило б виділити основні напрямки й характеристики соціальної системи та тим самим дало б детальний аналіз реальності й допомогло б в прийнятті управлінських рішень. Тому дослідження наявних засобів моделювання процесу інформаційної взаємодії (ПІВ) є важливим шляхом до управління соціальними процесами та є актуальним завданням на даний момент.

Були розглянуті різні методи моделювання.

Комп'ютерне моделювання з використанням агентів [1] має бути ефективним для моделювання складних соціальних процесів.

В основі такого підходу лежить поняття інтелектуального агента. Мультиагентні системи характеризуються тим, що, по-перше, кожен агент володіє інформацією, недостатньою для вирішення всього завдання, по-друге, немає глобального контролю, тобто кожен агент приймає рішення самостійно, по-третє, дані децентралізовані й, нарешті, обчислення можуть бути асинхронними.

Існують поняття мікро- та макроопису соціальных систем (СС) [2], під якими розуміють два підходи до побудови та дослідження СС: в рамках першого підходу мають на увазі структуру графа взаємовпливів учасників і їх індивідуальне прийняття рішень, а згідно з другим підходом структура зв’язків в СС усереднюється та поведінка її членів разглядається “в середньому”.

В [3] розглядається застосування нейромережних методів моделювання для опису й прогнозування феноменів в соціальних і гуманітарних науках. Володіючи всіма позитивними властивостями математичного апарату моделювання соціальних процесів, на відміну від класичних оптимізаційних й ігрових методів, нейромережі мають такі важливі особливості [3]:

1. Адаптивність – тобто здатність гнучко враховувати вплив зовнішніх факторів, а також виявляти нетривіальні, опосередковані види взаємовпливу факторів.

2. Здатність до навчання самостійно – облік передісторії при прийнятті рішень в наступних ітераціях роботи алгоритму. Ця властивість важлива при застосуванні методів математичної теорії ігор, де, наприклад, рівновага Неша може бути коректно знайдено тільки за допомогою багаторазового повторення ігрової ситуації.

3. Багатомірність – технологія нейронних мереж дозволяє враховувати роль факторів, що досліджуються, повністю з урахуванням багатовимірності й можливої протилежної спрямованості. Це дуже важливо, враховуючи суперечливість людської психіки.

При моделюванні ПІВ пропонується використовувати спеціальний інструментарій [2] – апарат теорії нечітких множин і нечіткого когнітивного моделювання, що дозволить більш точно оцінювати та враховувати суб'єктивні особливості учасників взаємодії, які не мають коректного кількісного вираження, і формалізовувати інформацію, що має вербальний характер.

В [2] розглядаються математичні моделі ПІВ, що розроблені з використанням методів системного аналізу, нечіткої логіки й теорії нечітких множин, теорії ймовірностей, математичної статистики та мультиагентного підходу.

Застосування нейромережних методик виявлення закономірностей в соціальних процесах дозволяє вирішити ряд проблем, які раніше були принципово нерозв'язні, й завдяки цьому істотно підвищити адекватність теоретичних моделей, що створюються, і наблизити їх до об'єктивної реальності. Для моделювання складних соціальних процесів комп'ютерне моделювання з використанням агентів має бути гарним рішенням.

Розглянуті в роботі моделі ПІВ дозволяють досліджувати закономірності розповсюдження інформації та динаміку формування думок в СС. Стає можливим проводити в СС інформаційні управлінські акції з різним ефектом.

Список літератури

[1] Н. С. Копылова, Ф. А. Мурзин., и И. А. Курков, “Моделирование социальных процессов и мультиагентный подход”, 2013. [Електронный ресурс]. Доступно: https: //cyberleninka.ru/article/n/modelirovanie-sotsialnyh-protses-sov-i-multiagentnyy-podhod. Дата обращения: Янв. 25, 2020.

[2] И. М. Ажмухамедов, и Д. А. Мачуева, “Микро- и макромодели процесса информационного взаимодействия в социальных системах” 2019 [Електронный ресурс]. Доступно: https://cyberleninka.ru/article/n/mikro-i-makromodeli-protsessa-informatsionnogo-vzaimodeystviya-v-sotsialnyh-sistemah. Дата обращения: Янв. 25, 2020.

[3] А. А.Обухов, “Нейросетевой анализ и математическое моделирование социальных процессов”, 2019 [Електронный ресурс]. Доступно: https:// cyberleninka.ru/article/n/ neyrosetevoy-analiz-i-matematicheskoe-modelirovanie-sotsia-lnyh-protsessov. Дата обращения: Янв. 25, 2020.

УДК 004.7

Л.В.Константинова, Р.М Минайленко., В.В Сидоренко

liliyashel976@gmail.com, aron70@ukr.net, sidrenkovl@rambler.ru

Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ AJAX

Для розробки швидких та зручних для користувачів веб-додатків існують різні технології (HTML, CSS, Javascript, XML та ін.), застосування яких у комплексі має певні переваги. AJAX – це технологія взаємодії з сервером без перезавантаження сторінки. Перед використанням AJAX, необхідно дослідити технологію на обмеження та проблеми, що можуть виникнути з веб – додатком при її застосуванні.

Зараз існує багато популярних продуктів, що використовують технологію AJAX, напр., коли користувач тільки починає вводити в рядок пошуку символи в Google або Youtube, спрацьовують множинні запити AJAX.

Технологія AJAX складається з п’яти частин: HTML; JavaScript; DHTML; DOM (об’єктна модель документа); XML.

AJAX застосовує асинхронну передачу даних, що дозволяє користувачам здійснювати різні дії під час “фонового” обміну інформацією з сервером.

В роботі AJAX можна виділити 4 етапи:

1. Користувач викликає AJAX, наприклад, при натисненні деякої кнопки, для завантаження даних.

2. Система відправляє запитна сервер. Наприклад, треба завантажити файл або здійснити запит до БД.

3. Сервер отримує відповідь від бази даних і відправляє інформацію у браузер.

4. JavaScript отримує відповідь, розшифровує її і виводить користувачу.

Для обміну даними на сторінці створюється об'єкт XMLHttpRequest, він виконує функцію посередника між браузером і сервером. Запити можуть бути GET або POST. Серверна частина обробляє запити і створює нові дані для клієнта.

Під час дослідження було виявлено такі переваги застосування AJAX:

– Покращена інтерактивність. Застосування асинхронних запитів дозволяє браузеру клієнта бути більш інтерактивним і швидше реагувати на вхідні дані. Більш зручна навігація.

– Скорочення трафіку .

– Зниження навантаження на сервер.

– Збільшення швидкості роботи сервісу.

А також було виявлено наступні недоліки:

– AJAX відкриває ще один вектор атаки для шкідливого коду, на який веб-розробники можуть не повністю перевірити.

– Інтерфейси AJAX значно складніше розвивати належним чином, ніж статичні сторінки.

– Будь-який браузер, який не підтримує Java Script або XML Http Request, не зможе використовувати сторінки, які залежать від технології AJAX.

– Неможлива інтеграція з інструментами браузера. При динамічному формуванні сторінок браузер не показує їх в історії відвідувань.

– Проблеми в індексації контенту пошуковими ботами. Часто той зміст, який завантажується на сторінки динамічним способом, виявляється недоступним для роботів. Тому рекомендується використовувати динамічне завантаження для строго визначених частин контенту. При цьому негативний вплив AJAX на SEO можна мінімізувати.

Використання AJAX потребує інформації про обмеження. Наприклад, може виникнути помилка, якщо запит посилається на локальний файл. Це виникає у випадку, коли відбувається спроба отримати доступ до даних з локального файлу, який зберігається не на сервері. Щоб вирішити цю проблему можна встановити локальний сервер і зберігати файли там.

AJAX відповідає методам конструювання додатків на основі Web і усуває проблему повільного завантаження сервера. Більшість гігантських Інтернет – компаній, таких як Google, Yahoo, Microsoft, Amazon і ін., розробляють веб-додатки на основі Ajax. Це гарне рішення для створення веб-додатків з високим рівнем взаємодії з користувачем. Грамотне використання AJAX за цільовим призначенням допомагає уникнути проблеми стосовно технології використання.

УДК 004.94

А.М. Копп, Д.Л. Орловський

kopp93@gmail.com, ordm@kpi.kharkov.ua

Національний технічний університет "Харківський політехнічний інститут", Харків

ПРОБЛЕМИ МОДЕЛЮВАННЯ МІЖПРОЦЕСНОЇ ВЗАЄМОДІЇ У НОТАЦІЇ BPMN

Протягом останніх років концепція процесного управління або BPM (Business Process Management) отримала значну увагу через свій потенціал щодо значного підвищення продуктивності та зменшення витрат, скорочення часу виконання бізнес-процесів.

Основним інструментом BPM є моделювання бізнес-процесів, яке використовується для кращого розуміння та документування діяльності організації, аналізу та вдосконалення бізнес-процесів [1]. Згідно з останніми дослідженнями, проведеними ще у 2016 році, найпопулярнішою нотацією моделювання бізнес-процесів є BPMN (Business Process Model and Notation) – її використовує понад 64% респондентів.

Основними типами елементів структури бізнес-процесу відповідно до нотації BPMN (рис. 1) є події (event), шлюзи (gateway), завдання (task) та потоки управління (control flow).

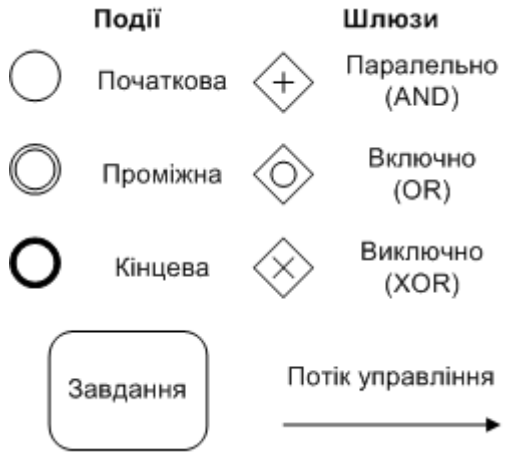


Рис. 1. Основні типи елементів структури бізнес-процесу

Події зображують інциденти, що трапляються на початку, під час та наприкінці виконання бізнес-процесу. Шлюзи використовуються для управління розгалуженнями (split) та з'єднаннями (join) потоків управління у бізнес-процесі. Завдання – це роботи, які виконуються в рамках бізнес-процесу.

Окрім основних структурних елементів (рис. 1) нотація BPMN визначає пули (pool), за допомогою яких задаються межі процесу, та доріжки (lane), які визначають відповідальність учасників процесу за виконання певних завдань.

Щодо різновидів дуг, окрім потоків управління нотація BPMN визначає також потоки повідомлень (message flow), які призначені для моделювання взаємодії декількох бізнес-процесів (choreography) всередині однієї організації або між організаціями.

До найбільш ймовірних помилок зображення взаємодії декількох бізнес-процесів належать:

1) пропущені початкові/кінцеві події (рис. 2, *а*);

2) пропущені вхідні/вихідні потоки управління у завдань (рис. 2, *б*);

3) потоки управління застосовуються замість потоків повідомлень для подання взаємодії бізнес-процесів (рис. 2, *в*).

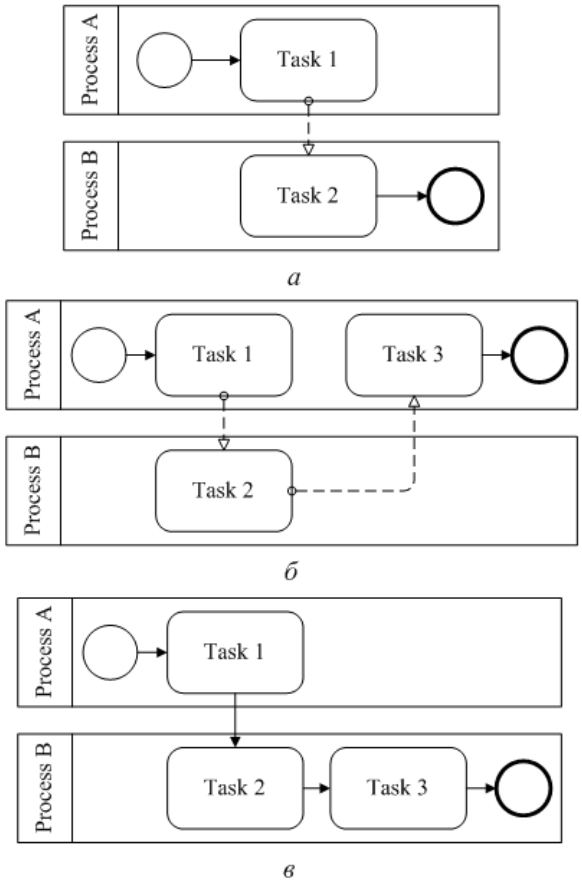


Рис. 2. Основні типи елементів структури бізнес-процесу

Необхідно створювати діаграми високої якості, які демонструватимуть зрозумілу структуру бізнес-процесів. Саме тому виникає необхідність контролю коректності створюваних моделей, оскільки якісні моделі бізнес-процесів зазвичай не мають помилок.

Список літератури

[1] W. van der Aalst, "W.M.P.: Business process management: a comprehensive survey", ISRN Software Engineering, vol. 4008 of Lecture Notes in Computer Science, p. 1 – 67, 2013.

УДК 621.391.26

О.Л. Кузнєцов[1], В.Д. Карлов[1], В.С. Кітов[1], А.М. Артеменко[2]

SAG 2121@ukr.net, Karlov@ukr.net, VSKitoff@i.ua, Artemenko.arther@gmail.com

[1]*Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків*
[2]*Об'єднаний оперативний штаб Збройних Сил України, Київ*

ТОЧНІСТЬ ВИМІРЮВАННЯ РАДІАЛЬНОЇ ШВИДКОСТІ ЦІЛІ В УМОВАХ ВПЛИВУ ФАЗОВИХ ФЛУКТУАЦІЙ РАДІОЛОКАЦІЙНОГО СИГНАЛУ

Визначення радіальної швидкості цілі реалізовано в когерентно-імпульсних радіолокаційних станціях (РЛС), які в якості зондувального сигналу використовують когерентну пачку радіоімпульсів. Реальні умови поширення та відбиття здатні суттєво обмежувати її когерентність. До вказаних умов можна віднести вплив атмосферних неоднорідностей, доплерівський шум цілі та відбиття радіохвиль від земної (морської) поверхні, які є причиною виникнення фазових флуктуацій радіоімпульсів пачки. Вважається, що дані флуктуації розподілені за нормальним законом з нульовим середнім, а кореляція фазових флуктуацій сусідніх радіоімпульсів пачки убуває за знакозмінним законом.

Дисперсія загальної похибки вимірювання частоти пачки радіоімпульсів визначається сумою дисперсії σ_{Ω}^2 похибки, що обумовлена впливом внутрішніх шумів приймального пристрою РЛС та дисперсії $\sigma_{\Omega фл}^2$ похибки, що викликана фазовими флуктуаціями радіоімпульсів пачки:

$$\sigma_{\Sigma}^2 = \sigma_{\Omega}^2 + \sigma_{\Omega фл}^2 .$$

На рис. 1 представлені графіки залежності квадрата добутку загальної середньоквадратичної похибки (СКП) вимірювання частоти пачки з десяти радіоімпульсів і періоду їх слідування $(\sigma_{\Sigma} T)^2$ від відношення сигнал/шум за потужністю q^2 при коефіцієнті кореляції фазових флуктуацій сусідніх радіоімпульсів пачки a=0,99.

Графіки отримані для різних значень дисперсії фазових флуктуацій $\sigma_{\varphi}^2 = 0,01;\ 0,1;\ 1;\ 10$ рад^2.

Отримані результати вказують на те, що збільшення дисперсії фазових флуктуацій на порядок в області малих значень ($\sigma_{\varphi}^2 = 0,01...0,1$ рад^2) майже не впливає на зміну величини дисперсії похибки вимірювання частоти пачки радіоімпульсів. Збільшення даної дисперсії на порядок в області суттєвих значень ($\sigma_{\varphi}^2 = 1...10$ рад^2), які можуть мати місце в практичних випадках, призводить до зростання дисперсії похибки вимірювання частоти пачки радіоімпульсів на порядок і більше.

Складові СКП вимірювання радіальної швидкості цілі при відношенні сигнал/шум за потужністю $q^2 = 1000$, для випадків когерентного накопичення короткої $n = 8$, середньої $n = 16$ та тривалої $n = 32$ пачок радіоімпульсів в РЛС супроводження наведені в табл. 1.

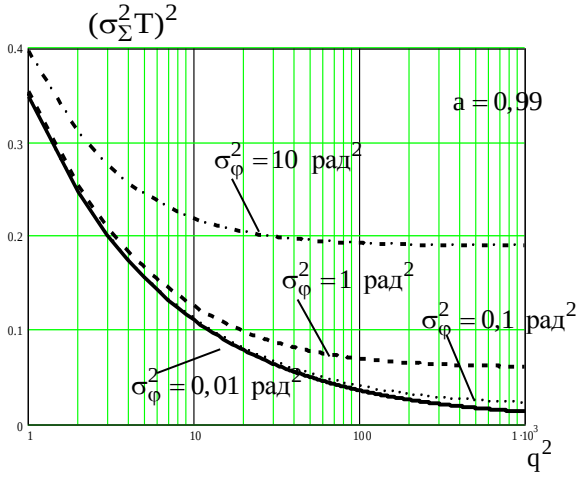


Рис. 1. Дисперсія похибки вимірювання частоти пачки радіоімпульсів

Таблиця 1.
Складові СКП вимірювання радіальної швидкості цілі для РЛС супроводження, м/с.

n	$\sigma_{\upsilon ш}$	$\sigma_{\upsilon фл}$
8	0,66	1,85…6,9
16	0,33	1,3…4,82
32	0,16	0,91…3,4

Таким чином, отримані результати свідчать про те, що значення складових СКП вимірювання радіальної швидкості цілі, обумовлені фазовими флуктуаціями радіоімпульсів прийнятої пачки здатні в декілька разів і більше перевершувати складові, що обумовлені впливом внутрішніх шумів приймального пристрою РЛС.

Окрім впливу неоднорідностей тропосфери, вплив допплерівського шуму цілі та багатотрасовості поширення радіосигналу обумовлює додаткове збільшення флуктуаційної складової СКП вимірювання радіальної швидкості цілі до декількох одиниць м/с.

При цьому, найбільш суттєво, фазові викривлення радіолокаційного сигналу, впливають на роботу РЛС супроводження, викликаючи небезпеку зриву цілі з автоматичного супроводження за дальністю та радіальною швидкістю.

УДК 519.876.330.115

Т.М Магеррамова, У.Т. Аббасов

Азербайджанский Государственный Университет Нефти и Промышленности, Баку

УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ ПИРОЛИЗА

В настоящее время, в промышленности широко используются автоматизированные системы управления производственными процессами.

Нефтехимическая промышленность одна из важнейших отраслей, продуктами которой мы пользуемся почти что ежеминутно, каждый пятый предмет, окружающий нас, произведен именно благодаря этой индустрии. Также, нефтехимия является одной из важнейших статей пополнения бюджета, наряду с добычей и экспортом нефти заграницу, при этом, чем глубже переработка нефтехимического сырья, тем выше стоимость полученного продукта. Целевыми продуктами нефтехимических комбинатов являются – олефины, яркие представители которых – этилен (C2H4), пропилен (C3H6) и их производные полиолефины.

Сначала, нефтегазовыми компаниями добываются природные углеводороды, такие как: нефть, природный газ и попутный нефтяной газ, а затем перерабатываются нефтеперерабатывающими и газоперерабатывающими комплекса-ми, где из них получают три основных вида сырья для дальнейшей переработки такие как:

1. Прямогонный бензин с нефтеперерабатывающих заводов;
2. ШФЛУ (широкая фракция легких углеводородов) получаемая газоперерабатывающими заводами;
3. Этан – ценное нефтехимическое сырье для нефтехимиков, содержащийся в природном газе.

Ход технологического процесса происходит следующим образом: сырье (смесь первичного переработанного бензина с газовым бензином в соотношении 3:1 и др.) под давлением 7÷9 кг/см^2 с сырьевого амбара J – 70, пройдя через электрический вентиль N5, далее подается в свободное межтрубное пространство теплообменника T – 7/3, где он за счет циркулирующего котельного масла, нагреваясь до 120^{o}C подается в общий коллектор печей F11÷F14. После теплообменника T – 7/3 температура бензина должна быть на таком уровне, чтобы он, проходя через диафрагму, не закипел.

Исследовав печь пиролиза как объект управления, разработав его математическую модель, дается математическая постановка задачи оптимизации рассматриваемого технологического процесса.

Для решения поставленной задачи разработаны линейные и нелинейные математические модели. Для использования математической модели на режимные параметры накладываются соответствующие ограничения.

Использовав стандартные пакеты программ, определяются регрессионные коэффициенты модели, и математическая модель проверяется на адекватность.

Одним из основных стадий в производстве этилена считается процесс пиролиза. Во время протекания процесса пиролиза в печах, использующих в качестве сырья первичный переработанный бензин и смесь газового бензина, осуществляется их разделение под высоким давлением и температуре [1].

В настоящее время на заводе Этилен-пропилен Производственного Объединения “АЗЕРХИМИЯ” проводятся работы по модернизации. В связи со всеобъемлющей модернизацией, наряду с технологией первичной переработки, предусмотрена также модернизация и совершенствование систем управления им. Технология разбавления сырья паром в свою очередь также определяет состав продуктов на выходе из печи пиролиза. Это обусловлено снижением парциального давления углеводородов, что позволяет увеличить выход низших олефинов и уменьшить скорость образования ароматических углеводородов, а также снизить коксообразование в змеевиках.

Для выполнения вышеуказанных требований используется система автоматизированного управления “ControlLogix 5580”, разработанная фирмой “Allen – Bradley”.

В соответствии с требованиями современных интеллектуальных машин и оборудований, контроллеры фирмы “ControlLogix 5580” в производстве обеспечивают более быстрое системное представление, производительность и безопасность.

Литература

[1] И. А. Ибрагимов, и И. Р. Эфендиев, “Методы оптимального управления нефтехимическими технологическими процессами. Теория и применение”, Баку, Азербайджан, 1997.

УДК 519.876.330.115

Магеррамова Тамелла Мутафа кызы, Гусейнов Абульфаз Кямиль оглы

Азербайджанский Государственный Университет Нефти и Промышленности, Баку

“TOP DRİVE” АВТОМАТИЧЕСКАЯ СИСТЕМА УПРАВЛЕНИЯ КРУТЯЩИМ МОМЕНТОМ И СКОРОСТЬЮ

Для развития буровой промышленности и повышения эффективности бурения скважин применение системы “Top Drive” сегодня является одной из наиболее актуальных задач. “Top Drive” – это механическое устройство, подвешенное на буровой вышке, предназначенное для бурения скважин и подачи крутящего момента на бурильную трубу как по часовой стрелке, так и против. Данное оборудование совместило в себе ротор и вертлюг в буровой промышленности, со многими преимуществами минимизирует время, затрачиваемое на бурение скважин и, максимально повышает техническую безопасность. “Top Drive” расположен на месте вертлюга, который движется вверх и вниз вдоль буровой вышки [2].

Кроме того, знание текущего значения крутящего момента позволяет судить о степени износа бурового инструмента, о сопротивляемости породы бурению, а так же позволяет определить проскальзывание или заклинивание бурового инструмента. При оптимизации процесса бурения как правило для увеличения достоверности прогноза последующих ситуаций необходимо информационное обеспечение целого ряда параметров. В процессе бурения такое информационное обеспечение определяется технологическими параметрами измерения, в которые входит не только значение крутящего момента, но и независимые параметры: осевая нагрузка, твердость породы, давление бурового раствора его расход, трение по длине скважины, силы сопротивления, скручивания колонны труб, автоколебания и т.д. Иными словами, для реализации прогноза ситуации необходим целый измерительный комплекс технологических параметров бурения. Но так как все перечисленные первичные параметры определяются крутящим моментом на валу привода, то целесообразно выявить данные зависимости и проводить контроль только по величине крутящего момента, что позволяет существенно упростить контрольно-измерительный комплекс. С этой точки зрения актуальность задачи разработки методов и средств измерения крутящего момента еще более возрастает. Показателем объективности информации о действительном состоянии наблюдаемой системы является достоверность оценки ее параметров. Она слагается из методической и инструментальной составляющих. Первая характеризуется совокупностью наблюдаемых параметров, методикой и критериями оценки состояния системы, вторая – точностью получаемых значений параметров. Оптимизация системы контроля процесса бурения возможна благодаря тому, что развитие компьютерной техники в последние годы способствует более рациональному использованию технических средств за счет перенесения акцента при анализе в область разработки компьютерных программ.

“Top Drive” позволяет бурить с более длинной буровой трубой. Принимая во внимание, что бурение ротором выполняется трубами длиной около 9,1 метра, а “Top Drive” обеспечивает бурение трубами длиной 18÷27 метров, то есть целой свечой буровых труб, в зависимости от высоты башни. Использование при бурении более длинных бурильных труб “Top Drive” позволяет больше проводить ежедневного бурения, так как уменьшается количество соединений со следующей длинной бурильной трубой. Еще одним преимуществом “Top Drive” является то, что он эффективен с точки зрения затрат времени. При бурении вертлюгом все бурильные трубы поднимаются на длину квадратной трубы, чтобы добавить новую бурильную трубу, но при бурении “Top Drive” наращиваемая буровая труба соединяется к общей буровой колонне труб [4].

Таким образом, более короткий и быстрый процесс закрытия сводит к минимуму риск перехвата скважины, даже когда буровой раствор не вводится в скважину. Существуют различные типы “Top Drive”, которые в основном классифицируются в зависимости от безопасности рабочей нагрузки оборудования, а также типов и размеров двигателей, вращающих бурильную трубу [1].

Процесс бурения в различных условиях осуществляется путем регулировки крутящего момента и скорости бурения на выходе вала “Top Drive”. В настоящее время крутящий момент и скорость вала блока регулируются потенцио-метрами, расположенными на панели управления, что приводит к задержкам в бурении и вызывает увеличение нагрузки на буровое долото и на трубы, что является одним из факторов, снижающих эффективность. Одним из ключевых вопросов здесь является потребность изменения мощности двигателя, воздействующего на вал.

Список литературы

[1] T. A. Atakishiev . Oil and Gas Field Electric Power. Moscow, Russia: Subsoil, 221 p.2008

[2] Varco TDS 11-SA Top Drive Operation Manual, 2011.

UDC 628.35:661.5.63

К.А. Мамедова

Азербайджанский Государственный Университет Нефти и Промышленности, Баку

ВЫЧИСЛЕНИЯ И ОПРЕДЕЛЕНИЯ С Z-НОМЕРАМИ

В большинстве случаев информация, относящаяся к реальному решению, и является частично надежной. Это можно объяснить с ненадежностью источника информации. Или можно объяснить с неправильной интерпретацией информации, неопытностью и т.д.

Формализация информации (Z – информация) на основе Z – чисел представляет собой значение интересующей переменной на основе естественного языка (Natural Language – NL), с соответствующей надежностью на основе NL. Необходимым моментом, который стоит учитывать, является то, что Z – информация, как правило, представляет несовершенную информацию, характерную для реального мира, но в то же время Z – информация имеет мощное описание с точки зрения человеческого восприятия по сравнению с нечетким числом.

В этой статья даны два метода для преобразования Z – числа в нечеткое число, а также для преобразования нечеткого числа в четкое число.

Представлен подход к принятию решений по Z – информации, основанный на прямых вычислениях по Z – числам. Этот подход использует парадигму ожидаемой полезности и применяется к задаче решения контрольных вопросов в области экономики.

Что касается теории принятия решений, то существует некоторая популяризация информации, связанная с решениями. Первая популяризация предназначена для четких чисел, а вторая больше заинтересована в использовании интервалов. Фактически, теории принятия решений в основном основаны на этих двух популяризациях. Основные доступные теории принятия решений можно разделить на следующие категории: теория ожидаемой полезности и перспективы, которая использует числовую информацию, и теории, основанные на множестве приоров, такие как ожидаемая полезность Maxmin, использующая информацию с интервалами.

Третья популяризация – нечеткие множества. В рамках этих наборов, кажется, существует множество работ, посвященных этой области лингвистическим предпочтениям, нечеткой функции полезности, нечеткому многокритериальному принятию решений и другим. Неопределенность вполне очевидна в реальной жизни, где большая часть информации, основанная на принятии решений, требует большей осторожности из-за отсутствия неопределенности. В результате трудно формализовать способность принимать рациональные решения, чтобы быть неопределенной, неточной и/или неполной информацией [1].

Теория принятия решений, предложенная в [3], имеет дело с несовершенной информацией, которая описана на естественном языке (NL).

Список литературы

[1] L. A. Zadeh, “A note on Z-numbers. Information Sciences”, vol. 181, № 14, p. 2923 – 2932, 2011.

[2] R. A. Aliev, and L. M. Zeinalova, “Decision making under Z-information. In Human-Centric Decision-Making Models for Social Sciences”, P. Guo and W. Pedrycz, Eds., vol. 502, p. 233 – 252, 2014.

[3] B. Kang, D. Wei, Y. Li, and Y. Deng, “Decision making using Z-numbers under uncertain environment”, Journal of Computational Information Systems, №8(7), p. 2807 – 2814, 2012.

UDC 628.35:661.5.63

Fuad Mammadov

Azerbaijan State Oil and İndustry University, Baku

OFDM PERFORMANCE ANALYSIS IN DVB-T

Orthogonal Frequency Division Multiplexing (OFDM) is a powerful technique employed in communications systems to combat with the frequency selective channel. Combined with smart antennas (multiple antenna system) at the transmitter and receiver, OFDM proves to be robust against channel delay spread. Moreover, it leads to significant data rates with improved bit error performance over links having only a single antenna at both the transmitter and receiver. In this work, the performance of the 2nd Generation Terrestrial Digital Video Broadcasting (DVB-T2) is analyzed, where high data rate is a must. To analyze this system, OFDM with Multiple-Input Multiple- Output (MIMO) systems have been used by applying an algorithm called Space-Time Block Code (STBC). Here, bit error rate (BER) of the system is analyzed in Additive White Gaussian Noise (AWGN) channel using QPSK modulation scheme. It has also been proved in this work that, the combination of OFDM-MIMO system is much more bandwidth efficient compared to normal OFDM system.

Digital technology has great advantages in terms of baseband efficiency, flexibility and RF performance. For this reason, the digital transmission of television signals has become a very attractive option for broadcasters. More than one program can be broadcasted within the bandwidth over which the digital broadcast is transmitted and may have better image quality. The paths of the special multi – carrier modulation method COFDM (Coded Orthogonal Frequency Division Multiplexing) and DVB crossed in the mid – 1990s, as a result, system becomes for efficient transmission of digital television broadcasts in terrestrial environments. In this study, the performance of OFDM in DVB – T system was investigated by using MATLAB. In order to improve performance, the number of OFDM carriers and frequency comparisons were made on the frequencies specified for DVB-T and the design of the optimum system was aimed and simulated.

Frequency Division Multiplexing (FDM) is a widely used technique for signal transmission in frequency selectable channels. Basically, in this technique, the channel bandwidth is divided into a number of subbands, thereby multiplying the carriers at low speeds at the frequencies allocated for each subcarrier. The carrier frequency gaps must not each other to separate the signals on the receiving side.

This necessity prevents full efficiency from the frequency spectrum. By the need to make more use of bandwidth, the orthogonal frequency division multiplexing technique (OFDM) has been proposed against this problem.

As shown in (fig. 1), the inverse fast fourier transform (IFFT) algorithm of OFDM is applied to real sample vectors.

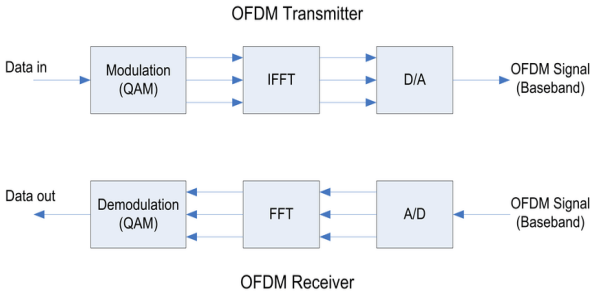


Fig.1. Block Diagram of OFDM Transmitter and Receiver

The protection interval is entered by repeating the vector end components at the beginning of the vector. The sign windowing function is required to limit the bandwidth. Most commonly used is increased cosine function.

References

[1] European Telecommunications Standards Institute, Radio Equipment and Systems (RES); High Performance Radio Local Area Network (HIPERLAN) Type 1; Functional specification, ETSI ETS 300 652 ed. 1, October 1996.

[2] N. Van Kliniken, W Renirie. "Receiving DVB-T: Technical Challenge", Proceedings of the International Broadcasting Convention, Amsterdam, 2000.

[3] Wu Jiang, and Wu Weiling, "A Comparative Study of Robust Channel Estimators for OFDM Systems," Proceedings of ICCT, p. 1932 – 1935, 2003.

[4] L. Hanzo, W. Webb, and T. Keller, 'Single- and Multi-carrier Quadrature Amplitude Modulation'. Chichester:IEEE Press and John Wiley & Sons, Ltd, 2nd edn, 2000.

УДК 621.3

Э.А Меликов, Р.Р. Зейналова

Азербайджанский Государственный Университет Нефти и Промышленности, Баку

ПЕРВИЧНЫЙ ИЗМЕРИТЕЛЬНЫЙ ПРЕОБРАЗОВАТЕЛЬ КОНЦЕНТРАЦИИ ВОДОРОДА С НЕПРЕРЫВНЫМ РЕЖИМОМ ГАЗОАНАЛИЗА

Известно, что многие первичные измерительные преобразователи концентрации водорода делают возможным проведение газового анализа. Однако, используемый в них импульсный метод ввода проб, неприменим в создании системы автоматического аналитического контроля, требованием которого является непрерывность потока, протекающего через преобразователь анализируемой смеси [1].

Анализатор состоит из системы пробоотбора, парамагнитной измерительной ячейки на O2 и контроллера.

Контроллер регулирует температуру в 4-х зонах (вход пробы, конденсатор серы, печь, сброс пробы), измеряет сигнал ячейки и формирует сигналы для регулирования расхода воздуха на технологическую установку.

Температура во входной линии пробы поддерживается выше точки росы технологического потока газа. Температура кожуха конденсатора серы, измерительной ячейки и печи поддерживается постоянной в диапазоне 20…140^{0}C (чуть выше точки росы), а конденсатор серы охлаждается воздухом КИП.

Проба газа, отобранная из технологического потока, подается в конденсатор серы, где жидкая сера возвращается обратно в поток. Конструкция конденсатора исключает также пропуск в ячейку паров серы.

Для создания измерительных устройств с непрерывным режимом газоанализа проведены исследования в области измерительных электрохимических систем, в процессе которых выявлена необходимость поддержания электрод-мембранного блока во влажном состоянии при условии диффузионной подачи анализируемой газовой смеси и необходимость применения дополнительных газов для обеспечения инвариантности выходного сигнала к побочным компонентам смеси [2].

Первичный измерительный преобразователь состоит из корпуса, внутри которого находится увлажненная ионная смола (H^+ форма), а также ионообменная мембрана в (OH^-) форме, по краям которой размещены рабочий и вспомогательный электроды. Выходной сигнал измерительной системы фиксируется регистратором, включенным во внешнюю цепь, подключенную к электродам. Данная гальваническая система состоит из иононосителя, заключенного между электродами, выполненными из различных материалов. Задача рабочего электрода заключается в ионизации водорода, протекающего по схеме, представленной в формуле:

$$H_2 \rightarrow 2H_{адс} \rightarrow 2H^+ + 2e^-$$

Материал, из которого он выполнен, относится к металлам платиновой группы. Задача вспомогательного электрода состоит в инициировании токообращения в ионообменной мембранной системе.

Материалом, соответствующим этим условиям является оксид серебра Ag_2O. Процессы, протекающие на нем и рабочем электроде, имеют вид, представленный формулой:

$$Ag_2O + H_2O + 2e^- \rightarrow 2Ag + 2OH^-$$

Суммарная реакция электрохимической системы имеет вид: $2H^+ + 2OH^- \rightarrow 2H_2O$

В качестве иононосителя выбран квазитвердый электролит, способный быть как в H^+, так и в OH^- форме. Схема, согласно которой данный элемент функционирует так: вспомогательный электрод *(Ag_2O)* → иононоситель *(H^+ (OH^-))* → рабочий электрод *(Pt)* → анализируемая газовая смесь. Электрохимический элемент, реализующий данную схему имеет выходной электрический сигнал, формируемый при постоянной подаче в преобразователь водородсодержащего газа, величина которого является функцией концентрации водорода в этой смеси. Отличительной особенностью этой схемы от других является исключение из цикла вспомогательного газа.

Список литературы

[1] B. Sorensen, and G. Spazzafumo. Hydrogen and Fuel Cells. U.S.A.: Academic Press, 2012.

[2] V. Hacker, and S. Mitsushima. Fuel Cells and Hydrogen: From Fundamentals to Applied Research, Netherlands: Elsevier, 2018.

УДК 004.652.4+004.827

Н.І. Мельникова

melnykovanatalia@gmail.com

Національний Університет "Львівська політехніка", Львів

МЕТОДИ ОПТИМІЗАЦІЇ РІШЕНЬ ЩОДО АНАЛІЗУ ПЕРСОНАЛІЗОВАНИХ ДАНИХ

У сучасних умовах розробка і здійснення єдиної фінансової політики займає значне місце в загальному механізмі управління підприємством. Роль управління фінансами визначається тим, що вона торкається всіх сторін її економічної діяльності: практичній, аналітичній, науково-технічній, маркетинговій, матеріально-технічного забезпечення і т. п., та відображає вплив численних внутрішніх і зовнішніх факторів. Особливе місце серед цілей і завдань підприємства в області управління фінансами займають: постійне збільшення вартості підприємства, максимізація вартості вкладених в нього власних коштів, мінімізація залучення зовнішнього капіталу. Саме тому вивчення раціонального оцінювання процесу управління фінансами є актуальною темою в сучасних умовах нестабільного фінансового ринку.

Використання показників комплексної оцінки стану підприємства під час проведення аналізу фінансової успішності дозволить передбачити динамічні зміни, що відбуватимуться у фінансовому стані компанії під впливом впроваджених рішень, а також підібрати найбільш адекватні рішення для зміни стратегії розвитку. Для вдалої реалізації пошуку стратегії необхідно забезпечити індивідуальний підхід щодо визначення якості управління фінансами, за рахунок урахування персональних даних діяльності підприємства.

Проблема управління фінансами завжди знаходилися в центрі уваги сучасного менеджменту, бо нестача або неправильний розподіл фінансових ресурсів можуть спричинити уповільнення рівня продуктивності підприємства за рахунок зниження важливих показників його діяльності. Ефективне управління фінансовими ресурсами забезпечує раціональне використання фінансових коштів на всіх управлінських ланках ринкової структури. Тому у країнах світу досліджуються проблеми фінансового управління, зокрема: В. Г. Гетьман, Д. Брюммерхофф, А. Премчанд, Н. А. Камордженова, Н. П. Кондраков, Н. Н.Тренев, Е. С. Стоянова, І. А. Домбровська і Ю. А. Малишева. Це обумовлюється практичною необхідністю щодо економії трудових, матеріальних та фінансових ресурсів. [1]

Одним з принципів, що реалізується в даних ЕС, є використання верхніх та нижніх порогів для імовірностей окремих гіпотез [2]. Якщо імовірність *P(H)* після врахування всіх подій перевищує верхній поріг *Max(H):*

$$P(H) > Max(H),$$

то гіпотеза *H* приймається як основа для можливого висновку. Якщо

$$P(H) < Min(H),$$

де *Min(H)* – нижній поріг, тоді гіпотеза *H* відкидається як неправдоподібна.

Якщо в певний момент роботи системи з'ясується, що для будь-якої гіпотези $H_к$ виконується умова:

$$P_{\min}(H_k) > P_{\max}(H_i), \text{ для } \forall i \neq k,$$

де $P_{min}(H)$ – поточна мінімальна імовірність гіпотези *H* та відповідно $P_{max}(H)$ –поточна максимально допустима імовірність для гіпотези *H*.

Тоді гіпотеза H_k є більш імовірною і продовження експертизи не є доцільним.

База знань відповідної ІСУФ містить записи, що торкаються знань про конкретні рішення (гіпотези) і знання по критеріях, при яких призначаються відповідні етапи. Кожна гіпотеза має відповідний формалізований запис:

$$N; P(H); \sum_{i=1}^{n} E_i; (n_k); P(E_{nk} / H); P(E_{nk} / H),$$

де *N* – назва гіпотези Н; $\sum_{i=`}^{n} E_i$ – кількість усіх подій цієї гіпотези, n_k – номер події, $P(E_{nk} / H)$ – імовірність виконання події для даної гіпотези, $P(E_{nk} / H)$ – імовірність виконання події при невірності даної гіпотези.

На підставі проведених спостережень, можемо стверджувати, що механізм логічного виведення є досить громіздким, вимагає постійних перерахунків параметрів після кожного запиту, що супроводжується перевіркою коректності виведених результатів системи, створює ефект більш "уважного" відношення експертної системи до предмету експертизи. При неоднозначності результатів, на підставі виконання різних умов вибірок, виникає багато альтернативних рішень, що ускладнюють процес пошуку цільових стратегічних рішень.

Список літератури

[1] N. Melnykova, U. Marikutsa, and U. Kryvenchuk, "The New Approaches of Heterogeneous Data Consolidation", 2018 IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), Lviv, 2018, p. 408-411. doi: 10.1109/STC-CSIT.2018.8526677/

[2] N. Melnykova, "Model of the system of personalized analysis of financial condition of the enterprise" Advances in Intelligent Systems and Computing, p. 334-345, 2018.

UDC 622.413.3

K.N. Nabizade

Azerbaijan State Oil and Industry University, Baky

ACCUMULATION AND PROCESSING OF GEOPHYSICAL EXPLORATION SIGNAL IN THE SEA CONDITION

The three principal geophysical methods used in petroleum exploration are seismic, magnetic, and gravity. The magnetic method is the oldest geophysical method and is based on the measurement of variations in the magnetic field due to changes of structure or magnetic susceptibility of the rocks. Sedimentary rocks generally have a smaller susceptibility than igneous or metamorphic rocks, so an interpretation of the recorded anomalies can yield the maximum depth values for a sedimentary basin. Magnetic surveys for hydrocarbon exploration are usually carried out from the air (aeromagnetics) or from a ship. The gravity method is based on the measurements of the variations in the pull of gravity from rocks in the upper layers of the earth's surface. Denser rocks have greater gravitational attraction than less dense rocks. Gravity surveys for hydrocarbons are carried out on land, in the air on helicopters, and at sea on ships. The most widely used geophysical method is the seismic method. Exploration seismology is divided into the branches of reflection seismology and refraction seismology. Most petroleum exploration is done by the reflection seismic method.

Currently, our oil workers in our republic are carried out drilling works in deep layers of the ground at the present time and have begun to increase the reserves of natural raw materials found. Recently, in addition to drilling works, various geophysical methods began to be used.

This will allow for the proper planning of the area where the mineral raw material is located and for selection the areas most suitable for drilling of exploration methods, by minimizing the number of wells drilled, increase the speed of research, which is of great importance to the national economy. For example, by carrying out the detection of any oil wells costs is twice cheaper than drilling method. It brings income about ten million manat to our economy.

It should be noted that large-scale geophysical exploration works is currently carried out at the bottom of water basins, seas and ocean, because the methods used by geologists are not strictly applied there. Geophysical methods of exploration have been used successfully in the study of offshore shelves to identify oil and gas and mineral deposits.

In addition to planning in the Earth's surface, exploration works are being carried out on mountain mines, ships and aircraft. In marine surveys, the greatest accuracy (0.1 – lmGal) is possible in measurements at the bottom of the sea, and for this purpose, vessels or helicopters can be used underwater. Depth is up to 200 meters [1].

These are the main provisions that differentiate the geophysical area from the geological point of view. If it is needed detailed information about the cost and from of the area, it should definitely measure the value of this area in each observation site. Different devices are used to measure these physical areas. while diving along the road, apart of these device continuously record the value of the area measured. Such device are placed on planes, satellites, helicopters, cars and vehicles.

The second group devices consist of non-stationary receivers (sensors) on the space, and signals coming from these are recorded on stationary receiver devices. Registrants record incoming signals, values of the physical area on the tape, or draw their schedule on a regular basis. Such devices are also used for research in wells and water basins. The third group devices determine the value of the physical site when the devices are fixed at the observation point. These form a large group and are widely used. Measurements are carried out with them at any scale on any section and route on the surface. Observation stations are located at distance from each other along the route.

During geophysical observation, the routers are laid perpendicular to the stretches in the area, and in most cases the routes are parallel to each other. The distance between the routes (profiles) depends on the scale of the study, but on the one hand, these distances also depend on the size of the geological object to be searched.

References

[1] "Stress state of the earth's crust in Azerbaijan. Proceeding of the International Workshop on recent geodynamics, georisk and sustainable development in the Black Sea to Caspian Sea region", Melville, New York, AIP Conference Proceeding, vol. 825, p. 97 – 102, 2006.

[2] E. Cardarelli, & R. de Nardis, Seismic refraction, isotropic and anisotropic seismic tomography on an ancient monument (Antonino and Faustina temple AD141). Geophys. Prosp., 49, 228–41, 2001.

[3] R. E. Bell, V. A. Childers, and R. A. Arko, D. D. Blankenship, & J. M. Brozena, Airborne gravity and precise positioning for geologic applications. J. Geophys. Res., № 104, 15281–92, 1999.

UDC 622.413.3

K. N. Nabizade

Azerbaijan State Oil and Industry University, Baky

PROCESSING OF GEOPHYSICAL SIGNAL IN THE SEA CONDITION

In geophysics, the seismic reflection method is widely used in exploratory surveys to detect and map subsurface structures and interfaces. It consists basically in characterizing the depth of the reflecting surfaces and their influence on the wave speed on subsurface layers. A seismic source induces a signal at a certain known location, and its reflections on the interfaces between physically different layers are recorded for further analysis.

High-resolution seismic has very limited applicability at shallower depths (ten to hundred meters, in the case of lagoon, estuary and river surveys) and has better resolution than the conventional seismic, since it is able to image structures of centimeters. Methods and concepts from solid Earth geophysics are used in high-resolution seismic and its objective is generally addressing economic, technological and environmental issues. From the 70s and 80s, applied geophysics has also been used in engineering, hydrogeology and the environment, in order to investigate shallow targets. Usually, the noise content in highresolution data makes very difficult to interpret the seismic profile and justifies the application of processing techniques to treat the acquired data.

Based on these facts, this study presents a proposal for processing high-resolution seismic data that differs in several aspects from the conventional seismic processing flow. Based on certain parameters, such as the behavior of high frequency wave, acoustic impedance, applicability of filters to suppress typical background noise and gain recovery, it is possible to obtain a much higher quality seismic profile compared to the original data. Our oil workers in our republic are carried out drilling works in deep layers of the ground at the present time and have begun to increase the reserves of natural raw materials found. Recently, in addition to drilling works, various geophysical methods began to be used. This will allow for the proper planning of the area where the mineral raw material is located and for selection the areas most suitable for drilling of exploration methods, by minimizing the number of wells drilled, increase the speed of research, which is of great importance to the national economy. For example, by carrying out the detection of any oil wells costs is twice cheaper than drilling method. It brings income about ten million manat to our economy.

It should be noted that large-scale geophysical exploration works is currently carried out at the bottom of water basins, seas and ocean, because the methods used by geologists are not strictly applied there. Geophysical methods of exploration have been used successfully in the study of offshore shelves to identify oil and gas and mineral deposits.

In addition to planning in the Earth's surface, exploration works are being carried out on mountain mines, ships and aircraft. In marine surveys, the greatest accuracy (0.1 – l mGal) is possible in measurements at the bottom of the sea, and for this purpose, vessels or helicopters can be used underwater. Depth is up to 200 meters [1].

These are the main provisions that differentiate the geophysical area from the geological point of view. If it is needed detailed information about the cost and from of the area, it should definitely measure the value of this area in each observation site. Different devices are used to measure these physical areas, while diving along the road, apart of these device continuously record the value of the area measured. Such device are placed on planes, satellites, helicopters, cars and vehicles. The second group devices consist of non-stationary receivers (sensors) on the space, and signals coming from these are recorded on stationary receiver devices. Registrants record incoming signals, values of the physical area on the tape, or draw their schedule on a regular basis. Such devices are also used for research in wells and water basins. The third group devices determine the value of the physical site when the devices are fixed at the observation point. These form a large group and are widely used. Measurements are carried out with them at any scale on any section and route on the surface. Observation stations are located at distance from each other along the route. During geophysical observation, the routers are laid perpendicular to the stretches in the area, and in most cases the routes are parallel to each other. The distance between the routes (profiles) depends on the scale of the study, but on the one hand, these distances also depend on the size of the geological object to be searched. The application of different geophysical techniques has shown to be a highly feasible solution to study coastal environments, such as assessing the impact of human activities on them.

References

[1] Lowrie W. 2006. Fundamentals of geophysics. 17a Ed. United Kingdom. Cambridge University Press. 354 pp.

[2] GTM DIAS & B. KEJRFVE, 2008. Geology and geomorphology of Holocene coastal barriers of Brazil. Louisiana State University. SpringerVerlag Berlin and Heidelberg & Co; 7: 225–252.

UDC 621.183.9

Aysel Mazhir Qojayeva

Azerbaijan State Oil and Industry University, Baku

DETERMINATION OF THE VOLUME SENSORS AND FLUID LEVELS STUDY OF CIRCUIT

Sensors are used to determine the level of various types of liquid, gaseous and bulk products and materials in tanks and pipelines.

To work with various substances, contact and non-contact sensor options are used. Depending on the structure of the housing and the method of measurement, the sensors can be installed directly in the housing of the tank or pipeline, and also mounted directly above the measurement object itself.

Level sensors are used in all industrial sectors working with liquid, bulk, gaseous, pasty, viscous, sticky, etc. materials. The sensors are designed for continuous measurement or for monitoring the limit values of a level in a vessel or pipe.

Different types of sensors are designed to work in different environmental conditions and are used depending on the characteristics and characteristics of the measured product.

Level sensors are used to work with:

1. oil, petroleum products, oils, lubricants, cutting lubricants,
2. water and aqueous solutions, wastewater,
3. acids and alkalis, cleaning fluids,
4. food products, including drinks,
5. plastic granules
6. building materials, dry building mixtures,

various viscous media.

Initially, the level sensors used the simplest physical principles: the hydrostatic buoyancy force that moves the float, and the electrical conductivity of materials that close the electrical circuit when the material reaches the electrodes. This led to the fact that this concept is associated primarily with measuring the liquid level or measuring the level of bulk materials in various tanks, tanks, silos, tanks, etc.Features: External DC output function, voltage, power C, line, filter function. Volume Indicator Series: Measures normal volume, measures equivalent volume, and measures static volume. photoelectric tachometer, laser tachometer, photoelectric contact velocity, wind speed measured (anemometer), ultrasound thickness gauge, volume calibrator, coating thickness indicator, thermometer, lighting table (photometer), dew point and thermal meter.

Sound Measurement Noise meter and challenge meter are some of the most basic and most popular tools for acoustic measurements, such as volume or volume level, based on a specific frequency meter weight and time measurement.

Sound leveling, electromechanical, measurement sounds, machine noise, vehicle noise and other noise measurements may be used; If the capacitor microphone replaces the accelerator sensor with the substitute, you can use the integrator. It measures the volume level for vibration measurement.

Sound level meters are generally used to measure noise. The classification of noise measurements is basically the following: separation of harmonic welding features in the measuring object in order to divide environmental noise (sound space) characteristics.

Regardless of the timing feature of the sound source or sound field, it can be divided into resolute noise measurements and unbalanced Master, noise measurements. The noise can be divided into noise, periodic change noise, and irregular noise.

The frequency characteristics of the sound source or sound can be separated by noise, broad band noise, narrow band noise and extraordinary pure sound components.

The accuracy of the measurement needs is divided into sensitive measurements, engineering measurements, and noise surveys.

Water Alarm (Electric Meter) is a portable, easy and reliable tool for measuring water levels, total depth, depth of wells, observation pipes, reservoir measurements and also pump tests.

When the measuring probe's electrode is in contact with the water surface, the warning lamp works with the acoustic signal on the device. The water level is read in meters and cm.

The range is 50 m, 100 m, 150 m, 200 m.

References

[1] А. А. Рульнов, и К. Ю. Евстафьев, Автоматизация систем водоснабжения и водоотведения, Москва, Россия: Инфра-М., 2007.

[2] А. А. Рульнов, И. И. Горюнов, и К. Ю. Евстафьев, Автоматизация и управление инженерными системами и сооружениями, Москва, Россия: МГСУ, 2002.

UDC 628.35:661.5.63

Sadigov Ilkin Gazanfar oglu

Azerbaijan State Oil and Industry University, Baku

CALCULATION OF THE VOLTAGE AMPLIFIER

An amplifier is a device designed to amplify power of electrical signals.

Amplifiers are classified according to the following criteria.

1. The range of amplified frequencies - low-frequency amplifiers amplifiers of a direct current, amplifiers of high frequencies, selective amplifiers.

2. According to the functional purpose - voltage, current amplifiers, power.

3. By the nature of the amplified signal - amplifiers continuous and pulse signals.

The voltage amplifier consists of an operational amplifier, resistors R1, R2 and R3. An amplifier signal of one volt is applied to the input of the amplifier.

$$U_{out} = U_l = \sqrt{2 \cdot Pl \cdot Rl} = \sqrt{2 \cdot 0{,}1 \cdot 1000} = 14V$$

The input impedance of the cascade is very large compared with the output impedance of the generator filter, so we assume that all the power will be applied to the input impedance of the voltage amplifier [1]. Given the task of adjusting the gain by ± 15%, to obtain the amplitude of the required value, we need to amplify the input signal by 15 times at the maximum value of K_U and 13 times at the minimum (minus 15%).

As a variable resistor R3, we choose a resistor SP2-2. Its characteristics are given in table 1.

Table 1

The characteristics of the resistor SP2-2

Nominal Resistance Range	22 – 100×10^3
Tolerance	±20%

Given its maximum and minimum resistance values, it is possible to choose the resistance value R2 connected in series with it:

$$K_{U\min} = -\frac{R2 + R3_{\min}}{R1} = -13,$$

$$K_{U\max} = -\frac{R2 + R3_{\max}}{R1} = -15.$$

Having solved these equations, we find the necessary values of $R_8 = 49{,}98\ kOhm$ and $R9 = 679{,}83\ kOhm$. As the resistance R8, we choose the resistor MLT-0.25-51kOhm ± 5%. As the resistance R2, we select the resistor MLT-0.25-680 kOhm ± 5%.

As an operational amplifier, we will choose OU 1408UD1. Its main parameters are shown in table 2.

Table 2

The main parameters of OU 1408UD1

Ku	100000
f, Mhs	0,8
Rin, MOhm	0,3
Rout, Ohm	250
Vuout,V/mkc	2
Uout max,V	21
Iout max,mA	4,2
U_{power},*V*	27
I_L ,*mA*	4

The low frequency of the generated oscillations allows us to conclude that this operational amplifier satisfies us in terms of speed and frequency parameters. The rated output voltage does not exceed the maximum possible output voltage of this operational amplifier [2].

An amplifier is a device designed to amplify power of electrical signals. Amplifiers are classified by the range of amplified frequencies, functional purpose. Feedback refers to the process of transmitting a signal from an output circuit to the input. The circuit providing this transmission is called a feedback loop. The feedback loop consists of a direct path formed by active element, and the return path formed by the feedback circuit.

Negative feedback stabilizes the operation of the circuit, reduces signal distortion caused by the non-linearity of the amplifier characteristics.

The introduction of negative feedback allows us not to take into account the output impedance of this amplifier stage when it is connected to the current amplifier stage.

References

[1] Y. Baoguo, K. B. Letaief, Roger S. Cheng and Zhigang Cao, "Channel Estiamtion for OFDM Transmission in Multipath Fading Channels Based on Parametric Channel Modeling", IEEE Transaction on Communications, vol. 49, p. 467 – 479, 2001.

[2] C. Li, and S. Roy, "Subspace-based blind channel estimation for OFDM by exploiting virtual carriers," IEEE Transaction on wireless Communications, vol. 2, No. 1, p. 141 – 150, 2003.

UDC 621.183.9

E.S. Satiyev

Azerbaijan State Oil and Industry University, Baky

INTELLECTUAL SYSTEMS DEFINED IN MAGISTRAL OIL PIPES

In this paper we present the unique the system uses optical fiber distributed sensors to provide simultaneous distributed measurements of temperature, strain and vibration for the detection, monitoring, and location of events including: Third Party Interference (TPI), including multiple simultaneous disturbances; geo-hazards and landslides; gas and oil leaks; permafrost protection. The Integriti technology also provides a unique means for tracking the progress of cleaning and instrumented pigs using existing optical telecom and data communications cables buried close to pipelines. The Integriti solution provides a unique and proactive approach to pipeline integrity management. It performs analysis of a combination of measurands to provide the pipeline operator with an event recognition and location capability, in effect providing a hazard warning system, and offering the operator the potential to take early action to prevent loss.

Through the use of remote, optically powered amplification, an unprecedented detection range of 100 km is possible without the need for any electronics and therefore remote power in the field.

A system can thus monitor 200 km of pipeline when configured to monitor 100 km upstream and downstream from a single location.

Protecting the environment while transporting hydrocarbons – oil and oil products – is one of the important issues. Due to the high pressure of oil transported through pipelines, their sealing can cause large leaks even in the presence of minor defects. This can result in not only raw materials loss to companies, but also the cost of detecting and eliminating these accidents, as well as imposing fines for environmental damage and a number of adverse environmental impacts.

The problem of oil and oil products leakage from oil pipelines is becoming more global, and thus the problem is becoming more relevant [1].

Pipeline system is the best way to transport oil or gas to another station. In this regard, the bulk of oil transportation is carried out through pipeline transport. Poor maintenance and low security can lead to massive financial losses. The pipelines are designed for long-term use and are prone to wear. This also creates conditions for leaks. For maximum efficiency, it is important to have a leak detection system that can be trusted by pipeline operators. It should be able to quickly and accurately detect leaks, minimize false alarms, operate efficiently in all working conditions, use sensors with high reliability and low maintenance. There are three main categories to classify leak detection methods:

– the first category, automatic leak detection systems that can be identified by pipelines monitoring system without installation of a human operator after installation;

– the second category, automated leak detection systems that work with specific operators;

– The third category includes methods of detection by means of a variety of devices and equipment based on local governance [2].

Detection of leaks in the main pipelines is one of the most pressing issues. Thus, the presence of leaks leads to many negative consequences. This does not have a negative impact on companies only with product losses. At the same time, imposing fines for environmental pollution can also lead to serious environmental disasters. From this point of view, the aim of the thesis is to develop proposals to improve the system parameters.

The problem of leakage of oil and oil products from oil pipelines is becoming more globalized and the solution to this problem has become more urgent.

Pipelines are an efficient and safe way to deliver large amounts of liquid oil over long distances. However, pipeline leakage cannot be completely regulated, and pipeline companies take various measures to maintain and track pipelines [3].

References

[1] H. F. Duan, “Uncertainty Analysis of Transient Flow Modeling and Transient-based Leak Detection in Elastic Water Pipeline Systems”, Water Resour. Manag., № 29, p. 5413 – 5427, 2015.

[2] А. Ф. Атнабаев, и С. В. Павлов, “Оценка последствий аварийных разливов нефти на магистральных нефтепроводах“, Нефтегазовое дело, №1, с. 239 – 242, 2006.

[3] American Petroleum Institute. PipelineVariable Uncertaintiesand TheirEffects onLeak Detectability; American Petroleum Institute Report 1149; American Petroleum Institute: Washington, DC, USA, 2005.

UDC 628.35:661.5.63

O.P. Seyidly

Azerbaijan State Oil and Industry University, Baku

INVESTİGATİNG WAVE ENERGY AS A RENEWABLE ENERGY SOURCE

Wave energy can generate large amounts of clean, safe, reliable, and economical renewable energy, thus making it an attractive source to meet the rapidly growing demand for energy [1]. Although in its infancy, the wave energy industry is expected, similar to the offshore wind power industry, to become established in several Nordic countries because of the rapid growth in the past decade.

Among the various renewable energy sources (such as solar, wind, and tidal power), wave energy has the highest power density and provides relatively continuous and reliable output, which is advantageous for the operation of the power grids [2]. Some large devices are designed, which indicate the diversity of the practical applications in the ocean. The cost of tapping the wave energy has increased from the 1980s but gradually declined and is likely to further reduce with advances in the technology industry. As energy costs from fossil fuels are exorbitant, wave energy could become economically feasible in the near future. Thus, policy-makers, the private sector, and the general public are interested in the conversion of wave energy into electrical energy. The two important steps in this process are assessment of the ability of a site to produce electricity and identification of surrounding ecosystems and the potential impacts and activities in support of electricity production.The demand for energy on Earth is increasing day by day. Research shows that the need for injection will be more than twice the current demand. At the same time, the use of gas and fuels associated with energy production also causes the formation of CO_2 gas. This, in turn, results in environmental pollution and climate change.

Therefore, demand for renewable energy is increasing day by day. As you know, there are enough renewable energy sources in nature. As an example, we can give examples of solar, wind, and wave energy sources.

As in the whole world, there is a great interest in the use of alternative and renewable energy sources in the Republic. That is why on July 28, 2018 the President of the Republic of Azerbaijan signed a decree on the electricity generation from renewable energy sources will be implemented [3].

One of the alternative sources of energy is wave energy. Research shows that the minimum wave height in the area of the Guba – Caspian is not less than 20cm, which means that there are several hundred megawatts of energy in the area. If that energy is used, the Republic's electricity needs can be fully met.

Wave energy is a source of energy derived from the wave action of water in the seas and oceans. The wave has characteristics such as flow, swing, and pressure. This allows us to generate electricity using these features. Efficient use of wave energy requires floats and turbines to be installed in a larger area. Consolidation of energy in this area is an important issue.

It is proposed to collect energy from sources using small powerful generators. The accumulated electricity is driven by an asynchronous engine by means of a frequency converter (inverter). In turn, an asynchronous engine activates an electric generator. As a result, stable electricity is obtained. Here the frequency converter allows you to adjust the power and frequency of the generated electricity.

References

[1] M.K. Hubbert, “Nuclear Energy and the Fossil Fuels”, Shell Development, Publ., № 95, 2001.

[2] Climate Change 2014: Synthesis Report. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Che Geneva, Switzerland, 2014.

[3] A. Akpinar, & M.İ. Kömürcü, 2013. Assessment of wave energy resource of the Black Sea based on 15-year numerical hindcast data. Applied Energy, 101, pp.502–512. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0306261912004461. Accessed on: January 24, 2013.

УДК 519.876.330.115

М.М. Сулейманлы, А.А.Сафарова

Азербайджанский Государственный Университет Нефти и Промышленности, Баку

ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ ПУСКОВЫХ РЕЖИМОВ В ТОПЛИВНЫХ ЭНЕРГЕТИЧЕСКИХ ПРЕДПРИЯТИЯХ

Нефтегазовая отрасль является лидирующей отраслью Азербайджане по поступлениям денежных средств в бюджет. Вместе с тем эксплуатация нефтегазовых объектов связана с рисками.

Структура АСУ ТП МПХГ представляет собой многофункциональную систему распределенного управления и содержит три уровня:

Нижний уровень (“полевые” средства КИПиА) состоит из исполнительного оборудования, технологического оборудования и информационно-измерительного комплекса датчиков.

Средний уровень представляет собой распределенную систему сбора данных и управления на базе управляющих программируемых логических контроллеров SIMATIC S7-300 (SIEMENS) и станций распределенного ввода-вывода ET200M (SIEMENS), выполняющих сбор и обработку информации для базы данных системы и реализующие все технологические функции системы управления. Также в ПТК среднего уровня входят распределенные аппаратные средства системы БЭАО (Блок Экстренного Аварийного Останова), размещенные в шкафах локальных контроллеров.

Верхний уровень – уровень центрального оперативного управления с реализацией дистанционного управления исполнительными механизмами, изменения задания режимов работы подсистем управления, представления информации на мониторах, звуковой и визуальной технологической сигнализации, средств ведения долгосрочного и краткосрочного архивов данных на базе промышленных станций SIEMENS и SCADA-системы WinCC (SIEMENS), а также центральная часть системы БЭАО состоящая из контроллера БЭАО SIMATIC S7-300 (SIEMENS) и пульта БЭАО.

Кроме обычных рисков проектов, здесь существует риск аварий, приводящих к материальным потерям, нарушению экологической обстановки и, что особенно существенно, к жертвам и болезням людей. Производственные объекты хранения, переработки и транспортировки горючих и токсичных веществ являются одними из наиболее опасных объектов хозяйственной деятельности. Ситуация усугубляется тем, что более 80 % всех объектов уже выработали нормативный срок эксплуатации.

Одним из основных факторов, влияющих на возникновение аварий и инцидентов, является человеческий фактор. Способность персонала принимать правильные решения в экстремальных ситуациях, уровень его квалификации трудно определить традиционными методами, поэтому целесообразно использовать различные подходы, в том числе и экспертные.

Недостаточная разработанность теоретических и методологических аспектов управления процессом обеспечения промышленной безопасности опасного производственного объекта (ОПО), а также необходимость создания системы оценки рисков аварий и инцидентов в нефтегазовой отрасли и применения на этой основе экономических решений по обеспечению безопасности определяют актуальность настоящей работы.

Цель исследования заключается в разработке оптимальное управление пусковых режимов в топливных энергетических предприятиях, алгоритмов и критериев, обеспечивающих оперативность и достоверность прогнозирования потерь, возможность управления процессом обеспечения промышленной безопасности в условиях неопределенности.

Список литературы

[1] В. Я. Ротац, Автоматизация настройки систем управления, Москва, Россия: Стандартинформ, 2014.

[2] И. А. Ибрагимов, и И. Р. Эфендиев, Методы оптимального управления нефтехимическими технологическими процессами. Теория и применение, Баку, Азербайджан: “ЭЛМ”, 2013.

[3] С. А. Ахметов, Технология глубокой переработки нефти и газа: учеб. пособ для ВУЗов, Уфа, Россия: Гилем, 2014.

УДК 519.876.330.115

Р. Сулейманова

Азербайджанский Государственный Университет Нефти и Промышленности, Баку

НЕДОСТАТКИ TDM СЕТЕЙ И ПЕРЕХОД ПРЕДПОСЫЛКОЙ К NGN

Внедрение систем IP-сигнализации способствует целый строй факторов. Это и архитектурные сокращения существующих сетей ОКС7, и нужда операторов связи снижать эксплуатационные затраты, и конвергенция сетей передачи выговора и данных, и ускорение решении развертывания новых услуг связи.

Присущая IP-технологиям высокая эффективность использования полосы пропускания позволяет операторам связи существенно экономить средства. Каналы с временным мультиплексированием (TDM) в традиционных телефонных сетях проектируются с учетом наиболее неблагоприятной ситуации – пиковой нагрузки. Протоколы ОКС7 требуют, чтобы в штатной ситуации загруженность TDM-каналов не превышала 40%. Это приводит к тому, что на практике их средняя загрузка составляет 20-30%. Значит, 70-80% канальных ресурсов постоянно простаивают. Технологии IP обеспечивают динамическое выделение полосы пропускания по требованию, при этом ее стоимость оказывается зачастую на 75% ниже стоимости полосы пропускания TDM-сети с коммутацией каналов.

Ограничения, накладываемые технологией TDM на полосу пропускания, негативно влияют и на работу других элементов сети: серверов приложений, регистров положения, блоков контроля услуг. Даже если мощности указанных элементов вполне достаточно для обработки большего объема трафика, ограничения протоколов ОКС7 на TDM-каналы, которые соединяют эти элементы с остальной сетью, не дают им “разогнаться”. Поэтому для повышения производительности сети операторам приходится докупать дополнительные устройства, притом, что имеющиеся ресурсы еще далеко не исчерпаны. Надо также иметь в виду следующее обстоятельство: добавление каждого нового элемента требует организации канала “точка-точка” и обновления маршрутных таблиц, а значит, дополнительных капитальных и эксплуатационных затрат. Хорошее масштабирование полосы пропускания в IP-сетях позволяет запросто справляться с флуктуациями трафика, упростить архитектуру сети, а различным базам данных работать с максимально возможной производительностью.

Характерная IP-технологиям высокая эффективность применения полосы пропускания позволяет операторам относительно существенно экономить средства. Связи с временным мультиплексированием (TDM) традиционных телефонных сетях спроектируют с учетом наиболее неблагоприятной условии – пиковой нагрузки. Протоколы ОКС7 призывают, чтобы в штатной ситуации занятость TDM-каналов не превосходила 40%. Это приводит к тому, как на практике их средняя нагрузка составляет 20 – 30%. Значит, 70 – 80% канальных ресурсов постоянно бездействуют. Технологии IP обеспечивают динамическое предъявление полосы пропускания по требованию, и ее стоимость оказывается нередко на 75% ниже стоимости полосы выпускания TDM-сети с коммутацией линии.

Ограничения, накладываемые технологией TDM в полосу пропускания, негативно воздействуют и на работу остальных элементов сети: серверов приложений, регистров положения, объединений контроля услуг. Даже если силы указанных элементов вполне довольно для обработки большего объемности трафика, ограничения протоколов ОКС7 в TDM-каналы, которые соединяют данные элементы с остальной сетевой инфраструктурой, не дают им “разогнаться”. Благодаря этому для повышения производительности сетевой инфраструктуры операторам приходится докупать дополнительные системы, притом, что ресурсы уже имеющихся далеко не исчерпаны. Надо иметь в виду следующее обстоятельство: добавление каждого нового элемента вызывает организации канала “точка-точка” и обновления маршрутных табличек, а значит, дополнительных обстоятельных и эксплуатационных затрат. Неплохое масштабирование полосы пропускания на IP-сетях позволяет запросто справляться с флуктуациями трафика, упростить преобразование сети, а различным базам предоставить возможность работать с максимально возможной продуктивностью.

В дополнение к той умеренности, которая обеспечивается за счет действенного использования полосы пропускания и остальных ресурсов, IP-технологии разрешают операторам более экономично формировать сети.

Список литературы

[1] T.F Wu., H.S Nien., C.L Shen., and T.M. Chen, “A Single-Phase Inverter System PV Power Injection and Active Power Filtering with Nonlinear Inductor Consideration”, IEEE Transactions on Industry Applications, Vol.41, No.4, 2005.

УДК 004.773.2

О.Р. Трач

olya@trach.com.ua

Національний університет "Львівська політехніка", Львів

СТВОРЕННЯ ВІРТУАЛЬНИХ СПІЛЬНОТ ОСВІТНЬОГО ХАРАКТЕРУ

Враховуючи сучасні тенденції та популярність мережі Інтернет усе частіше пошук інформації, комунікація відбувається у віртуальних спільнотах.

Віртуальні спільноти для певних людей є залежністю. Часто у віртуальних спільнотах люди годинами спілкуються, роблять покупки, знаходять корисну та необхідну інформацію тощо. У сучасному світі це є нормою, особливо для покоління Y та Z, які є залежними від мережі Інтернет.

Основою для здійснення організаційних та комунікаційних функцій віртуальної спільноти є учасники та інформаційне наповнення.

Учасники – зареєстровані у віртуальній спільноті користувачі мережі Інтернет, які взаємодіють у спільноті та формують інформаційне наповнення.

Інформаційне наповнення – дописи, коментарі та інші інформаційні повідомлення (текстові, графічні, аудіо та відео), що їх створили адміністратор чи учасники віртуальної спільноти.

На сьогодні найпопулярнішими соціальним мережами для створення віртуальних спільнот є Facebook та Instagram. Віртуальні спільноти освітнього характеру в соціальних мережах є актуальними для:

- інформаційного представлення вищого навчального закладу, кафедри, певної дисципліни;
- комунікації з студентами, учнями, абітурієнтами (для швидкого інформування про події);
- онлайн навчання (доступ до матеріалів навчання та швидка комунікація з викладачем);
- селф-брендингу викладача (популярний напрям створення спільноти освітнього характеру при пошуку учнів для приватного навчання).

На рис. 1 представленні етапи створення спільноти освітнього характеру.

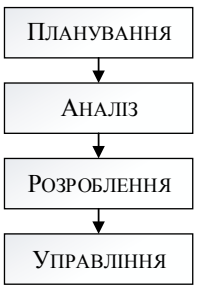


Рис. 1. Етапи створення освітньої спільноти.

Планування – при плануванні віртуальної спільноти необхідно врахувати освітній напрямок, цілі та мету створення, на яку віку групу буде націлена спільнота.

Аналіз – етап необхідний для якісного прийняття рішення щодо доцільності створення віртуальної спільноти. Здійснюється аналіз предметної області та еталонних спільнот, також етап аналізу варто робити протягом усього часу існування спільноти.

Розроблення – на цьому етапі обирається платформа для створення спільноти, розробляється дизайн, узгоджується інформаційне наповнення та формується контент-план.

Управління – етап розвитку, підтримки та управління. За виконання етапу відповідає адміністратор спільнот та smm-спеціаліст. Здійснюється наповнення віртуальної спільноти інформацією (постами), комунікація з користувачами, оновлення контент-плану.

На етапі управління значну увагу приділяють інформаційному та користувацькому напрямі діяльності віртуальної спільноти. Особливо, в освітній тематиці інформаційне наповнення повинне бути грамотне, якісне, достовірне та актуальне.

Створення віртуальних спільнот освітнього характеру є актуальним та необхідним завданням. І, враховуючи, що кількість таких спільнот збільшується до якісного їхнього створення потрібно підходити з певним набором етапів та ресурсів.

Список літератури

[1] R. Korzh, A. Peleshchyshyn, O. Trach, and M. Tsiutsiura, “Analysis of the integrity and completeness of the higher education institution informational image coverage”, In: Proceedings of International Scientific Conference Computer Sciences and Information Technologies (CSIT-2019), vol. 3, p. 48 – 50, 2019.

[2] R. Korzh, A. Peleshchyshyn, Yu. Syerov, and S. Fedushko, “University’s Information Image as a Result of University Web Communities’ Activities”, Advances in Intelligent Systems and Computing, Shakhovska N. (Ed.), Springer International Publishing, V. 512, p 115 – 127, 2017.

[3] S. Fedushko, Y. Syerov, and R. Korzh, “Validation of the user accounts personal data of online academic community”, на XIII Міжнар. конф., 23–26 лютого 2016 р., Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії, Львів, 2016, с. 863 – 866.

UDK 009.4

O. Tymchenko [1], B. Havrysh [2]

o_tymch@ukr.net, dana.havrysh@gmail.com

[1] *University of Warmia and Mazury, Olsztyn, Poland*
[2] *Ukrainian Academy of Printing, Lviv, Ukraine*

APPLICATION OF THE METHODOLOGY OF NEURO-FUZZY PROCESSING OF TEXTS IMAGES FOR ITS RECOGNITION

With the development of information technology, it has become possible to facilitate, accelerate and improve the quality of printed or handwritten texts recognition. The first element of the letter recognition system is a scanner or a digital camera that inserts text images into the computer. To create a text document, you need to recognize individual characters in this image. There is a range of software that have virtually automated process of texts recognizing. However, it is not always possible to ensure a satisfactory result in the case of distortions of printer or handwritted text images of various types (geometric, noise, etc.).

The problem of effective text recognition plays an important role in the informatization areas of various human activity processes. The textual presentation of information, in comparison with graphic, allows significantly reduce the costs of storing and information transmitting, and also allows us to implement all methods of electronic documents using and analyzing. Therefore, the greatest interest from a practical point of view is precisely the transformation of information from paper carriers into a text electronic document.

Thus, the purpose of this work is to develop methods and algorithms for constructing a neuro-fuzzy recognition system for text images that contain:

1. noise of text images reduction;
2. images binarization;
3. boundaries allocation and characters segmentation;
4. grammar realization for the structural recognition of text images;
5. verification of proposed methods.

After binarization, the image enters the system of fuzzy image processing (fig. 1).

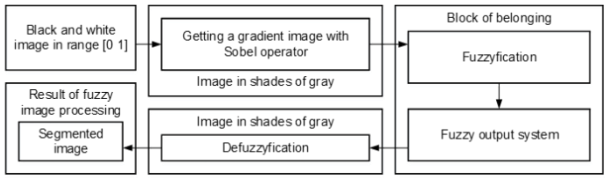


Fig. 1. Algorithm of fuzzy images processing to allocate boundaries

Fuzzy image processing consists of three main phases: F-image, fuzzy-output system (*M*) on the values of affiliation, and defuzzifications of the (*D*) images. After transferring the image from the gray-level image to the phase-out, the fuzzy output system is determined by the value of the accessory function.

An image of *X*-size $M \times N$ with L gray levels $g = 0,...,L-1$ can be defined as a fuzzy single-point set that specifies the value of each pixel attribute relative to the image property (for example, brightness, smoothness, etc.):

$$X = \bigcup_{m=1}^{M} \bigcup_{n=1}^{N} \frac{\mu_{mn}}{g_{mn}}, \ \mu_{mn} \in [0.1],$$

where μ_{mn} and g_{mn} – assignments of the *mn* pixel in the fuzzy set. Determining the values of affiliation depends on the specific application requirements and knowledge base.

Also, the symmetric bonding of the membership function is not always effective. That is why the attempting in using fuzzy logic to improve the quality of the half-tone images leads to the need to construct *S*-like fuzzy functions. These functions have changed symmetry center and are described as two glued parabolic links with a continuous derivative in the place of gluing, that is, functions of the second order.

To construct a non-structural character recognition system, there is used a neural network of reverse error distribution, which consists of several layers of neurons, and each neuron of the previous layer is associated with each neuron of the next layer. In such networks, after determining the number of layers and the number of elements of each layer, it is necessary to calculate the values of the weights and thresholds of the network in such a way to minimize the forecast error. For network teaching it is used an algorithm for reverse error spreading. It calculates a vector gradient surface error. Then it moves to a certain value in the direction of the vector (it will indicate the direction of the fastest descent), where the error value will be less. This gradual progression will gradually lead to a minimization of the error.

Below is a review of the developed neuro-fuzzy system work (with a 5x5-pixel window) with the commercial product ABBYY FineReader 11 Corporate Edition (the image of the page text is 702 characters; the Gaussian noise is 0.03 from the black level).

Number of errors (in percent) of image recognition

Developed system		FineReader 11	
Work time	% errors	Work time	% errors
40 s	16%	< 2 s	2

The methods and algorithms that are considered allow us to approximate the methods of OCR systems to those that are used by people.

УДК 519.876.330.115

Н.М Ширинова, Х.М. Гамзаев

Азербайджанский Государственный Университет Нефти и Промышленности, Баку

МОДЕЛИРОВАНИЕ ВОЛНОВОГО ВОЗДЕЙСТВИЯ НА ПРОЦЕСС ВЫТЕСНЕНИЯ НЕФТИ ИЗ ПЛАСТА ВОДОЙ

В данной работе рассматриваются вопросы моделирования процесса вытеснения нефти водой при воздействии на пласт упругими волнами. Для описания данного процесса предложены одномерная математическая модель в виде нелинейного дифференциального уравнения гиперболического типа. Построен алгоритм решения метода конечных разностей и проанализированы полученные результаты.

Большая часть нефтяных месторождений отрасли вступили в позднюю стадию разработки, доля трудноизвлекаемых запасов (ТРИЗ) месторождений неуклонно растет. Прогрессирующее обводнение скважин и пластов, выбытие скважин из действующего фонда по причине предельной обводненности и физического износа, снижение эффективности проводимых геолого-технических мероприятий, уменьшение добычи нефти – вот видимые сложности разработки нефтяных месторождений с трудноизвлекаемыми запасами. Традиционные методы не позволяют извлечь остаточные запасы нефти месторождений и актуальными являются методы увеличения нефтеотдачи пластов (МУН) и интенсификации добычи нефти (МИДН). Использование МУН при разработке с за-воднением предполагает решение следующих задач:

Во-первых, повышение гидродинамической со-ставляющей метода заводнения в результате цикличности процесса закачки, изменения направления фильтрационных потоков, организации новых очагов за-воднения, оптимизации плотности сетки скважин, форсированного отбора и др. Это задача гидродинамических МУН.

Во-вторых, снижение различия физико-химиче-ских свойств пластовой нефти и вытесня-ющей воды за счет добавок в последнюю ПАВ, полимеров-загустителей, щелочей и других химических реагентов, позволяющих снизить межфазное натяжение на границе нефть-вода, повысить вязкость воды, улучшить ее отмывающие свойства; это задача физико-химических МУН.

Для увеличения выхода нефти и интенсивности добычи нефти и газа методы воздействия улучшаются и разрабатываются новые. Несмотря на то, что много работы было посвящено изучению проблемы увеличения добычи нефти в глине, она все еще остается актуальной проблемой. Поэтому построение основы математической модели этого процесса сопуствует повышению ее эффективности и имеет как научное так и практическое значение

Пусть имеется горизонтально расположенный недеформируемый нефтеносный пласт протяженностью L, постоянной толщины и ширины. На границе $x=0$ расположена нагнетательная галерея, а на границе $x=L$ эксплуатационная галерея.

Уравнения движения в этом случае имеют вид:

$$u_w = -\lambda_w\left(\frac{dP_w}{dx} - \omega^2 A\rho_w\right)$$

$$u_o = -\lambda_o\left(\frac{dP_o}{dx} - \omega^2 A\rho_o\right)$$

Здесь, $\lambda_w = \frac{k}{\mu_w}k_w(s)$, $\lambda_o = \frac{k}{\mu_o}k_o(s)$.

Математическая модель процесса выглядит следующим образом::

$$m\frac{\partial S}{\partial t} = \frac{\partial}{\partial x}\left(\varphi(S)\frac{\partial S}{\partial x}\right) - \frac{\partial \varphi_1(s)}{\partial t}Q(t) - A\omega^2\left[\frac{\partial\left(f(s)\varphi_1(s)\right)}{\partial x} - \frac{\partial f_1(s)}{\partial x}\right]$$

$$\begin{cases} \varphi(s) = -\dfrac{\lambda_o\lambda_w}{\lambda_w+\lambda_o}\dfrac{dP_c}{dx} \\ \varphi_1(s) = \dfrac{\lambda_w}{\lambda_w+\lambda_o} \\ f(s) = \lambda_w\rho_w + \lambda_o\rho_o \\ f_1(s) = \rho_w\lambda_w \end{cases}$$

Начальные и граничные условия:

$$S\big|_{t=0} = \xi(x)$$

$$\frac{k\cdot k_w}{\mu_w}\frac{\partial P_w}{\partial S}\frac{\partial S}{\partial x}\bigg|_{x=0} = q(t)$$

$$\frac{\partial S}{\partial x}\bigg|_{x=L} = 0$$

Разработан алгоритм решения данной задачи методом конечных разностей.

Список литературы

[1] Э. М. Симкин, “Вибросейсмический метод увеличения продуктивности обводненных нефтяных и газовых пластов”, Нефтегазовые технологии (Oil and Gas Technology), № 2, 1998.

[2] М. Л. Сургучев, Вторичные и третичные методы увеличения нефтеотдачи пластов, Москва, Россия: Недра, 1985.

ЗМІСТ

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

СЕКЦІЯ 2. ПРОГРАМУВАННЯ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

СЕКЦІЯ 3. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ, МЕДИЦИНІ ТА ОСВІТІ

ТЕЗИ ДОПОВІДЕЙ
II Міжнародної науково-практичної конференції
“Інформаційна безпека та інформаційні технології”

“Information Security and Information Technologies”

2–3 квітня 2020 р.

Відповідальний за випуск: *С.П. Євсеєв*

Комп`ютерна верстка: *А.А. Гаврилова*

Підписано до друку 30.03.2020. Формат 60×84/8. Папір офсетний.
Гарнітура «TimesNewRoman». Друк ризографічний. Ум.-друк. арк. – 6,6. Ціна договірна.
Наклад 250 прим.Зам. 0330/9-18

Видавництво «Цифрова друкарня №1»
Свідоцтво суб’єкта видавничої справи: серія ДК № 4354 від 06.07.2012 р.
61001, м. Харків, пл. Повстання, 7/8
e-mail: zebra-zakaz@mail.ru

Віддруковано з готових оригінал-макетів у друкарні ФОП Петров В.В.
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 24800000000106167 від 08.01.2009.
61144, м. Харків, вул. Гв. Широнінців, 79в, к. 137, тел. **(057)778-60-34**e-mail: **bookfabric@rambler.ru**