ISSN 2073-7394

Полтавський національний технічний університет імені Юрія Кондратюка

СИСТЕМИ УПРАВЛІННЯ, НАВІГАЦІЇ ТА ЗВ'ЯЗКУ

1 (41) ' 2017

Заснований
у 2007 році

Наукове періодичне видання,
в якому відображені результати
наукових досліджень з розробки та
удосконалення систем управління,
навігації та зв'язку у різних
проблемних галузях.

Засновник:
Полтавський національний технічний
університет імені Юрія Кондратюка

Адреса редакційної колегії:
Україна, 36011, м. Полтава,
Першотравневий проспект, 24

Телефон: +38 (066) 706-18-30
(консультації, прийом статей).

E-mail:
kozelkovae@ukr.net

Інформаційний сайт:
http://www.pntu.edu.ua

Реферативна інформація
зберігається: у загальнодержавній
реферативній базі даних
„Україніка наукова" та публікується
у відповідних тематичних серіях
УРЖ „Джерело".

Журнал індексується наукометричною базою Google Scholar

Затверджений до друку науково-технічною радою Полтавського національного технічного університету імені Юрія Кондратюка (протокол № 3 від 15 лютого 2017 року)

Занесений до "Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук", затвердженого наказом Міністерства освіти і науки, молоді та спорту України від 25.01.2013 р., № 54

Свідоцтво про державну реєстрацію КВ № 19512-93/2ПР від 16.11.2012 р.

З М І С Т

Кібернетична безпека

УДК 004.056.53; 004.056.55

Н.І. Алішов, С.В. Зінченко, А.Н. Алішов, Н.О. Сапунова

Інститут кібернетики імені В.М. Глушкова НАН України, Київ

ЗАСТОСУВАННЯ НЕРОЗКРИВНИХ ШИФРІВ ДЛЯ УБЕЗПЕЧЕННЯ VOIP-ТЕЛЕФОНІЇ

Статтю присвячено проблемам безпеки VOIP-телефонії. Розглянуто основні види загроз для VOIP-телефонії, заходи щодо їх усунення. Запропоновано програмно-апаратний комплекс захисту на базі використання нерозкривних шифрів, який працює в потоковому режимі.

***Ключові слова**: потокова інформація, VOIP-телефонія, захист інформації, нерозкривні шифри, протоколи передавання інформації, пристрій захисту інформації.*

Вступ

Проблеми безпеки мережевих голосових повідомлень за технологією VOIP мало чим відрізняються від проблем безпеки мережі в цілому [1 – 4]. Основну небезпеку становлять хакери, які, знаючи про уразливості системи, створюють атаки, що сприяють відмові систем, перехопленню особистих даних через користувальницьке ПЗ, наприклад X-lite, Skype, Ekiga та ін. Докладна технічна інформація про велику кількість протоколів VOIP також створює проблеми, пов'язані з маршрутизацією голосового трафіка через брандмауери і мережні адреси, які використовуються для з'єднання транзитних мереж. Граничні контролери застосовуються для захисту дзвінків. Інші методи вимагають завантаження допоміжних протоколів (STUN або Interactive Connectivity Establishment (ICE) тощо).

Зазвичай організації вдаються до різних заходів безпеки для захисту VOIP-трафіка − голосових повідомлень, що передаються по безпечним IP. Це досягається за рахунок застосування різних методик шифрування.

Багато користувальницьких систем VOIP не підтримують шифрування передачі голосових даних, надаючи у результаті можливість підслуховувати VOIP-виклики. У статті описуються технологія й апаратно-програмні засоби організації захисту передавання потокової мультимедійної інформації в реальному часі для VOIP-телефонії на базі розробленого в Інституті кібернетики НАНУ USB-пристрою шифрування [5].

Основні види загроз для VOIP-мереж

Перехоплення та маніпулювання даними. Найпоширеніша уразливість телефонних мереж, особливо небезпечна для IP-телефонії. У випадку застосування IP-телефонії зловмисникові не потрібен фізичний доступ до лінії передавання даних. Пристрій перехоплення, що знаходиться усередині корпоративної мережі, найімовірніше може бути виявлений, а от зовнішнє прослуховування відстежити практично неможливо. Крім того, перехоплені дані або голос можна передати далі у зміненому вигляді. У таких умовах весь незашифрований голосовий потік необхідно вважати небезпечним.

Підміна та злом користувальницьких даних. Відмова від використання або спрощення механізмів автентифікації й авторизації в IP-телефонії відкриває для зловмисника можливість несанкціоновано отримати доступ до системи, підмінивши дані про користувача своїми даними. Можливий також злом облікових даних користувачів за допомогою перебору або прослуховування незахищених каналів зв'язку. Подібна уразливість може бути використана, наприклад, для здійснення дорогих дзвінків за рахунок жертви або для прийому важливих для зловмисника дзвінків і їхнього записування з метою застосування даної інформації в корисливих цілях. У будь-кому випадку така «дірка» в безпеці здатна звести нанівець всю можливу вигоду від використання IP-телефонії.

Обмеження доступності. Одним з різновидів атак є «відмова в обслуговуванні» (Denial of Service, DoS). Ця атака націлена на перевищення граничного навантаження на систему великою кількістю коротких дзвінків або інформаційного непотребу. Якщо не організовано постійне відстежування ознак подібних атак і застосування пасивних засобів захисту, сервери IP-телефонії врешті-решт не справляться зі зрослим навантаженням і не зможуть обслуговувати підключених абонентів.

Інформаційна безпека VOIP-телефонії

Підхід до організації інформаційної безпеки, у тому числі VOIP-телефонії, має бути комплексним,

оскільки кожен спосіб захисту не тільки закриває свою частину інформаційного периметра, але й доповнює інші рішення. Тому пропонований комплекс реалізує захист двох частин − серверної та клієнтської.

Убезпеченню сервера буде сприяти організація запобіжних заходів, зокрема таких традиційних:

Застосування політики складних паролів. Одержання облікових даних методом перебору (bruteforce) вимагає значних витрат часу й обчислювальних ресурсів, ускладнення паролів дозволить зробити даний метод атак недоцільним.

Відключення гостьових дзвінків. Дозвіл на здійснення вихідних дзвінків надається тільки користувачам системи, це унеможливить спроби подзвонити ззовні без попередньої авторизації.

Обмеження напрямків дзвінків, доступних абонентам, застосування схеми «заборонено все, крім дозволеного». Зловмисник, якому вдалося отримати облікові дані користувача системи, зможе реалізувати дзвінки тільки по певних напрямках. Це дозволить уникнути несанкціонованого здійснення дорогих міжнародних дзвінків.

Відключення відповіді про неправильний пароль. За замовчуванням VOIP-сервер видає одну помилку про неправильний пароль для існуючого й іншу для неіснуючого VOIP-клієнтів. Зловмисник, скориставшись якоюсь з безлічі програм для підбирання паролів, зможе перевірити всі короткі номери й збирати паролі лише до існуючих акаунтів, які дали відповідь «неправильний пароль».

Регулярні перевірки системи на предмет спроб злому, контроль параметрів. Організація системи моніторингу стану системи дозволить поліпшити якість IP-телефонії та визначити типові для даної конфігурації параметри. Відхилення цих параметрів від отриманих типових значень свідчить про проблеми з устаткуванням, каналами зв'язку або наявність спроб вторгнення зловмисників.

Використання систем блокування доступу після невдалих спроб реєстрації. Переглядаючи періодично звіти системи з метою виявлення спроб злому, можна виділити й заблокувати IP-адреси нападників, що дозволить скоротити непотрібний SIP-трафік і захиститися від множинних спроб злому.

Застосування міжмережних екранів. Міжмережний екран пропускає вихідний трафік від сервера телефонії до SIP-провайдера та фільтрує вхідний за певними правилами. Доцільно закривати на міжмережному екрані всі мережеві порти для IP-телефонії, крім необхідних для її коректної роботи й адміністрування. Цей метод захисту застосовується на VOIP-сервері, щоб захистити його від внутрішніх атак. У такому разі сервер телефонії буде доступний із зовнішніх мереж тільки по певних службових портах, підключення до яких має виконуватися із застосуванням шифрування.

Убезпечення VOIP-даних. Для захисту конфіденційних переговорів і мінімізації можливості потрапляння конфіденційної або комерційної інформації в руки зловмисника необхідно захистити передані відкритими каналами зв'язку дані від перехоплення та прослуховування.

Оскільки для здійснення дзвінка клієнт і сервер попередньо обмінюються службовими даними для встановлення з'єднання, цю проблему можна розділити на дві складові − захист службових даних IP-телефонії (SIP-протокол) і захист голосового трафіка (RTP-протокол) (рис. 1).

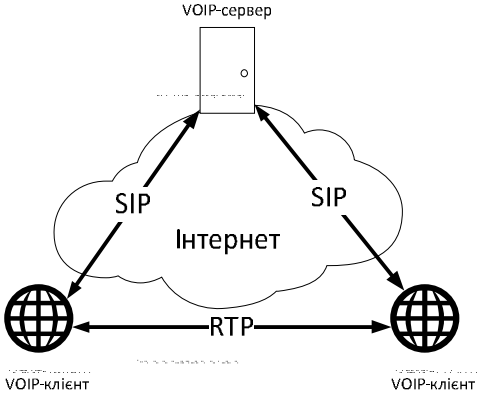


Рис. 1. Схема організації VOIP-телефонії

Протоколи передавання потокової інформації. На даний час існують безліч стандартних міжнародних протоколів, призначених для передавання потокової інформації в комп'ютерних мережах. Крім того, багато відомих фірм пропонують програмні застосування, які є надбудовами над цими протоколами для передавання мультимедійної потокової інформації в комп'ютерних мережах. Тому розробку власних протоколів не можна вважати актуальною задачею. Завдання авторів полягало в тому, щоб інтегрувати розроблені програмні засоби для пристрою шифрування з існуючими протоколами та застосуваннями (рис. 2, 3, табл. 1). Таке завдання не є тривіальним і вимагає високого професіоналізму, оскільки ці системи не призначені для «чужорідних» пристроїв.

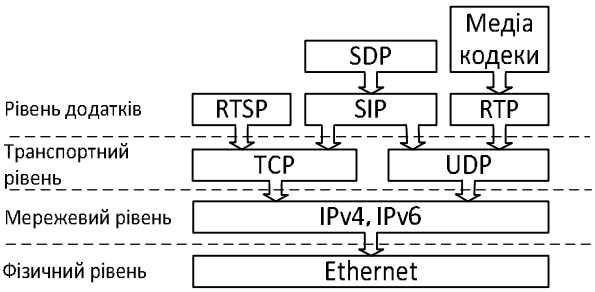


Рис. 2. Місце протоколів VOIP-телефонії у стеці протоколів TCP/IP

Протоколи, що застосовуються у VOIP-телефонії:

Таблиця 1

Базові мультимедіа-кодеки, що використовуються у VOIP-телефонії

Назва	Тип	Опис	Швидкість передачі даних (Кбіт)	Частота дискретизації (кГц)
G.711	аудіо	Імпульсно-кодова модуляція (ІКМ)	64	8
G.711.1	аудіо	Імпульсно-кодова модуляція (ІКМ)	80-96 Кбіт	8
G.721	аудіо	Адаптивна диференціальна імпульсно-кодова модуляція (ADPCM)	32	8
G.722	аудіо	7 кГц аудіо-кодування в межах 64 Кбіт /с	64	16
G.722.1	аудіо	Кодування на 24 і 32 Кбіт/с для гучного зв'язку в системах з малими втратами кадрів	24/32	16
GSM 06.10	аудіо	-	13	8
Speex	аудіо	-	8, 16, 32	2.15-24.6
Ilbc	аудіо	-	8	13.3
THEORA	відео	Стиснення з втратами	-	-
H.264	відео	MPEG-4 AVC/H.264, стиснення з втратами та без втрат	від 64 Кбіт/с до 960000 Мбіт/с	-
H.263	відео	MPEG-4 AVC/H.264, стиснення з втратами та без втрат	192 Кбіт/с	-
H.261	відео	MPEG-4 AVC/H.264, стиснення з втратами та без втрат	від 40 Кбіт/с до 2 Мбіт/с	-

– **SIP** (Session Initiation Protocol) − протокол ініціювання сеансів, є протоколом прикладного рівня і призначається для організації, модифікації і завершення сеансів зв'язку: мультимедійних конференц- і телефонних з'єднань, розподілу мультимедійної інформації. Користувачі можуть брати участь в існуючих сеансах зв'язку, запрошувати інших користувачів і бути запрошеними ними до нового сеансу зв'язку. Запрошення можуть бути адресовані певному користувачеві, групі користувачів або всім користувачам.

– **SDP** (Session Description Protocol) − протокол прикладного рівня, призначений для опису сесії передавання потокових даних, включаючи VOIP-телефонію, Інтернет-радіо, програми мультимедіа. Сесія SDP може реалізовувати кілька потоків даних. У протоколі SDP в даний час визначені аудіо, відео, дані, управління і застосування (потокові), подібні до MIME-типів електронної пошти в Інтернет-адресах. Повідомлення SDP, що передається від одного вузла іншому, може вказувати:

- адреси місця призначення, які можуть бути адресами мультикастингу для медіапотоків;
- номери UDP-портів для відправника й одержувача;
- медіа-формати (наприклад, кодеки, описувані профілем), які можуть застосовуватися під час сесії;
- час старту й зупинки. Використовується в разі широкомовних сесій, наприклад, телевізійних або радіопрограм. Можна внести час початку, завершення і часи повторів сесії.

– **RTP** (Real-time Transport Protocol) – працює на прикладному рівні і є основним протоколом для передавання даних у реальному масштабі часу. Протокол RTP переносить у своєму заголовку дані, необхідні для відновлення аудіо або відео в приймальному вузлі, а також дані про тип кодування інформації (JPEG, MPEG і т.п.). У заголовку даного протоколу, зокрема, передаються часова мітка і номер пакета. Ці параметри дозволяють при мінімальних затримках визначити порядок і момент декодування кожного пакета, а також інтерполювати втрачені пакети.

– **RTCP** (Real-time Control Protocol) – заснований на періодичній передачі пакетів управління всім учасникам сеансу зв'язку при використанні того ж механізму розподілу, що і протокол RTP. Протокол нижчого рівня повинен забезпечити мультиплексування інформаційних і керуючих пакетів, наприклад, з використанням різних номерів портів UDP. Протокол RTCP виконує чотири основні функції:

- забезпечення зворотного зв'язку для оцінювання якості розподілу даних,
- синхронізація звукового та відеосигналу,
- передача параметрів, необхідних для розрахунку частоти відправлення пакетів,
- управління сеансом зв’язку.

На рис. 3 наведено спрощену схему взаємодії клієнта з мультимедійним сервером через базові протоколи передачі потокової інформації.

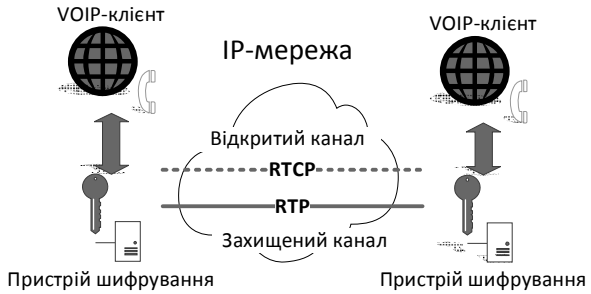


Рис. 3. Схема взаємодії клієнтів IP-мережі

Як видно з рис. 3, відкритий канал організовано з використанням протоколів RTSP і RTCP. Перший керує передачею потокової інформації в реальному масштабі часу, другий контролює зміни в мережі для надання інформації RTP-протоколу.

Захищений канал базується на використанні RTP-протоколу. Як зазначалося, існує безліч застосувань, що забезпечують взаємодію клієнтів через відкритий канал (наприклад, застосування XLITE, EKIGA і т.п.). Тому основним завданням при виконанні роботи було створення не тільки інтерфейсу взаємодії з цими застосуваннями для організації передавання відкритих даних, але й способу використання інтерфейсу протоколу RTP для інтеграції з розробленим пристроєм шифрування переданих потокових мультимедійних даних у реальному масштабі часу. У даній реалізації для цієї мети використовуються проксі-сервери, хоча можливі й інші варіанти. Вважаємо, що наразі представлений варіант є найбільш ефективним.

Комплекс захисту VOIP-телефонії

З погляду системної інтеграції розроблений комплекс складається з двох підсистем: програмної підсистеми, що забезпечує інтерфейс з мережевим протоколом, й апаратної підсистеми, яка реалізує запропонований алгоритм шифрування потоків інформації на базі нерозкривних шифрів. Узагальнену схему взаємодії цих підсистем показано на рис. 4.

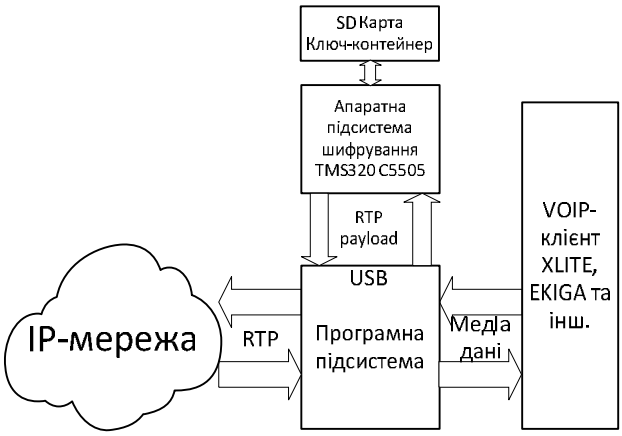


Рис. 4. Загальний схема роботи пристрою захисту

Пропонована система захисту працює в потоковому режимі, тобто зашифровані дані, що передаються каналом зв'язку, розшифровуються в прикінцевому пристрої й далі обробляються іншими застосуваннями або апаратними пристроями. Тому реалізований режим функціонування системи захисту не припускає збереження переданих даних у зашифрованому вигляді.

Програмна підсистема. Програмна підсистема надає необхідний набір API-функцій для сторонніх застосувань, а також реалізує розроблений функціонал.

Апаратна підсистема. Для застосувань апаратна підсистема представляється у вигляді набору функцій, які викликаються при виклику заданих API-функцій із програмної підсистеми. Така реалізація дозволяє гнучко модифікувати різні підпрограми без необхідності повторного перепрограмування всього пристрою. Крім цього з'являється можливість додавати в апаратну частину нові реалізації алгоритмів генерації псевдовипадкових чисел, протоколів узгодження, спеціалізованих функцій обробки різного контенту та ін.

З урахуванням зростаючої необхідності в передаванні потокової мультимедійної інформації в комп'ютерних мережах пристрій (рис. 5, 6) був створений на базі процесора серії TMS320 C5505 для цифрової обробки сигналів, що забезпечило необхідну продуктивність.

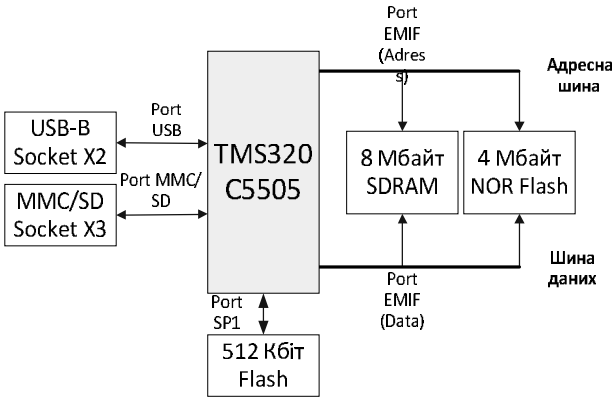


Рис. 5. Блок-схема
розробленого пристрою шифрування

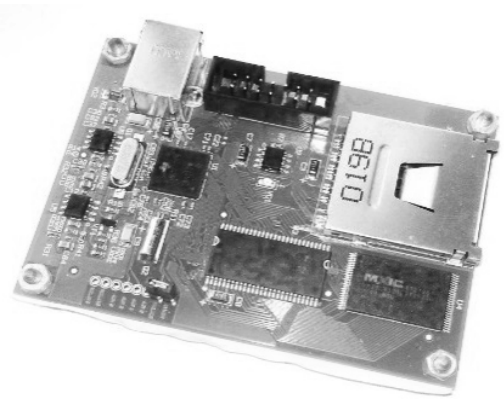


Рис. 6. Загальний вигляд пристрою шифрування

Алгоритм передавання зашифрованої потокової інформації в реальному часі. Суть розробленого алгоритму шифрування полягає в такому. У масив пам'яті на базі SD-картки записуються істинно випадкові числа (шум лісу, шум автомобільного двигуна й т.п.), з яких зорганізується спеціальний масив (він і буде секретним ключем). Береться байт мультимедійного файлу, який треба зашифрувати, у секретному ключі розшукується його адреса й ця адреса передається по мережі. На приймальній стороні є такий самий масив істинно випадкових чисел (секретний ключ), де відповідно до прийнятої адреси розшукується значення байта, яке стане байтом зашифрованої послідовності. Даний алгоритм є гранично криптостійким. Існує безліч варіантів його реалізації. Наприклад, вибира-

ється один із кращих алгоритмів генерації псевдовипадкових чисел з певними параметрами («зерно»). Передавальна сторона на базі істинно випадкових чисел (відповідно до описаного алгоритму) відправляє приймальній стороні «зерно». Приймальна сторона, використовуючи ці параметри, на льоту генерує відповідні псевдовипадкові числа й із цих чисел вибирає байти переданої мультимедійної інформації. У такому випадку обсяг вихідного масиву чисел може бути значно меншим.

Схему спрощеного варіанта пропонованого алгоритму шифрування наведено на рис. 7.

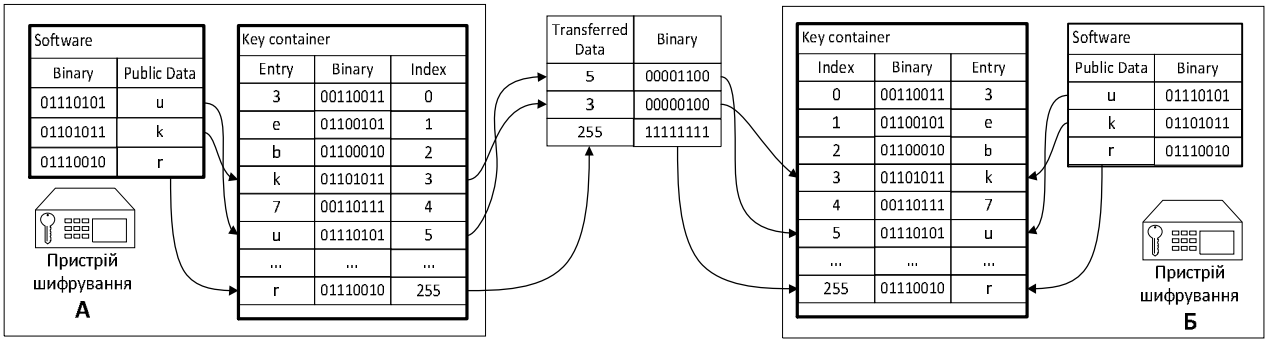


Рис. 7. Спрощений алгоритм передавання зашифрованої потокової інформації в реальному часі

Висновки

Отже, створення програмно-апаратних комплексів захисту на базі використання нерозкривних шифрів є перспективним напрямком досліджень в області інформаційної безпеки. Оскільки даний клас шифрів володіє доведеною криптостійкістю й відповідно не може бути зламаний, це дозволяє використовувати гарантовану криптостійкість. Особливою перевагою описаного комплексу захисту є робота в потоковому режимі, що дозволяє застосовувати його у VOIP-телефонії, в системах аудіо-, відеотрансляції, а також у різних розподілених системах з підвищеними вимогами до параметрів використовуваних каналів зв'язку. Наразі розроблений апаратно-програмний комплекс проходить експериментальне дослідження в настільних комп'ютерах, локально-корпоративній мережі комп'ютерів, а також у глобальній мережі Інтернет.

Список літератури

1. Method of shared data access in distributed computer networks / [Nycolaychuk Y.M., Humenniy P.V., Alishov N.I., Hladyuk V.M.]// Journal of Qafgaz University (Baku): Mathematics and Computer Science. – 2013. – V 1, N 1. – P. 17−23.

2. Computer technologies in information security/ [Valery Zadiraka, Yaroslav Nykolaichuk, Nadir Alishov, Ivan Albanskyi, Boris Bredelev et al.]. − Ternopil: Kart-Blansh, 2015. − 387 p.

3. Goto A. Safe and Secure Ubiquitous Communication/ A. Goto // Intern. workshop on network security and wireless communications 27 Jan 2005. – Accessed to: http://www.it.ecei.tohoku.ac.jp/~kato/workshop2005/NTT-goto-slides.pdf.

4. Network Security: Know It All / [J. Joshi, S. Bagchi, B.S. Davie et al.]. – Burlington: Morgan Kaufmann, 2008. – 368 p.

5. Технология системной интеграции аппаратно-программных средств защиты потоковой информации на базе нераскрываемых шифров [Алишов Н.И., Алишов А.Н., Бойко А.Я. и др.] // Системи обробки інформації: зб. наук. праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2016. – Вип. 3 (140). – С. 7-10.

Надійшла до редколегії 2.02.2017

Рецензент: д-р техн. наук, проф. В.М. Опанасенко, Інститут кібернетики імені В.М. Глушкова НАН України, Київ.

ПРИМЕНЕНИЕ НЕРАСКРЫВАЕМЫХ ШИФРОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В VOIP-ТЕЛЕФОНИИ

Н.И. Алишов, С.В. Зинченко, А.Н. Алишов, Н.А. Сапунова

Статья посвящена проблемам безопасности VOIP-телефонии. Рассмотрены основные виды угроз для VOIP-телефонии, мероприятия по их устранению. Предложен программно-аппаратный комплекс защиты на основе использования нераскрываемых шифров, который работает в потоковом режиме.

***Ключевые слова**: потоковая информация, VoIP-телефония, защита информации, нераскрываемые шифры, протоколы передачи информации, устройство защиты информации.*

APPLICATION OF UNBREAKABLE ENCRYPTION TO ENSURE SECURITY IN VOIP TELEPHONY

N.I. Alishov, S.V. Zintchenko, A.N. Alishov, N.A. Sapunova

The article is devoted to security VOIP telephony issues. Considered the main types of threats to VOIP telephony and activities to eliminate them. Proposed a VOIP protection system based on using unbreakable cipher. It includes hardware and software that operates in streaming mode.

***Keywords:** streaming, VOIP telephony, data protection, unbreakable cipher, data protocols, data security device.*

УДК 004.732.056

С.Ю. Гавриленко, И.В. Шевердин

Национальный технический университет «ХПИ», Харьков

УСОВЕРШЕНСТВОВАННАЯ КОНЦЕПЦИЯ ЗАЩИТЫ ДАННЫХ НА БАЗЕ МНОГОУРОВНЕВОГО АНАЛИЗА КАРТ ОПЕРАЦИОННОЙ СИСТЕМЫ

Разработана многоуровневая антивирусная система, базирующаяся на анализе системных событий и низкоуровневых команд. Архитектурно система операционно-зависима, что позволяет сформировать карты уровней конкретно выполняемой операционной системы, основываясь на различии драйверов устройств и различных системных компонентах. Анализ процессов, а не групп системных компонентов, позволяет увеличить быстродействие системы по сравнению с существующими реализациями эвристического анализа.

Ключевые слова: *компьютерные системы, антивирусные системы, анализ процессов в операционной системе, многоуровневые системы анализа данных.*

Введение

Постановка проблемы и анализ литературы. Одним из самых актуальных вопросов современной безопасности является обеспечение целостности и защиты информации [1]. Мы живем в эру развития информационной компьютерной компетенции, с каждым днем наша работа, образование и отдых трансформируется в автоматизированные сервисные решения, реализованные на базе компьютерного оборудования и соответствующего программного обеспечения. Наша жизнь становится цифровой и наравне с физической безопасностью нам необходимы средства защиты информации нашего цифрового мира.

Современные антивирусные программы позволяют не только выявлять, но и предотвращать несанкционированный доступ вредоносных программ [2, 3]. Большинство современных антивирусных программ запускается автоматически операционной системой, и постоянно проверяют безопасность осуществляемых другими программами действий, а также контролируют оперативную память и файловую систему компьютера. Но антивирусная программа не может дать достаточно высокий уровень защиты, так как она зависит от обновления и сигнатурных баз вирусов. Эта проблема частично решается эвристическим методом, но данный метод реализованный в современных антивирусных программах не дает абсолютную гарантию обнаружения из-за основных принципов работы [4, 5]. Основным минусом существующих методов эвристического анализа является большая нагрузка на выполняющую систему, ложные срабатывания, отсутствие методов адаптации и обучения.

Именно поэтому актуальной темой является разработка эффективных методов и технологий противодействия компьютерным вирусам.

Цель статьи. Разработка многоуровневой антивирусной системы формирования карт анализа процессов в операционной системе, для обнаружения вредоносного программного обеспечения.

Основная часть

В работе предложена многоуровневая антивирусная система формирования карт (MAP – Monitor Automatic Page) которая выполняет анализ процессов в операционной системе, что позволяет обнаружить все виды вирусных атак, так как для выполнения какого-либо вредоносного воздействия вирусу необходим процесс. Даже если данный вирус является набором скриптов, будут использованы интерпретаторы операционной системы, которые в свою очередь также являются процессами.

Предложенная система не зависит от большого объёма сигнатурных баз, обладает быстрым временем обнаружения вредоносного операционного процесса и выполнена в виде отдельного модуля специального назначения для антивирусных программ.

Архитектурно данная система является операционно-зависимой. Это обеспечивает формирование карт уровней для конкретно выполняемой операционной системы, основываясь на различии драйверов устройств и различных системных компонентах.

Для построения карточного анализа используется многоуровневая система анализа поведения состояний операционной системы (рис. 1). Основной принцип работы данной системы – это формирование карт уровней 0 и 1, а также выполнение анализа посредством второго уровня для проверки инструкций процесса. В качестве механизма сопоставления карт используется метод нечеткой логики, позволяющий сделать вывод о возможности вредоносного воздействия данного процесса на систему.

Карты уровня 0 – это карты аппаратного уровня, которые описывают систему в целом, а именно реестр, оперативную память, дисковое пространство, поток интернет пакетов. Карты уровня 1 – это карты уровня процессов, которые описывают поведение процесса, а именно выполнение операций с дисковым пространством, изменение реестра, взаимодействие с сетевыми ресурсами, формирование новых потоков и коммуни-

кация со сторонними процессами. Карты уровня 2 – это карты низкоуровневого анализа инструкций процесса, представляющие собой команды языка ассемблера. Карты содержат последовательность вредоносных команд.

Для повторного анализа существующих карт каждого уровня применяется два механизма: ретроспектива для уровня 1 и интроспектива для уровня 2. Ретроспектива карт – это повторный анализ состояния процессов уровня 1 с построением дерева карт, используя уровень 2.

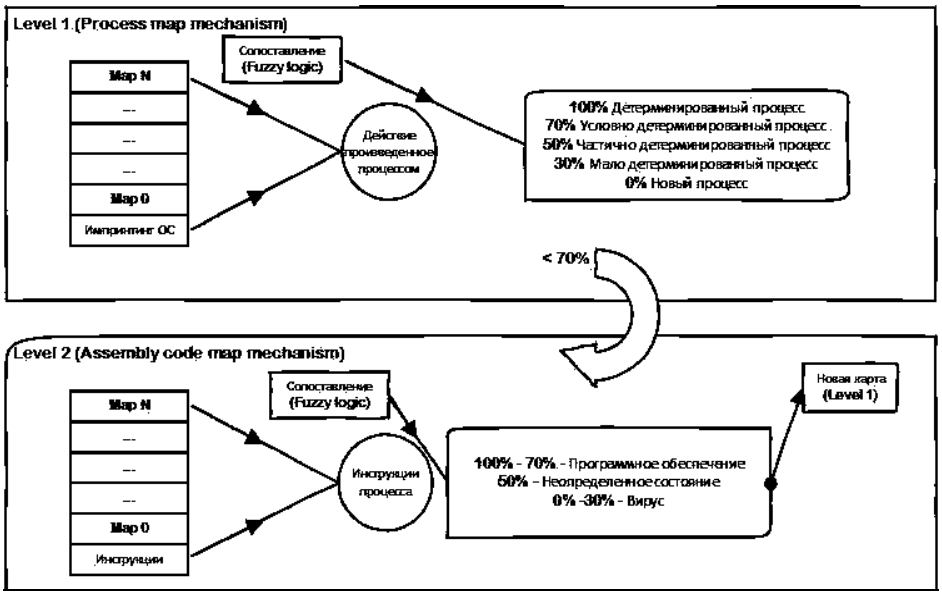


Рис. 1. Многоуровневая антивирусная система формирования карт

Дерево карт – это специализированная структура данных, которая агрегирует ряд состояний процесса до 10-го поколения и связывает системные события с процессами, которые породили данное событие. Интроспектива карт – это анализ низкоуровневых вредоносных команд для карт уровня 2, путем формирования зависимостей между существующими командами. Ретроспектива проводится в случае простоя компьютерного оборудования.

Карты для уровня 1 создаются после функционального исследования процессорных команд на уровне 2. Карты для уровня 2 формируются оператором антивирусной системы и являются перманентной частью системы, агрегирующей ряд инструкций языка ассемблера согласно критерию опасности команд, что позволяет в дальнейшем, используя данный ряд инструкций выполнить интроспективу карт и скорректировать карты. Так как большинство информации, получаемой из системных событий представляет собой строковый набор данных, то карты уровней представляются в виде хеш-таблиц. Для быстрого поиска в ней используется алгоритм Рабина-Карпа, что позволяет находить и сопоставлять информацию за асимптотически минимальное время.

Многоуровневый подход позволяет получить минимальное количество ложных срабатываний, путем анализа всех системных событий в целом, а не определенного набора команд процессов. Современные антивирусы анализируют определенный ряд команд процессов и при наличии последовательности вредоносных команды блокируют вызывающий процесс. Предложенный метод анализирует все события операционной системы, что повышает вероятность обнаружения вирусной активности. Для предотвращения ложного определения реализованы дополнительные уровни анализа, это уровень 0 и 2, что позволяет анализировать не только события, но и содержимое памяти, реестра, интернет пакетов на уровне 0, а уровень 2, соответственно позволяет провести анализ системных команд процессов в момент поступления события на уровне 1. Таким образом достигается полная информационная консистентность статистических данных, формирующих карты операционной системы.

Результаты разработки и исследований основных этапов работы MAP. MAP инсталлируется после установки операционной системы семейства Windows 7/8/8.1/10 и выполняет формирование первоначальных карт уровня 1 операционной системы, описывая все процессы в системы (импринтинг операционной системы). После установки нового программного обеспечения MAP запускает механизм сопоставления карт, который укажет наличие новых процессов в системе, и выполнит переход на уровень 2 для определения новых инструкции в процессе. Полученный набор новых инструкций подвергается анализу, используя аппарат нечеткой логики и определяется наличие вредоносных команд в данном процессе (рис. 2). После чего формируется новая карта для уровня 1. Так как точность в данный момент может варьироваться от 0% или 100% MAP, то необходимо сформировать список интроспективного анализа и занести процессы в очередь.

При повторении процессов, есть вероятность изменения статистики путем добавления новых состояний в виде карт, что может привести в дальнейшем к переходу от неопределенного состояния к определению процесса как программного компонента или вируса (пузырек интроспекции). Если система не задействует свои ресурсы, то MAP выполнит ретроспективу. Пользователь также будет статистически описан системой MAP с помощью механизма, который формирует специфическую карту зеркально насыщенного нейронного повторения. Карта зеркально насыщенного нейронного повторения представляет собой статистически построенную карту выполнения

пользователем перманентных действий в системе, которые формируют пользовательское (административное) состояние системы, описанное нейронной сетью в течение недели работы операционной системы. Результаты показали целесообразность использования карт и алгоритмических механизмов для обнаружения вредоносного программного обеспечения.

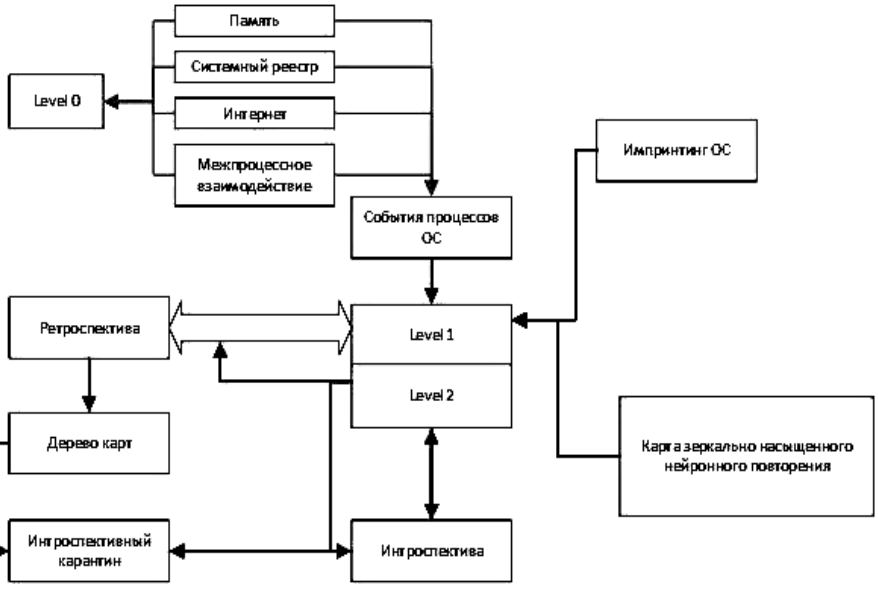


Рис. 2. Структурная схема антивирусной системы защиты данных на базе многоуровневого анализа карт операционной системы

Выводы

В работе впервые предложена многоуровневая антивирусная система формирования карт анализа процессов в операционной системе для обнаружения вредоносного программного обеспечения. Анализ процессов, а не групп системных компонентов, позволяет увеличить быстродействие системы по сравнению с существующими реализациями эвристического анализа. Для быстрого анализа и сопоставления результатов различных карт на всех уровнях MAP используются хеш-таблицы. Максимально возможное предотвращение ложных срабатываний, достигается путем внедрения многоуровневой системы анализа, компенсирующей и формирующей статистический ряд по масштабно ориентированному набору, а именно система анализируется глобально, оцениваются масштабные изменения, изменения событий процессов системы, а также низкоуровневые системные команды. Отсутствие методов адаптации и обучения решается путем внедрения новых карт во все уровни путем обучения, каждый уровень способен создать карту для предыдущего уровня.

Список литературы

1. *The best antivirus protection of 2017 [Електронний ресурс] – Режим доступу: http://uk.pcmag.com/antivirus-reviews/8141/guide/the-best-antivirus-protection-of-2017.*

2. *Касперський К. Записки дослідника комп'ютерних вірусів. / К. Касперський. - СПб .: Пітер, 2006. - 316 с.*

3. *Semenov. S.G. and Davydov V.V. and S.Y. Gavrilenko (2014), Data protection in computerized control systems, Ed. «LAP LAMBERT ACADEMIC PUBLISHING» Germany, 236 p.*

4. *Кнут Е. Д. Мистецтво програмування. Том 1. Основні алгоритми. М .: Видавничий дім «Вільямс», 2000. - 832 с.*

5. *Bart Kosko (1986). "Fuzzy Cognitive Maps". International Journal of Man-Machine Studies, 1986.– cc. 65–75.*

Надійшла до редколегії 31.01.2017

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

УДОСКОНАЛЕНА КОНЦЕПЦІЯ ЗАХИСТУ ДАНИХ НА БАЗІ БАГАТОРІВНЕВИХ АНАЛІЗУ КАРТ ОПЕРАЦІЙНОЇ СИСТЕМИ

С.Ю. Гавриленко, І.В. Шевердін

У статті розроблена багаторівнева антивірусна система, що базується на аналізі системних подій і низькорівневих команд. Архітектурно дана система є операційно-залежною. що дозволяє сформувати карти рівнів конкретно виконуваної операційної системи, ґрунтуючись на відмінності драйверів пристроїв і різних системних компонентах. Аналіз процесів, а не груп системних компонентів, дозволяє збільшити швидкодію системи в порівнянні з існуючими реалізаціями евристичного аналізу.

Ключові слова: *комп'ютерні системи, антивірусні системи, аналіз процесів в операційній системі, багаторівневі системи аналізу даних.*

IMPROVED DATA PROTECTION CONCEPT ON THE BASIS OF MULTI-LEVEL ANALYSIS OF THE OPERATING SYSTEM CARD

S.Yu. Gavrilenko, I.V. Sheverdine

The article developed a multi-level antivirus system, based on the analysis of system events and low-level commands. Architecturally, this system is operationally dependent. Which allows you to create maps of the levels of a specific operating system, based on the differences between device drivers and various system components. Analysis of processes, rather than groups of system components, allows to increase the speed of the system in comparison with existing implementations of heuristic analysis.

Keywords: *computer systems, anti-virus systems, analysis of processes in the operating system, multi-level systems for data analysis.*

УДК 004.056.53

В.В. Давыдов, Д.С. Гребенюк

Национальный технический университет «ХПИ», Харьков

КОМПЛЕКС ПРОЦЕДУР ГЕНЕРАЦИИ ЛИЦЕНЗИОННОГО КЛЮЧА ДЛЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

В статье описан процесс разработки программного комплекса генерации лицензионного ключа защиты авторских прав интеллектуальной собственности на программное обеспечение, учитывающего индивидуальные данные конечного пользователя. Верификация лицензионного ключа выполняется единожды при каждом запуске программного обеспечения в режиме «offline», т.е. без выполнения запросов на сервер, так как вся необходимая информация уже хранится локально.

Ключевые слова: *защита авторских прав, лицензионный ключ, клиент-серверная архитектура, защита от тиражирования, кроссплатформенное программное обеспечение, REST-сервисы.*

Введение

Постановка проблемы. В условиях повсеместного использования компьютерных, телекоммуникационных и других компьютеризированных средств, а также постоянного совершенствования и обновления их программного обеспечения (ПО), достаточно актуальной задачей является защита интеллектуальной собственности и авторских прав на программные продукты (обеспечение).

Особенно острой эта проблема выглядит в Украине, где компании-разработчики ПО несут финансовые потери из-за несанкционированного (незаконного) использования авторских прав на созданные программные продукты.

Анализ последних исследований и публикаций. Анализ литературы [1, 2, 4, 6] показал, что одним из наиболее эффективных средств защиты интеллектуальной собственности на ПО является лицензионный ключ защиты приложений (ЛКЗП). Обычно ключ применяется во время установки. Программа-установщик применяет алгебраические вычисления к вводимому ключу для проверки его на подлинность. Например, алгоритму необходимо определить, что вводимый ключ должен содержать 5 чисел, сумма которых равна 25, и что ключ также должен содержать 3-5 литер так, что после перевода их в числовые эквиваленты получим сумму 42 [3, 11].

Проведенные исследования [2, 4, 6, 7] показали, что в настоящее время существует ряд подходов к формированию ЛКЗП. Их основой являются известные криптографические алгоритмы, позволяющие формировать последовательности различного уровня сложности и стойкости. Следует заметить, что у большинства фирм-разработчиков ПО эта информация является конфиденциальной. В то же время, анализ открытых интернет-ресурсов [3] показал массовое предложение на программное обеспечение, позволяющее формировать так называемые keygen, которые пишутся как отдельными программистами, так и хакерскими группами, например, C.O.R.E., ORiON, Z.W.T, REVOLUTiON, XNTeam, Fight For Fun и др., специализирующимися на взломе программного обеспечения. Иногда такие группы заявляют о себе также тем, что включают своё название в сгенерированный ключ в открытом либо зашифрованном виде [3].

Поэтому актуальной является разработка генератора ЛКЗП, реализующего современные принципы контроля разрешений исполнения прикладного кода, который бы позволил минимизировать риск хакерской подделки, и тем самым повысил уровень защиты авторских прав на интеллектуальную собственность. Решение поставленной задачи невозможно без разработки соответствующего программного комплекса.

Цель статьи. Таким образом, целью статьи является разработка комплекса процедур генерации ЛКЗП для защиты авторских прав на ПО. Данные процедуры легли в основу программного комплекса генерации ЛКЗП.

Основные результаты исследований

В ходе разработки программного комплекса генерации ЛКЗП, с целью защиты программного комплекса от тиражирования, была разработана клиент-серверная архитектура, позволяющая продемонстрировать работу разработанного метода генерации лицензионного ключа.

Клиентское ПО, которое имеет защиту от тиражирования, использующую разработанный комплекс, имеет в своей структуре:

– полезный код, т.е. код самого программного продукта;

– client-processor.jar – разработанная библиотека, подтверждающая легальность лицензионного ключа и реализующая обмен сообщениями с серве-

ром. Данная библиотека обфусцирована, что уменьшает вероятность анализа алгоритма злоумышленниками. Библиотека состоит из:

1) сервисов доступа к базе данных на стороне клиента;

2) client-systeminfo.jar - модуля, отвечающего за получение информации о комплектующих клиентской компьютерной системы;

3) client-decoder.jar - модуля, декодирующего переданный лицензионный ключ. Выявляет в лицензионном ключе закодированный программный код, запускает его;

4) common-license.jar - модуля, отвечающего за генерацию цифровой подписи к сообщению, а также проверку подписи сообщения на основе тела сообщения, хэш-суммы и имеющегося публичного ключа. Его дубликат находится также на сервере;

5) common-api.jar - модуля, представляющего собой интерфейс доступа к сервисам сервера. Содержит интерфейсы функций реализованных возможностей для использования путем обмена REST-запросами. Его дубликат находится также на сервере;

Серверная часть состоит из:

– сервисов доступа к базе данных сервера;

– server-encoder.jar, - модуля, который на основе входного java-файла, содержащего код, выполняющийся на стороне клиента, а также дополнительных настроек – информации о конкретном программном продукте, создает class-файл (скомпилированный java-файл), который в последствии кодируется описанным в статье [5] алгоритмом;

– common-license.jar;

– common-api.jar.

Все нижеописанные диаграммы последовательностей состоят из четырех структур:

1. База данных клиента. В связи с тем, что предполагается хранение данных в формате «ключ-значение» и отсутствием связанных объектов, была выбрана база данных MapDB [9], предназначенная специально для хранения пар «ключ-значение». Данная база данных позволяет ввести систему аутентификации для защиты от несанкционированного доступа. При этом, в качестве пароля для базы данных используется хэш-сумма строки, содержащей информацию о комплектующих данной компьютерной системы, которая описана работе [5], и является практически уникальной для каждой компьютерной системы. Это уменьшает вероятность использование злоумышленником базы данных другого пользователя с зарегистрированным программным продуктом и позволяет избежать «тиражирования» лицензии на данный программный продукт.

2. Клиентское ПО. Состоит из программного обеспечения, которое имеет лицензионный ключ, и надстройки сервисов программного обеспечения по обработке лицензий, предназначенных для регистрации пользователя, регистрации программного продукта, верификации лицензионного ключа. При запуске данного ПО:

– происходит обращение к клиентской базе данных с использованием пароля, который вычисляется «на лету» (т.е. пароль от базы данных нигде не хранится. В случае, если поменялась конфигурация системы, то пароль уже подходить не будет);

– из базы данных берется закодированный лицензионный ключ для данного программного продукта и происходит его верификация, в частности выполнение закодированного в нем кода. Код представлен в виде блока программы на языке программирования Java, что дает как возможность кроссплатформенности использования данного подхода лицензирования, так и возможность перехватывания выполнения недопустимых команд, приводящих к аварийному завершению программы или доступа к «чужой» памяти.

3. Сервер. Находится в центре сертификации компании, поставляющей данное программное обеспечение. Представлен в виде REST API компонентов, которые работают под управлением сервера приложений Jboss Wildfly 8.2.0. При текущей реализации системы генерации лицензионных ключей используется Java 1.7. На сервере приложений настроен SSL доступ для повышения защиты механизма обмена сообщениями между сервером и клиентом от злоумышленного воздействия.

4. База данных сервера. Согласно бизнес требованиям была выбрана база данных MongoDB [10], имеющая более высокие показатели производительности чтения данных по сравнению с другими базами данных. Содержит информацию о всех зарегистрированных клиентах, приобретенных ими лицензиях, а также информацию о каждой зарегистрированной пользовательской компьютерной системе для возможности восстановления пароля или организации возможности обновления пароля/лицензионного ключа, если конечный пользователь согласованно меняет комплектующие системы.

Сервер предоставляет следующие возможности:

– регистрация нового пользователя;

– авторизация пользователя при утере/повреждении клиентской базы данных;

– регистрация новой компьютерной системы.

Любая покупка программного обеспечения начинается с того, что пользователь вносит свою клиентскую информацию в базу данных сервера, который владеет лицензией на данное программное обеспечение. Диаграмма последовательностей данного процесса представлена на рис. 1. При помощи надстроек сервисов программного обеспечения по обработке лицензий пользователь передает свои клиентские данные, которые сохранятся на сервере и будут отражать его в клиентской базе.

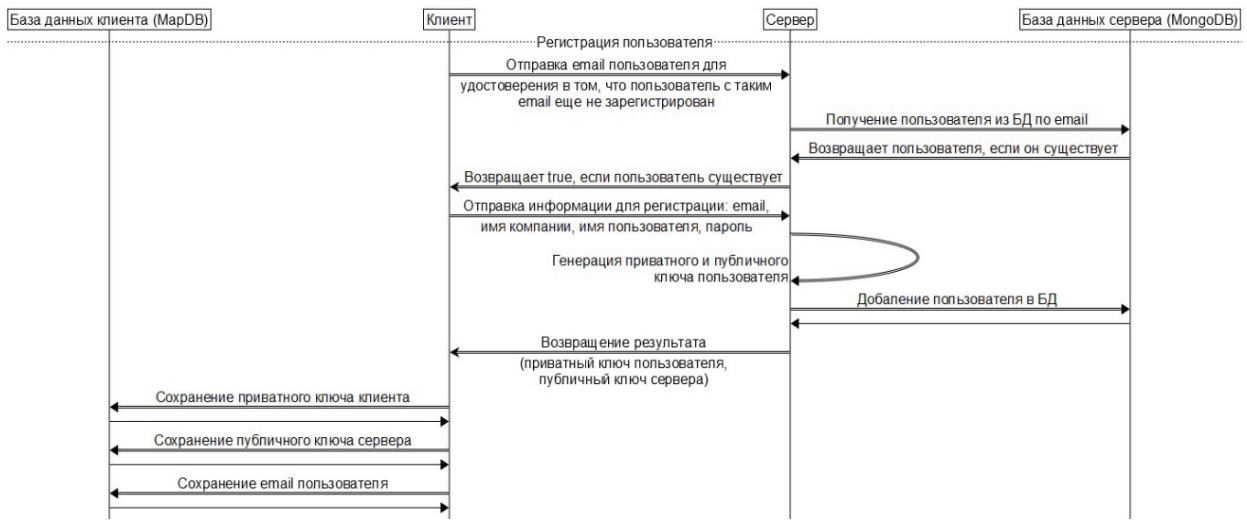


Рис. 1. Диаграмма последовательностей процесса регистрации пользователя в системе

К таким данным на текущий момент относятся:

– E-mail пользователя;

– имя компании, которую представляет данный пользователь. В случае, если пользователь – физическое лицо, это поле может оставаться пустым;

– ФИО пользователя, на имя которого происходит регистрация;

– пароль пользователя.

При этом, e-mail и пароль пользователя могут выступать в процессе аутентификации пользователя, в связи с этим, e-mail должен быть уникален в системе, а пароль должен быть безопасным согласно политике паролей [11].

После того, как система-сервер получила информацию о пользователе, активизируются следующие действия:

– проверяется наличие данного пользователя в своей базе данных. В случае, если пользователь с таким идентификатором-email уже существует, возвращается ответ с соответствующей ошибкой;

– генерируется пара ключей, с учетом собственного центра сертификации, конечного пользователя для возможности дальнейшего безопасного обмена сообщения с ним.

– сохраняется в базе данных переданная информация о пользователе, а также пара ключей. При этом, в целях защиты пользовательских данных, пароль пользователя не хранится в открытом виде, а хранится только его хэш-сумма, созданная при помощи утилиты BCrypt [8], основанная на шифре Blowfish.

– в качестве ответа, сервер возвращает клиенту публичный ключ сервера и приватный ключ клиента для возможности безопасного обмена сообщениями. Данный ответ не подлежит дополнительным средствам защиты от злоумышленника.

Получив успешный ответ от сервера, клиент сохраняет полученные ключи, а также свой e-mail в клиентской базе данных. Пользователь зарегистрирован в системе, и имеет возможность регистрировать конкретную компьютерную систему для данного программного обеспечения.

Проведенные исследования показали, что очень часто, в случае воздействия злоумышленного программного обеспечения или переустановки операционной системы, возникают ситуации утери или повреждения базы данных клиентского программного обеспечения. Пренебрежение этим существенно снижает практическую ценность разработки. Поэтому для учета данного фактора был разработан механизм восстановления указанной информации при наличии сохраненного e-mail и пароля зарегистрированного пользователя. Механизм аутентификации пользователя с восстановлением его данных представлен на рис. 2.

Процесс аутентификации происходит следующим образом:

1. Пользователь отправляет на сервер свои e-mail и пароль. В целях безопасности пароль отправляется в виде хэш-суммы, построенной утилитой BCrypt.

Сервер сверяет пользовательские e-mail и пароль. В случае ошибки авторизации – возвращается соответствующий ответ с ошибкой. Если пользовательские данные корректные, то из базы извлекается уже имеющаяся информация о конечном пользователе – его приватный ключ, и возвращается ответом с сервера вместе с публичным ключом сервера.

2. Получив успешный ответ от сервера, клиент сохраняет полученные ключи, а также свой e-mail в клиентской базе данных.

После того, как пользователь аутентифицировался на сервере, он имеет возможность добавлять/получать лицензии на конкретную компьютерную систему. Процесс добавления клиентской компьютерной системы описан на рис. 3, и состоит из описанных ниже этапов.

Рис. 2. Диаграмма последовательностей
процесса аутентификации пользователя в системе

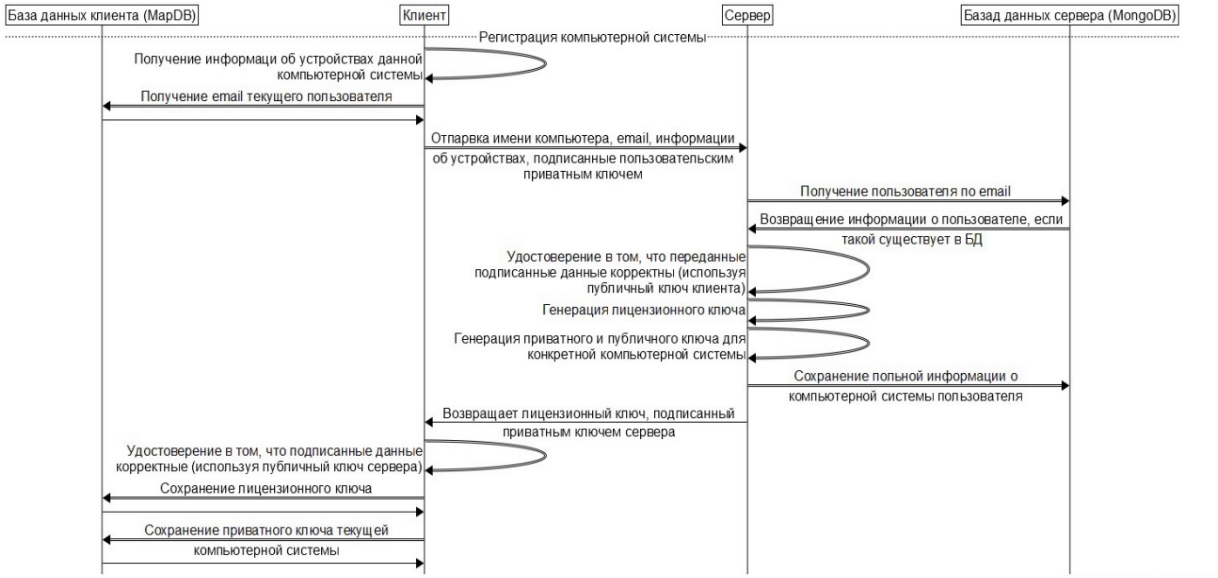


Рис. 3. Диаграмма последовательностей
процесса регистрации клиентской КС на сервере

1. Лицензионный модуль программного обеспечения получает информацию о компонентах компьютерной системы.

2. На основе хранимой в базе данных информации о пользователе, происходит отсылка запроса на сервер, содержащий следующую информацию: имя компьютерной системы (должно быть уникальным для пользователя, например, «Мой ПК 1»), e-mail пользователя, сгенерированная информация об устройстве. Вся эта информация подписывается приватным ключом клиента.

3. В связи с тем, что любая лицензия требует оплаты, пользователь отправляется на страницу оплаты лицензии через платежную систему, например, на paypal.com. Дальнейшая регистрация клиентской компьютерной системы осуществляется только при подтверждении транзакции от платежной системы.

4. Сервер получает информацию о зарегистрированном пользователе на основе полученного e-mail, проверяет достоверность переданного сообщения на основе имеющегося публичного ключа пользователя.

5. Сервер генерирует лицензионный ключ, кодирует его.

6. Копия лицензионного ключа хранится на сервере в закодированном виде с целью возможности его восстановления.

7. Сервер отправляет сгенерированный лицензионный ключ. Сообщение подписывается приватным ключом сервера.

8. Лицензионный модуль клиентского программного обеспечения проверяет достоверность переданного сообщения на основе имеющегося публичного ключа сервера и сохраняет лицензионный ключ в закодированном виде в базе данных, находящейся на стороне клиента.

9. Лицензионный ключ декодируется и запускается, что, в случае успешной работы, приводит к тому, что программное обеспечение бу-

дет зарегистрированным. Данный процесс выполняется каждый раз при запуске программного обеспечения.

Выводы

Таким образом, разработан программный комплекс генерации лицензионного ключа защиты приложений для защиты авторских прав интеллектуальной собственности на программное обеспечение. Отличительной особенностью данного комплекса является учет индивидуальных данных конечного пользователя, что предотвращает возможность тиражирования лицензионного ключа злоумышленниками.

В результате выполнения функций генерации сформированный лицензионный ключ представляет собой программный код, исполняемый на стороне конечного пользователя, что дает дополнительную защиту программного продукта от злоумышленного воздействия.

Для защиты баз данных от воздействия вредоносного программного обеспечения или переустановки операционной системы, разработан механизм аутентификации пользователя с восстановлением его данных.

Кроме этого, для защиты баз данных предусмотрена процедура обфускации.

Список литературы

1. Закон України «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних» від 13.01.2016 [Електронний ресурс] / - Режим доступу: http://zakon3.rada.gov.ua/laws/show/1587-14.

2. Болтенков В.А. Практическое исследование современных систем электронной цифровой подписи / Болтенков В.А., Еникеев Р.И. – Одесса: ОНПУ, 2014. – Том 4. - № 3. – 201-209 с.

3. Генератор ключей [Электронный ресурс] : - Режим доступа : ru.wikipedia.org.

4. Семенов С.Г. Исследования технологий динамического анализа бинарного кода программного обеспечения / С.Г. Семенов, С.Ю. Гавриленко, А.В. Мовчан // Компьютерные системы и проектирование технологических процессов и оборудования: Мат-лы Всеукр. научтехн. конф. – Черновцы: ЧФ НТУ «ХПИ», 2016. – С. 152-154.

5. Семенов С.Г. Система формирования цифрового идентификатора программного обеспечения для защиты авторских прав / С.Г. Семенов, В.В. Давыдов, А.В. Мовчан // Современные проблемы информатики в управлении, экономике, образовании и преодолении последствий Чернобыльской катастрофы: Мат-лы XV Междунар. науч. сем. - К.: Национальная академия управления, 2016. – С. 110-116.

6. Цифровые подписи в исполняемых файлах и обход этой защиты во вредоносных программах [Электронный ресурс] : - Режим доступа : https://habrahabr.ru/post/112289/

7. A.M. Bahaa-Eldin A comprehensive Software Copy Protection and Digital Rights Management platform / A.M. Bahaa-Eldin, M.A.A. Sobh // Ain Shams Engineering Journal, 2014 – Volume 5. – Issue 3. – P. 703-720.

8. BCrypt [Электронный ресурс] : - Режим доступа : ru.wikipedia.org.

9. Introduction to MapDB [Электронный ресурс] : - Режим доступа : https://www.gitbook.com/book/jankotek/mapdb/details.

10. Introduction to MongoDB [Электронный ресурс] : Режим доступа : https://docs.mongodb.com/manual/introduction/

11. Password Policy [Электронный ресурс] : Режим доступа : en.wikipedia.org

Надійшла до редколегії 24.01.2017

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

КОМПЛЕКС ПРОЦЕДУР ГЕНЕРАЦІЇ ЛІЦЕНЗІЙНОГО КЛЮЧА ДЛЯ ЗАХИСТУ АВТОРСЬКИХ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ НА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

В.В. Давидов, Д.С. Гребенюк

В статті описано процес розробки програмного комплексу генерації ліцензійного ключа захисту авторських прав інтелектуальної власності на програмне забезпечення, що враховує індивідуальні дані кінцевого користувача. Верифікація ліцензійного ключа виконується один раз при кожному запуску програмного забезпечення в режимі «offline», тобто без виконання запитів на сервер, так як вся необхідна інформація вже зберігається локально.

Ключові слова: *захист авторських прав, ліцензійний ключ, клієнт-серверна архітектура, захист від тиражування, кросплатформенність, REST-сервіси.*

LICENSE KEY GENERATION PRODUCT FOR SOFTWARE INTELLECTUAL PROPERTY COPYRIGHT PROTECTION

V.V. Davydov, D.S. Hrebeniuk

The article describes the process of developing a software system generating license key copyright protection of intellectual property rights of software, taking into account the individual end-user data. License key verification is performed only once each time you start the software in «offline» mode, that is without executing queries to server, since all the necessary information is already stored locally.

Keywords: *copyright protection, license key, the client-server architecture, protection from replication, cross-platform software, REST-services.*

УДК 004.056.5

Д.Д. Левченко

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

АНАЛИЗ МОДЕЛЕЙ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

Главной идеей статьи является защита данных от несанкционированного доступа. В работе были рассмотрены проблемы безопасности, а также проанализированы основные угрозы для баз данных. В работе упоминается о политики безопасности, которая определяет какие виды информации не должны быть общедоступными. В статье проведен анализ моделей безопасности баз данных, которые формулируют политику безопасности.

Ключевые слова: *база данны, политика безопасности, модель безопасности, доступность, целостность, дискриционная модель, мандатная модель.*

Введение

Актуальность. Термин «база данных» (БД) очень популярен сегодня. Информация, которая хранится в базах данных часто рассматривается в качестве ценного и важного корпоративного ресурса. Многие организации стали настолько зависимы от надлежащего функционирования их систем, что нарушение службы или утечки хранимой информации может вызвать непредвиденные последствия. Корпоративные данные могут относиться к финансовым отчетам, другие могут иметь важное значение для успешного функционирования организации, могут представлять коммерческую тайну, или может описать информацию о лицах, чья частная жизнь должна быть защищена. Таким образом, общая концепция безопасности баз данных является весьма обширной и влечет за собой морально-этические проблемы государства и общества, юридические вопросы управления законодательством над сбором и разглашением хранимой информации, или более технические аспекты, например, как защитить сохраненную информацию от потери или несанкционированного доступа, уничтожения, использования, модификации или разглашения.

Анализ литературы [1-10] показал, что безопасность БД не может рассматриваться как изолированная проблема, поскольку она осуществляется также другими компонентами компьютерной системы. Потребность в безопасности системы определяются с помощью политики безопасности, которая затем обеспечивается различными механизмами безопасности.

Целью данной статьи является анализ угроз и моделей безопасности баз данных.

Основная часть

Безопасность баз данных. Безопасность баз данных является весьма широкой областью, которая решает многие проблемы, в том числе следующие:

– Правовые и этические проблемы, касающиеся права на доступ к определенной информации. Некоторые данные могут считаться приватными и не могут быть доступными на законном основании посторонними лицами. В Соединенных Штатах, существуют многочисленные законы, регулирующие конфиденциальность информации:

– вопросы политики безопасности как на государственном, институциональном, так и на корпоративном уровне, определяют какие виды информации не должны быть общедоступными, например, кредитные рейтинги и личные медицинские записи;

– проблемы, относящиеся к системе, такие как уровни системы, при которой различные функции обеспечения безопасности должны быть приведены в исполнение, например, должна ли функция безопасности обрабатываться на физическом или аппаратном уровне обеспечения, на операционном системном уровне или DBMSlevel;

– необходимость в некоторой организации выявления многоуровневой безопасности, а также для категоризации данных и пользователей на основе этих классификаций, например, совершенно секретно, секретно, конфиденциально и несекретные. Политика безопасности организации в отношении обеспечения доступа к различным классификациям данных должно быть приведена в исполнение. [1]

Угрозы безопасности баз данных. Угрозы для баз данных в результате потери или деградации некоторых или всех из следующих целей безопасности: целостность, доступность и конфиденциальность.

– потеря целостности: целостность базы данных означает требование о том, что информация будет защищена от неправильной модификации. Модификация данных включает в себя создание, вставку, изменение, изменение состояния данных и удаление. Целостность теряется, если данные несанкционированно изменены. Если установленная потеря системы или целостность данных не будет исправлена, то дальнейшее использование зараженной системы или искаженных данных может привести к неточности, мошенничеству или неправильным решениям;

– потеря доступности: доступность базы данных относится к созданию объектов, доступных для

пользователя или программы, на которые они имеют законное право;

– потеря конфиденциальности: конфиденциальность базы данных относится к защите данных от несанкционированного раскрытия. Последствием несанкционированного раскрытия конфиденциальной информации может варьироваться от нарушения закона о конфиденциальности данных до обеспечения национальной безопасности. Несанкционированные, непредвиденные или непреднамеренное разглашение могут привести к потери доверия населения, смущение, или судебный иск против организации [10].

Цель политики безопасности баз данных. Политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. На практике политика безопасности трактуется несколько шире – как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса.

После того как политика безопасности определена, должен решаться вопрос о технологии ее реализации в автоматизированном контуре. Для реализации сформулированных в терминах естественного языка правил и норм политики безопасности необходимо использовать (или разработать) некоторую формальную модель, которая допускает эффективное программирование на каком-либо формальном языке [9].

Целью формализации политики безопасности для информационной системы является четкое изложение взглядов руководства организации на существо угроз информационной безопасности, организации и технологий обеспечения безопасности ее информационных ресурсов. Политика безопасности обычно состоит из двух частей: общих принципов и конкретных правил работы с информационными ресурсами и, в частности, с базами данных для различных категорий пользователей [7].

Наличие политики безопасности поможет управлять бизнес-процессами, очертит объекты, нуждающиеся в защите, и заложит прочную основу для реализации компенсирующих элементов контроля. Успех программы по ведению журнала безопасности и мониторингу базы данных зависит от целей и имеющихся нормативов. Во-первых, понимание задач бизнеса, законов, правил и ресурсов, необходимых для защиты компании поможет разработать эффективную политику безопасности, а также базовые бизнес-процессы на основе все этой информации. Как упоминалось ранее, эта предварительная работа имеет критически важное значение, но часто упускается многими компаниями. Однако закладка фундамента не гарантирует успешности всей кампании, а только подготовит организацию к работе по построению успешной программы. [9]

Модели безопасности БД. Из-за разнообразия доменых приложений для баз данных, различных моделей и методов защиты, были предложены модели безопасности для борьбы с различными угрозами.

Модель безопасности это формальное выражение и формулирование политики безопасности.

Модель безопасности включает в себя:

– модель информационной системы;

– принципы, критерии, целевые функции и ограничения защищенности данных от угроз;

– ограничения, алгоритмы, формализованные правила, механизмы и схемы безапосного функционирования системы. [8]

Большинство моделей безопасности основывается на субъектно-объектной модели компьютерных систем, в том числе и баз данных.

Простейшая одноуровневая модель безопасности на основе дискреционного принципа разграничения доступа безопасности являются фундаментальными для операционных систем и СУБД (систем упраления базами данных). Однако, появление более продвинутых моделей данных не имеет повышенный интерес к дискреционной политики. [4]

Дискреционная политика безопасности. Дискреционная политика безопасности - политика осуществляемая на основании заданного администратором множества разрешенных отношений доступа. Дискреционное управление доступом определяется двумя свойствами:

– все субъекты и объекты должны быть идентифицированы;

– права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила.

Дискреционная безопасность обеспечивается в большинстве коммерческих СУБД и базируется на концепции представлений базы данных. Вместо того, чтобы разрешать пользователю базовые отношений с системой информационной матрицы контроля доступа, которая предназначена для ограничения доступа пользователя к определенному подмножеству данных [2, 4].

Мандатная модель безопасности. Мандатная политика безопасности – политика, основанная на совокупности предоставления определенного доступа, на множестве атрибутов безопасности субъекта и объекта. Мандатная политика решает более высокий уровень угрозы, чем дискреционная политика, потому что в дополнение к управлению доступом к данным, они могут также управляют потоком данных. Кроме того, мандатные методы защиты преодолеть структурные ограничения защиты основанные на DAC [2, 4]. Основу мандатной политики безопасности составляет мандатное управление доступом (Mandatory Access Control – MAC).

В то время как дискреционная модели связаны с определением, моделированием, а также обеспечением доступа к информации мандатных моделей безопасности в дополнение к имеющим отношение к потокам информации в системе. Мандатная безопасность требует, чтобы объекты безопасности и субъекты назначаются определенные уровни безопасности, представленных меткой. Меткой для объекта О называется его классификация (class(o)), а метка для субъекта s называется ее разрешением (clear(s)). Классификация отображает чувствительность к меченым данным. Метка защиты состоит из двух компонентов: уровня иерархии секретности или доступа классов и представителя не иерархических категорий. Уровни разрешения и классификация полностью упорядочены в то время как метка безопасности только частично упорядочеа - таким образом, множество классификаций образует решетку [3, 4].

Адаптирование модели мандатного контроля доступа, для большего приспособления к основной цели обработки данных и предлажения конструкции для разработки баз данных, содержащих конфиденциальную информацию, является главной целью адаптированной модели мандатного контроля доступа (AMAC). Для того, чтобы преодолеть ограничения MAC, AMAC предлагает несколько функций, которые помогают проектировщику базы данных при выполнении различных видов деятельности, участвующих в разработке базы, содержащей конфиденциальную информацию. Для AMAC в методике безопасности баз данных существуют следующие преимущества:

– Методика поддерживает все этапы проектирования базы данных и может быть использована для построения защиты дискреционной, а также для построения мандатных защищенных баз данных.

– в случае мандатной защиты требуется вспомогательная политика для выведения фрагментов базы данных обеспечивается целевой защитой;

– в случае мандатной защиты требуется автоматизированной защита маркировки для объектов безопасности и поддерживается субъектами;

– в AMAC безопасность обеспечивается с помощью триггеров базы данных и, при этом, они могут быть доработаны для соответствия требованиям безопасности зависимых приложений. [4, 6]

Модель Кларка и Уилсона. Эта модель была впервые резюмирована и была сравнена с MAC Кларком и Уилсоном в 1987 году. Авторы утверждают, что их модель основана на концепции, которая уже хорошо зарекомендовала себя. Это представление о субъектах и объектах безопасности, набор хорошо сформированных операций и принципов разделения обязанностей. Если перевести эти принципы в мир баз данных и безопасности, то они интерпретируются следующим образом: пользователи системы имеют ограничения только на выполнение определенного набора операций, допустимых им и каждая транзакция работает только на заданном множестве объектов данных. Точнее, подход Кларка и Уилсон интерпретируется следующим образом:

1. Субъектам безопасности назначаются роли. На основе их ролей в организации пользователи выполняют определенные функции. Каждая бизнес-роль отображается в функции базы данных, и в идеале в определенный момент времени конкретный пользователь играет только одну роль. Функция базы данных соответствует набору (wellformed) операций, которые необходимы для пользователей, действующих в роли. В рамках этой модели необходимо указать соответсвие пользователям их ролей и, в какое время, для какой роли, какие транзакции необходимо выполнять. Для того, чтобы контролировать несанкционированное раскрытие и модификация данных Кларк и Уилсон предлагают доступ, который будет разрешен только посредством выполнения определенных программ, wellformed сделок, и что права пользователей на выполнение такого кода будет ограничено в зависимости от роли каждого пользователя.

2. Правильное построение транзакции. Правильно составленная транзакция работает на заданном множестве данных и гарантирует, что все соответствующие свойства безопасности и целостности удовлетворены. Кроме того, она обеспечивает журналирование и атомарность, а также упорядоченность результатов частных операций, таким образом, что параллелизм и механизмов восстановления могут быть установлены. Важно отметить, что в этой модели элементы данных, на которые ссылаются транзакций не задаются пользователями действующей транзакции. Вместо того, элементы данных назначаются в зависимости от той роли, в которой пользователь действует. Таким образом, модель не позволяет специальные запросы к базе данных.

3. Разделение обязанностей. Этот принцип требует, чтобы каждой группе пользователей назначался определенный набор функций в зависимости от роли пользователя в организации. Единственный способ получить доступ к данным в базе данных с помощью заданного набора - это хорошо сформированная транзакция, характерная для роли каждого из пользователей. В тех случаях, когда пользователь запрашивает дополнительную информацию, другой пользователь (который находится на более высоком уровне), действующий в отдельной роли должен использовать wellformed транзакции, который действует из домена транзакций роли, чтобы предоставить временное разрешение пользователю выполнить большой набор корректно сформированных операций. Кроме того, роли должны быть определены таким образом, чтобы не было возможным для одного пользователя нарушить целостность системы. Например, проектирование, внедрение и поддержание корретно сформированных транзакций, должны быть отнесены к другой роли, чем исполнение этих же транзакций. [4, 5]

Выводы

Таким образом, безопасность баз данных не является отдельной проблемой - в самом широком смысле это общая системна проблема. Безопасность баз данных зависит не только от выбора конкретной продукта СУБД или от поддержки определенной модели безопасности, но и от операционной среды, а также вовлеченных людей. Дальнейшие вопросы безопасности базы данных включают в себя требования к операционной системе, сетевой безопасности, дополнительные пакеты безопасности, шифрование данных, безопасность статистических баз данных, аппаратных средств защиты, верификации программного обеспечения и др.

При выборе подхода к обеспечению безопасности дискреционный может быть первым выбором, если высокая степень безопасности не требуется. Сохраняя ответственность за соблюдение безопасности на стороне пользователей, если потенциальные угрозы безопасности не приведет к значительному ущербу.

Мандатные политики являются более эффективными, поскольку они предполагают, что пользователи не имеют контроль над созданием и изменением параметров безопасности. Политика безопасности подходит для конкретного приложения также могут иметь как обязательный и дискреционный компонент. Кроме того, реальные системы часто предлагают утечки на строгих обязательного контроля, например, для привилегированных пользователей, таких как системные администраторы и сотрудников службы безопасности. Такие точки входа часто представляют собой серьезный источник уязвимости. Многоуровневые приложения могут стать очень сложными.

Хотя очень эффективные мандатные политики могут применяться только в средах, где доступна метка информации. Это считается одним из самых сильных пунктов в пользу модели безопасности AMAC. AMAC предлагает среду разработки для баз данных с основным акцентом на безопасность. Она включает в себя дискреционное, а также мандатное управление

Модель Кларка и Уилсона получила широкое внимание в последние годы. Многое из защиты соответствующих действий сгенерировано для прикладных программ и моделей не поддерживают специальные запросы к базе данных. В частности авторы ссылаются на потенциальные угрозы безопасности системы таких, как распространение данных, несанкционированные действия и злоупотребление привилегиями со стороны авторизированных пользователей.

Список литературы

1. Elmasri, Ramez. Fundamentals of database systems / Ramez Elmasri, Shamkant B. Navathe.--4th ed. – Pearson. Additson Wesley, 2003. – 1029p. – ISBN 0-321-12226-7.

2. Fernandez, E., Summers, R., and Wood, C. [1981] Database Security and Integrity, Addison-Wesley, 1981.

3. Günther Pernul. Database Security. - Vienna, Austria, 1994. – 75 p.

4. Meg Coffin Murray. Database Security: What Students Need to Know/ Meg Coffin Murray. Journal of Information Technology Education: Innovations in Practice, 9, 2010 – P. 61-77

5. Защищеныые системы – общие принципы [Электронный ресурс]. Режим доступа : http://crypto.pp.ua/2010/06/319/

6. Информационная безопасность в современных системах управления базами данных [Электронный ресурс]. Режим доступа : http://compress.ru/article.aspx?id=10099

7. Общие сведения о параметрах политики безопасности [Электронный ресурс]. Режим доступа - https://technet.microsoft.com/ru-ru/library/hh831424(v=ws.11).aspx

8. Понятие и модели безопасности данных [Электронный ресурс]. Режим доступа : http://www.razgovorodele.ru/moresec/materials13/automated_control_systems_7/adm_systems04.php

9. Разработка политики безопасности [Электронный ресурс]. Режим доступа - http://sernam.ru/ss_31.php

10. Угрозы безопасности информации. Угрозы конфиденциальности, целостности доступности АС. Понятие политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности. [Электронный ресурс]. Режим доступа – http://ofsky0.narod.ru/17.htm.

Надійшла до редколегії 3.02.2017

Рецензент: д-р техн. наук, проф. А.В. Горбенко, Національний аерокосмічний університет імені М.Є. Жуковського «ХАІ», Харків.

АНАЛІЗ ПОЛІТИКИ ТА МОДЕЛЕЙ БЕЗПЕКИ БАЗ ДАННИХ

Д.Д. Левченко

Головною ідеєю даної статті є захист даних від несанкціонованого доступу. У роботі були розглянені роблеми безпеки, а також проаналізовані загрози для баз даних. У роботі згадується про політику безпеки, яка визначає які види інформації не повинні бути загальнодоступними. У статті проведено аналіз моделей безпеки баз данних, які формулюють політику безпеки.

Ключові слова: *база даних, політика безпеки, модель безпеки, доступність, цілісність, дискриціонна модель, мандатна модель.*

ANALYSIS OF SECURITY POLICIES AND MODELS DATABASE SECURITY

D.D. Levchenko

The main idea of the article is to protect data from unauthorized access. In this work we were considered security concerns, and the analysis of the main threats to the database. The paper refers to the security policy, which defines the type of information that should not be publicly available. The article analyzes the database security model data to formulate a security policy.

Keywords: *data base, security policy, security model, availability, integrity, discretionally model credentials model.*

УДК 004.056

И.В. Лысенко, Ю.В. Трегуб

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ВОЗМОЖНОСТЕЙ ПРОГРАММНЫХ ПЛАТФОРМ И ЯЗЫКОВ ПРОГРАММИРОВАНИЯ С ТОЧКИ ЗРЕНИЯ РЕАЛИЗАЦИИ КРИПТОАЛГОРИТМОВ

Проанализированы одни из наиболее популярных программных платформ и языков программирования в отношении возможностей реализации криптографических алгоритмов обеспечения конфиденциальности (симметричные и несимметричные алгоритмы шифрования), целостности и аутентичности данных (ключевые и бесключевые хеш-функции и алгоритмы цифровой подписи), а также протоколов формирования сеансовых ключей пользователей. Результаты сравнительного анализа могут служить основой для принятия решения пользователю в отношении создания собственной подсистемы криптозащиты данных.

Ключевые слова: *криптоалгоритмы, программные платформы, языки программирования.*

Введение

Постановка задачи. С увеличением объёма циркулирующей в открытых сетях информации, а также информации, хранящейся на жёстком диске пользователя, возрастает актуальность задачи её защиты.

Часто данная задача решается преимущественно за счёт применения программно-реализованных криптографических алгоритмов, позволяющих обеспечить такие свойства защищаемых данных, как конфиденциальность, целостность и аутентичность. К числу других важных задач, решаемых криптографическими алгоритмами, относится задача формирования сеансовых ключей удалённых пользователей.

Существующие программные платформы и языки программирования позволяют пользователю реализовать подсистему криптозащиты данных на основе встроенных библиотек криптоалгоритмов (криптопримитивов). Так, в [1, 2] приводятся данные об используемых в одних из наиболее популярных платформ (MS .Net Framework и Java) алгоритмов шифрования.

Что же касается языков программирования, то в данной работе рассматриваются, PHP, Python, C++, Delphi. При этом, хотя Delphi никак нельзя относить к числу наиболее популярных языков, он выбран для сравнительного анализа с точки зрения широты рассмотрения вопроса.

В [7, 8] содержится перечень криптоалгоритмов, используемых в некоторых из вышеперечисленных языков программирования.

Целью работы является анализ упомянутых программных платформ и языков программирования с точки зрения возможности реализации криптопримитивов.

1. Возможности программных платформ

Возможности программных платформ по реализации криптопримитивов представлены в табл. 1 [3, 4].

Таблица 1

Возможности платформ .Net Framework и Java

Криптопримитивы	Программная платформа	
	.Net Framework	Java
Симметричное шифрование	AES, DES, 3DES, RC2, RC4	AES, DES, DESede, RC2, RC5, RC4, IDEA, Blowfish
Несимметричное шифрование	RSA	RSA, El-Gamal
Цифровая подпись	RSA, DSA, ECDSA	RSA, DSA, ECDSA
Бесключевые хеш-функции	MD5, SHA-1, SHA256, SHA384, SHA512	MD2, MD5, SHA-1, SHA-256 SHA-384 SHA-512
Ключевые хеш-функции	MACTrileDES, HMAC	HMAC-SHA1

Как видно из табл. 1, наибольшим набором криптопримитивов среди программных платформ обладает Java. В частности, что касается симметричных алгоритмов шифрования, в Java, помимо алгоритмов, реализованных в .Net Framework, присутствуют блочные криптоалгоритмы RC5 и Blowfish, а также потоковые алгоритмы RC4 и Arcfour (в .Net Framework потоковые алгоритмы отсутствуют). Кроме того, в Java имеется возможность реализации несимметричного алгоритма шифрования Эль-Гамаля (кроме RSA), в то время как в .Net Frame-

work несимметричное шифрование представлено только алгоритмом RSA. Помимо этого Java позволяет реализовать гибридную схему шифрования на основе эллиптических кривых ECIES. Криптопримитивы цифровой подписи в платформах .Net Framework и Java представлены одним и тем же набором алгоритмов.

Что касается бесключевых хеш-функций, то их набор в программной платформе Java является практически идентичным набору в .Net Framework, за исключением того, что в Java реализована хеш-функция MD2 (не используется, как криптопримитив). В отношении ключевых хеш-функций платформа .Net Framework обладает такими алгоритмами хеширования, как MACTripleDES и HMAC, в то время как в Java используется лишь криптопримитив HMAC-SHA1.

Также следует отметить, что рассматриваемые платформы позволяют реализовать протокол Диффи-Хеллмана формирования общего секретного ключа пользователей на основе эллиптических кривых (ECDiffieHellman).

2. Возможности языков программирования

Возможности языков программирования по реализации криптопримитивов представлены в табл. 2.

Как видно из табл. 2, наибольшим набором криптопримитивов среди рассмотренных языков программирования обладает язык C++.

В отличие от других языков программирования, несимметричное шифрование в нём представлено не только алгоритмом RSA, но и алгоритмом шифрования Эль-Гамаля. Возможность реализации данного алгоритма присутствует и в платформе Java. Особенностью языка C++ с точки зрения симметричного блочного шифрования является то, что в нём, помимо множества алгоритмов семейства RC (автор – всемирно известный криптолог Рональд Райвест), представлены оба алгоритма ещё одного всемирно известного криптолога Брюса Шнайера Blowfish и Twofish. В то же время, в C++ отсутствует реализация симметричного поточного шифрования, представленного в языках Delphi и PHP алгоритмом RC4.

Также в языках C++ и Python, в отличие от других языков, имеется реализация гибридной схемы шифрования ECIES, использующей математический аппарат эллиптических кривых.

Если говорить о цифровой подписи, то набор криптопримитивов в языке программирования C++ идентичен языку Delphi, и содержит, помимо реализованных в других языках (за исключением PHP) алгоритмов RSA и DSA, алгоритм на эллиптических кривых ECDSA.

Таблица 2

Возможности языков программирования

Криптопримитивы	Языки программирования			
	Delphi	PHP	C++	Python
Симметричное шифрование	AES, DES, 3DES, IDEA, RC2, RC4, RC5, RC6, XOR	AES, DES, Blow-fish, RC4	AES DES, 3DES, IDEA, RC2, RC5, RC6, Blowfish, Twofish	AES, DES, 3DES, XOR
Несимметричное шифрование	RSA	RSA	RSA, ElGamal, ECIES	RSA ECIES
Цифровая подпись	RSA, DSA, ECDSA	RSA	RSA, DSA, ECDSA	RSA, DSA
Бесключевые хеш-функции	MD4, MD5, SHA-1, SHA256 SHA384 SHA512	MD5 SHA-1 SHA-256	MD2, MD4, MD5, SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 SHA-3	MD2, MD4, MD5, SHA-1, SHA-256, SHA-384, SHA-512
Ключевые хеш-функции	HMAC-SHA-1, HMAC-SHA256	HMAC-MD5	HMAC	HMAC

Что касается бесключевых хеш-функций, то во всех рассмотренных языках, помимо практически вышедших из употребления алгоритмов семейства MD и SHA-1, реализовано семейство хеш-функций SHA-2 с длиной дайджеста 224, 256, 384 и 512 битов. Однако в языке программирования C++ также поддерживается и бесключевая хеш-функция SHA-3. Ключевые хеш-функции во всех рассматриваемых языках представлены схемой HMAC на основе разных бесключевых хеш-функций.

В целом же, что касается языков программирования, важно заметить тот факт, что реализация протокола Диффи-Хеллмана формирования общего секретного ключа пользователей на основе эллиптических кривых (ECDiffieHellman), присутствует не только в языке программирования C++, но и в практически вышедшем из употребления языке Delphi, который, как можно видеть, почти не уступает C++

с точки зрения разнообразия реализованных криптопримитивов.

Следует отметить, что возможность реализации протокола Диффи-Хеллмана присутствует и в платформах .Net Framework и Java.

Заключение

Результаты проведенного анализа позволяют пользователю, желающему реализовать собственную подсистему криптозащиты данных, иметь представление о возможностях программных платформ и языков программирования с точки зрения реализации базовых криптопримитивов и осуществлять выбор программной системы на основе собственных предпочтений и навыков программирования. В частности, что касается производительности криптоалгоритмов реализованных в .Net Framework, результаты соответствующих исследований, опубликованы в [7, 8].

Список литературы

1. Java Cryptography Architectur Standard Algorithm Name Documentation for JDK 8 [Электронный ресурс] / Oracle.com – Режим доступа: https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html .

2. Msdn.microsoft.com, .NET Framework Cryptography Model [Электронный ресурс] / Msdn.microsoft.com – Режим доступа : https://msdn.microsoft.com/enus/library/0ss79b2x(v=vs.110).aspx.

3. Wikipedia.org . Crypto++ [Электронный ресурс] / Wikipedia.org – Режим доступа: https://en.wikipedia.org/wiki/Crypto%2B%2B .

4. Efg2.com, Cryptography and Multiple-Precision Arithmetic [Электронный ресурс] / Efg2.com – Режим доступа: http://www.efg2.com/Lab/Library/Delphi / MathFunctions/Cryptography.htm.

5. Авдошин, С.М. Криптотехнологии Microsoft / С.М. Авдошин, А.А. Савельева // Приложение к журналу «Информационные технологии» – 2008. – №9. – С. 23–30.

6. Смарт, Н. Криптография: пер. с англ. / Н. Смарт – М.: Техносфера, 2005. – 528 с.

7. Лысенко, И.В. Исследование быстродействия алгоритмов шифрования на базе технологии .Net Framework / И.В Лысенко, А.Г.Проценко, // Системи обробки інформації / ХУПС. – Х., 2011. – Вип. 4(94). – С. 176-181.

8. Проценко, А.Г. Исследование быстродействия алгоритмов обеспечения целостности на базе технологии .Net Framework / А.Г.Проценко // Системи обробки інформації: ХУПС. – Х.в, 2011. – Вип. 8(52). – С. 228-232.

References

1. "Java Cryptography Architecture Standard Algorithm Name Documentation for JDK 8", available at: https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html .

2. ".NET Framework Cryptography Model, available at: https://msdn.microsoft.com/enus/library/0ss79b2x (v=vs.110).aspx .

3. "Crypto++", available at: https://en.wikipedia.org/wiki/Crypto%2B%2B .

4. "Cryptography and Multiple-Precision Arithmetic", available at: http://www.efg2.com/Lab/Library/ Delphi/MathFunctions/Cryptography.htm.

5. Avdoshin, S.M., Savel'eva, A.A. (2008), "Microsoft Cryptotechnologies" [Kriptotehnologii Microsoft], Prilozhenie k zhurnalu «Informacionnye tehnologii», no.9, pp. 23–30.

6. Smart, N. (2005), Cryptography, Trans. from Russ. ed.: [Kriptografija, Per. s Russ. ed], Tehnosfera Publ. 528 p.

7. Lysenko, I.V., Procenko, A.G.(2011), "Speed encryption algorithm study based on .Net Framework technology", Information processing systems ["Issledovanie bystrodejstvija algoritmov shifrovanija na baze tehnologii .Net Framework", Sistemi obrobki informacii], HUPS, Kharkiv, Vol. 4(94). pp. 176-181.

8. Procenko, A.G., (2011), "Research performance integrity algorithms based on the .Net Framework technology", Information processing systems ["Issledovanie bystrodejstvija algoritmov obespechenija celostnosti na baze tehno-logii .Net Framework", Sistemi obrobki informacii], HUPS, Kharkiv, Vol. 8(52). pp. 228-232.

Надійшла до редколегії 3.02.2017

Рецензент: д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА МОЖЛИВОСТЕЙ ПРОГРАМНИХ ПЛАТФОРМ І МОВ ПРОГРАМУВАННЯ З ТОЧКИ ЗОРУ РЕАЛІЗАЦІЇ КРИПТОАЛГОРИТМІВ

І.В. Лисенко, Ю.В. Трегуб

Проаналізовано деякі найбільш популярні програмні платформи і мови програмування щодо можливостей реалізації криптографічних алгоритмів забезпечення конфіденційності (симетричні і несиметричні алгоритми шифрування), цілісності й автентичності даних (ключові і бесключові хеш-функції та алгоритми цифрового підпису), а також протоколів формування сеансових ключів користувачів. Результати порівняльного аналізу можуть бути основою для прийняття рішення користувачеві з питання створення власної підсистеми криптографічного захисту даних.

Ключові слова: *криптоалгоритми, програмні платформи, мови програмування.*

COMPARATIVE CHARACTERISTICS OF OPPORTUNITIES SOFTWARE PLATFORMS AND PROGRAMMING LANGUAGES IN TERM OF IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS

I.V. Lysenko, J.V. Tregub

Some of the most popular software platform and programming language were analyzed regarding the feasibility of cryptographic algorithms ensure confidentiality (symmetric encryption and asymmetric encryption algorithms), the integrity and authenticity of data (key hash, keyless hash function, and digital signature algorithms), and protocols form of session keys of users. Results of comparative analysis can serve as the basis for a user who makes a decision regarding the establishment of its own data encryption subsystem.

Keywords: *cryptographic algorithms, software platforms, programming languages .*

УДК 621.391.037

С.С. Мешечко, В.Я. Певнев, В.А. Погорелов

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ CMS WORDPRESS

WordPress — идеальная платформа для публикации, ориентированная на красоту, поддержку стандартов и удобство использования. На сегодняшний день Wordpress как никогда популярен. Блоги, минисайты, а то и целые порталы — всё это строится на основе такого удобного движка-конструктора как Wordpress. Но за удобностью и лёгкостью освоения кроются, прежде всего, вопросы, связанные с безопасностью вашего сайта. Большая распространённость — большее внимание злоумышленников. В статье проведен анализ методов и способов защиты CMS WordPress. Описаны детальные действия по повышению устойчивости системы к DDos-атакам. Расписаны основные ошибки при администрировании сайта.

Ключевые слова: *безопасность, защита, надежность, администрирование, пароли, поддержка.*

Введение

Развитие инфокоммуникационных технологий позволяет резко увеличить скорость обмена информации и ее передаваемый объем. Это приводит к необходимости увеличения затрат на обеспечение информационной безопасности создаваемых сайтов и разнообразных веб-приложений. Обеспечение кибербезопасности, как составляющей информационной безопасности, достаточно сложная задача, включающая в себя решение вопросов конфиденциальности, целостности, доступности. Основную угрозу несет в себе возможность несанкционированного доступа к информации с целью ее модификации или уничтожения. Такой доступ позволяет производить действия с исполнительными устройства вне зависимости от показания соответствующих датчиков, разрушение программного кода и т.п.

Хакерские атаки на всевозможные веб-приложения стали обыденными вещами, но реальных методов защиты не существует. Обеспечение безопасности является одной из основных задач разработчиков и требует не стандартных решений. Одним из таких решений было предложено в системе создания и управления сайтами WordPress. Идея такого решения заключается в том, что при установке нового блога система создает аккаунт администратора с уникальным случайно сгенерированным в реальном времени паролем. То позволяет блокировать всеобщий доступ к настройкам системы, контролируя его с помощью страницы авторизации.

В предлагаемой статье рассмотрены на вопросы усиления безопасности WordPress — как административной панели, так и настроек блога, подразумевая все содержимое папки «wp-admin», которое отображается только после авторизации. Авторами сознательно выделена фраза "после авторизации" — это подчеркивает то, что только пароль отделяет хакера и администратора всего вашего блога или сайта! А защита пароля определяется его размером и символами, которые используются при его наборе.

Целью статьи является анализ существующих методов защиты системы создания и управления сайтами WordPress.

Результаты анализа

1. Переименуйте папку wordpress. Начиная с версии 2.6, стало возможным изменять путь к папке wp-content. К сожалению это до сих пор неприменимо к папке wp-admin. Думающие о безопасности блоггеры смирились с этим и стали надеяться, что это станет возможным в будущих версиях. Пока этого не случилось, возможно следующее альтернативное решение проблемы. После распаковки архива с файлами WordPress, создается папка «WordPress». Необходимо переименовать папку (в идеале во что-то непонятное вроде "*wordpress_live_Ts6K"*) и после этого настроить соответственным образом файл wp-config.php, который находится в корневой директории [1]. Что дает это изменение?

- все файлы WordPress не будут смешаны с другими файлами в корне сайта, таким образом повысится ясность корневого уровня;
- множество копий WordPress может быть установлено параллельно в папке с разными именами, исключая их взаимодействие, что делает это идеальным для тестирования;
- административная зона (и весь блог в целом) больше не находится в корневой папке и для проведения каких-либо действий по взлому сначала ее нужно будет найти. Это проблемно для людей, но что касается ботов – вопрос времени.

Примечание: Если системные файлы WordPress больше не находятся в корневой директории, и имя папки инсталяции изменено в соответствии с рекомендациями, описанными выше, блог будет все равно доступен по адресу wp-config.ru. Зайдите в раздел «Общие настройки (General settings)» вашего блога и введите в поле «WordPress address (URL)» реальный адрес блога на сервере.

2. Усовершенствуйте файл wp-config.php. Конфигурационный файл WordPress wp-config.php

содержит в себе некоторые настройки сайта и информацию для доступа к базе данных. Также там другие настройки, касающиеся безопасности (они представлены в списке ниже). Если таких значений в этом файле нет, или же имеются только установленные по умолчанию, вам необходимо, соответственно, добавить или изменить их: ɾлючи безопасности**:** начиная с версии 2.7, в WordPress есть четыре ключа безопасности, которые должны быть правильно установлены. WordPress спасает вас от необходимости выдумывать эти строки самому, автоматически генерируя правильные ключи с точки зрения безопасности. Вам просто нужно вставить ключи в соответствующие строки файла wp-config.php. Эти ключи являются обязательными для обеспечения безопасности вашего блога [1]. Префикс таблицы заново установленного WordPress блога не должен быть стандартным **«wp_».** Чем больее сложным будет значение префикса, тем менее вероятна возможность несанкционированного доступа к таблицам вашей MySQL базы данных. Плохо**:** *$table_prefix = 'wp_';*. Намного лучше: *$table_prefix = 'wp4FZ52Y_'***.** Если у вас на сервере доступно **SSL** шифрование, рекомендуется включить его для защиты административной зоны. Это можно сделать, добавив следующую команду в файл wp-config. php: *define('FORCE_SSL_ADMIN', true);*

3. Переместите файл wp-config.php. Также начиная с версии 2.6, WordPress позволяет перемещать файл wp-config.php на высший уровень. По причине того, что этот файл содержит в себе намного более важную информацию, чем какой либо другой, и потому что всегда намного сложнее получить доступ к корневой папке сервера, имеет смысл хранить его не в той же директории, где и остальные файлы. WortdPress автоматически обратится к высшей папке в поиске файла wp-config.php. Любые попытки пользователей самим настроить путь бесполезны.

4. Защитите файл wp-config.php. Не все ISP серверы позволят вам передавать данные на более высокие уровни, чем корневая директория. Другими словами, не у всех хватит прав для осуществления предыдущего шага. Или по другим причинам: например, если у вас несколько блогов, при определенной структуре папок у вас не получится положить в корень все файлы, так как их имена будут совпадать для каждого из блогов. В этом случае мы можем запретить доступ к файлу wp-config.php извне при помощи файла .htaccess [2].

Очень важно убедиться, что файл .htaccess находится в той же директории что и файл wp-config.php. процесс, драйвера, которые он запрашивает, влияние на другие процессы и прочие параметры, которые каждый HIPS реализует по-своему.

5. Удалите учетную запись администратора. Во время процесса установки WordPress создает учетную запись администратора с ником «admin» по умолчанию. С одной стороны это вполне логично, с другой — пользователь с известным ником, т.е. ID — 1, обладающий административными правами, является вполне предсказуемой мишенью для хакеров с их программами подбора паролей. Отсюда следует совет: Создайте еще одного пользователя с административными правами и вашим ником. Завершите сеанс работы. Залогиньтесь под новым аккаунтом. Удалите учетную запись "admin".

Если у вас не новый блог и под учетной записью admin вы уже публиковали посты или комментарии, то из предложенных вариантов в момент удаления, выберите пункт «Связать все записи и ссылки с:» и выберите имя нового пользователя: В идеале желательно чтобы логин нового пользователя отличался от отображаемого имени пользователя в постах, чтобы никто не узнал ваш логин.

6. Выберите сильный пароль. Вероятность и частота потенциальных атак прямо зависит от популярности блога. И желательно до этого момента быть уверенным, что в вашем сайте не осталось слабых звеньев в цепи безопасности.

Чаще всего именно пароли являются самым слабым звеном в этой цепи. Почему? Способы выбора пароля у большинства пользователей зачастую необдуманны и беспечны. Многие проведенные исследования показали, что большинство паролей — односложные существующие слова, набранные строчными буквами, которые не сложно подобрать. В программах подбора паролей существуют даже списки самых часто используемых паролей. В WordPress реализован интуитивно понятный индикатор стойкости набираемого пароля, который показывает цветом его уровень сложности[3]. Мы рекомендуем использовать как минимум семь символов, комбинировать строчные и прописные и использовать служебные символы, такие как! "? $ % ^ & ( ).

7. Защитите папку «wp-admin». Следуя пословице «две головы лучше одной», существует способ вдвое усилить защиту административной зоны. Защита регулируется файлом **.**htaccess**,** который должен находится в папке «wp-admin» вместе с файлом .htpasswd, который хранит логин и пароль пользователя. После обращения к папке, вам нужно будет ввести логин и пароль, но разница в том, что в этом случае авторизация контролируется на стороне сервера, а не силами самого WordPress.

8. Запретите отображение ошибок на странице авторизации. Страница авторизации WordPress — это дверь в административную зону вашего блога, которая становится доступна после безошибочного прохождения верификации. У каждого пользователя существует бесконечное количество попыток авторизации, и каждый раз по умолчанию услужливый WordPress указывает, в чем именно была ошибка. То есть, если введенный логин окажется неверным — WordPress так и скажет. Это удобно для пользователя, но также и для хакера[3]. Несложно догадаться, как быстро сокращается вероятность подбора комбинации логина/пароля, когда система указывает что именно введено неверно. Простая строка кода,

поможет решить эту проблему, достаточно добавить её в файл functions.php вашей темы:

9. Поддерживайте актуальные версии. Как правило разработчики WordPress очень быстро реагируют, если находят уязвимости в движке. Поэтому следите за обновлениями и обновляйтесь, когда возможно. Благо сам WordPress оповещает о выходе новой версии. Это касается и плагинов — держите их версии актуальными. Запомните: меньше значит лучше, когда это касается любых надстроек и аддонов. Как администратор, вы должны удостовериться, что у вас установлены и активны, только те плагины, которые действительно вам нужны. Каждый плагин — это потенциальный риск и угроза безопасности, так как все они разрабатываются посторонними разработчиками.

10. Ограничьте количество неудачных попыток авторизации. WordPress не ведет статистику авторизаций, как удачных, так и нет. Это очень неудобно для администратора, так как у него нет возможности увидеть были ли попытки несанкционированного доступа, чтобы принять какие-либо меры, если они участятся. Предлагаем два решения [3]: плагины Login LockDown и Limit Login Attempts. После установки они не только ведут лог авторизаций, но также ограничивают количество неудавшихся попыток авторизации, блокируя на определенное время IP пытающегося.

11. Защищаем Wordpress от XSS-инъекций. Программисты всегда стараются защитить GET- и POST- запросы, однако, иногда этого недостаточно. Необходимо защитить блог от XSS-инъекций и попыток модификации переменных GLOBALS и _REQUEST. Этот код блокирует использование XSS-инъекций и попытки модифицировать переменные GLOBALS и _REQUEST[4]. Вставьте код в ваш файл *.htaccess*, расположенный в корне сайта. (И не забывайте бэкапить этот файл перед внесением любых изменений).

```
Options +FollowSymLinks
RewriteEngine On
RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
RewriteRule ^(.*)$ index.php [F,L]
```

Код позволяет проверять все запросы. Если запрос содержит тег или попытку модифицировать значение переменных GLOBALS и _REQUEST, он блокирует его и выдаёт 403-ю ошибку.

12. Защита директорий на сервере от просмотра. Очень многие хостеры позволяют просматривать директории на своих серверах. Поэтому, если ввести в адресную строку www.вашблог.ru/wp-includes, то очень часто можно увидеть всё содержимое этой директории. Безусловно это небезопасно, поэтому лучше это сразу запретитьх[4].

Вы можете либо добавить пустые файлы index.html в папки, просмотр которых хотели бы запретить. Либо дополнить наш *.htaccess* ещё одной строкой: Пустой *index.html* будет выдаваться каждый раз, когда последует запрос к директории. Ну а директива в *.htaccess* просто запрещает апачу выдавать список содержимого директории.

Выводы

Защита WordPress – вещь сложная, и описанные в этой статье способы не гарантируют на 100%, что ваш сайт будет полностью защищен от каких-либо действий мошенников. Однако, пренебрегать ими не стоит, так как они значительно уменьшат возможность взлома сайта злоумышленниками.

Список литературы

1. *10 шагов для защиты вашего WordPress блога [Электронный ресурс] – Режим доступа: https://habrahabr.ru/post/62814/ 18.01.17.*
2. *Ещё 10 уловок для защиты Wordpress'a [Электронный ресурс] – Режим доступа: https://habrahabr.ru/post/98083/ 17.01.17.*
3. *17 способов защитить сайт на WordPress [Электронный ресурс] – Режим доступа: https://hostiq.ua/blog/17-ways-to-secure-wordpress/#17 18.01.17*
4. *[Электронный ресурс] – Режим доступа: https://ru.wordpress.org/ 18.01.17.*

Надійшла до редколегії 3.02.2017

Рецензент: д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

МЕТОДИ І СПОСОБИ ЗАХИСТУ CMS WORDPRESS

С.С. Мєшечко, В.Я. Пєвнєв, В.А. Погорєлов

WordPress - ідеальна платформа для публікації, орієнтована на красу, підтримку стандартів і зручність використання. На сьогодніь Wordpress як ніколи популярний. Блоги, міні-сайти, а то й цілі портали - все це будується на основі такого зручного движка-конструктора як Wordpress. Але за зручністю і легкістю освоєння криються, перш за все, питання, пов'язані з безпекою вашого сайту. Авторами проведено аналіз методів і способів захисту CMS WordPress. Описано детальні дії щодо підвищення стійкості системи до DDos-атакам таі основні помилки при адмініструванні сайту.

Ключові слова: *безпека, захист, надійність, адміністрування, паролі, підтримка.*

THE METHODS AND WAYS TO PROTECT CMS WORDPRESS

S.S. Meshechko, V.Y. Pevnev, V.A. Pogorelov

WordPress - an ideal platform for publishing, focused on beauty, standards support, and usability. Today, more than ever popular Wordpress. Blogs, mini-sites, and even entire portals - all this is based on such a convenient engine-designer like Wordpress. But for convenient and ease of development lie, first and foremost, issues related to the security of your site. Most prevalence - more hackers attention. The article analyzes the methods and ways of protection CMS WordPress. We describe the detailed steps to improve the sustainability of the system to DDos-attack. Painted Common Errors in site administration.

Keywords*: safety, protection, reliability, administration, passwords, support.*

УДК 621.391.037

Е.О. Новаков, М.В. Цуранов

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

ИСПОЛЬЗОВАНИЕ ОБУЧАЕМЫХ HIPS-АНТИВИРУСОВ ДЛЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

В статье проведен анализ методов построения антивирусных систем. Указаны преимущества и недостатки основных методов защиты. Описаны виды HIPS антивирусов. Разработан алгоритм обучения HIPS-антивируса, устраняющий недостатки классических и экспертных реализаций антивируса. Описана программная модель предлагаемого антивирусного продукта.

Ключевые слова: *антивирусы, безопасность информации, проактивная защита, обучения антивирусов.*

Введение

В данный момент использование систем антивирусной защиты подвергается большой критике со стороны разработчиков. Основные претензии к антивирусам следующие: крупные антивирусные продукты (не считая встроенного в Windows) не обеспечивают повышение безопасности, а, скорее, вредят компьютерам. Как пример, можно посмотреть на список критических ошибок в антивирусном ПО, перечисленные в Project Zero компании Google [1]. Приведенные уязвимости показывают, что антиврусные продукты не только предоставляют множество способов для атак, но и в целом их разработчики не следуют стандартным правилам безопасности. Кроме этого, программный код всех сторонних антивирусов зачастую некорректно написан, и из-за этого разработчикам браузеров (и любого другого ПО прикладного уровня) сложнее следить за безопасностью своих продуктов [1].

Большинство разработчиков прикладного ПО при внедрении функции безопасности сталкиваются с противодействием со стороны антивирусных программ. Например, при внедрении технологии ASLR, используемую для изменения расположения в адресном пространстве процесса важных структур данных, в браузер Firefox для Windows. Тогда оказалось, что многие антивирусные программы мешают обновлению безопасности, интегрируя собственные библиотеки ASLR. Более того, несколько раз антивирусы даже заблокировали обновления Firefox, из-за чего пользователи не смогли получить важные исправления безопасности [1].

Однако, разработчики антивирусов реагируют на возникшие проблемы и активно внедряют приходят новые технологии антивирусостроения: Host-based Intrusion Prevention System (HIPS), Sandbox, Virtual-based Intrusion Prevention System (VIPS). Эти технологии позволяют пользователю активно мониторить процессы в системе и принимать решения о допуске их к различным функциям ОС.

Цель предложенной работы: разработка метода обучения HIPS-антивируса.

Изложение основного материала

Первые антивирусы использовали принцип реактивной защиты, которая была наиболее проста в реализации. Ее суть — обнаружение вторжения, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы. В случае соответствия какого-либо участка кода просматриваемой программы известному коду вируса в словаре, программа антивирус может заняться выполнением одного из следующих действий [2]: удалить инфицированный файл; отправить файл в «карантин»; попытаться восстановить файл, удалив сам вирус из тела файла.

Классические реактивные системы обнаружения вредоносных программ, несмотря на кажущуюся простоту реализации и надежность, имеют ряд существенных недостатков [3]: слабая эффективность против угроз типа zero-day, так как эффективность напрямую связана с базой сигнатур вредоносного ПО, в которую внесены сигнатуры только известного, на данный момент, вредоносного ПО; необходимость постоянного обновления базы сигнатур вирусов для эффективной защиты от нового вредоносного ПО; для определения вредоносного ПО необходима процедура сканирования, которая отнимает достаточно много времени и системных ресурсов.

Указанные причины послужили толчком к развитию проактивных систем защиты. Основная причина — требование к постоянному пополнению базы сигнатур вирусов для реактивных методов, которые составляют большинство, на данный момент, ведь количество вирусов с каждым днем растет. Постоянно пополняющиеся базы сигнатур затрудняют поиск, что замедляет работу классических антивирусов, в то время как один вирус может иметь несколько сигнатур. К примеру, руководитель Comodo подверг критике стратегии антивирусной защиты [4]:

«Нельзя мириться с существованием отрасли, в которую вкладывается 10 миллиардов долларов без видимого результата. Давайте сравним. Допустим, вы платите три доллара за таблетки от головной боли, вы их принимаете, и боль проходит – ваша проблема

решена; и в то же время мы все платим индустрии безопасности 10 млад за решение проблем с вредоносным программным обеспечением, но оно не исчезает – напротив, его становится все больше и больше. Почему? Потому что нет корректной бизнес-модели».

В мае 2014 г. Брайан Дай (Brian Dye), старший вице-президент Symantec по информационной безопасности, рассказал газете Wall Street Journal, что классические антивирусы «обречены на неудачу». Он признался, что выпуск локальных решений для защиты персональных компьютеров «не прибыльный бизнес», и что компании необходимо это учитывать в своей стратегии. Представитель Symantec пояснил, что сегодня хакеры проводят атаки на компьютеры и вычислительные сети, а не занимаются рассылкой почтовых сообщений с зараженными вложениями. Хотя антивирусные продукты по-прежнему приносят Symantec весомую часть выручки (около 40%), компания не может добиться роста в этом сегменте [5].

Исходя из всего написанного, а также высказывания директора Comodo и перехода Symantec на полностью безсигнатурную работу, можно сделать вывод, что классический подход к обеспечению безопасности компьютера становится все менее актуальным и следует переходить к более современным проактивным методам защиты. Это позволит отойти от использования громоздких баз, поиск по которым потребляет все больше ресурсов ПК пользователя и увеличить надежность антивирусных систем против угроз zero-day. Примером такой проактивной системы защиты являются HIPS-антивирусы. Существуют следующие типы HIPS-систем: классические, экспертные, песочница. Классические HIPS-продукты предоставляют пользователю информацию об активности того или иного приложения, однако решение о разрешении/запрещении той или иной операции должен принимать пользователь, т.о. классические HIPS-продукты позволяют пользователю тонко настроить те или иные правила контроля, но создание правил требует высокой квалификации пользователя. Это системы, в инвентарь которых входит специальная таблица правил открытого вида. Она представляет собой перечень правил, согласно которым фиксируется неправомерное действие потенциально опасных процессов. Она формируется пользователем либо производителем продукта и может быть модифицирована. Ориентируясь на эту таблицу, драйверы HIPS могут автоматически запретить или разрешить какие-либо действия различных приложений, а также отправить пользователю запрос, чтобы он сам принял решение. Как следствие, для успешной работы классического HIPS пользователь должен обладать хоть какими-либо знаниями о системе, т.к. устройство, по сути, ориентировано на ручное управление, что является недостатком. Однако есть и достоинства: данную систему легче реализовывать, и она не требует значительных ресурсов для функционирования. Для примера подобного вида HIPS можно взять программы System Safety Monitor и AntiHook [6]. Экспертные HIPS способны проводить анализ активной работы запущенного приложения и оценивать его действия "в целом". Это значит, что если совокупность действий приложения схожа на разрушающую программу или на любое другое вредоносное действие - система сообщит пользователю о возможной опасности.

Поведенческие эвристики — это набор правил, которыми руководствуется программа для пометки процесса как «вредоносного» или нет в процессе его работы или запуска. Анализ проводится по таким параметрам как: память, к которой обращается процесс, драйвера, которые он запрашивает, влияние на другие процессы и прочие параметры, которые каждый HIPS реализует по-своему. В отличие от классических HIPS-продуктов, экспертные HIPS могут самостоятельно принимать решение о блокировке той или иной активности, исходя из правил и алгоритмов, заложенных разработчиком продукта. Для использования экспертных HIPS-продуктов пользователю не обязательно обладать определенной квалификацией. Экспертные HIPS-продукты в ряде случаев могут блокировать легитимную активность пользовательского программного обеспечения. Причинами этого могут быть: не идентификация данной активности программы как вредоносной из-за ошибок в алгоритме или коде программы, из-за неправильных настроек, либо идентификация безопасных процессов как опасных из-за особенностей их работы. Можно сказать, что качество экспертных HIPS зависит от того, насколько хорошо программа отличает опасные процессы от безопасных, ведь чем больше легитимных процессов блокируются, тем сложнее работать пользователю. Такие продукты основаны на черных и белых списках. Черный список (blacklist) — системы, суть работы которых заключается в проверке вхождения неизвестного файла, программы или действия в некий список заранее известных недоверенных объектов. Белый список (whitelist) — такие системы разрешают работу лишь программам из доверенного списка [6].

Следующий тип HIPS, песочница — специально выделенная среда для безопасного исполнения компьютерных программ. Обычно представляет собой жёстко контролируемый набор ресурсов для исполнения гостевой программы — например, место на диске или в памяти. Доступ к сети, возможность связи с главной операционной системой или считывания информации с устройств ввода, обычно частично эмулируют, либо сильно ограничивают. Песочницы представляют собой пример виртуализации. Как правило, песочницы используют для запуска непроверенного кода из неизвестных источников или «сырого» кода, который может случайно повредить систему или испортить сложную конфигурацию, как средство проактивной защиты от вредоносного кода, а также для обнаружения и анализа вредоносных, либо новых или недоверенных программ. Такие «тестировочные» песочницы копируют основные элементы среды, для которой пишется код, и позволяют разработчикам быстро и безболезненно экспериментировать с неотлаженным кодом.

В связи с большим распространением вредоносных программ, а также применением злоумышленниками специальных технологий (например, полиморфизм), классические сигнатурные сканеры уже не могут эффективно противостоять новым угрозам [6].

Основной недостаток HIPS систем: экспертных – ложные срабатывания, классических – потенциальная некомпетентность пользователя. Для устранения этих недостатков необходимо либо улучшить алгоритмы эвристики (для экспертных), что повлечет большие денежные и временные затраты, либо повышать компетентность пользователя, что тоже может привести к большим затратам. Однако, мы можем переложить формирование алгоритмов эвристики на опытного пользователя, с последующей передачей настроенной системы неопытному пользователю под конкретную сферу применение ПК пользователя антивируса. Это позволит сделать алгоритм эвристики более гибким, подстраивающимся под сферу использования системы защиты.

Исходя из этих пунктов, методика обучения антивируса состоит из таких пунктов:

1) формирование черного списка из базы данных антивируса или любого другого источника;

2) составление белого списка, добавлением в него ПО от доверенных разработчиков;

3) конструирование эвристических алгоритмов путем подключения модулей, каждый реагирует только на конкретное потенциально опасное поведение;

4) в случае, если процесс не был идентифицирован как опасный или безопасный, пользователь может принять решение: в какой список внести процесс.

Антивирусный продукт должен состоять из следующих модулей: UI (пользовательский интерфейс); Analyzer (блок перехвата процессов); Core (ядро системы). Блок «UI» представляет собой удобный пользовательский интерфейс с возможностью настройки модульного алгоритма эвристики, доступом к черному и белому спискам, списком заблокированных процессов с возможностью их разблокировать и всплывающего окна в случае, если был обнаружен неидентифицированный процесс. Блок «Analyzer» зависит от используемой ОС, так как осуществляет перехват процессов, что зависит от API конкретной системы и не может быть кроссплатформенным решением. Следовательно, этот блок должен быть реализован на native-code. Перехватив процесс, блок «Analyzer» передает сведения в блок «Core» для последующей обработки и выдачи автоматизированного решения, либо запроса к пользователю. Блок «Core» состоит из метода приведения процесса к понимаемому программой объекту, черного и белого списка, модулей алгоритма эвристики. Данный блок решает, будет ли процессу разрешен доступ в систему, основываясь на автоматизированной системе, либо ответе пользователя.

Выводы

Предлагаемая методика формирования модулей эвристики позволяет привлекать экспертов в своих областях для конкретных сфер применения продукта, в то же время, пользователю дана возможность формировать правила самостоятельно, если он уверен в своей компетентности. Это повышает гибкость системы, оставляя элементы автоматизированной работы. Модульность алгоритмов позволяет сосредоточиться на максимально опасных угрозах для каждой сферы или их совокупности, без затрат на обработку несущественных уязвимостей.

Список литературы

1. *Разработчик Firefox призвал пользователей Windows 10 отказаться от сторонних антивирусов [Электронный ресурс] – Режим доступа: https://4pda.ru/2017/1/31/334759/ 06.02.16*

2. *Обнаружение, основанное на сигнатурах [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/ 06.02.16.*

3. *Проактивные методы антивирусной защиты [Электронный ресурс] – Режим доступа: https://www.anti-malware.ru/blog/199/1300 06.02.16 .*

4. *Почему Comodo бесплатен? [Электронный ресурс] – Режим доступа: http://comodo.comss.ru/pochemu-comodo-besplaten.html 06.02.16.*

5. *Легендарный Norton Antivirus уходит с рынка [Электронный ресурс] Режим доступа: http://www.cnews.ru/news/top/legendarnyj_norton_antivirus_uhodit. 06.02.16.*

6. *HIPS [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/HIPS 06.02.16.*

Надійшла до редколегії 1.02.2017

Рецензент: д-р техн. наук, проф. О.А. Серков, Національний технічний університет «ХПІ», Харків.

ВИКОРИСТАННЯ НАВЧАЄМИХ HIPS-АНТИВІРУСІВ ДЛЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Є.О. Новаков, М.В. Цуранов

У статті приведений аналіз методів побудови антивірусних систем. Вказані переваги та недоліки основних методів захисту. Описані види HIPS-антивірусів. Розроблений алгоритм навчання HIPS-антивірусу, усуваючий недоліки класичних та експертних реалізацій антивірусу. Описана програмна модель пропонованого антивірусного продукту.

Ключові слова: *антивіруси, безпека інформації, HIPS, проактивний захист, навчання антивірусів.*

USING OF EDUCABLE HIPS-ANTIVIRUSES FOR CYBERCRIME OPPOSITION

Ye.O. Novakov, M.V. Tsuranov

The article has analysis of antivirus systems developing. Advantages and disadvantages of general security methods are listed. HIPS-antiviruses kinds are described. Teaching method which removes disadvantages of classical and expert antivirus implementations is designed in the article. Program model of the offered antivirus product is described.

Keywords*: antiviruses, information security, HIPS, proactive defense, antiviruses teaching.*

УДК 651. 34

А.С. Семенова, М.В. Бартош

Национальный технический университет «ХПИ», Харьков

ОЦЕНКА УСТОЙЧИВОСТИ СЕТИ INTERNET OF THINGS С ПОМОЩЬЮ ПОКАЗАТЕЛЕЙ ЦЕНТРАЛЬНОСТИ СВЯЗЕЙ

На основе результатов исследования существующих уязвимостей компьютерных сетей INTERNET OF THINGS (IoT) в статье определены ряд перспективных направлений дальнейшего совершенствования методов и средств обеспечения безопасности данных. В рамках одного из перспективных направлений проведен анализ основных показателей центральности связей компьютерной сети IoT. Определено сопоставимость результатов использования как уже известных, так и новых (усовершенствованных) показателей при оценке устойчивости сетей к злоумышленным атакам. Также выявлена эффективность использования усовершенствованного показателя Local Vector Centrality при оценке устойчивости сети к межосевым атакам.

Ключевые слова: *INTERNET OF THINGS, показатели центральности (централизации) связей, компьютерная сеть, устойчивость, безопасность.*

Введение

Постановка проблемы. Интернет вещей (IoT) одно из новых направлений современных информационных технологий. Это направление имеет своей стратегической целью компьютеризацию и автоматизацию процессов управления в широком диапазоне сфер обслуживания. Обеспечивается это повсеместной связью между различными техническими цифровыми устройствами с минимизацией включения человеческого фактора. Это существенно расширяет границы применимости компьютерной и другой цифровой техники и является в свою очередь своеобразным двигателем прогресса в различных отраслях экономики. На рис. 1 представлена обобщенная концепция построения общей структуры IoT.

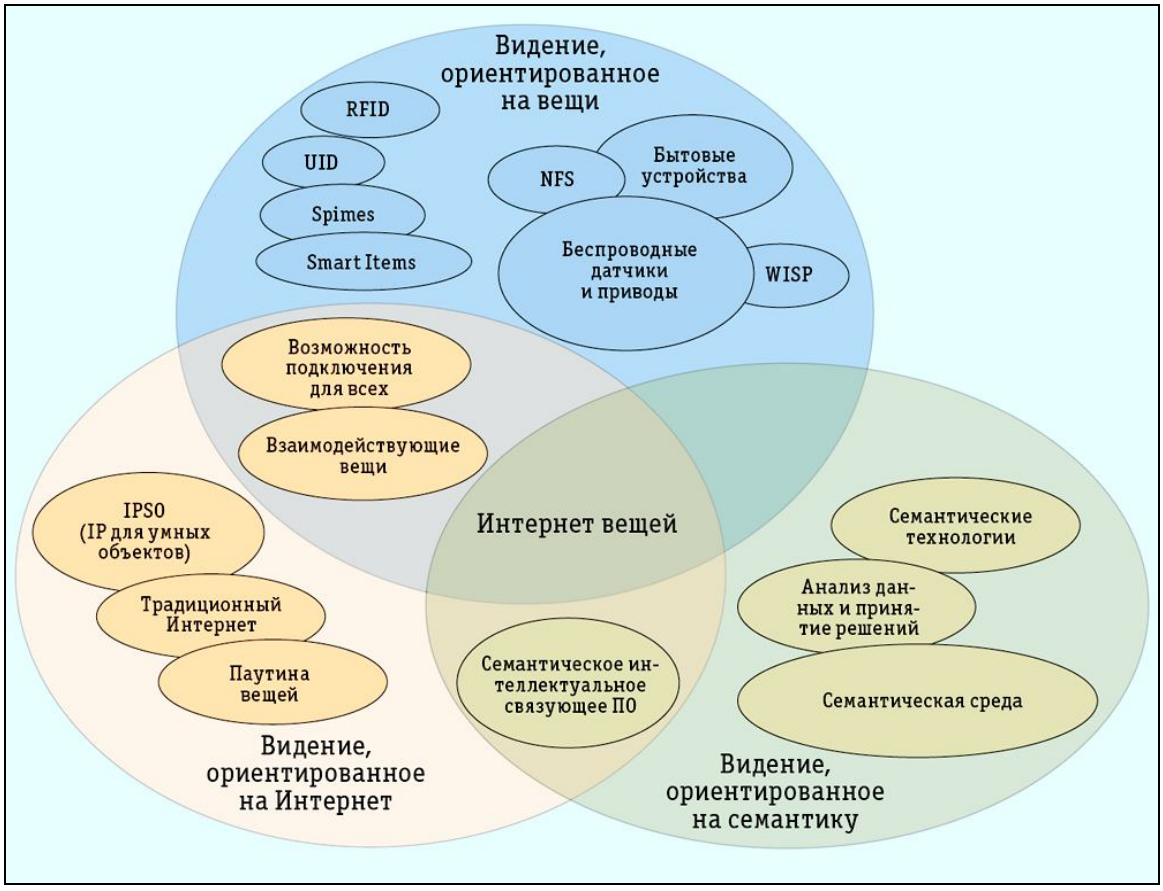


Рис. 1. Схема основных составляющих обобщенной концепции построения общей структуры IoT

В то же время, как показали исследования [1, 5], функциональность и операции IoT в значительной степени зависят от топологии и базовой структуры подключения к сети. Данный факт неизбежно вызывает проблемы безопасности в связи с возможностью незаметного подключения и автоматизированной интеграции между различными видами приложений. Например, злоумышленник может использовать взаимосвязанные устройства для распространения вредоносных программ. Проблема усугубляется разнородностью аппаратно-программных средств обеспечивающих функционирование IoT. Поэтому именно в последнее время этому вопросу начали уделять большое внимание. Так на базе Стэндфордского университета США была сформирована группа специалистов для разработки унифицированных предложений защиты данных в IoT [7].. А департамент США по энергетике (DOE) приступил к разработке предложений защиты от активных атак на уровне топологии.

Анализ литературы показал, что одним из недостатков и факторов, снижающих эффективность (в том числе и безопасность) функционирования компьютерных сетей IoT является стратегия на централизованной управление облачными ресурсами.

Это подтверждается фактами успешно проведенных злоумышленных атак на ключевые узлы коммутации IoT. Поэтому ряд фирм [5] предлагают альтернативные решения, связанные с созданием полностью децентрализованной экосистемы Интернета вещей, работающей независимо от центральных авторитетов.

В такой среде устройства смогут самостоятельно обнаруживать другие устройства, безопасно подключаться к ним и устанавливать с ними доверительные отношения с помощью контрактов.

Возможно, устройства даже смогут передавать друг другу ценности – например, платить за доступ к сенсорам или аренду вычислительной мощности.

Следует заметить, что создание децентрализованного IoT – сложная задача. Необходимо разработать протоколы обнаружения устройств, безопасности и управления идентичностью, реализовать схемы доверия, интегрировать в сеть криптовалюты и решить многие другие задачи.

Проведенные исследования показали, что одной из первоначальных задач в перечне является разработка оптимальной топологической структуры компьютерной сети IoT.

Для ее решения необходимо предварительно провести анализ и исследования существующих показателей централизации (децентрализации) узлов сети и степень влияния их возможного выхода из строя на общий показатель безопасности компьютерной сети IoT.

Проведенный анализ литературы [2-7] показал, что в настоящее время существует ряд основных показателей центральности (централизации) связей сети.

Так в источниках [2, 4] определено, что это показатели степень связности (degree centrality); степени близости к другим узлам (closeness centrality); степени посредничества (betweenness centrality) и влиятельности (eigenvector centrality). Кроме этого в последнее время представлено ряд новых, усовершенствованных разработок, в которых этот список расширяется.

Так, например в [3] предлагается рассматривать еще такой показатель, как эгоцентричность (Ego centrality), а в статье [6] рассматривается показатель локальной центральной плотности (Local Vector Centrality).

Результаты исследований

Рассмотрим более подробно следующие показатели:

1. Степень связности (degree centrality) – исторически первая и концептуально простая мера C_0 важности узлов в сети. Эта мера определяется как количество связей deg(v), инцидентных данному узлу v:

$$C_0(v) = \deg(v).$$

Степень связности узлов компьютерной сети IoT можно интерпретировать как меру активности узлов в процессе выполнения различных задач, характерных данному виду IoT.

2. Степень близости к другим узлам (closeness centrality) $C_c(v)$ – обратная величина суммы кратчайших путей $d(v_i, w_i)$ от узла v до других узлов w_i:

$$C_c(v) = \Big/ \sum_{i=1}^{|V|} d(v, w_i),$$

где $|V|$ – число всех узлов сети.

Таким образом, чем более важным является узел в соответствии с указанным показателем, тем меньше сумма кратчайших путей от него к другим узлам.

3. Степень посредничества (betweenness centrality) – характеристика узла, показывающая, насколько часто данный узел лежит на кратчайших путях между другими узлами.

Этот параметр вычисляется следующим образом

$$C_b(v) = \sum_{k \neq i} \sum_{j \neq i,\ j > k} \frac{\sigma_{kj}(v)}{\sigma_{kj}},$$

где σ_{kj} – количество кратчайших путей из узла k в узел j, а $\sigma_{kj}(v)$ – количество этих путей, проходящих через узел v.

Через узел с высокой степенью посредничества будет проходит большой объем данных, при условии что передача будет осуществляться по кратчайшим путям.

Это подразумевает большую уязвимость таких узлов к атакам злоумышленников.

4. Влиятельность (eigenvector centrality) – рекурсивная мера $C_e(v)$ важности узла, основанной на важности соседних узлов.

5. Чем более влиятельны узлы, с которыми связан узел, тем больше влиятельность самого узла:

$$C_e(v) = \frac{1}{\lambda}\sum_{i\in M(v)} C_e(t) = \frac{1}{\lambda}\sum_{i\in G} A_{v,t}C_e(t),$$

где $M(v)$ – множество соседних узлу v узлов; λ – константа; $A_{v,t}$ – элемент матрицы смежности (задается на основе связности узлов сети).

Значения $C_e(v)$ можно получить, решив уравнение

$$A_x = \lambda x,$$

где A – матрица смежности, λ и x – соответственно собственное значение и собственный вектор матрицы A.

6. Эгоцентричность (Ego centrality) – показатель, который можно описать следующим образом.

Пусть матрица смежности узла i – A_i имеет размерность $(d_i + 1)\times(d_i + 1)$.

Пусть I – единичная матрица.

Так как $\left|A^2(i)\right|_{kj}$ может задавать число двухходовых переходов между k и j, и

$$\left|A^2(i)\circ I - A(i)\right|_{kj} -$$

общее число кратчайших путей с двумя хопами между k и j для всех $k \neq j$, (символ $\circ$ обозначает матричное произведение), центральность $C_r(v)$ определяется как

$$C_r(v) = \sum_k \sum_{j>k} \Big/ \left|A^2(i)\circ I - A(i)\right|_{kj}^{1}.$$

В целом можно заметить, что данный показатель может рассматриваться как частный случай степени посредничества (betweenness centrality).

7. $C_{LVC}(i)$ (Local Vector Centrality (LVC)) – это показатель, характеризующий уязвимость компьютерной сети IoT к удалению узлов. Узел с более высоким LVC более важен для структуры сетевого соединения.

Пусть y – собственный вектор, связанный со вторым наименьшим собственным значением $\mu(L)$ матрицы Лапласса L.

Тогда $C_{LVC}(i)$ можно рассчитать как

$$C_{LVC}(i) = \sum_{j\in N_i}\left(y_i - y_j\right)^2.$$

Следует заметить, что хоть $C_{LVC}(i)$ – это и обобщенная центральная мера, ее можно точно аппроксимировать локальными вычислениями и передачей сообщений с использованием метода распределенной мощности для вычисления вектора y.

При оценке устойчивости сети по показателям централизации к различным атакам мы можем сравнить количество выведенных из строя узлов, необходимых для успешной атаки.

Это необходимо для уменьшения наибольшего размера показателя до определенного значения, например, количества узлов, необходимых для уменьшения размера наибольшего компонента до 10% от исходного размера.

На рис. 2 представлены результаты исследования показателя устойчивости сети IoT (графики зависимости нормализированных значений выбранных показателей централизации от количества выведенных из строя узлов сети IoT) в соответствии с базой данных GTS-CE [4].

Рассматривался практический случай когда сеть состоит из 149 узлов и 193 соединительных линий.

Как видно из графика в представленной сети IoT межосевые атаки и атаки LVC имеют сопоставимую эффективность, что приводит к снижению на 20% наибольшего количественного показателя путем удаления 10 узлов из сети.

Выводы

В результате проведенных анализа литературы и исследований были определены наиболее информативные показатели централизации сети IoT.

Проведены исследования возможности их использования для анализа устойчивости компьютерной сети IoT к атакам злоумышленников, направленных на выведение из строя центральных, наиболее ванных узлов.

Результаты показали в целом сопоставимость результатов в рассмотренном конкретном случае, и преимущество до 20% п показателя Local Vector Centrality при удалении 10 узлов.

Дальнейшие исследования будут направлены на построение топологически защищенной компьютерной сети IoT.

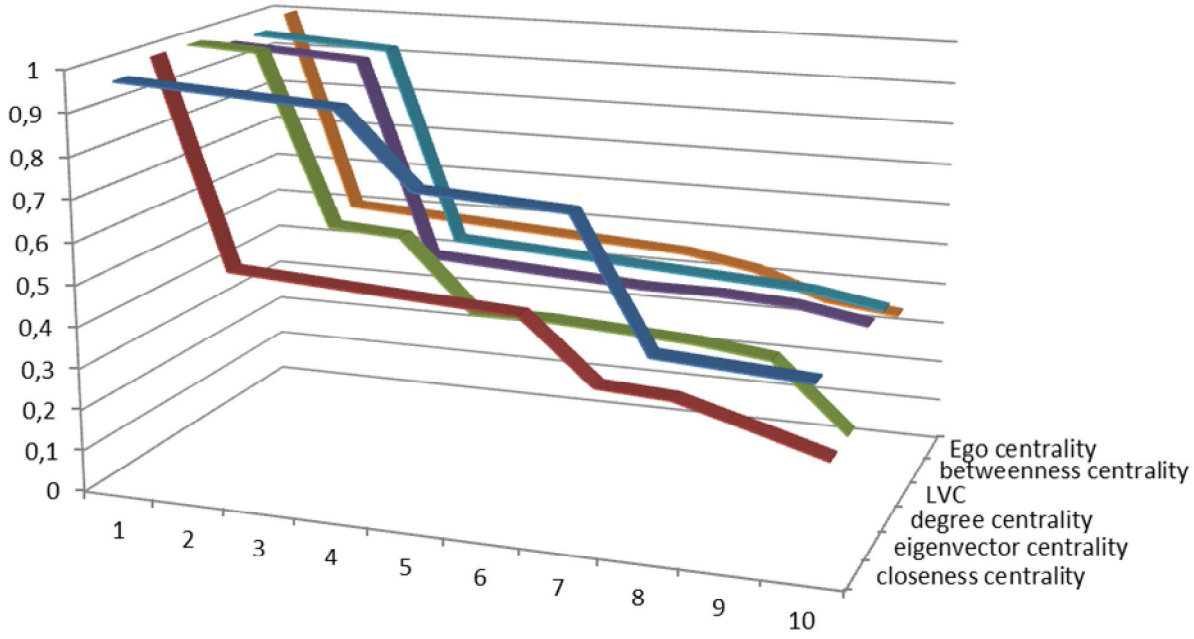


Рис. 2. Графики зависимости нормализированных значений выбранных показателей централизации от количества выведенных из строя узлов сети IoT

Список литературы

1. Черняк Л. Интернет вещей: новые вызовы и новые технологии [Электронный ресурс] / Л. Черняк // Открытые системы. СУБД 2013 № 04. Режим доступа: https://www.osp.ru/os/2013/04/13035551.

2. Юдина М.Н. Узлы в социальных сетях: меры центральности и роль в сетевых процессах / М.Н. Юдина // Омский научный вестник 2016, С. 161-165.

3. Everett Martin Ego network betweenness. / Martin Everett, Stephen P. Borgatti. // Social Networks, 27(1):31–38, 2005.

4. Knight Simon The Internet topology zoo. / Simon Knight, Hung X. Nguyen, Nickolas Falkner, Rhys Bowden, and Matthew Roughan. // IEEE J. Sel. Areas Commun., 29(9):1765–1775,October 2011.

Matviishyn Oleksandr Decentralization in the Internet of Things [Электронный ресурс] / Oleksandr Matviishyn. – Режим доступа: https://united.softser veinc.com/blog/decentralization-internet-of-things.

5. Pin-Yu Chen Local Fiedler vector centrality for detection of deep and overlapping communities in networks. /Yu Chen, Alfred O. Hero // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 1120–1124, 2014.

6. Rethinking a Secure Internet of Things [Электронный ресурс]. – Режим доступа: http://iot.stanford.edu.

Надійшла до редколегії 1.02.2017

Рецензент: д-р техн. наук, проф. О.А. Серков, Національний технічний університет «ХПІ», Харків.

ОЦІНКА СТІЙКОСТІ МЕРЕЖІ INTERNET OF THINGS ЗА ДОПОМОГОЮ ПОКАЗНИКІВ ЦЕНТРАЛЬНОСТІ ЗВ'ЯЗКІВ

Г.С. Семенова, М.В. Бартош

На основі результатів дослідження існуючих вразливостей комп'ютерних мереж INTERNET OF THINGS (IoT) в статті визначено ряд перспективних напрямків подальшого вдосконалення методів і засобів забезпечення безпеки даних. В рамках одного з перспективних напрямків проведено аналіз основних показників центральності зв'язків комп'ютерної мережі IoT. Визначено порівнянність результатів використання як уже відомих, так і нових (удосконалених) показників при оцінці стійкості мереж до зловмисним атакам. Також виявлено ефективність використання вдосконаленого показника Local Vector Centrality при оцінці стійкості мережі до міжосьовим атакам.

Ключові слова: *INTERNET OF THINGS, показники центральності (централізації) зв'язків, комп'ютерна мережа, стійкість, безпеку.*

ESTIMATION OF THE STABILITY OF THE INTERNET OF THINGS NETWORK WITH THE INDICATORS OF CENTRALITY OF CONNECTIONS

H.S. Semenova, M.V. Bartosz

Based on the results of a study of the existing vulnerabilities of computer networks INTERNET OF THINGS (IoT), the article identifies a number of promising areas for further improvement of methods and tools to ensure data security. Within the framework of one of the prospective directions, the analysis of the main indicators of the centrality of the IoT network connections was carried out. The comparability of the results of using both known and new (improved) indicators in assessing the stability of networks for malicious attacks was determined. Also, the effectiveness of using the improved indicator of Local Vector Centrality in assessing the stability of the network to inter-axial attacks was revealed.

Keywords: *INTERNET OF THINGS, indicators of centrality (centralization) of communications, computer network, stability, security.*

УДК 004.91

О.Д. Смоктій[1], К.В. Смоктій[1], О.В. Іванченко[2]

[1] *Донецький національний університет імені Василя Стуса, Вінниця*
[2] *Університет митної справи та фінансів, Дніпро*

АНАЛИЗ МЕХАНИЗМА И ПОСЛЕДСТВИЙ ВОЗДЕЙСТВИЯ DDOS-АТАК НА ЭТАЛОННУЮ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ OSI

В статье рассмотрен механизм воздействия DDoS-атак на облачные серверы на прикладном и инфраструктурном уровнях модели OSI, приведены основные направления атак данных уровней. На каждом из OSI-уровней проведен анализ последствий и выработаны рекомендации по ослаблению воздействияDDoS-атак.В работе приведены данные исследований основных направлений атак, мотивации атакующих и применяемых ими техник атак. Сделаны выводы относительно наиболее уязвимых для атак злоумышленников протоколов передачи данных и самых распространенных направлений DDoS-атак.

***Ключевые слова**: DDoS-атаки, распределенный отказ в обслуживании, модель OSI, атаки прикладного уровня, атаки уровня инфраструктуры, SYN-флуд, HTTP-флуд, облачный сервер.*

Введение

Постановка задачи. Современные условия применения интернет-технологий требуют обеспечения высокоэффективной защиты информационного пространства, являющегося важнейшим фактором влияния на национальную безопасность государства. На сегодняшний день одной из актуальных проблем в национальном кибернетическом пространстве является защита киберактивов различных инфраструктурных образований, включая активы отдельных предприятий, от воздействия DDoS-атак.

Фактически DDoS-атака (Distributed Denial of Service) представляет распределённый отказ в обслуживании вычислительных мощностей, вызванный действиями злоумышленников. Это один из многих возможных способов несанкционированного захвата компьютерных систем, который занимает ведущее место по численности попыток совершения взломов в силу гибкости и высокой степени безотказности его применения в компьютерных сетях любой архитектуры. Поэтому DDoS-атаки являются серьезной угрозой как для информационного пространства отдельных предприятий, поскольку наносят им серьёзный материальный ущерб, так и для глобального интернет пространства, т.к. воздействующий вредоносный трафик снижает скорость и эффективность работы корневых интернет серверов.

Известные методы защиты инфраструктуры от DDoS-атак направлены на максимальное её ослабление. К сожалению,в силу несовершенства механизмов воздействия на кибернетических злоумышленников спрогнозировать и полностью предотвратить атаку практически невозможно.

Анализ последних исследований и публикаций. Одним из основных инструментариев реализации DDoS-атаки является бот (Bot), представляющий собой вредоносную программу, которая имитирует действия пользователя в сети Интернет и работает автоматически по заданному графику [1]. Это подтверждается исследованиями, проведёнными компанией Imperva. В отчёте компании сказано, что за 3 месяца 2016 года соотношение числа пользователей случайно выбранного домена к количеству ботов того же домена составляет один к трём [2]. Исходя из этого, аналитики компании сделали вывод, что бот-атаки менее опасны, чем направленные DDoS-атаки. Тем не менее, для небольших слабо защищенных сайтов бот-атаки представляют серьезную угрозу, поскольку по данным компании из 100000 случайно выбранных доменов 94% хотя бы один раз в три месяца отказывали в обслуживании, подвергаясь воздействию этого вида атак.

На рис. 1 представлена диаграмма наиболее распространенных технологий совершения взломов компьютерных сетей по данным компании Hack mageddon за январь 2017 года [3].

Из рис. 1 видно, что DDoS-атаки составляют 5,6% от общего числа атак. Кроме того, по данным компании Hackmageddon мотивацией злоумышленников к нанесению DDoS-атак служит в основном стремление получить выгоду от совершённогокибер-преступления, в первую очередь, от взлома финансовых систем, а также хакерство – как применение техник взлома новых защитных механизмов и изучение принципов их работы (рис. 2).

Наибольший интерес для атаки отказа в обслуживании представляют облачные сервисы, поскольку используются крупными корпорациями и финансовыми организациями для хранения данных и осуществления электронной коммерции. Облачные хранилища наиболее уязвимы при работе UDP-протокола, по которому происходит обмен сообщениями между хостами.

Рис. 1. Наиболее распространенные техники атак злоумышленниками вычислительных систем

Рис. 2. Мотивация DDoS-атакующих по данным на январь 2017 г.

Поэтому чрезвычайно важно при реализации соответствующих мер защиты контролировать входной облачный трафик и осуществлять мониторинг активности действий поставщика данных. В качестве превентивных мер защиты рассматривается вариант «самоконтроля» и «арбитражного контроля» со стороны поставщика данных [4]. На рис. 3 представлен рейтинг основных направлений DDoS-атак по данным компании Imperva [5].

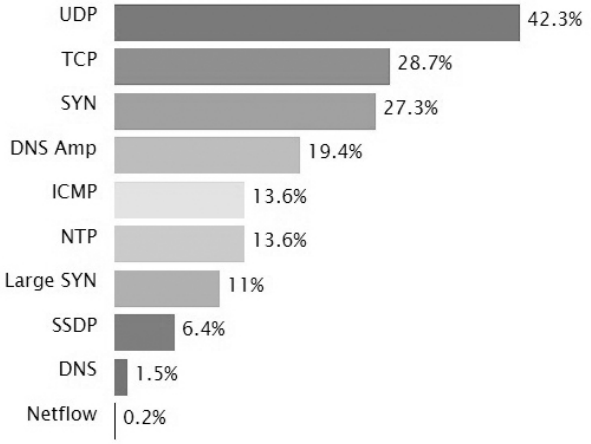


Рис. 3. Распределение DDoS-атак по основным протоколам 2016 г.

Одним из первых шагов по ослаблению DDoS воздействия является идентификация атаки, а именно: выявление источника; определение типа, масштаба атаки; оценка возможных последствий. В работах [6-8] предложены методы выявления DDoS-атак на основе методов MapReduce, искусственных нейронных сетей, аппарата нечеткой логики.

Основные уязвимости, на которые направлены действия DDoS-атак, а также меры по ослаблению атак исследованы в работах [9, 10].

Формулировка цели статьи

К облачным вычислениям, как и к любой сетевой инфраструктуре, применима модель OSI (Open Systems Interconnection), которая условно разделяет коммуникацию на семь уровней. На каждом уровне модели применим свой механизм ослабления DDoS-атаки, учитывающий разную природу и особенности вредоносного воздействия.

Целью статьи является рассмотрение механизма реализации DDoS-атак на каждом из OSI-уровней, анализ последствий и выработка рекомендаций по ослаблению их воздействия.

Изложение основного материала

На протяжении последних четырех лет атаки отказа в обслуживании были сосредоточены на трех уровнях: сетевой (3), транспортный (4) и прикладной (7).

Атаки третьего и четвертого уровней – инфраструктурные атаки, которые нацелены на перегрузку пропускной способности сети путем отправки большого количества фальшивых запросов (ICMP флуд, SYN флуд, Smurf-атака). Атаки седьмого уровня – прикладные атаки – преследуют цель нарушить работу приложений и критически важного программного обеспечения, тем самым вывести из строя серверы и другие обеспечивающие работу

сети устройства (GET запросы, HTTP GET, HTTP POST и т.д.).

Наиболее популярными направлениями инфраструктурных DDoS-атак являются такие направления [10]:

- DNS-отражение;
- TCP SYN флуд;
- UDP флуд;
- ICMP флуд.

Первое направление, к которому относятся DNS-отражение или DNS-усиление заключается в том, что злоумышленник посылает на DNS-сервер жертвы запрос небольшого размера, в котором изменен IP-адрес отправителя на IP-адрес компьютера-жертвы (так называемый IP spoofing). DNS-сервер отвечает на запрос сообщением гораздо большего размера и посылает его на IP-адрес компьютера-жертвы. Схема повторяется до тех пор, пока сеть не заблокируется вследствие перегрузки DNS-запросами.

Второе направление TCP SYN флуд работает с механизмом трехкратного обмена сообщениями (“рукопожатиями”) между сервером и клиентом перед установкой TCP соединения. Злоумышленник имитирует запрос на установку соединения от клиента серверу с отметкой SYN. На этот запрос сервер отвечает сообщением SYN-ACK клиенту, после чего клиент должен закрыть соединение, отослав серверу ACK-сообщение. Поскольку в роли клиента выступает злоумышленник, то он не закрывает соединение, тем самым оставляя серверу «полуоткрытое» соединение. Таких соединений устанавливается столько, сколько требуется для блокировки работы сети.

Третье направление UDP флуд – наиболее распространенный вид инфраструктурной DDoS-атаки, поскольку работает через UDP-протокол (User Datagram Protocol), который использует простую модель передачи сообщений, без обменов сообщениями и сеансов. Достаточно направить большое количество UDP-пакетов хосту-жертве, на каждый из которых атакуемый хост должен отправить ответ, и сеть окажется перегруженной. Если подменить IP-адрес отправителя UDP флуда, то злоумышленник сохранит анонимность и не подвергнется ответному потоку сообщений.

Четвёртое направление CMP флуд или PING флуд – простой способ DDoS-атаки, при котором на компьютер-жертву посылается большое количество ICMP-пакетов с целью блокировать TCP/IP стек.

На прикладном уровне действие DDoS-атак направлено на захват управления или вывод из строя программного обеспечения удаленного компьютера. Облачные вычисления особенно подвержены таким атакам в силу их веб-ориентированности. При DDoS-атаке на седьмой уровень OSI сеть не перегружается избыточным трафиком, тем самым снижается вероятность обнаружения взлома.

Основные инструменты, которые используются при атаках прикладного уровня, - это запросы HTTP, GET, DNS, SIP INVITE, отправленные на сервер-жертву. Эти запросы дают сверхнагрузку на текущую сессию сервера, блокируют его процессы и переполняют ресурсы.

Отдельно следует обратить внимание на атаку прикладного уровня типа DNS-усиление (DNS Amplification).

Ее принцип заключается в том, что атакующий посылает запрос просмотра DNS имен на открытый DNS сервер с IP-адресом источника равном IP-адресу жертвы. DNS сервер посылает ответ вместо источника атакуемому серверу. Таким образом на сервере создается избыточное количество пакетов от DNS до тех пор, пока работа сервер не блокируется из-за нехватки ресурсов. Такие атаки ослабляются ограничением количества принимаемых пакетов от DNS-сервера.

В табл. 1 представлено краткое описание возможных DDoS-атак на каждом из уровней OSI, протоколы, которые подвержены действиям злоумышленников, основные инструменты атакующих и методы, направленные на смягчение действий атаки.

Выводы из данного исследования и перспективы дальнейшего развития

Несмотря на то, что DDoS-атаки составляют 5,6% от общего количества известных атак, они оказывают разрушительное воздействие на кибернетические активы инфраструктурных образований и отдельных предприятий.

Мотивацией злоумышленников в подавляющем большинстве случаев является получение личной выгоды от атаки. Облачные вычисления подвержены DDoS-атакам наиболее часто по протоколам UDP иTCP – протоколам обмена сообщениями между хостами.

Атаки, направленные на 2-4 уровни OSI, ослабляются и предупреждаются настройками роутера или свитча (использование линейных списков контроля доступа, ограничение скорости канала и др.); атаки 5-7 уровней – конфигурацией брандмауэра и операционной системы сервера (использование UDP-,ICMP-экранов, ограничения сеансов, SYN cookie; использование брандмауэров с динамической проверкой и др.).

Первый уровень OSI защищается использованием качественного оборудования и мониторингом работы физического сетевого оборудования.

Таблица 1

Методы смягчения DDoS-атак на каждом уровне модели OSI

Уровень модели OSI	Задействованные протоколы	Инструменты DDoS	Возможные последствия атаки	Методы, смягчающие действие атаки
Прикладной уровень (7)	FTP, HTTP, POP3, SMTP, DNS и шлюзы, которые их используют	PDF GET запросы, HTTP GET, HTTP POST	Достижение предела по ресурсам сервисов атакуемого ресурса	Использовать мониторинг приложений для выявления 0day-уязвимостей приложений. Идентифицировав такие атаки, их можно раз и навсегда остановить и отследить их источник. Использовать коммерческие продукты, такие как ArborPeakflow SP и ArborPeakflow SP TMS, которые созданы для глобального анализа трафика инфраструктуры [1]. Использовать проксирование трафика.
Представительский уровень (6)	Протоколы шифрования и кодирования ASCII, EBCDIC, SSL, HTTPS, SSH	Подложные SSL запросы,THC-SSL-DoS атаки,HTTPS флуд	Не принимаются SSL соединения; автоматическая перезагрузка сервера	Проверка трафика приложений на предмет атак или нарушения политик на платформе приложений. Распределение шифрующей SSL инфраструктуры: размещение SSL на отдельном сервере, если это возможно. Использование протокола шифрования TLS (SSL-3), который защищает от атак типа man-in-the-middle.
Сеансовый (5)	Протоколы входа/выхода (RPC, PAP)	Слабые места программного обеспечения Telnet-сервера на свитче	Свитч не доступен администратору	Использование надежной аппаратной части – свитчей, маршрутизаторов и т.д.
Транспортный (4)	TCP, UDP	SYN флуд, Smurf-атака (атакаICMP-запросами с измененными адресами)	Достижение пределов по пропускной способности канала или по количеству допустимых подключений	Использовать фильтрациюDDoS-трафика, известная как blackholing[11]. Однако этот подход делает атакуемый ресурс недоступным как для трафика злоумышленника, так и для легального трафика пользователей. Тем не менее, блокировка доступа используется в борьбе с DDoS-атаками для защиты от таких последствий, как замедление работы сетевого оборудования и отказ работы сервисов.
Сетевой (3)	Протоколы IP, ICMP, ARP, RIP и роутеры, которые их используют	ICMP флуд, UDP флуд, DNS отражение	Снижение пропускной способности атакуемой сети и возможная перегруженность брандмауэра	Ограничение количества обрабатываемых запросов по протоколу ICMP, запрет ICMP форвардинга. Ограничение скорости для трафика UDP, защита прокси-серверов и настройка маршрутизатора для остановки передачи по прямому IP-адресу [1].
Канальный (2)	Протоколы 802.3, 802.5, контроллеры, точки доступа, мосты, которые их используют	MAC-флуд – переполнение пакетами данных сетевых коммутаторов	Потоки данных от отправителя получателю блокируют работу всех портов	Ограничить количество MAC адресов надежными, которые проходят проверку аутентификации, авторизации и учета на сервере (протокол AAA) и в последствии фильтруются. Для настройки фильтрации MAC-адресов используются конфигурируемые свитчи моделей, выпущенных в последние 5 лет. Наиболее эффективна фильтрация MAC-адресов в проводных сетях.

Окончание табл. 1

Физический (1)	Протоколы 100BaseT, 1000 Base-X, а также концентраторы, розетки, патч-панели	Физическое разрушение, физическое препятствие работе	Физическое сетевое оборудование приходит в негодность	Использовать систематический подход к мониторингу работы физического сетевого оборудования.

Многообразие механизмов реализации соответствующих стратегий DDoS обуславливает индивидуальные подходы к ослаблению атак на каждом уровне OSI модели.

Приведенные в статье методы ослабления действий DDoS-атак не являются исчерпывающими, что подтверждает необходимость дальнейших исследований механизмов и инструментариев противодействия DDoS-атакам.

Список литературы

1. Rashmi V. Deshmukh. Understanding DDoS Attack & its Effect in Cloud Environment / Rashmi V. Deshmukh, Kailas K. Devadkar // Procedia Computer Science, 2015. - Tokyo, Japan. - Vol. 49. - P. 202-210.

2. Bot Traffic Report 2016 [Electronic resource] / Access regime: https://www.incapsula.com/blog/bot-traffic-report-2016.html.

3. Hackmageddon Information Security Timelines and Statistics [Electronic resource] / Access regime: http://www.hackmageddon.com/

4. Gartner: Start security monitoring in the public cloud [Electronic resource] /Access regime: http://www.networkworld.com/article/2167209/security/gartner--start-security-mo-nitoring-in-the-public-cloud.html.

5. Global DDoS Threat Landscape Q1 2016 [Electronic resource] / Access regime: https://www.incapsula.com/ddos-report/ddos-report-q1-2016.html.

6. Головін А. Виявлення DDoS-атак прикладного рівня шляхом використання моделі Map Reduce / А. Головін // Інформаційні технології та безпека. - К.:Ін-т спец. зв'язку та захисту інформації Нац. техн. ун-ту України "Київ. політехн. ін-т", 2015. - Том. 3, вип. 2 (5). - С. 117-124.

7. Jie-Hao C. DDoS defense system with test and neural network / C. Jie-Hao, Z. Ming, C. Feng-Jiao, Z. An-Di // Proceedings of the IEEE International Conference on Granular Computing, 2012. - Hangzhou, China. - P. 38-43

8. Shanmugam B. Improved Intrusion Detection System using Fuzzy Logic for Detecting Anamoly and Misuse type of Attacks / B. Shanmugam, N. Idris // Proceedings of the International Conference of Soft Computing and Pattern Recognition, 2009. - Malacca. - P. 212-217.

9. Рубан І.В. Исследование удаленных атак на распределительно вычислительные сети / І.В. Рубан, С.С. Сєров // Системи обробки інформації. - Х.: Харьковский университет Воздушных Сил им. И. Кожедуба, 2013. - Вип. 5 (112). - С. 118-120.

10. FuiFui Wong. A survey of trends in massive ddos attacks and cloud-based mitigations / FuiFui Wong, Cheng Xiang Tan // International Journal of Network Security & Its Applications (IJNSA), 2014. - Vol. 6, No. 3. - P. 57-71

11. Види DDoS-атак та алгоритми виявлення DDoS-атак типу Flood-Attack / Н.В. Багнюк, В.М. Мельник, О.В Клеха, І.А. Невідомський // Науковий журнал "Комп'ютерно-інтегровані технології: освіта, наука, виробництво", 2015. - Луцьк. - Вип. 18. - С. 6-12

Надійшла до редколегії 30.01.2017

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

АНАЛІЗ МЕХАНІЗМУ І НАСЛІДКІВ ВПЛИВУ DDOS-АТАК НА ЕТАЛОННУ МОДЕЛЬ ВЗАЄМОДІЇ ВІДКРИТИХ СИСТЕМ OSI

О.Д. Смоктій, К.В. Смоктій, О.В. Іванченко

У статті розглянуто механізм впливу DDoS-атак на хмарні сервери на прикладному та інфраструктурному рівнях моделі OSI, наведені основні напрямки атак даних рівнів. На кожному з OSI-рівнів проведено аналіз наслідків і вироблені рекомендацій щодо ослаблення впливу DDoS-атак. В роботі наведені дані досліджень основних напрямків атак, мотивації атакуючих і використаних ними технік атак. Зроблено висновки щодо найбільш вразливих для атак зловмисників протоколів передачі даних і найпоширеніших напрямків DDoS-атак.

***Ключові слова**: DDoS-атаки, розподілена відмова в обслуговуванні, модель OSI, атаки прикладного рівня, атаки рівня інфраструктури, SYN-флуд, HTTP-флуд, хмарний сервер.*

ANALYSIS OF MECHANISM AND CONSEQUENCES OF DDOS-ATAKS ON THE STANDARD OPEN SYSTEMS INTERACTION OSI-MODEL

O.D. Smoktii, K.V. Smoktii, O.V. Ivanchenko

The article the DDoS-attacks mechanism on the application and infrastructure levels, gives recommendations for mitigating the effects of DDoS attacks.

The article shows the mechanism of the DDoS attacks impact on cloud servers via the application and infrastructural OSI-model levels, gives the main directions of attacks on these levels. At each of the OSI-levels, an analysis of the consequences and recommendations for DDoS-attacks mitigation are given. The paper presents research data of the main attacks directions, the attackersmotivationand the techniques they are using. The paper consists conclusionsabout the most vulnerable protocols for attacks and the most common directions for DDoS attacks.

***Keywords**: DDoS attacks, distributed denial of service, OSI model, applicationlevel attacks, infrastructure level attacks, SYN flood, HTTP flood, cloud server.*

УДК 004.056

В.Д. Хох, Є.В. Мелешко, О.А. Смірнов

Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ МЕТОДІВ АУДИТУ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

В роботі розглянуто поняття аудиту інформаційної безпеки, його цілі, ініціатори, принципи, фази та методи. Проведено дослідження сучасних методів аудиту систем управління інформаційною безпекою.

Ключові слова: *аудит інформаційної безпеки, системи управління інформаційною безпекою, інформаційна безпека, інформаційні технології, комп'ютерні системи та мережі.*

Вступ

Важко уявити собі сучасний бізнес, який би не підтримувався певною інформаційною системою. Зараз навіть малий бізнес опирається на інформаційні технології, використовуючи їх можливості для комунікації з постачальниками, фінансових транзакцій, ведення фінансової звітності, реклами та багато іншого. Середній та великий бізнес все частіше розгортають особисті інфраструктури, необхідні безпосередньо для здійснення підприємницької діяльності. Наприклад, для взаємозв'язку водіїв таксі з диспетчерами. Зростає ринок Інтернет-магазинів, найбільші з яких віддають перевагу розгортанню своєї інфраструктури серверів, ніж залишатися клієнтами хостинг-компаній.

Разом із збільшенням можливостей до розгортання особистих інформаційних систем: збільшенням доступності їх компонентів та із підвищенням загальної освіченості у галузях інформаційних технологій – зростає і кількість «чуттєвої» інформації, що циркулює Інтернетом або інтранетом певних компаній. Ті ж самі умови призводять і до все більшої розгалуженості інфраструктури систем та їх ускладнення. Контролювати їх стає все складніше, на плечі адміністраторів цих систем лягає все більша кількість обов'язків, і все важче стає відслідковувати джерела нових, потенційних проблем. Процеси управління такими системами та підтримка їх працездатності також ускладнюються.

Метою даної статті є дослідження основних методів проведення аудиту систем управління інформаційною безпекою.

1. Класифікація методів аудиту інформаційної безпеки

Поняття аудиту використовується у багатьох галузях людської діяльності. Розглянемо загальні відомості про процес аудиту, згодом виділивши характерні особливості для процесу аудиту систем управління інформаційною безпекою.

Цілями проведення аудиту можуть бути [1]:

• Визначення ступеня відповідності системи менеджменту об'єкту до критеріїв аудиту.

• Визначення ступенів відповідності видів робіт та процесів методикам системи керування.

• Визначення відповідності нормативним документам та нормам системи керування.

• Визначення ефективності системи керування.

• Визначення шляхів поліпшення системи керування.

Окрім цілей, аудити можливо поділити за сторонами-ініціаторами проведення аудиту. Згідно з міжнародним стандартом ISO 19011:2011 [2] їх три:

• *Аудит першої сторони* – ініціатором проведення аудиту є сама організація.

• *Аудит другої сторони* – ініціатором проведення є партнери організації або зацікавлені у діяльності організації інші організації.

• *Аудит третьої сторони* – ініціатором проведення виступають треті сторони, не задіяні у функціонуванні організації, наприклад, регулюючі органи або органи сертифікації.

У [2] надається визначення: аудит – це систематичний, незалежний та документований процес отримання доказів (свідоцтв) аудиту та об'єктивного їх оцінювання, для визначення ступеня їх відповідності критеріям аудиту. Також у [2] визначаються деякі додаткові терміни, необхідні, на думку авторів, для розуміння цього процесу, а саме:

• *Критерії аудиту* – сукупність політик, методик або вимог, що використовуються як еталон, який порівнюється з свідоцтвами (доказами) аудиту.

• *Свідоцтва аудиту* – протоколи, факти або інша інформація, яка стосується критеріїв аудиту і може бути перевірена.

• *Дані аудиту* – результати оцінки свідоцтв аудиту за критеріями аудиту.

• *Висновок аудиту* – результат аудиту, після розгляду всіх даних аудиту з врахуванням його цілей.

Визначення, що дані у [2] є дуже гнучкими і можуть бути інтерпретовані та адаптовані для тої галузі, де буде організоване проведення аудиту.

Більш специфічні для галузі захисту інформації у комп'ютерних мережах та системах визначення даються у [3]. Тут дається наступне визначення процесу *оцінки інформаційної безпеки* – це процес визначення того, наскільки ефективно сутність, що

оцінюється, відповідає певним вимогам захищеності. І виділяється три типи методів такої оцінки – тестування, експертиза та інтерв'ю.

• *Тестування* – це процес виконання одного або декількох оціночних завдань за певних умов для порівняння очікуваної (заявленої) поведінки оцінюваної сутності з реальною.

• *Експертиза* – це процес перевірки, інспектування, розгляду, спостереження, вивчення або аналізу одного або більше об'єктів оцінки для полегшення розуміння, отримання роз'яснень та доказів.

• *Інтерв'ю* – це процес проведення співбесід задля отримання роз'яснень та відомостей про можливе розташування доказів (свідоцтв) з персоналом або окремими особами організації.

Легко помітити спільне у визначеннях, і хоча [2] використовує термін *аудит*, а [3] *оцінка інформаційної безпеки*, суть процесів полягає у оцінці відповідності об'єкту перевірки до вимог або критеріїв, що визначаються стосовно цього об'єкту. Така ж спільна риса у визначенні присутня і у [4]. Окрім цього [4] визначає п'ять цілей аудиту стосовно безпеки комп'ютерної системи:

1. Забезпечити огляд моделей доступу до окремих об'єктів, історії доступу конкретних процесів і окремих осіб, використання різних механізмів захисту, які підтримуються системою, їх ефективності.

2. Механізм аудиту повинен дозволити виявити спроби обходу механізмів захисту, як зі сторони внутрішніх користувачів системи, так і з боку зовнішніх.

3. Механізм аудиту повинен надавати можливість виявлення підвищення привілеїв користувача.

4. Механізм аудиту повинен діяти як стримуючий фактор проти спроб обійти механізм захисту системи.

5. Механізм аудиту має забезпечувати можливість фіксації діяльності правопорушника.

Окрім вищезгаданого існує серія стандартів ISO27k [5] [6], яка посилається на [2], і є, по-суті, системою управління інформаційною безпекою (СУІБ). В результаті співпраці міжнародного співтовариства, що активно використовує сімейство стандартів ISO27k – була створена директива [7]. У цій директиві, окрім, згаданих визначень з [2], надається визначення *аудиту системи управління інформаційною безпекою*, як аудиту, що орієнтується на системи керування інформаційною безпекою організації. А також виділяються три принципи аудиту, що характерні саме для аудиту СУІБ:

1. Загальні принципи аудиту залишаються важливими як, наприклад, незалежна оцінка відповідно до узгоджених критеріїв, а також більш специфічні принципи, що орієнтовані на аудит СУІБ.

2. Функція аудиту СУІБ не повинна залежати від області її застосування.

3. У розпорядженні аудитора СУІБ повинні бути актуальні дані стосовно організації (штатів, бізнес процесів, технологічних процесів), а також стосовно галузі інформаційної безпеки (наприклад, останні знайдені вразливості ПЗ).

То що ж є методами аудиту СУІБ? В [3] виділяється три методи аудиту – тестування, експертиза та інтерв'ю. В [4], окрім того, що визначається п'ять цілей, також визначаються критерії аудиту до систем класів C2, B2, B3, A1, до яких згідно з [8] повинен застосовуватись процес аудиту за критеріями [4]. Важливо те, що кожен з блоків вимог до кожної з систем поділяється на три розділи:

• події, що повинні бути об'єктами аудиту;

• інформація, яка піддається аудиту;

• підстави, за якими можуть бути обрані події для аудиту.

Це перекликається з методами, вказаними у [3], оскільки завданням тестування є спроба викликати певну подію або певну їх кількість для подальшого вивчення поведінки системи, а у першому розділі вимог вказується, які саме події повинні бути досліджені. Експертиза передбачає дослідження інформації, яка зібрана із системи, що визначається у другому пункті вимог до критеріїв аудиту у [4]. У третьому розділі вказуються підстави, за якими певна подія може бути додана до розгляду в рамках аудиту, а інтерв'ю є методом пошуку додаткових свідоцтв аудиту. У [7] виділяють шість фаз аудиту:

1. *Оцінка* – аудитори визначають основну площину аудиту та його області на основі інтерв'ю з ініціатором аудиту та експертизи документів.

2. *Планування* – загальний обсяг критеріїв аудиту розбивається на більш докладні частини, створюється план аудиту.

3. *Робота на місці* – збір аудиторських свідоцтв шляхом інтерв'ю з персоналом, експертизою документів та проведенням тестів.

4. *Аналіз* – вивчаються свідоцтва, що були зібрані під час роботи на місцях, визначаються можливі прогалини у плані аудиту.

5. *Звітування* – важлива фаза аудиту. Формується звіт, в якому відображається вся необхідна інформація.

6. *Завершення аудиту* – якщо аудит був ініційований третьою стороною, то СУІБ отримує необхідні дозволи та сертифікати. Окрім цього готуються документи з помітками для наступних аудитів.

Отже, як видно з описів кожної з фаз, інструменти, якими оперують аудитори незмінні: методи тестування; методи експертизи; методи інтерв'ю.

Розглянемо детально зазначені методи аудиту СУІБ та способи їх реалізації.

2. Методи тестування

Методи тестування полягають у виконанні одного або декількох оціночних завдань за певних умов, для порівняння очікуваної (заявленої) поведінки оцінюваної сутності з реальною.

Якщо розглядати метод тестування у розрізі [7], то він застосовується лише у третій фазі проведення аудиту – роботі на місці. У [7] метод тестування

пов'язують з суто технічним процесом, завдяки якому визначається правильність конфігурування інформаційних систем відносно політики інформаційної безпеки, стандартів та технічних керівництв. Також, вказується на можливість використання автоматизованих засобів перевірки та виявлення вразливостей системи і конфігурацій, але попереджається про те, що, незважаючи на підвищення швидкості цього процесу, є велика вірогідність того, що у звітах автоматизованих засобів буде і спотворена інформація, що обумовлено помилками у самих засобах.

У [3] тестування СУІБ поділяють на три групи:

• *Перегляд методів (технік).* Ця група тестів зосереджена на оцінці систем, додатків, мереж і процедур для виявлення вразливих місць і, як правило, проводяться вручну. Група включає у себе перегляд документації, лог-записів, набори правил (наприклад, брендмауеру), конфігурацій, сніфінг мережі, а також перевірку цілісності файлів.

• *Ідентифікація та аналіз технік.* Ці методи націлені на визначення систем, портів, сервісів і потенціальних вразливостей, можуть бути проведені вручну, але зазвичай використовуються автоматизовані засоби. Вони включають у себе ідентифікацію мережі, портів, сервісів, сканування на вразливості, сканування бездротової мережі та вразливостей застосунків.

• *Валідація вразливостей.* Ці техніки можуть бути застосовані із залученням автоматизованих засобів чи вручну, в залежності від техніки та рівня спеціалізації тест-команди. Цілями цієї техніки є злам паролів, тести на проникнення, соціальна інженерія та тестування застосунків на вразливості.

Варто зупинитися на останній групі, а саме на тестах на проникнення. Головним завданням тестів на проникнення є визначення вразливостей у контрольованих умовах, для того щоб їх можливо було позбутися до того, як ними скористуються зловмисники. Фахівці використовують тест на проникнення для вирішення проблем, пов'язаних з оцінкою ризиків, зосереджуючись на найнебезпечніших вразливостях [9]. Тестування на проникнення полягає у тому, щоб моделювати поведінку зловмисника, який намагається обійти засоби безпеки організації. Цей метод, зазвичай, включає застосування реальних атак на реальні системи та дані організації з використанням справжніх засобів, що застосовуються зловмисниками. Метод тестування на проникнення передбачає не лише технічні засоби, наприклад, під час тесту може бути прийнята спроба фізично дістатися носіїв даних чи викрасти їх [3]. Тестування на проникнення дає змогу зібрати необхідні для аудиту свідчення відповідності або невідповідності вимогам [10]. Існують три стратегії проведення тесту на проникнення [10]:

• *Чорна скринька.* Стратегія реалізується у випадку, коли у фахівця немає жодної інформації про ціль. В такому випадку він збирає інформацію з чистого листа, і проводяться усі дії та процедури, які б поводив реальний зловмисник.

• *Сіра скринька.* Фахівець має певну інформацію про ціль, але недостатню, що змушує його шукати далі.

• *Біла скринька.* Реалізується, коли фахівцю надають всю необхідну інформацію щодо цілі.

Тест на проникнення складається з трьох фаз: підготовка, тест, аналіз. Під час підготовки визначаються цілі та стратегії, у другій фазі виконується збір інформації про цілі, пошук та аналіз вразливостей, спроби використати вразливості, у випадку якщо вразливість використана вдало, тест переходить у фазу аналізу отриманих даних [9].

Окрім цього у групі з тестуванням на проникнення стоїть *соціальна інженерія*, вона передбачає використання соціальних навичок для отримання паролів, даних про кредитні картки або компромату. Методів соціальної інженерії багато, люди, що їх використовують надзвичайно винахідливі і швидко адаптуються. Цей метод використовує внутрішню природу людей, щоб маніпулювати ними і отримувати конфіденційну інформацію. Було визначено п'ять моделей переконання, які засновані на: простоті, цікавості, розбіжності, впевненості в собі і співпереживанні [11]. Навіть потужні системи безпеки не можуть протистояти цій загрозі, оскільки люди легко «ламаються», що робить їх телефони, комп'ютери, сторінки соціальних мереж легкими цілями, що у подальшому призводить до заражень або встановлення бекдорів у корпоративних мережах. Серед засобів протидії методам соціальної інженерії є поліпшення обізнаності робітників організації та їх підготовка в рамках інформаційної безпеки. А також формування грамотної політики безпеки, що робить методи експертизи та інтерв'ю не менш важливими, ніж методи тестування [12].

3. Методи експертизи

Методи експертизи полягають у перевірці, інспектуванні, розгляді, спостереженні, вивченні або аналізі одного чи більше об'єктів оцінки. Якщо завдяки методам інтерв'ю аудитор отримує дані про можливе існування свідоцтв аудиту від персоналу організації, а завдяки тестуванню перевіряє наявність свідоцтв – то метод експертизи дозволяє отримати інформацію про існування свідоцтв аудиту, найчастіше шляхом вивчення документації організації. Більш того, вивчення документації організації може вносити серйозні корективи у цілі аудиту. Одним з найважливіших документів організації, стосовно інформаційної безпеки, є документ політики безпеки.

Зазвичай, організація, що зацікавлена у забезпеченні інформаційної безпеки своєї інфраструктури, визначає вимоги до її забезпечення у документі політики безпеки організації. У цьому ж документі може визначатись і порядок проведення аудитів. Добре розроблена політика безпеки визначає, що необхідно зробити для забезпечення безпеки інформації організації і які заходи для цього необхідні. Політика також може складатися з документів високого рівня та до-

кументів низького, які визначають більш детально певні аспекти забезпечення безпеки інформації організації [14].

Згідно з ISO/IEC 27002:2005 [6] політика інформаційної безпеки повинна переглядатись у заплановані терміни або за появи істотних змін з метою забезпечення її актуальності. При розробці політики інформаційної безпеки необхідно враховувати не лише інтереси організації, а й інші нормативні документи та закони країни, в якій вона функціонує. Також у ній повинні бути відображені інциденти інформаційної безпеки, рекомендації уповноважених організацій і, звісно ж, – результати минулих аудитів.

Згідно з ISO/IEC 27001:2005 [5] документація організації повинна містити записи управлінських рішень. Дані документації повинні бути відтворювані та відображати зворотній зв'язок, тобто обрані заходи проаналізовано з точки зору результатів оцінки і процесу обробки ризиків. Також [5] визначає, які саме записи повинні бути у документації:

- Законодавчі положення щодо політики та цілей СУІБ.
- Визначення сфери застосування.
- Перелік процедур та заходів безпеки, що підтримується системою.
- Опис методології оцінки ризиків.
- Звіт та план оцінки ризиків.
- Положення щодо застосовності.
- Процедури, що необхідні для ефективного планування і контролю процесів СУІБ, а також опис вимірювання ефективності заходів безпеки.

У [7] процес вивчення документації, у тому числі політики безпеки, відноситься до першої фази – оцінювання, під час якої аудитори визначають основну площину аудиту та його області. Також процес експертизи документації згадується як типовий процес для першої частини фази роботи на місці.

Окрім вищезгаданих документів, організація може розробити правила безпечної роботи [13]. Це документ, в якому зібрані всі необхідні користувачам правила. Він складається з фрагментів правил всієї організації і відображає обов'язки користувачів у галузі інформаційної безпеки. Правила безпечної роботи повинені бути чіткими і короткими, а сам документ, в ідеалі, складатися з декількох сторінок.

У [8] для деяких систем передбачаються чіткі керівництва щодо того що, як, ким і коли повинно бути задокументовано. Такі дані мають велику цінність для аудиторів у тому числі і тому що це дозволяє проводити аудит певного проміжку часу. Окрім цього, такий підхід до ведення документації дозволяє частково автоматизувати процес аудиту [15], [16]. У спеціальній публікації NIST [4] були внесені зміни щодо інформації, яка підлягає аудиту.

Окрім цього, метод експертизи може бути застосовано відносно лог-записів. Лог-записи можливо поділити на дві групи: лог-записи систем безпеки та записи операційної безпеки. Лог-записи можуть зберігати широкий спектр різноманітної інформації про події. В рамках аудиту лог-записи використовуються як додатковий матеріал [17].

4. Методи інтерв'ю

Завданням методів інтерв'ю є збір інформації про можливе розташування свідоцтв аудиту, роз'яснення певної поведінки системи, роз'яснення щодо процесів організації шляхом опитування персоналу організації.

Інформаційна безпека – це не лише питання технологій та процесів, вона пов'язана і з людьми, і тому не можна автоматизувати кожен її аспект [18]. Варто зауважити, що найчастіше спеціалісти з інформаційної безпеки вказують на персонал як на найслабкішу ланку в інформаційній безпеці.

У [2] наголошується на необхідності проведення наради на самому початку проведення аудиту, обов'язково з головуванням лідера групи аудиту (якщо аудит проводить група). На цій нараді, бажана, якщо вона доцільна, присутність всіх або певної частини персоналу, який відповідає за об'єкти організації, що проходять аудит або частково залучені у проведенні аудиту. Нараду слід проводити за присутності керівництва організації. Необхідно надати можливість задавати питання учасникам наради. Під час фази збору даних група аудиту повинна розглядати інформацію, яка отримана шляхом інтерв'ю, з такої позиції, що враховуватись повинна лише та інформація, яку точно можливо перевірити. У ISO/IEC 27001:2005 [5] в розділі про відповідальність керівництва зазначається, що організація повинна забезпечити, щоб весь персонал, для якого встановлено визначені в СУІБ відповідальності, був компетентним для виконання необхідних завдань. Така вимога, що визначена у стандарті, сама по собі може стати об'єктом аудиту, а у випадку, якщо компанія приймає відповідний стандарт або країна, в якій функціонує організація прийняла цей стандарт як державний, то аудит третьої сторони обов'язково буде включати перевірку компетентності персоналу, для отримання відповідних сертифікатів або дозволів з боку регулюючих органів.

У [4] пропонується розділити персонал, який залучено у користуванні СУІБ, на дві категорії – системні адміністратори та користувачі. До того ж, у разі проведення внутрішніх аудитів або у випадку, коли аудит має постійний характер – у ролі аудитору виступає сам системний адміністратор. В такому випадку завданням інтерв'ю буде збір даних про використання системи, роз'яснень щодо певних подій та певної діяльності користувачів у системі.

У [19] розглядається п'ять категорій персоналу – старший, керування СУІБ, програмні та функціональні менеджери, постачальники технологій, користувачі. Кожній з категорій відповідає своя роль у системі безпеки та свої обов'язки. Тут же звертається увага на небезпеку з боку "ображених" співробітників та комерційного шпіонажу. Виявити потенційну загрозу такого роду можливо, якщо компанія постійно веде внутрішній аудит.

Висновки

В процесі вивчення документів [2, 5-8], стає зрозумілим, що незалежно від різної термінології, яка в них використовується, основна мета аудиту СУІБ – систематичне та якомога більш повне визначення актуального стану СУІБ та його відповідності вимогам. Для досягнення цієї мети використовуються різноманітні методи, їх можна розділити на три групи – методи тестування, експертизи та інтерв'ю. Методи інтерв'ю охоплюють область, яка стосується персоналу організації і дозволяють визначити рівень кваліфікації персоналу та отримати додаткову інформацію, яка може бути критично важливою для процесу аудиту. Методи експертизи дозволяють сформувати загальну картину стану СУІБ, знайти критично важливі вузли системи. Методи тестування дозволяють ефективно перевірити адекватність системи, здатність її працювати як в рамках штатного режиму, так і в режимі атак. Методи тестування дають змогу визначити прогалини у СУІБ, про які не було зазначено в документації, а персонал про них міг і не здогадуватись. Така класифікація методів аудиту дає змогу більш чітко визначати ті роботи, які необхідно провести в рамках певного аудиту. До того ж такий підхід до класифікації методів аудиту дає змогу розглядати способи автоматизації процесу аудиту системи управління інформаційною безпекою, визначити джерела інформації для системи автоматизації та джерела зворотного зв'язку, а також області впливу системи автоматизації.

Список літератури

1. Teck-Heang L. The evolution of auditing: An analysis of the historical development / L. Teck-Heang, A. Azham. // Journal of Modern Acc. and Auditing. – 2008. – №12. – P. 1-8.

2. ISO 19011:2011 Guidelines for auditing management systems (Міжнародний стандарт)

3. Scarfone K. Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-115) / K. Scarfone, M. Souppaya, A. Cody, A. Orebaugh. – Gaithensburg: NIST, 2008. – 80 p.

4. A Guide to Understanding Audit in Trusted Systems – Fort Feorge G. Meade: Nat. comp. security center, 1987.– 25 p.

5. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements (Міжнародний стандарт).

6. ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management (Міжнародний стандарт)

7. ISMS Auditing Guideline // ISO27k Forum. – 2008. – №1. [Електр. ресурс]. – Режим доступу: http:// www.iso 27001security.com/ISO27k_Guideline_on_ISMS_audit_v1.docx.

8. Trusted computer system evaluation criteria, 1985. – (Department of defense standard).

9. Bacudio A. An overview of penetration testing / A. Bacudio, Y. Xiaohon, C. Bei-Tseng. // Int. Journal of Network Security & Its Appl. (IJNSA). – 2011. – №6. – P. 19-38.

10. Tewai A. Evaluation and Taxonomy of Penetration Testing / A. Tewai, K. M. Arun. // International Journal on Recent and Innovation Trends in Computing and Communication. – 2015. – №3. – P. 5297-5302.

11. Greavu-Şerban V. Social Engineering a General Approach / V. Greavu-ŞErban, O. Şerban. // Informatica Economică. – 2014. – №18. – P. 5-14.

12. Conteh N.Y. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks / N.Y. Conteh, P.J. Schmick. // International Journal of Advanced Computer Research. – 2016. – №6. – P. 31-38.

13. Бармен С. Разработка правил информационной безопасности / Скотт Бармен // М.: Издательский дом "Вильямс", 2002. – 208 с.

14. Tuyikeze T. An Information Security Policy Development Life Cycle / T. Tuyikeze, D. Pottas. // Proceedings of the South African Information Security. – 2010. – P. 165-176.

15. Tsudik G. AudES – An Expert System for Security Auditing / G. Tsudik, R. Summers. // IAAI-90 Proceedings. – 1990. – P. 221-232.

16. Sodiya A. S. An Expert System-based Site Security Officer / A. S. Sodiya, O. Adeniran, R. Ikuomola. // Journal of Computing and Information Technology – CIT. – 2007. – №15. – P. 227-235.

17. Karen K. Guide to Computer Security Log Management / K. Karen, M. Souppaya. // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. – 2006.

18. Montesino R. Information security automation: how far can we go? / R. Montesino, S. Fenz. // Sixth Int. Conf. on Availability, Reliability and Security. – 2011. – P. 280-285.

19. Guttman B. An Introduction to Computer Security: The NIST Handbook / B. Guttman, R. A. Edward. – Gaithersburg, MD 20899-0001: National Institute of Standards and Technology, 1995. – (U.S. Government printing office).

Надійшла до редколегії 30.01.2017

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

ИССЛЕДОВАНИЕ МЕТОДОВ АУДИТА СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

В.Д. Хох, Е.В. Мелешко, А.А. Смирнов

В работе рассмотрено понятие аудита информационной безопасности, его цели, инициаторы, принципы, фазы и методы. Проведено исследование современных методов аудита систем управления информационной безопасностью.

Ключевые слова: *аудит информационной безопасности, системы управления информационной безопасностью, информационная безопасность, информационные технологии, компьютерные системы и сети.*

RESEARCH OF METHODS OF AUDITING INFORMATION SECURITY MANAGEMENT SYSTEMS

V.D. Khokh, E.V. Meleshko, O.A. Smirnov

In this paper we considered the concept of information security audit, its objectives, initiators, principles, phases and methods. Modern methods of auditing information security management systems were researched.

Keywords: *information security audit, information security management system, information security, information technology, computer systems and networks.*

УДК 651. 34

Г.Г. Швачич, С.Г. Семенов, М.И. Главчев, Кассем Халифе

Национальный технический университет «ХПИ», Харьков

МОДЕЛЬ РАСЧЕТА ВРЕМЕННЫХ ГРАНИЦ ПРОЕКТОВ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В статье обозначена необходимость прогнозирования временных затрат на разработку программного обеспечения (ПО) и представлена обобщенная математическая модель для расчета временных границ проектов. С целью прогнозирования разработан комплекс математических моделей основных этапов разработки программного обеспечения. Разработана математическая модель этапа инициализации процесса разработки ПО, основанная на концептуальных положениях Agile, что позволило выделить ряд наиболее важных параметров оценки временных затрат инициализации и определить их зависимости от качественных характеристик участников проекта. Усовершенствована математическая модель этапа реализации функционала ПО, отличающаяся от известных учетом показателей безопасного программирования.

Ключевые слова: *безопасное программирование, временные затраты на разработку ПО, SCRUM, Agile.*

Введение

Постановка проблемы. Проведенные исследования показали, что в настоящее время существует несколько наиболее популярных методологий разработки ПО. Среди них целесообразно выделить семейство «гибких» методологий Agile (XP, SCRUM) и методологии «бережного производства» (Kanban). Следует заметить, что в литературе [1, 4-7] и такие методологии зачастую относят к разряду «гибких». У каждой из них есть свои особенности, которые стоит учитывать, выбирая ту или иную методологию для управления проектом.

Кроме того для успешного управления процессом разработки программного обеспечения бывает недостаточно выбрать ту или иную методологию и следовать ей на протяжении всего процесса. В случае достаточно большого проекта, разработка которого ведется достаточно долгий период времени, важной может оказаться способность быстро адаптировать используемую в данный момент методологию в соответствии с изменяющимися обстоятельствами, то есть по существу синтезировать различные варианты использования «гибких» и «бережных» методологий в один проект.

Таким образом, в настоящее время вопросы, связанные с оптимизацией процесса разработки ПО, несмотря на многообразие «гибких» методологий управления, остаются актуальными.

Анализ литературы [4-7] показал, что одним из первых этапов процесса разработки ПО является этап планирования. На данном этапе команда решает, как она будет достигать цели, поставленной на предыдущем этапе. Этот этап часто разделяется на два этапа – верхнеуровневое планирование и детальное планирование. На верхнем уровне определяются общие моменты исполнения проекта. Именно на этом этапе должны выполняться задачи прогнозирования временных затрат на выполнение работ. Результатами данного прогноза должны стать данные о сроках выполнения (окончания) различных этапов (заданий) в рамках отдельного проекта (время необходимое на разработку и уточнение документации, кодирование, тестирование, верификации и др.). Затем проводится детальное планирование, на котором составляются финальные планы реализации проекта, и проводится корректировка стратегического плана в зависимости от возможно изменяющихся обстоятельств.

Проведенные исследования, а так же анализ литературы [2, 3] показали, что в настоящее время на практике для решения этих задач практически не используются современные методы интерполяции и экстраполяции. Существующие методики расчёта предлагают только грубые оценки, а необходимые для выполнения задач ресурсы определяются исключительно на основе опыта и субъективного мнения людей, выступающих в роли экспертов, далеко не всегда являющихся специалистами в данной области. Кроме того при описании методологии «бережного производства» (Kanban) это зачастую приводит к неудовлетворительной точности полученных результатов оценки сроков выполнения (окончания) различных этапов в рамках проекта разработки ПО.

Одним из путей решения поставленной задачи прогнозирования является использование подхода, основанного на оценке временных затрат на отдельные этапы разработки ПО, с учетом функций зависимости текущего числа активных дефектов приложения от времени, полученных экспериментальным путём а так же с помощью математического моделирования. Такое комплексное использование априорных и апостериорных данных должно позволить учесть специфику современных методик разработки

ПО с возможным динамическим изменением (расширением) рамок проекта по желанию заказчика либо по иным причинам.

Модель для расчета временных границ проектов разработки ПО

Анализ перечисленных выше методологий разработки программного обеспечения показал, что в практически каждом проекте можно выделить три обязательных этапа: инициация, реализация функционала и тестирование. Работы, выполняемые на первых двух этапах, структурированы и представляют собой совокупность действий «мозговых штурмов» A1, A2 и т.д., на которых определяется что же должен представлять из себя продукт проекта и реализацию функционала B (реализация подзадачи B1 и т.д.).

Для математической формализации первого этапа разработки ПО воспользуемся следующими допущениями.

Пусть $A = \bigcup_{i=1}^{N} A_i$ – множество характеристик вопросов, вынесенных на рассмотрение в процессе «митинга», где N – количество вопросов, которые рассматриваются. $A_i = \langle a_i, b_i, n_i \rangle$ – кортеж общих характеристик, где a_i – время, отведенное докладчику i – го вопроса, b_i – время, отведенное на обсуждение i – го вопроса, n_i – количество участников «митинга», участвующих в обсуждении i -го вопроса.

Пусть $\tilde{a}_i, \tilde{b}_i$ – случайные величины, имеющие распределения Q_{a_i}, Q_{b_i} соответственно. При этом Q_{a_i} имеет усеченное экспоненциальное распределение с матожиданием $m[\tilde{a}_i] = a_i + \Delta t_i$, где Δt_i – отклонение времени выступления докладчика при обсуждении i – го вопроса. (обобщенный пример-иллюстрация усеченного экспоненциального распределения представлен на рис. 1). Также следует заметить, что характеристика Q_{b_i} это сумма распределений $Q_{b_{ij}}$, где j – номер выступления при обсуждении вопроса i. Учтем, что $n_i > \tilde{n}_i$ – количественный состав группы разработки ПО, принявших участие в обсуждении вопросов.

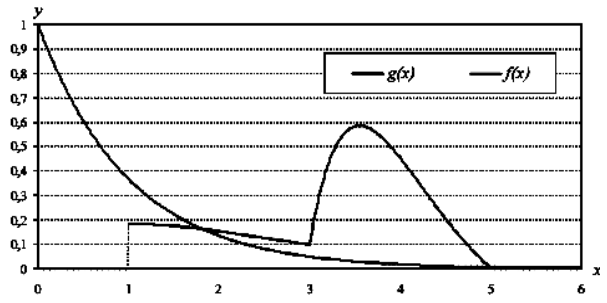


Рис. 1. Пример-иллюстрация усеченного экспоненциального распределения

Проведенные исследования показали, что распределение $Q_{b_{ij}}$ можно аппроксимировать усеченным экспоненциальным распределением с математическим ожиданием $m[\tilde{b}_{ij}] = b_i/\tilde{n}_i + \Delta t_{ij}$, где Δt_{ij} – отклонение времени обсуждения i -го вопроса j -м участником обсуждения. Следует заметить, что при увеличении $\tilde{n}_i$ или Δt_{ij} распределение Q_{b_i} приближается к усеченному нормальному (обобщенный пример-иллюстрация усеченного нормального распределения представлен на рис. 2). Учитывая линейные особенности математического ожидания, можно рассчитать математическое ожидание общих характеристик времени, необходимого для проведения «митингов» без определения его распределения.

$$M[T] = \sum_{i=1}^{N}\left(a_i + \Delta t_i + \sum_{j=1}^{\tilde{n}i}\left(\frac{b_i}{\tilde{n}_i} + \Delta t_{ij}\right)\right). \qquad (1)$$

Используем предложенные математические допущения для предварительных расчётов на этапах инициации, реализации функционала и разработаем комплекс математических моделей описывающих указанные этапы разработки ПО.

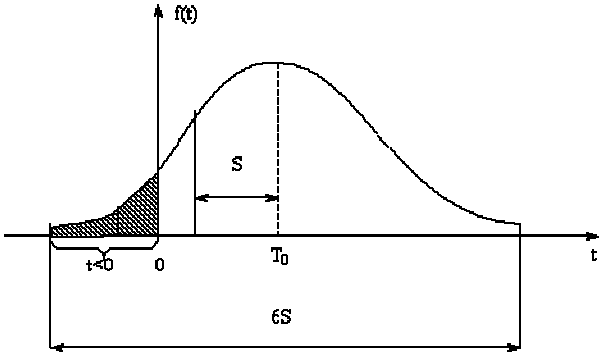


Рис. 2. Пример-иллюстрация усеченного нормального распределения

2. Комплекс математических моделей этапов инициации, реализации функционала ПО

2.1. Математическая модель этапа инициализации процесса разработки ПО

Из литературы [4 – 7], описывающей процесс управления разработкой ПО известно, что в настоящее время в гибких методологиях используются ряд положений, суть которых зафиксирована в манифесте Agile, и которые кратко можно сформулировать следующим образом:

– разработка ведется короткими циклами (итерациями), продолжительностью 1-4 недели;

– в конце каждой итерации заказчик получает ценное для него приложение (или его часть), которое можно использовать в бизнесе;

– команда разработки сотрудничает с Заказчиком в ходе всего проекта;

– изменения в проекте приветствуются и быстро включаются в работу.

Анализ примеров практической реализации гибких методологий позволил определить, что этап инициализации процесса разработки ПО в соответствии представленными положениями включает в себя ряд мероприятий (митингов), имеющих различные тактические и стратегические цели. Например, Daily meetings (Ежедневный контроль). Daily meetings, иначе называемый Stand-up Meeting проводится каждый день. На этом мероприятии каждый член команды должен отчитаться о проделанной работе в течении прошлого дня, наметить план работы на день и решить, существующие к остальным участникам «митинга», вопросы. Продолжительность такого мероприятия должна быть не более 15 минут. При этом за регламент «митинга» следит Scrum-мастер.

С точки зрения временной оптимизации этого процесса существенных «выигрышей» добиться сложно, поскольку данное мероприятие не занимает существенного рабочего времени.

В то же время еще одним подобным мероприятием в гибких методологиях является «retrospective meeting» (Ретроспективное совещание). Именно эти мероприятия занимают значительное время, и могут быть неэффективными при несоблюдении регламента, методологий проведения мероприятия, низкого профессионального уровня участников и других факторов. Рассмотрим более подробно данный процесс и математически формализуем его.

Для математической формализации первого этапа предлагается воспользоваться 4 параметрами оценки временных затрат: длительностью первоначальной коллективной оценки сложности проекта $T_{оц}$, временными затратами на отчет о проделанной работе с момента предыдущего SCRUM-митинга $T_{от}$, временными затратами на обсуждение проблем, возникших во время работы $T_{об}$, время на постановку задач до следующего митинга $T_{пост}$.

Тогда время инициации $T_{и}$ можно описать как:

$$T_{и} = T_{оц} + T_{от} + T_{об} + T_{пост}. \qquad (2)$$

При этом указанные временные затраты зависят от ряда объективных и субъективных факторов. В целом, используя математические допущения и выражение (1), эти показатели можно описать следующим образом.

Одним из наиболее важных и детально описанных процессов в Scrum, является процесс планирования «спринта», промежутка времени в течении которого выполняется работа над продуктом. Длительность первоначальной коллективной оценки сложности проекта $T_{оц}$ зависит во многом от методики оценки, числа участников SCRUM-митинга, их профессиональной подготовки и коммуникативности, что существенно влияет на количество разногласий и спорных моментов при оценке сложности проекта.

Рассмотрим одну из наиболее популярных методик планирования и оценки сложности проекта – покер планирования (англ. Planning Poker, а также англ. Scrum poker). Это методика оценки проектов при разработке программного обеспечения, главной целью которой является достижение договорённости, относительно сложности предстоящей работы или объёма решаемых задач [6].

Анализ данной методики показал, что среднее время первоначальной коллективной оценки сложности проекта можно описать как

$$T_{оц} = \sum_{g=1}^{n_{итт_g}} \left(\frac{t_{итт_g}}{n_{итт_g}} + \Delta t_g + \sum_{j=1}^{\hat{n}_g} \left(a_{g_j} + \Delta t_j \right) \right), \qquad (3)$$

где $t_{итт_g}$ – время, необходимое на проведение g-й итерации оценки сложности проекта; $n_{итт_g}$ – число итераций, необходимое для достижения консенсуса; Δt_g – отклонение времени проведения g-й итерации оценки сложности проекта; a_{g_j} – время, отведенное участникам с высокими и низкими оценками сложности проекта на g-й итерации; Δt_j – отклонение времени высказывания участников обсуждения в g-й итерации при обосновании своей оценки; $\hat{n}_g$ – число участников с высокими и низкими оценками сложности проекта на g-й итерации.

Следует заметить, что время Δt_g чаще всего не велико и существенно не влияет на общее время оценки сложности проекта. Связано это с тем, что это показатель во многом зависит от квалификации только одного участника – модератора, который следит за временем проведения итерации. Однако уровень профессиональной подготовки и коммуникативности остальных участников SCRUM-митинга существенно влияет на показатель Δt_{ij}, который в свою очередь может изменяться в большом диапазоне. Исходя из этого, данный показатель определим следующим образом.

$$\Delta t_j = v \cdot e^{-k \cdot c \cdot \hat{n}_g}, \qquad (4)$$

где k – коэффициент, характеризующий средний уровень профессиональной подготовки участников SCRUM-митинга (варьируется от 0,1 до 0,3); c – коэффициент, характеризующий средний уровень коммуникативности участников SCRUM-митинга (варьируется от 1 до 3); v – усредненный коэффициент сложности решаемой обобщенной задачи.

Для учета временных затрат на отчет о проделанной работе с момента предыдущего SCRUM-митинга $T_{от}$ воспользуемся мнениями экспертов, которые определяют, что чаще всего этот показатель ограничивается регламентом, устанавливаемым

модератором. Поэтому в математической модели этапа инициализации процесса разработки ПО его можно принять за константу, при этом используя практические данные фирм-разработчиков ПО.

Проведенные исследования показали, что для определения затрат на обсуждение проблем, возникших во время работы $T_{об}$ можно воспользоваться положениями, описанными выше (выражение (1)). Тогда среднее время на обсуждение проблем, возникших во время работы, формализуем следующим выражением.

$$T_{об} = \sum_{i=1}^{\breve{N}} \left(a_i + \Delta t_i + \sum_{j=1}^{\breve{n}_i} \left(\frac{b_i}{\breve{n}_i} + \Delta t_{ij} \right) \right), \qquad (5)$$

где $\breve{N}$ – количество проблем, возникших во время работы, и вынесенных на обсуждение в SCRUM-митинге; $\breve{n}_i$ – количество участников обсуждения озвученных проблем.

Несложно заметить, что сокращение временных затрат на обсуждение проблем напрямую связано с временными показателями Δt_i и Δt_{ij}, которые соответственно зависят от профессиональной подготовки участников команды разработчиков и их числа. Проведенные исследования показали, что эти характеристики можно описать таким образом:

$$\Delta t_i = z1 \times e^{-\left(k/\breve{N}\right)}, \qquad (6)$$

$$\Delta t_{ij} = z2 \times e^{-\left(k \cdot \breve{n}_i\right)}, \qquad (7)$$

где z1 и z2 – усредненные коэффициенты сложности проблем обсуждения и управления участниками обсуждения соответственно.

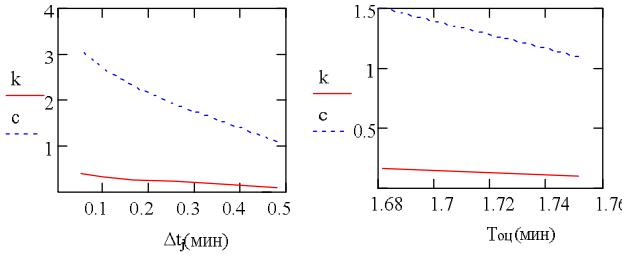
Как указано в начале подраздела еще одним показателем, входящим в общее аналитическое выражение для расчета среднего времени инициализации процесса разработки ПО, является время на постановку задач до следующего митинга $T_{пост}$. Для расчета данного показателя также как и в предыдущем случае воспользуемся выражением 1. Тогда время $T_{пост}$ равно:

$$T_{пост} = \sum_{i=1}^{\breve{\breve{N}}} \left(\breve{\breve{a}}_i + \breve{\Delta t}_i \right), \qquad (8)$$

где $\breve{\breve{N}}$, $\breve{\breve{a}}_i$ – количество задач и время, отведенное на поставку i-й задачи до следующего SCRUM-митинга соответственно, $\breve{\Delta t}_i = \exp\left(-\breve{\breve{N}}/r\right)$ – отклонение времени на поставку i-й задачи до следующего SCRUM-митинга, r – усредненный коэффициент сложности задач ($r = \{2,3,\ldots 45\}$).

Проведем исследования степени влияния, приведенных в подразделе характеристик, на общее время проведения SCRUM-митинга. На рис. 3, а приведены кривые графиков зависимости отклонения Δt_{ij} времени высказывания участников обсуждения в g-й итерации при обосновании своей оценки от коэффициента k, характеризующего средний уровень профессиональной подготовки участников SCRUM-митинга и коэффициента c, характеризующего средний уровень коммуникативности участников SCRUM-митинга, в условиях когда $v = 0,6$, $\hat{n}_g = 2$. Как видно из этих графиков коэффициенты существенно (до 2,5 раз) увеличивают время Δt_{ij}.

На рис. 3, б приведены кривые графиков зависимости длительности $T_{оц}$ первоначальной коллективной оценки сложности проекта от от коэффициента k, характеризующего средний уровень профессиональной подготовки участников SCRUM-митинга и коэффициента c, характеризующего средний уровень коммуникативности участников SCRUM-митинга, в условиях когда $v = 0,6$, $\hat{n}_g = 2$, $t_{итт_g} = \{0,5\ldots 1\}$ мин., $n_{итт_g} = 6$, $\Delta t_g = 0,1$ мин., $a_{g_j} = \{0,1\ldots 0,22\}$ мин.

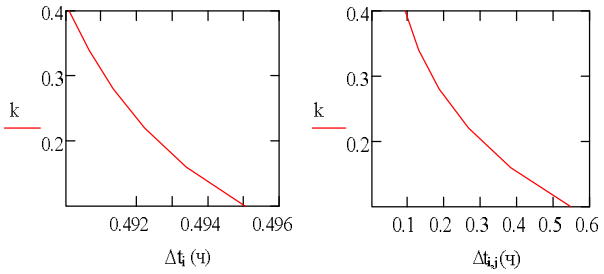


а б

Рис. 3. Графики зависимости отклонения Δt_{ij} от коэффициентов k и c

Как видно из приведенных на рис. 3.3.б графиков улучшение показателя среднего уровня коммуникативности участников SCRUM-митинга в 1,1 раза (до 10 минут в одном часе) уменьшит время первоначальной коллективной оценки сложности проекта. Следует заметить, что приблизительно аналогичных результатов можно добиться при повышении уровня профессиональной подготовки участников SCRUM-митинга.

Проведем исследования модели процесса обсуждения проблем, возникших во время работы. На графиках рис. 4 приведены кривые зависимости временных показателей Δt_i и Δt_{ij} от коэффициента, характеризующий средний уровень профессиональной подготовки участников SCRUM-митинга, в условиях, когда $a_i = \{20,30,\ldots,70\}$ с, $b_i = \{10,20,\ldots,60\}$ с, $\breve{n}_i = 6$. Как видно из этих графиков повышение коэффициент k профессиональной подготовки в 4 раза приблизительно в 1,013 раз (приблизительно 36 с.) уменьшает время Δt_i, и в 6 раз уменьшает время Δt_{ij} (приблизительно 3,5 минуты).



а б

Рис. 4. Графики зависимости временных показателей Δt_i и Δt_{ij} от коэффициента k

Заметим, что в целом повышение уровня профессиональной подготовки участников проекта уменьшает время, необходимое на обсуждение проблем, до 4 минут (в зависимости от входных данных), что наглядно иллюстрирует график рис. 5.

Так на рис. 5 приведена кривая графика зависимости времени обсуждения проблем, возникших во время работы $T_{об}$ от коэффициента k в условиях, когда $\sum_{i=1}^{\breve{N}}(a_i) = 2$ мин., и $\sum_{i=1}^{\breve{N}} \frac{b_i}{\breve{n}_i} = 1$ мин.

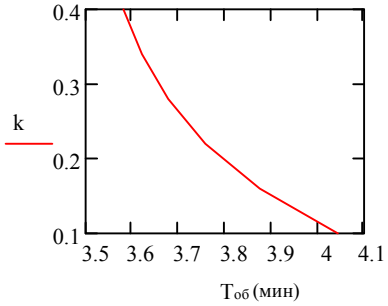


Рис. 5. График зависимости $T_{об}$ от коэффициента k

Исследуем взаимовлияние показателей, используемых в аналитическом выражении для расчета времени на постановку задач до следующего митинга $T_{пост}$. На рис. 6 приведен график зависимости отклонения времени $\Delta\overset{=}{t}_i$ на поставку i-й задачи до следующего SCRUM-митинга от усредненного коэффициента сложности задач r, выполненный при условии, что $\overset{=}{N}$ – количество задач до следующего SCRUM-митинга равно 6.

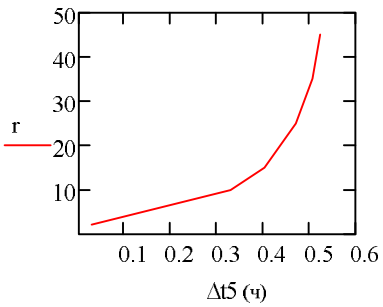


Рис. 6. Зависимость отклонения времени $\Delta\overset{=}{t}_i$ от усредненного коэффициента сложности задач r

Данный график наглядно иллюстрирует, что увеличение усредненного коэффициента сложности задач в 4 раза приводит к увеличению отклонения времени в 1,5 раз. Следует заметить, что в соответствии с выражением 3.8. можно наблюдать аналогичную зависимость времени на постановку задач до следующего митинга $T_{пост}$ от коэффициента сложности задач.

Оценим степень влияния коэффициентов k и c на общее время SCRUM-митинга. На рис. 7 представлен график зависимости времени инициации разработки ПО $T_и$ от показателей k и c в условиях когда временные затраты на отчет о проделанной работе с момента предыдущего SCRUM-митинга $T_{от}$ =50мин, $a_i = \{20,30,\ldots,70\}$ c, $b_i = \{10,20,\ldots,60\}$ c, $\breve{n}_i = 6$, $\overset{=}{N}$ =6, $v = 0,6$, $\hat{n}_g = 2$.

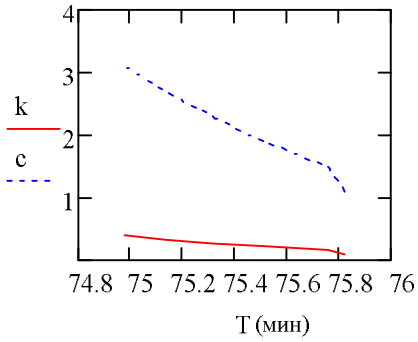


Рис. 7. График зависимости времени $T_и$ от показателей k и c

Как видно из этого графика повышение коэффициентов k и c в указанных выше размерах уменьшает время проведения этапа инициализации процесса разработки ПО (по графику на минуту).

Следует заметить, что представленные результаты имеют больше качественный характер. Это вызвано тем, что величины Δt_j, $\Delta\overset{=}{t}_i$, Δt_i, а так же $\Delta t_{i,j}$ могут иметь как положительное, так и отрицательное значение. Кроме того выбранные эмпирическим путем значения коэффициентов имеют скорее качественный чем количественный характер, и могут варьироваться в зависимости от определенной экспертной оценки. Кроме того, при моделировании не учитывалось, что в командах в настоящее время не задействуются специалисты безопасного программирования и тестирования безопасности. А это в свою очередь существенно снижает средний уровень подготовки участников команды, и соответственно коэффициент k может быть существенно ниже (меньше 0,01) указанного в работе диапазона значений.

Следующим этапом после инициализации является этап реализации функционала ПО. Разработаем модель, формализующую данный этап.

2.2. Математическая модель этапа реализации функционала ПО

Проведенные анализ литературы [3-7] и исследования показали, что в настоящее время существует ряд подходов к математической формализации этапа реализации функционала ПО. В абсолютном большинстве эти модели подразумевают простейший вариант – линейную оценку времени, необходимого для реализации проекта. С одной стороны это упрощает модель, а с другой стороны дает возможность внесения изменений (уточнений) в случае возникновения дополнительных факторов, влияющих на точность результатов моделирования.

В качестве основы воспользуемся подходом, описанным в работе [3], где модель оценки временных затрат на реализацию функционала ПО предлагается ограничить тремя параметрами: сложностью выполнения, важностью точности вычислений и новизной. Однако, как было указано в предыдущем разделе пренебрежение фактором безопасности ПО в значительной степени ухудшает его качество. Поэтому, большинство фирм-разработчиков ПО для учета фактора безопасности выделяют дополнительные ресурсы и силы. Исходя из этого усовершенствуем математическую модель этапа реализации функционала ПО, путем учета фактора безопасного кодирования ПО. В этом случае время необходимое на реализацию функционала ПО можно представить в виде выражения:

$$T_{реал} = K_{рез} \times \times \sum_{\ell} \left(K_{слож} D + K_{важн} П_{важн} + K_{нов} П_{нов} + K_{без} G \right), \quad (9)$$

где $K_{рез}$ – коэффициент резервного времени, связанный с учетом различных рисков проекта, среднего времени задержки выполнения задач в команде. В идеальном случае он может быть принят за 1, но на практике изменяется в пределах от 1,3 до 1,5; $K_{слож}$ – коэффициент сложности задачи; D – сложность задачи, выраженная в человеко-часах; $K_{важн}$; $П_{важн}$ – коэффициент и параметр важности точности вычислений. В любых программах, в частности, ориентированных на финансовые операции, чрезвычайную важность приобретает точность вычислений. Известен случай, когда из-за возможной ошибки в одном из младших разрядов при вычислениях с плавающей точкой компания Intel проводила кампанию по отзыву своих процессоров; $K_{нов} П_{нов}$ – коэффициент и параметр новизны решения; $K_{без} G$ – коэффициент и параметр безопасности ПО. Коэффициент безопасности определяется уполномоченной организацией, проводящей тестирование ПО на безопасность, а параметр безопасности определяется временем на реализацию функциональности, соответствующим требованиям грифа секретности ПО; ℓ – число требований к системе.

Следует заметить, что число факторов и степень их влияния на проект не являются жестко заданными, однако для конкретного проекта могут быть выведены аналитически. Данные факторы можно как априорно так и апостериорно закладывать в параметры сложности задачи или новизны решения. Например, время добавления в проект дополнительных идентичных SQL-запросов линейно зависит от числа запросов (повышается сложность), а необходимость изучения ранее не применявшейся технологии в ходе выполнения проекта (в том числе и правил безопасного кодирования) может привести к экспоненциальному росту времени выполнения поставленной задачи.

Оценим показатель времени необходимого на реализацию функционала ПО в соответствии с выражением (9). На рис. 8 представлен график зависимости времени реализации функционала ПО $T_{реал}$ от коэффициента резервного времени $K_{рез}$, полученный при условии, что $K_{слож}$ варьируется от 2 до 45, D – сложность задачи равна $D = \{40, 45, \ldots, 65\}$ чел-час, $K_{важн} = \{1, 2, \ldots 6\}$, $П_{важн} = \{2, 4, \ldots, 12\}$ чел-час, $K_{нов} = \{1, 2, \ldots, 6\}$, $П_{нов} = \{2, 3, \ldots, 7\}$ чел-час, $K_{без} = \{1, 2, \ldots 6\}$, $G = \{6, 8, \ldots, 16\}$ чел-час.

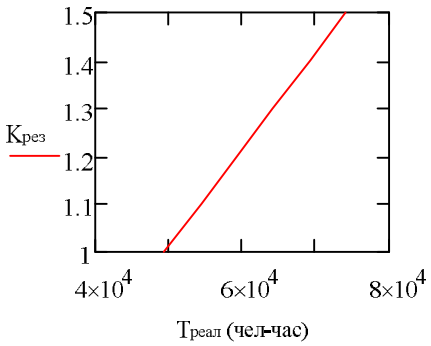


Рис. 8. График зависимости времени реализации функционала ПО $T_{реал}$ от коэффициента резервного времени $K_{рез}$

Как видно из графика зависимость времени реализации функционала ПО $T_{реал}$ от коэффициента резервного времени $K_{рез}$ достаточно велика. Так, при $K_{рез} = 1$, $T_{реал} = 4,944 \times 10^4$ чел-час. А при $K_{рез} = 1,3$, $T_{реал} = 6,427 \times 10^4$ чел-час, что в 1,3 раз больше предыдущего результата. В целом, полученные результаты времени реализации функционала ПО представлены в табл. 1. Следует заметить, что в этой же таблице (столбец 3) приведены значения времени необходимого на реализацию функционала ПО без учета показателей безопасного программирования ($K_{рез}$, G) – $T^*_{реал}$.

Таблица 1

Сравнительные результаты
времени реализации функционала ПО

$K_{рез}$	$T_{реал}$	$T^{*}_{реал}$
1	2	3
1	4.944*104	4.784*104
1.1	5.438*104	5.263*104
1.2	5.933*104	5.741*104
1.3	6.427*104	6.22*104
1.4	6.922*104	6.698*104
1.5	7.416*104	7.177*104

Как видно из этой таблицы, пренебрежение учетом показателей безопасного программирования занижает прогнозируемое время в 1,033 раза, и это с учетом того, что для входных данных показателей безопасного программирования ($K_{без}$, G) взяты достаточно низкие значения. На практике эти значения могут быть больше и, соответственно, прогнозируемое время так же увеличивается.

Выводы

Разработана математическая модель этапа инициализации процесса разработки ПО, основанная на концептуальных положениях Agile, что позволило выделить ряд наиболее важных параметров оценки временных затрат инициализации и определить их зависимости от качественных характеристик участников проекта.

Усовершенствована математическая модель этапа реализации функционала ПО, отличающаяся от известных учетом показателей безопасного программирования. Это позволило повысить точность результатов моделирования на 3%.

Дальнейшее развитие данные модели получат в способе масштабирования существующей методологии разработки с учетом требований безопасности программного обеспечения.

Это позволит повысить безопасность проекта и обеспечивать как быстрый рост функционала, так и приемлемый уровень качества сервиса.

В комплексе синтез разработанных математических моделей и способа масштабирования позволили усовершенствовать метод масштабирования методологии разработки программного обеспечения с учетом требований безопасности, отличающийся от известных возможностью управления существующими в организации (фирме) силами (специалистами) как в составе команды, так и в плоскости специалистов смежного направления (специалистов безопасного программирования и тестирования безопасности ПО).

Список литературы

1. Вэйдер Майкл Томас Инструменты бережливого производства. Мини-руководство по внедрению методик бережливого производства / Майкл Томас Вэйдер – Альпина Паблишер, 2012, 125 с.

2. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М.: Высшая школа, 2003. – 479 с.

3. Полицын С. А. Подходы к вычислению временных затрат на проекты в сфере разработки программного обеспечения на основе использования прецедентов / С.А. Полицын // Программная инженерия №7 2011 С.9-14

4. Канер Сем Тестирование программного обеспечения. Фундаментальные концепции менеджмента бизнес-приложений / С.Канер. – К.:ДиаСофт, 2001. – 544 с.

5. Макконнелл С. Сколько стоит программный проект / С. Макконнелл – Питер, 2007 – 304 с.

6. Kniberg Henrik Scrum and XP from the Trenches - 2nd Edition / Henrik Kniberg – InfoQ 2015 – 94 с.

7. Ruby Sam Agile Web Development with Rails / Sam Ruby, Dave Thomas, David Heinemeier Hansson – The Pragmatic Bookshelf Год: 2011, 2011 – 480 с.

Надійшла до редколегії 1.02.2017

Рецензент: д-р техн. наук, проф. О.О. Можаєв, Національний технічний університет «ХПІ», Харків.

МОДЕЛЬ РОЗРАХУНКУ ЧАСОВИХ КОРДОНІВ ПРОЕКТІВ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Г.Г. Швачич, С.Г. Семенов, М.І. Главчев, Кассем Халіфі

У статті вказано на необхідність прогнозування часових витрат на розробку програмного забезпечення (ПО) і представлена узагальнена математична модель для розрахунку часових меж проектів. З метою прогнозування розроблений комплекс математичних моделей основних етапів розробки програмного забезпечення. Розроблено математичну модель етапу ініціалізації процесу розробки ПО, заснована на концептуальних положеннях Agile, що дозволило виділити ряд найбільш важливих параметрів оцінки тимчасових витрат ініціалізації і визначити їх залежності від якісних характеристик учасників проекту. Удосконалено математичну модель етапу реалізації функціоналу ПЗ, що відрізняється від відомих урахуванням показників безпечного програмування.

Ключові слова: *безпечне програмування, тимчасові витрати на розробку ПО, SCRUM, Agile.*

MODEL OF CALCULATING THE ADVANCED BORDERS OF PROJECTS OF SOFTWARE PROCESSING

G.G. Shvachich, S.G. Semenov, M.I. Glavchev, Kassem Khalifi

The article identifies the need to forecast the time costs for the development of software (software) and presents a generalized mathematical model for calculating the time boundaries of projects. For the purpose of forecasting, a complex of mathematical models of the main stages of software development has been developed. A mathematical model of the initialization phase of the software development process was developed, based on the Agile conceptual provisions, which made it possible to identify a number of the most important parameters for estimating the time costs of initialization and to determine their dependence on the qualitative characteristics of the project participants. The mathematical model of the implementation phase of the software functional is improved, which differs from the known ones taking into account the indices of safe programming.

Keywords: *safe programming, time costs for software development, SCRUM, Agile.*

Питання управління в складних системах

УДК 519.7

В.И. Барсов, А.В. Кравцова

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

ИССЛЕДОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ УГЛОВЫМ ПОЛОЖЕНИЕМ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

Приведены результаты исследования системы управления беспилотным летательным аппаратом в канале продольного движения (управление углом тангажа). Была исследована система с сервоприводом с жёсткой обратной связью, скоростной обратной связью и изодромной обратной связью, при изменении коэффициентов датчика угловой скорости и датчика угла. Исследование системы управления было выполнено в среде моделирования Simulink пакета Matlab.

Ключевые слова: *беспилотный летательный аппарат, система управления, продольный канал, сервопривод, обратная связь.*

Введение

Рост восторженности в беспилотных летательных аппаратах (БПЛА) вызван расширением масштабов научно-исследовательских, аварийно-спасательных работ, решением актуальных вопросов по экологической безопасности и охране окружающей среды.

Эффективное использование летательных аппаратов, прежде всего, таких специфических классов летательных аппаратов, как беспилотные летательные аппараты невозможно без помощи систем автоматического управления (САУ), позволяющих оперативно и точно решать задачи пространственной ориентации и стабилизации.

Для САУ беспилотного летательного аппарата (БПЛА) одной из наиболее важных решаемых задач является исполнение всей программы полета, в независимости от воздействия случайных возмущающих факторов, возникающих в процессе полета [5].

Одним из главных элементов реализации процессов управления полётом летательного аппарата является сервопривод (СП) – электрический привод с обратной связью по положению, применяемый в автоматической системедля привода управляющих элементов и рабочих органов.[3]

Сервопривод получая на вход значение управляющего параметра (в реальном времени), основываясь на показаниях датчика стремится создать и поддерживать это значение на выходе исполнительного элемента [1].

В данной работе было проведено исследование влияния на систему стабилизации по углу тангажа сервопривода с жёсткой обратной связью, скоростной обратной связью и изодромной обратной связью.

Схема сервопривода применяемого при исследовании САУ БПЛА представлена на рис. 1 [3], где приняты следующие обозначения:

Ус. СП- усилитель сервопривода;
РМ – рулевая машинка;
ДОС – датчик обратной связи;
ОС – обратная связь;
РА – рулевой агрегат;
Блок ус. РА – блок усиления РА;
$U_{упр}$ – сигнал управления;
δ – угол отклонения рулевой поверхности.

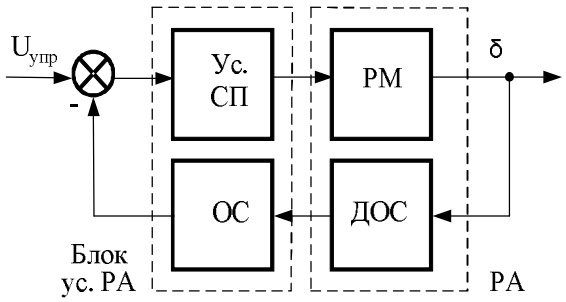


Рис. 1. Типовая схема сервопривода

Для элементов сервопривода приняты следующие передаточные функции:

$$W_y(s) = k_y = 3;$$

$$W_{рм}(s) = k_y / s = 0{,}2 / s;$$

$$W_{дос}(s) = k_{дос} = 1.$$

Данные передаточные функции использовались при проведении моделирования исследуемых процессов.

Основная часть

Для исследования динамики беспилотного летательного аппарата использовались методы теории линейных, систем математического и машинного моделирования.

Для моделирования процессов протекающих в САУ беспилотного летательного аппарата использовалась среда графического моделирования Simulink пакета Matlab [4].

Было рассмотрено три вида обратной связи (ОС) сервопривода: жёсткая обратная связь (ЖОС), скоростная обратная связь (СОС) и изодромная обратная связь (ИОС).

При жёсткой обратной связи — на вход регулятора поступает сигнал, пропорциональный выходному сигналу объекта в любой момент времени. При этом, входному управляющему сигналу соответствует пропорциональное отклонение штока исполнительного устройства, пропорциональный углу отклонения рулевой поверхности [2].

Передаточная функция жёсткой обратной связи имеет вид:

$$W_{жос}(s) = k_{ос} = 1.$$

Таким образом, передаточная функция сервопривода с ЖОС равна:

$$W_{сп\_жос} = \frac{k_у \cdot k_{рм}/s}{1 + k_у \cdot (k_{рм}/s) \cdot k_{дос} \cdot k_{ос}} = \frac{1}{1,667 \cdot s + 1}.$$

При скоростной обратной связи — на вход регулятора поступает не только сигнал, пропорциональный выходному сигналу объекта, но и сигнал, пропорциональный производным выходной переменной. Для такой ОС сервопривода в цепи обратной связи стоит идеальное дифференцирующее звено [2].

Передаточная функция скоростной обратной связи имеет вид:

$$W_{сп\_сос}(s) = s \cdot k_{ос} = s \cdot 1.$$

Передаточная функция сервопривода с СОС имеет вид:

$$W_{сп\_сос}(s) = \frac{k_у \cdot k_{рм}/s}{1 + k_у \cdot (k_{рм}/s) \cdot k_{дос} \cdot s \cdot k_{ос}} = \frac{0,375}{s}.$$

Сервопривод со СОС является интегрирующим звеном.

При использовании изодромной обратной связи в цепи обратной связи стоит реальное дифференцирующее звено. Его можно рассматривать как последовательно соединенные идеальное дифференцирующее и апериодическое звенья [2].

Передаточная функция ИОС имеет вид:

$$W_{иоы\_сос}(s) = k_{ос} \cdot \frac{s \cdot T_и}{s \cdot T_и + 1} = 1 \cdot \frac{s}{s+1}.$$

Передаточная функция сервопривода с ИОС:

$$W_{сп\_сос}(s) = \frac{k_у \cdot k_{рм}/s}{1 + k_у \cdot (k_{рм}/s) \cdot k_{дос} \cdot k_{ос} \cdot \frac{s \cdot T_и}{s \cdot T_и + 1}} = \frac{0,6 \cdot (s+1)}{1,6 \cdot s \cdot (0,625 \cdot s + 1)}.$$

При проведении моделирования была реализована модель САУ БПЛА позволяющая исследовать систему автоматического управления с сервоприводом для трёх видов обратной связи при различных коэффициентах датчика угловой скорости (ДУС) и датчика угла (ДУ). Машинная модель системы управления по углу тангажа, реализованная в среде Simulink, представлена на рис. 2.

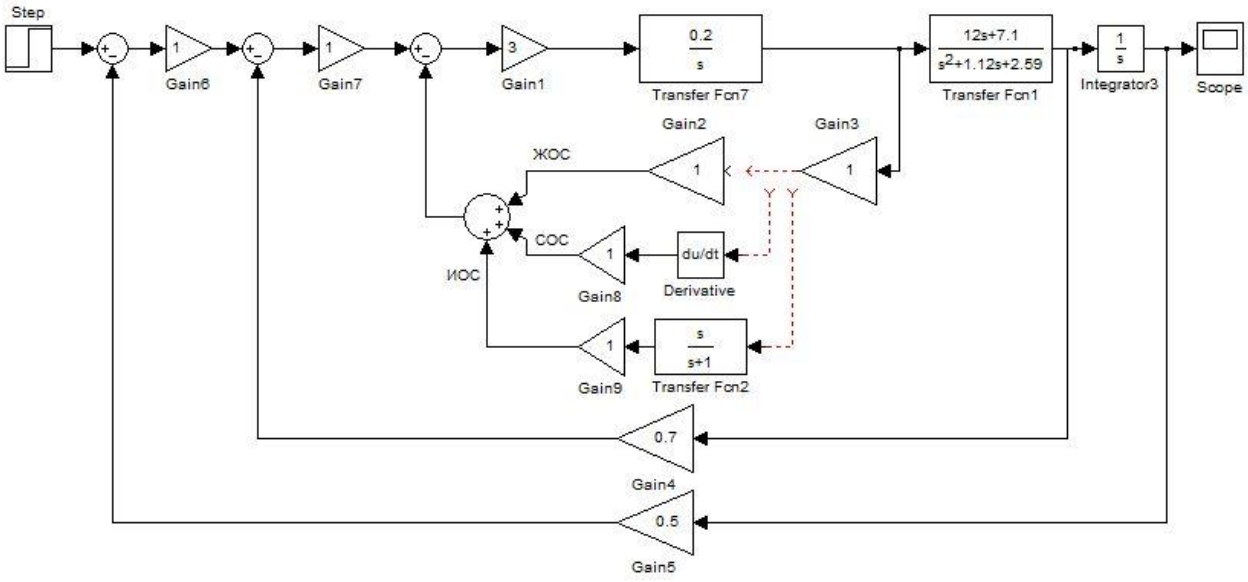
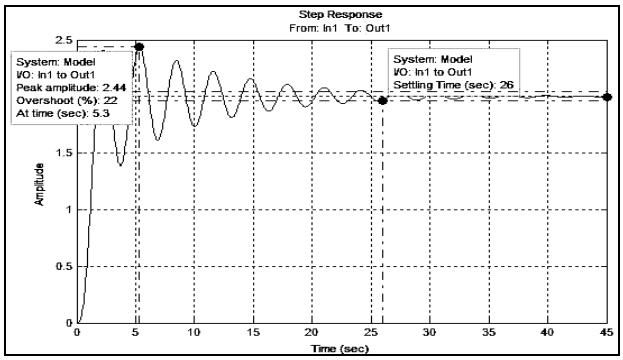
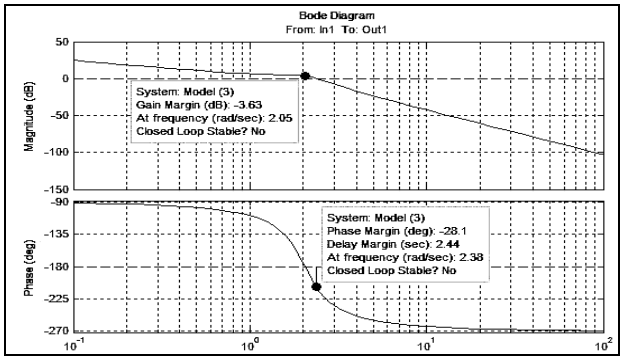


Рис. 2. Машинная модель САУ по углу тангажа

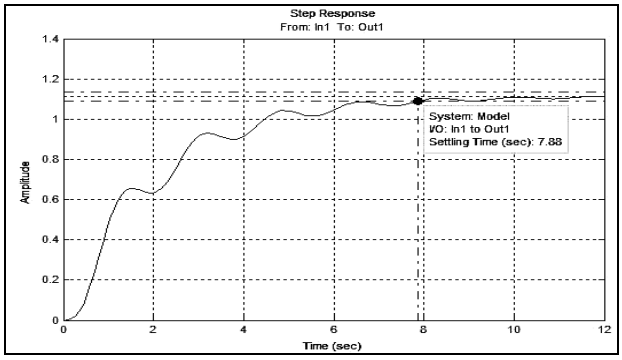
В ходе проведения исследования были получены результаты системы стабилизации углового положения беспилотного летательного аппарата для разных видов обратной связи при разных коэффициентах датчика угловой скорости и датчика угла, которые приведены на рис. 3.

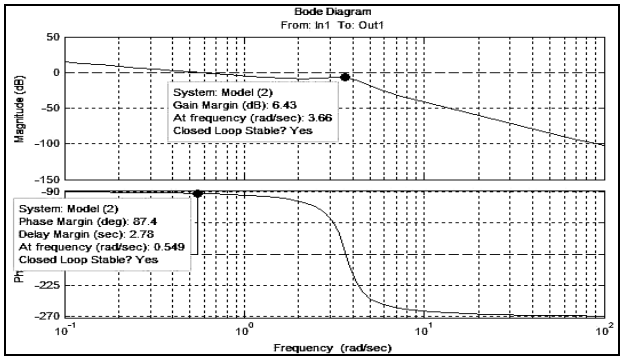




$k_{дус} = 0{,}225,\ k_{ду} = 0{,}5$

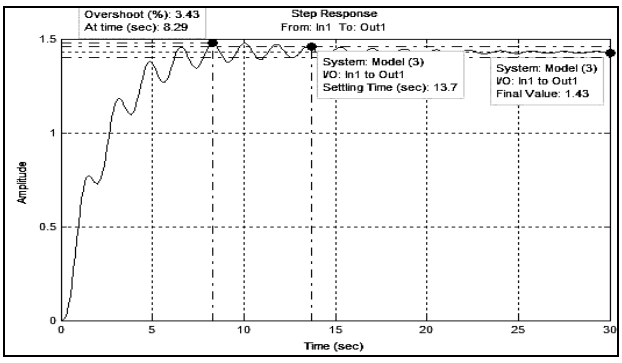
а б

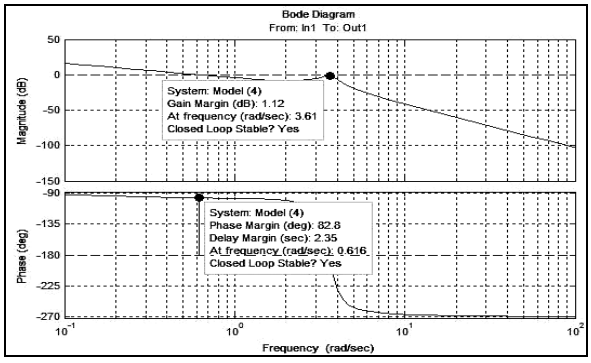




$k_{дус} = 1{,}5,\ k_{ду} = 0{,}9$

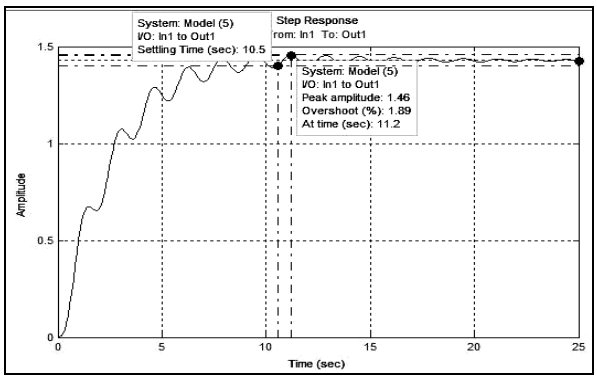
в г

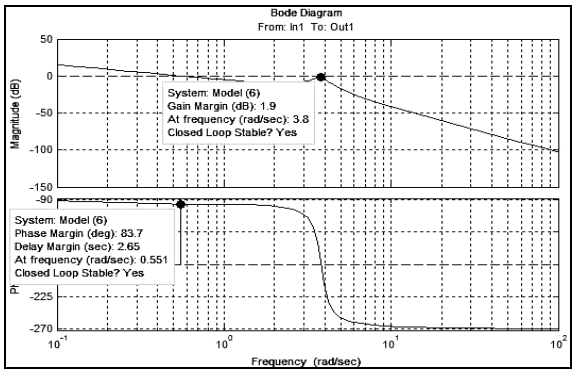




$k_{дус} = 1{,}5,\ k_{ду} = 0{,}7$

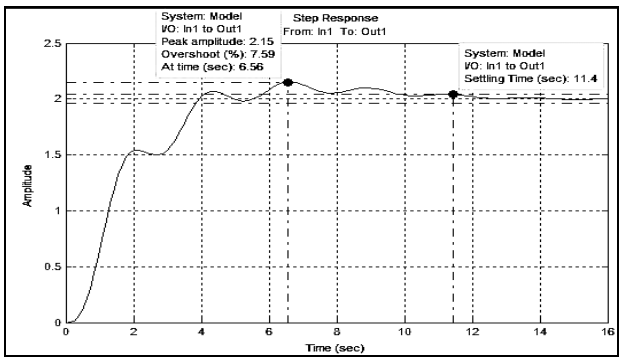
д е

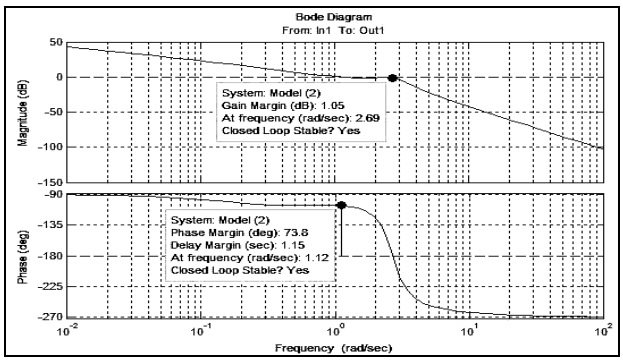




$k_{дус} = 1{,}7,\ k_{ду} = 0{,}7$

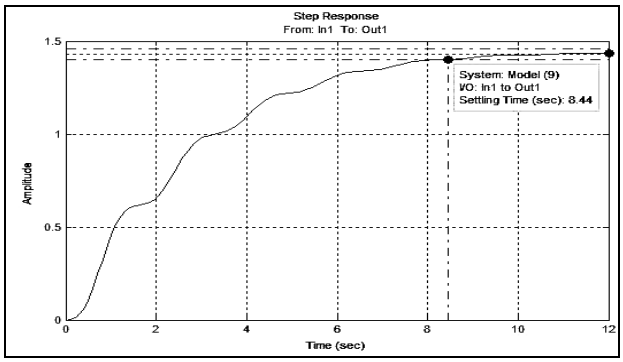
ж з

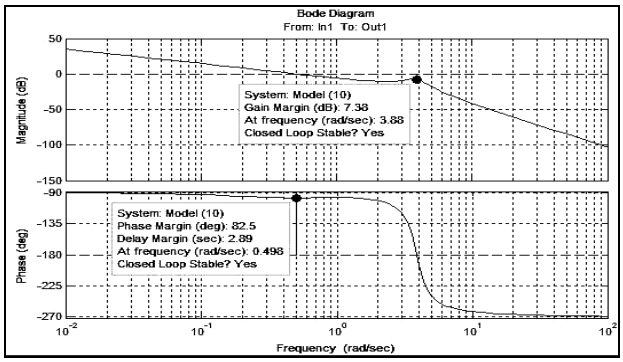




$k_{дус} = 0,7,\ k_{ду} = 0,5$

и к





$k_{дус} = 1,8,\ k_{ду} = 0,7$

л м

Рис. 3. Переходная характеристика (а, в, д, ж, и, л), и АЧХ и ЛФЧХ САУ (б, г, е, з, к, м)
САУ с СП с СОС

В табл. 1 – 3 приведены показатели качества системы с сервоприводом с жёсткой ОС, со скоростной ОС и изодромнойОС для разных коэффициентов ДУС и ДУ.

Таблица 1

Показатели качества системы стабилизации с СП с ЖОС

$K_{дус}$	$K_{ду}$	$t_{пп}$, с	σ, %	M	$\varepsilon_{уст}$, В	Lз, дБ	Фз, град
0,225	0,5	26	22	0,158	1	0	0
0,7	0,5	8,17	0	0,7	1	1,54	79,2
1	0,5	10,7	0	1,03	1	3,71	84,6
1,5	0,7	9,95	0	1,4	0,42	6,43	87,4
1,5	0,9	7,88	0	1,2	0,11	6,43	87,4

Таблица 2

Показатели качества системы стабилизации с СП с СОС

$K_{дус}$	$K_{ду}$	$t_{пп}$, с	σ, %	M	$\varepsilon_{уст}$, В	Lз, дБ	Фз, град
0,7	0,5	21,7	12,6	0,208	1	0	0
1,5	0,7	13,7	3,43	0,437	0,43	1,12	82,8
1,5	0,6	10,9	1,6	0,537	0,67	1,12	82,8
1,6	0,6	10,8	1,05	0,591	0,67	1,52	83,3
1,7	0,7	10,5	1,46	0,544	0,43	1,9	83,7

Таблица 3

Показатели качества системы стабилизации с СП с ИОС

$K_{дус}$	$K_{ду}$	$t_{пп}$, с	σ, %	M	$\varepsilon_{уст}$, В	Lз, дБ	Фз, град
0,7	0,5	11,4	7,59	0,629	1	1,05	73,08
1	0,5	10,6	2,75	0,954	1	3,25	78,3
1,5	0,5	9,57	0,4	1,5	1	6,04	81,3
1,5	0,7	6,44	1,33	1,3	0,43	6,04	81,3
1,8	0,7	8,44	0	1,64	0,43	7,38	82,5

Выводы

По результатам сравнительного анализа показателей качества, приведенных в табл. 1 – 3, можно сделать следующие выводы:

1) система с сервоприводом с ЖОС показала наилучший результат при $k_{дус} = 1,5$, $k_{ду} = 0,9$ со следующими показателями:

$t_{пп}$, с– 7,88; σ, % – 0; M – 1,2;
$\varepsilon_{уст}$, В – 0,11; Lз, дБ – 6,43; Фз, град – 87,4;

2) система с сервоприводом с СОС показала оптимальный результат при $k_{дус} = 1,7$, $k_{ду} = 0,7$ с такими показателями качества:

$t_{пп}$, с – 10.5; σ, % – 1,46; M – 0,544;
$\varepsilon_{уст}$, В – 0,43; Lз, дБ – 1,9; Фз, град – 83,7;

3) система с сервоприводом с ИОС показала лучший результат при $k_{дус} = 1,5$, $k_{ду} = 0,7$ со следующими показателями качества:

$t_{пп}$, с– 6,44; σ, % – 1,33; M – 1,3;
$\varepsilon_{уст}$, В – 0,43; Lз, дБ – 6,04; Фз, град – 81,3.

Таким образом, для системы автоматического управления стабилизацией углового положения БПЛА по углу тангажа на и более эффективным является применение с сервоприводом с изодромной обратной связью.

Список литературы

1. Рулевые приводы и сервоприводы [Электронный ресурс]. – Режим доступа к материалу: http://ooobskspetsavia.ru, свободный.

2. Транспортные системы. Сервоприводы и виды обратных связей в них. Способы включения исполнительных устройств САУ в контур управления. – [Электронный ресурс]. – Режим доступа к материалу: http://transporton.ru, свободный.

3.Москаленко, В.В. Электрический привод: учебник для вузов [Текст] / В.В. Москаленко. – М.: Академия, 2007.

4. Краснопрошина А.А Современный анализ систем управления с применением Matlab, Simulink, Control System [Текст] / Репейникова Н.Б., Ильченко А.А. – К.: «Корнийчук», 1990. – 86 с.

5. Боднер В.А. Системы управления летательными аппаратами [Текст] / В.А. Боднер. – М.: Машиностроение. 1973. – 506 с.

Надійшла до редколегії 3.02.2017

Рецензент: д-р техн. наук, проф. О.О. Можаєв, Національний технічний університет «ХПІ», Харків.

ДОСЛІДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ КУТОВОГО ПОЛОЖЕННЯ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ

В.І. Барсов, А.В. Кравцова

Наведено результати системи управління безпілотним літальним апаратом в каналі поздовжнього руху (управління кутом тангажа). Була досліджена система з сервоприводом з жорстким зворотним зв'язком, швидкісним зворотним зв'язком і ізодромним зворотним зв'язком, при зміні коефіцієнтів датчика кутової швидкості і датчика кута. Дослідження системи управління було виконано в середовищі графічного моделювання Simulink пакета Matlab. Виходячи з отриманих результатів машинного моделювання був запропонований оптимальний варіант зворотного зв'язку сервоприводу.

***Ключові слова**: безпілотний літальний апарат, система управління, поздовжній канал, сервопривід, зворотний зв'язок.*

THE REASEARCHOF CONTROL SYSTEM OFANGULAR POSITION OF UNMANNED AERIAL VEHICLE

V.I. Barsov, A.V. Kravtsova

The results of the control system of unmanned aircraft in the channel longitudinal motion (pitch angle control). A system has been studied with actuator with rigid feedback, speed feedback and izodromic feedback when changing the coefficients of the angular velocity sensor and the angle sensor. The research of system of control was performed in the graphical modeling environment Simulink Matlab package. Based on the results of computer simulation was proposed optimal variant of the actuator feedback.

***Keywords**: unmanned aerial vehicles, control system, longitudinal channel, actuator feedback.*

УДК 621.313

С.Г. Буряковський

Український державний університет залізничного транспорту, Харків

РЕГУЛЬОВАНИЙ СТРІЛОЧНИЙ ПЕРЕВІД З ДВИГУНОМ ПОСТІЙНОГО СТРУМУ НА БАЗІ МІКРОПРОЦЕСОРНОГО ТИРИСТОРНОГО ПЕРЕТВОРЮВАЧА

В статті наведені варіанти модернізації системи керування двигуном постійного струму стрілочного переводу на баз мікропроцесорного тиристорного перетворювача.

Ключові слова: *стрілочний перевід, тиристорний перетворювач, система підлеглого керування, модальне керування, спостерігач стану.*

Вступ

Стрілочний перевід (СП), по суті, є сервоприводом. Недолік стрілочних переводів, що застосовуються в Україні, з цієї точки зору полягає в тому, що в них застосовуються стандартні промислові двигуни змінного і постійного струму, які не є серводвигунами, тобто не адаптовані по швидкодії. Швидкість обертання валу - від 1700об/хв до 3000 об/хв, момент інерції якоря (ротора) – стандартний для свого типорозміру і т.д. Звичайно, застосувавши спеціальні двигуни, наприклад, синхронні з постійними магнітами, можна ці недоліки звести до мінімуму. Однак, на залізницях України порядку 40000 стрілочних переводів, добра половина з яких – з двигунами постійного струму. Де знайти кошти на придбання такої кількості комплектуючих елементів?

Аналіз літератури. Передумови до створення системи керування стрілочним переводом були описані Резніковим Ю.М. в теоретичному вигляді [3]. Розвиваючи тему, в роботах, опублікованих раніше [1], автори підняли і обґрунтували питання розробки і застосування сучасного вітчизняного, мікропроцесорного, електроприводу стрілочного переводу. Тим більше, що в Європейському союзі роботи по такому шляху не тільки ведуться теоретично, але і промислово випускаються зразки [11]. Безумовно, це важливе завдання, яке потребує негайного вирішення, оскільки швидкісний рух складається не тільки з «швидких» локомотивів, а й зі «швидких» стрілочних переводів.

Мета статті: Залучення уваги інженерного і керівного персоналу залізниць до можливості модернізації систем залізничної автоматики, що експлуатуються, засобами електроприводу, яким би застарілим він не був.

Результати досліджень

В даній статті піде мова про синтез і порівняльний аналіз систем керування електроприводом стрілочного переводу з двигуном постійного струму типу МСП-0.25. Доцільним представляється розгляд системи підлеглого керування (СПК) положення гостряків [9] (рухомих частин), системи з модальним регулятором (МР) [7] і системи зі спостерігачем стану (СС) [8].

Тут слід згадати, що існуючі стрілочні електроприводи не мають системи регулювання швидкості, відключення двигуна відбувається при ударі рухомих частин об нерухомі, зі спрацьовуванням фрикційного захисту. Як було зазначено вище, в дослідженнях Ю.М. Резнікова [3] закон керування двигуном представлявся у вигляді рис. 1.

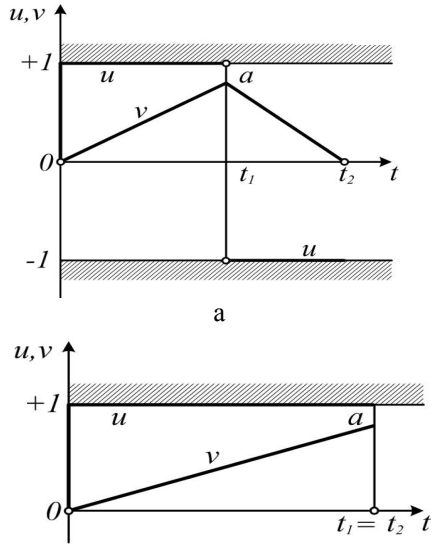


Рис. 1. Процес роботи електроприводу стрілочного переводу: а – перспективний за Резніковим; б – існуючий

На рис. 1, б показані керуючі координати процесу переводу гостряка, u – напруга двигуна і v – швидкість обертання валу. В даний час процес переводу відбувається так: в нульовий момент часу подається сигнал напруги на двигун (координата керування u) і з'являється відповідна швидкість руху (координата керування v); тривалість перекладу визначається механічно: в момент часу t_2 шестерні редуктора упруться в обмежувач і перевід завершиться примусово. У перспективі ж (рис. 1, а) передбачалося, що в процесі переводу система керу-

вання вирахує такий момент часу t1, в який можна почати гальмування, до повної зупинки у момент t_2.

Однак, на той момент апаратна частина засобів автоматики не дозволяла реалізувати залежності рис. 1, а. З негативними наслідками прямого пуску під навантаженням боролися конструктивними методами: потужним, металомістким чотириступінчатим редуктором; застосуванням зазору в кінематичній лінії для полегшення пуску двигуна; установкою фрикційного зчеплення в другій передачі редуктора, щоб в кінці переводу при ударі і притисненні гостряка до рамної рейки не вийшов з ладу двигун через перевантаження. Зараз же повсюдне впровадження програмованих логічних контролерів (ПЛК) сприяє впровадженню алгоритмів керування електродвигуном за допомогою перетворювальної техніки, що дає цілий ряд переваг, якими не можна не скористатися [5].

Отже, серцем пропонованої системи керованого стрілочного переводу (з двигунами постійного струму) є тиристорний перетворювач (ТП). Керуючий модуль ТП має широкий спектр комунікаційних можливостей і ідеально вписується в будь-яку систему автоматизації з використанням ПЛК [10], в тому числі залізничних систем диспетчеризації (МПЦ). За допомогою обчислювальних потужностей ТП і/або ПЛК реалізуються зазначені вище алгоритми регулювання (СПК, МР, НС). Для розуміння вигод застосування регулювання процесу переводу гостряків стрілки розглянемо рис. 2.

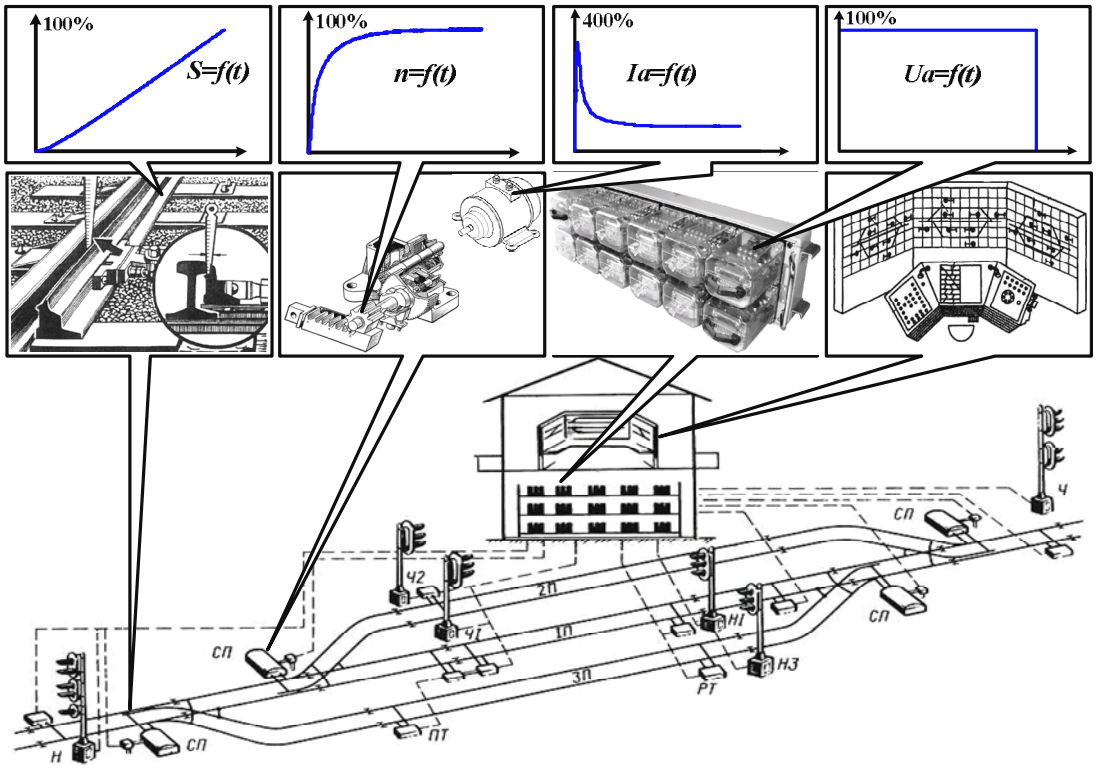


Рис. 2. Існуюча система централізації залізничної станції

На рис. 2 показано, що відбувається при натисканні черговим по станції кнопки переведення стрілки: сигнал приходить в релейну схему керування станцією, реле включає напругу на двигун, редуктор переміщує шибер, який тягне (або штовхає) гостряк стрілки, і він переміщується. Графіки над відповідними зображеннями ілюструють фізичну суть процесу переводу при прямому пуску двигуна. Як було зазначено вище, процес переводу неконтрольований, тому в його початку відбувається значний стрибок струму якоря. В кінці переводу внаслідок механічного переривання руху рухомої рейки відбувається неминучий удар.

Негативні наслідки цих процесів неодноразово були описані авторами в публікаціях раніше [2], та й зрозумілі із загальних інженерних міркувань. Покажемо, як такі явища можна компенсувати за допомогою системи керування [4, 5, 7 – 9], варіанти структури якої наведені на рис. 3. Застосування задатчика інтенсивності дозволяє значно знизити пусковий струм, зниження швидкості руху гостряків перед закінченням перекладу зменшує силу удару, інтенсивність збільшення зазорів в місцях кріплень тяг і т.п. Наявність мережевої інформаційної комунікації дозволяє передавати дані переводу на екран монітора диспетчера.

Покажемо, що зміниться у фізиці процесу переводу (за допомогою математичного моделювання [6]) в процесі реалізації закону управління (рис 1, а) засобами системи керування зі структурою підлеглого керування (рис. 3, а) і структурою з модальним регулятором і спостерігачем стану (рис. 3, б, в) на базі сучасної контролерної і перетворювальної техніки.

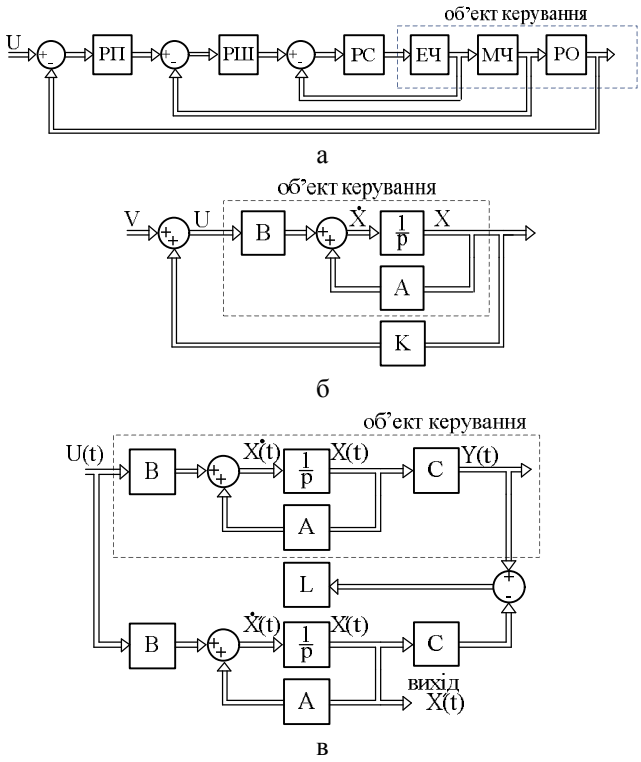


Рис. 3. Структурні схеми систем керування ТП:
а – система підлеглого керування; б – модальний регулятор; в)– спостерігач стану

Як видно з рис. 4, перевід в модернізованій системі здійснюється дещо по-іншому, а саме з екрану монітора. При цьому з інформаційної мережі керуюча команда в цифровому вигляді надходить на ПЛК, який передає сигнал завдання на виконавчий прилад, в даному випадку ТП, а перетворювач формує потрібну форму напруги, контролює величину струму якоря двигуна і регулює швидкість обертання його вала. При цьому графік переміщення гостряків (рис. 5, 6) має відповідні вигини на початку і кінці перекладу, що є наслідком зміни швидкості їх руху (рис. 5, 6). У початковий момент помітно дворазове зниження пускового струму, а швидкість при гальмуванні становить 15-20% від номінальної (рис. 6), що дозволяє уникнути удару при притисненні гостряка до рамної рейки. На графіках показані зміни координат при прямому пуску і при регульованому.

Висновки

З вищевикладеного можна зробити висновок про необхідність регулювання процесу переведення стрілки. На стрілках з двигунами постійного струму засобом для цього може служити будь-який із запропонованих вище варіантів системи керування ТП. Незважаючи на необхідні капіталовкладення ефект від впровадження подібного роду систем очевидний – це захист електродвигуна засобами ПЛК, зниження витрат на обслуговування переводу і його металоконструкцій, детермінованість і повний контроль процесу переводу гостряків. Вибір того чи іншого варіанту диктується особливостями експлуатації конкретного стрілочного переводу.

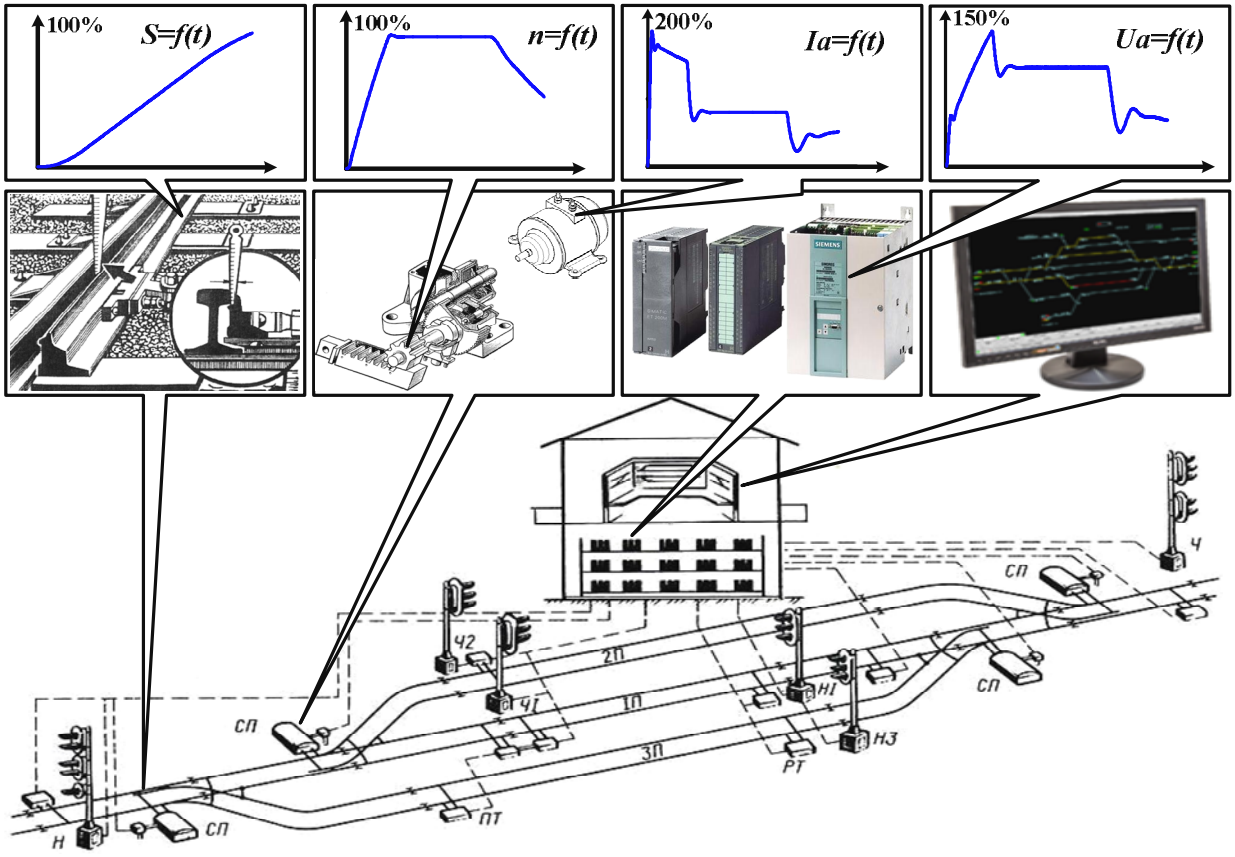


Рис. 4. Перспективна система централізації залізничної станції

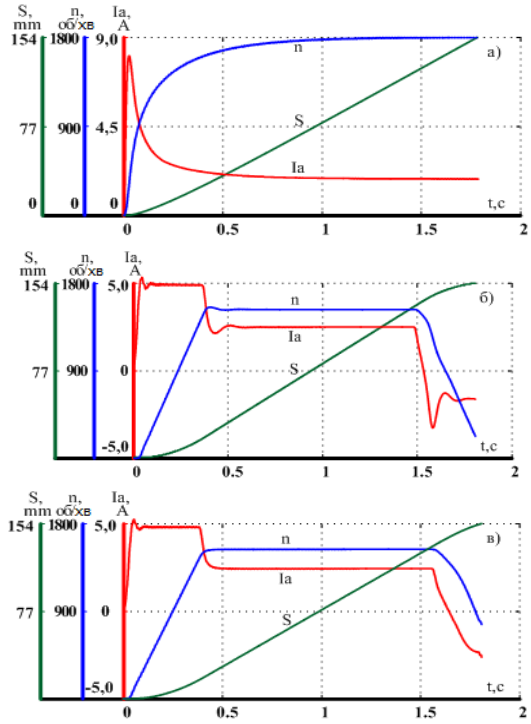


Рис. 5. Графіки регульованих координат при прямому пуску (а), СПК (б), МР зі СС (в)

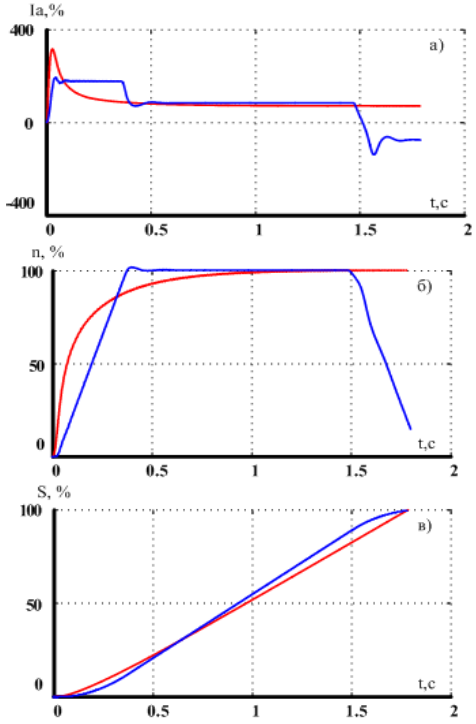


Рис. 6. Порівняння процесу переводу стрілки при прямому и керованому пуску

Список літератури

1. Улучшение динамики железнодорожного стрелочного перевода с частотно-регулируемым электроприводом при нестационарных режимах работы / Л.В. Акимов, С.Г. Буряковский, А.С. Маслий, В.В. Смирнов // Електротехнічні та комп'ютерні системи. - Київ: Техніка, 2012. - № 05(81). - С.22-30

2. Смирнов В.В. Регулируемый стрелочный электропривод / С.Г. Буряковский, В.В. Смирнов // Локомотивінформ. – Х.: корп. «Техностандарт». – 2010. - №7. –С.8-9

3. Резников Ю.М. Стрелочные электроприводы электрической и горочной централизации / Ю.М. Резников. – Москва: Транспорт, 1975. - 152 с.

4. Ключев В.И. Теория электропривода / В.И. Ключев. - Москва: Энергоатомиздат, 1985. – 560 с.

5. Дитце Х.У. Меры по уменьшению износа стрелочных переводов / Х.У. Дитце, Х.П. Мюллер // Железные дороги мира. – М.: ОАО «РЖД». - 1991. - № 4. - С. 64-65.

6. Герман-Галкин С.Г. Компьютерное моделирование полупроводниковых систем / С.Г. Герман-Галкин – Санкт-Петербург: КОРОНА-принт, 2007. – 320 с.

7. Акимов Л.В. Синтез системы модального управления упругими электромеханическими объектами с нагрузкой типа пара трения / Л.В. Акимов, А.В. Клепиков, В.Б. Клепиков // Вісник національного технічного університету «ХПІ». – Х.: НТУ «ХПІ». -1998. Вип. 52. –С. 59-62.

8. Акимов. Л.В. Обобщенный наблюдатель для системы подчиненного регулирования скорости тиристорных электроприводов с устойчивой и неустойчивой одномассовой механической частью / Л.В. Акимов, В.И. Колотило, В.Н. Шамардина // Электротехника. – Москва: «Галлея-принт». -1999. - №5. – С.12-20.

9. Акимов Л.В. Методики синтеза астатической системы подчиненного регулирования скорости неустойчивого двухмассового объекта / Л.В. Акимов, В.С. Марков // Интегрированные технологии и энергосбережение. – Харьков: НТУ «ХПИ». – 2000. - №1. –С.41-52.

10. Sinamics Function Manual: каталог-справочник / Austria: Siemens A.G. - 2011.

11. Офіційний сайт компанії «Бомбардьє» [Електронний ресурс]. / Режим доступу: www.bombardier.com/ files/en/ supporting_docs/ EPD_EBI_Switch.pdf.

Надійшла до редколегії 23.01.2017

Рецензент: д-р техн наук, проф. Б.М. Горкунов, Національний технічний університет «ХПІ», Харків.

РЕГУЛИРУЕМЫЙ СТРЕЛОЧНЫЙ ПЕРЕВОД С ДВИГАТЕЛЕМ ПОСТОЯННОГО ТОКА НА БАЗЕ МИКРОПРОЦЕССОРНОГО ТИРИСТОРНОГО ПРЕОБРАЗОВАТЕЛЯ

С.Г. Буряковский

В статье приведены варианты модернизации системы управления двигателем постоянного тока стрелочного перевода на баз микропроцессорного тиристорного преобразователя.

Ключевые слова: *стрелочный перевод, тиристорный преобразователь, система подчиненного управления, модальное управление, наблюдатель состояния.*

ADJUSTABLE RAILROAD SWITCH WITH ENGINE DC ON THE BASIS OF MICROPROCESSOR THYRISTOR

S.G. Buryakovskyi

The article presents the options for the modernization of DC motor control crossing piece on the base of microprocessor thyristor converter.

Keywords: *railroad switch, thyristor, slave system controller, modal control, observer status.*

УДК 621.396.96

Е.Л. Казаков[1], А.Е. Казаков[2]

[1] *Кировоградская летная академия НАУ, Кропивницкий*
[2] *Харьковская государственная академия культуры, Харьков*

ВОЗМОЖНОСТИ УЧЕТА ВЛИЯНИЯ ВРЕМЕННЫХ ФЛУКТУАЦИЙ ИНТЕНСИВНОСТЕЙ ОТРАЖЕННЫХ МНОГОЧАСТОТНЫХ СИГНАЛОВ И ОСОБЕННОСТЕЙ РЛС КРУГОВОГО ОБЗОРА ПРИ ОПРЕДЕЛЕНИИ ПРИЗНАКОВ РАСПОЗНАВАНИЯ ЦЕЛЕЙ

Рассмотрены основные методы и разработано устройство компенсации ошибок получения признаков распознавания целей, возникающих за счет влияния характеристик трактов различных классов РЛС при использовании многочастотных сигналов.

Ключевые слова: *радиолокационный сигнал, радиолокационная цель, модуляция, коэффициент корреляции, амплитудные флуктуации, диаграмма направленности антенны, многочастотный сигнал.*

Введение

Постановка проблемы. В последнее время в научно-технической литературе большое внимание уделялось вопросам распознаванию радиолокационных целей (РЛЦ) при использовании различных видов сигналов. На точность определения признаков распознавания целей оказывают существенное влияние характеристики трактов различных используемых классов РЛС. Поэтому необходимо рассмотреть возможности уменьшения этого влияния для повышения точности определения признаков распознавания.

В статье рассматриваются методы и устройства, позволяющие уменьшить влияние таких характеристик РЛС на признаки распознавания, как изменение потенциала РЛС, влияние диаграммы направленности антенны РЛС, отношение сигнал/шум на выходе приемника. Также рассматриваются методы уменьшения искажений амплитуд отраженных многочастотных сигналов (МЧС) разными факторами на получаемые признаки распознавания.

Предлагаемые методы рассматриваются применительно к РЛС кругового обзора и к РЛС сопровождения целей.

Анализ последних исследований и публикаций. В настоящее время адаптивные системы находят применение в таких областях, как биология, связь, радиолокация, гидролокация, сейсмология, проектирование механических систем, навигация и биомедицинская электроника [1, 2]. Широкое применение они нашли в радиолокации. В этой области рассматриваются адаптивные системы к различным типам помех, адаптивные антенные решетки, адаптация к ионосферным ошибкам, адаптация к медленным изменениям параметров сред распространения радиоволн и т. д. [3]. Однако, несмотря на проведенные подробные исследования по использованию различных видов радиолокационных (РЛ) сигналов [2 – 5] для распознавания целей, вопросам компенсации ошибок получения признаков распознавания при использовании МЧС внимания не уделялось.

Целью статьи является рассмотрение общих принципов компенсации ошибок получения признаков распознавания и целесообразность ее применения при использовании МЧС.

Основной материал

При использовании в РЛС кругового обзора для определения признаков распознавания МЧС с перестройкой частоты от импульса к импульсу на точность получения этих признаков будут оказывать влияние временные флуктуации отраженных сигналов.

Рассмотрим коротко причины, порождающие амплитудные флуктуации отраженных от воздушных целей МЧС применительно к РЛС кругового обзора.

Амплитудные флуктуации возникают, во-первых, в результате модуляции отраженного сигнала движущимися частями воздушных целей (турбинами двигателей, воздушными винтами, антеннами бортовых РЛС и т.п.), во-вторых, вследствие изменения во времени ракурса цели относительно линии визирования РЛС. Влияние вращающихся турбин и компрессоров двигателей проявляется для длин волн короче 10 – 15 см, максимальная частота модуляции составляет несколько килогерц, поэтому при типовых значениях частоты следования импульсов в РЛС (менее 1 кГц) турбинную модуляцию можно рассматривать как слабокоррелированный аддитивный шум. Отношение мощности полезного сигнала и такого шума при $\lambda > 10$ см имеет порядок 20 дБ и более.

Модуляция, вызванная вращением воздушных винтов, наблюдается практически во всем диапазоне

длин волн РЛС и имеет порядок десятки-сотни герц. В этом случае время корреляции модуляционной составляющей сигнала оказывается порядка нескольких миллисекунд. Если время формирования некогерентного многочастотного сигнала сравнимо с этой величиной, то возможно перепутывание, например, вертолетов с самолетами больших размеров (бомбардировщиками). В последнем случае можно использовать различие в скорости полета для устранения ошибок такого рода.

Модуляция сигнала может быть вызвана также вращением антенн РЛС и прежде всего при обзоре передней полусферы воздушной цели. Максимальная частота вращения таких антенн может достигать 10 Гц, а размеры 1,5 м. Время корреляции сигнала, отраженного от вращающейся антенны, ограничено снизу величиной $\lambda/100$ секунд, если длина волны выражена в сантиметрах.

Вторая группа факторов, вызывающих временные флуктуации сигнала, связана с изменением ракурса цели, который содержит две переменные составляющие.

Первая обусловлена регулярным поступательным движением, а вторая – случайными колебаниями цели вокруг центра масс (рысканье), вызванными турбулентностью атмосферы.

Выполнив элементарные расчеты, можно показать, что оценка снизу для времени корреляции флуктуаций сигнала, связанных с движением цели, определяется выражением

$$\tau > \frac{\varphi_{0,5}}{\alpha_1+\alpha_2}, \qquad (1)$$

где $\varphi_{0,5}$ – ширина лепестка диаграммы, обратного вторичного отражения цели на уровне 0,5;

α_1 и α_2 – максимальные угловые скорости изменения ракурса цели за счет поступательного движения и рыскания соответственно.

Значение α_1 зависит от скорости цели (V), дальности до нее (R) и ракурса цели β:

$$\alpha_1 = \frac{V\sin\beta}{R}. \qquad (2)$$

По имеющимся экспериментальным данным в качестве оценки параметра α_2 для тяжелых самолетов можно принять величину $(2 \div 3)10^{-3}$ рад/с. Ширина лепестка $\varphi_{0,5}$ связана с длиной волны РЛС и размером цели L соотношением

$$\phi_{0,5} \geq \lambda/(2L).$$

Если длина волны выражена в сантиметрах, то для стратегического бомбардировщика (L = 50 м) при $R \geq 100$ км, $V \leq 300$ м/с, $-90^0 \leq \beta \leq 90^0$, приведенная выше оценка имеет следующий вид:

$$\tau > \lambda/50, \text{ сек.}$$

Таким образом, при длине волны $\lambda \approx 10$ см можно считать, что время корреляции сигналов, отраженных от реактивных самолетов, составляет $\tau_к \approx 0,1$ сек. Наличие вращающейся антенны бортовой РЛС мало сказывается на времени корреляции. Если автокорреляционную функцию флуктуаций амплитуд отраженных сигналов на одной частоте с учетом движения цели аппроксимировать функцией типа $\sin x/x$, то выражение для временного коэффициента корреляции при $\tau_к = 0,1$ сек примет вид

$$\rho(\tau) = \frac{\sin 10\pi\tau}{10\pi\tau} \qquad (3)$$

Проведенные расчеты показывают, что при осуществлении вращения антенны РЛС кругового обзора со скоростью 6 об/мин, частоте зондирования 350 Гц и ширине диаграммы направленности антенны 1 град. приемное устройство может принять пачку отраженных от цели сигналов, состоящих из 10 импульсов различных частот за время $t_{пр} = 0,028$ сек. Подставив в выражение (3) это время, получим значение коэффициента корреляции между амплитудами отраженных сигналов на одной из частот первого и десятого зондирования $\rho(0,028) = 0,875$.

Данные расчеты показывают, что амплитуды отраженных сигналов при перестройке частоты излучения от импульса к импульсу с частотой 350 Гц подвергаются 13% дополнительной модуляции, которая возникает за счет движения цели. Следовательно, при определении признаков распознавания ее необходимо учитывать.

Для уменьшения этой величины дополнительной модуляции за счет движения цели необходимо либо уменьшать количество используемых частот, либо повышать частоту излучения импульсов разных частот.

При распознавании целей по МЧС в РЛС кругового обзора необходимо учитывать также следующее:

1) на устройства, определяющие признаки распознавания, отраженные сигналы на различных частотах должны поступать одновременно и только от одной цели, то есть необходимо осуществлять стробирование видеотракта приемника РЛС по дальности (времени);

2) влияние диаграммы направленности антенны РЛС на амплитуду принятых на различных частотах сигналов;

3) зависимость мощности отраженных сигналов от дальности цели;

4) изменение потенциала РЛС по времени;

5) так как импульсы на любой из излучаемых частот могут оказаться в начале отраженной от цели пачки импульсов, то возникает необходи-

мость привязки значений амплитуд принятых сигналов к программе получаемых частот перед поступлением их на устройства определения признака распознавания.

На рис. 1 приведена структурная схема одного из возможных устройств учета перечисленных факторов и особенностей РЛС перед вводом значений амплитуд отраженных сигналов в устройства определения признаков распознавания. Данная структурная схема содержит несколько различных схем. Рассмотрим последовательно работу каждой из них.

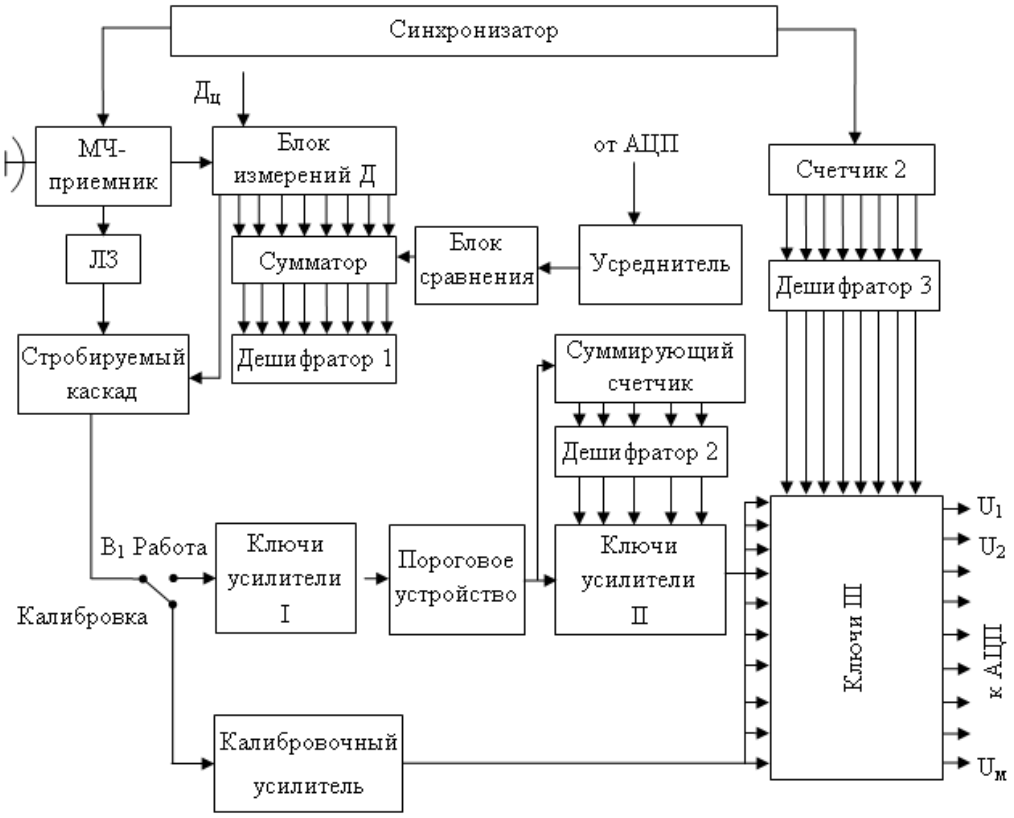


Рис. 1. Структурная схема устройства учета влияния особенностей РЛС

Отраженная от цели многочастотная пачка радиоимпульсов поступает в одноканальный приемник с перестраиваемым гетеродином в соответствии с частотами излученных сигналов, детектируется и поступает в блок измерения дальности до цели и формирования строба. Этот блок формирует на измеренной дальности (времени с момента излучения зондирующего сигнала) строб такой длительности, чтобы в него попал сигнал, отраженный только от одной цели.

Далее импульсы отраженной пачки задерживаются на время формирования строба, проходят стробируемый каскад и поступают на входы ключей-усилителей 1 схемы учета дальности до цели. В нее входят дешифратор 1 и упомянутый выше блок измерения дальности до цели.

В блоке измерения дальности до цели формируется двоичный код дальности, который поступает через сумматор на дешифратор 1. Дешифратор управляет включением соответствующих коду дальности ключей-усилителей 1.

Исследования эффективности распознавания некоторых типов целей, показали, что наиболее оптимальными значениями отношения сигнал/шум на входе приемника для решения задачи распознавания являются величины (20...25) дБ [6]. Поэтому естественно предположить, что амплитуду отраженного от цели сигнала нужно изменить так, чтобы она соответствовала амплитуде отраженного сигнала с дальности R (рис. 2), на которой отношение сигнал/шум равно (20...25) дБ.

Эта дальность может быть либо вычислена при известных характеристиках РЛС, либо найдена экспериментальным путем.

Поскольку амплитуда отраженного сигнала обратно пропорциональна квадрату расстояния до цели, то коэффициент усиления ключей-усилителей следует выбирать пропорционально этой зависимости.

На рис. 2 сплошной и пунктирной линиями приведены соответственно качественные зависимости значений коэффициентов усиления усилителей и амплитуды отраженного сигнала от дальности до цели.

Рассмотрим работу схемы учета изменений потенциала РЛС и методику калибровки РЛС.

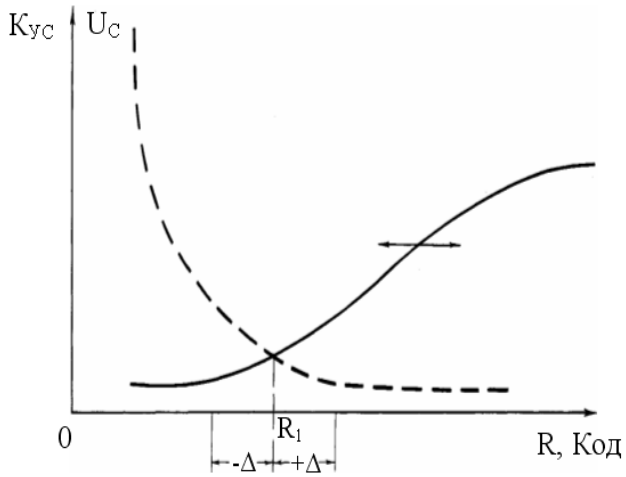


Рис. 2. Зависимости значений коэффициентов усиления
и амплитуды отраженного сигнала от дальности до цели

Так как отношение сигнал/шум, равное (20...25) дБ достигается, в основном, на средних дальностях, где значения коэффициентов ключей-усилителей в схеме учета дальности до цели меняется практически линейно, то влияние изменения потенциала РЛС на амплитуды отраженных сигналов можно учесть с помощью схемы, состоящей из усреднителя, блока сравнения и сумматора (рис. 1).

Основное изменение потенциала РЛС происходит за счет изменения чувствительности приемного устройства. Поэтому калибровку РЛС в режиме боевой работы целесообразно проводить по калибровочному сигналу, вводимому в раскрыв антенны. Для учета долговременных изменений потенциала РЛС за счет изменения мощности передающего устройства, погодных условий и др. необходимо осуществлять настройку описываемой схемы учета изменений потенциала.

Порядок настройки (калибровки) и работа схемы заключается в следующем. Периодически, во время регламентных работ или с изменением условий распространения радиоволн антенна РЛС устанавливается максимумом диаграммы направленности на какой-либо известный местный отражатель или вышку с установленным на ней эталоном (шар, уголковый отражатель).

В схеме устанавливается режим калибровки. При этом сигналы, отраженные от эталона, на всех частотах проходят через блок ключей-усилителей 1 и другие блоки с одинаковым для подобных настроек коэффициентом усиления на аналого-цифровой преобразователь (АЦП).

Коды амплитуд поступают на усреднитель и блок сравнения, где запоминается двоичный код усредненной по частоте амплитуды сигнала, отраженного от эталона. При этом блок измерения дальности формирует код „калибровочной дальности”, то есть включает один из ключей-усилителей 1, коэффициент усиления которого подбирается таким, чтобы сигналы не ограничивались.

В режиме боевой работы подстройка схемы производится следующим образом. После излучения зондирующего сигнала (на малых дальностях) в схеме включается режим подстройки. При этом в раскрыв антенны приемного устройства вводится контрольный сигнал на той же частоте, что и зондирующий, калиброванной мощности.

Поступивший из АЦП код амплитуды контрольного сигнала сравнивается в блоке сравнения с хранившимся там кодом усредненной амплитуды сигнала, отраженного от эталона. Разность этих кодов со своим знаком поступает в сумматор в качестве поправки к коду дальности.

Затем включается режим боевой работы РЛС и поправка к коду дальности будет сохраняться до прихода контрольного сигнала на очередной частоте.

Из рис. 2 видно, что такая поправка к коду дальности как бы „сдвигает” кривую зависимости коэффициентов усиления ключей-усилителей 1 вправо или влево при увеличении или уменьшении потенциала РЛС от первоначального. Очевидно, что такая схема осуществляет также корректировку АЧХ приемного тракта РЛС.

Рассмотрим далее работу схемы учета влияния диаграммы направленности антенны на амплитуды отраженных сигналов в режиме кругового обзора РЛС.

Предварительно заметим, что на малых дальностях цели пачка отраженных сигналов будет иметь число импульсов $M > 10$, так как отраженные сигналы будут приниматься в соответствии с диаграммой направленности по уровню 0,2 Р, а не 0,5 Р, как это предполагалось ранее.

Поэтому целесообразно на входе схемы учета диаграммы направленности установить пороговое устройство.

Таким образом, в состав описываемой схемы входит пороговое устройство, блок ключей-усилителей 2, дешифратор и суммирующий счетчик, который формирует двоичный код номера импульса в пачке. Код поступает на дешифратор 2, который открывает поочередно ключи-усилители 2, коэффициенты усиления которых устанавливаются пропорционально значениям огибающей пачки принятых сигналов. Огибающие пачки можно аппроксимировать функцией типа $\frac{\sin x}{x}$.

Схема разделения каналов не отличается по своему составу от предыдущей, нет только порогового устройства. Схема работает следующим образом. С синхронизатора поступают импульсы на счетчик 2 с частотой зондирования РЛС, при этом в счетчике формируется код номера излучаемой частоты. Обнуление счетчика осуществляется импульсом запуска РЛС на первой частоте. Данный код номера частоты излучаемого импульса поступает на дешифратор, который открывает соответствующий коду ключ.

Таким образом, при излучении импульсов с последовательно меняющейся частотой заполнения, будет открыт ключ номера частоты, на которой излучен зондирующий импульс. Выходы ключей могут быть подключены к АЦП и устройству определения признака распознавания.

Очевидно, что при работе в различных режимах и для различных РЛС могут не понадобиться некоторые из приведенных схем.

Так, например, при работе РЛС в режиме сопровождения цели отпадает необходимость учитывать диаграмму направленности РЛС.

Также необходимо отметить, что необходимость каждой из рассмотренных схем и целесообразность их использования именно в таком виде надо рассматривать при наличии конкретных характеристик РЛС.

Выводы

Таким образом, с помощью предложенных методов и устройства компенсации ошибок получения признаков распознавания можно учесть влияние характеристик трактов различных используемых РЛС и их особенности, которые оказывают существенное влияние на амплитуды отраженного многочастотного сигнала.

Список литературы

1. Радиоэлектронные системы: Основы построения и теория / Под ред. Я.Д. Ширмана. Справочник. – М.: Радиотехника, 2007. – 510 с.

2. Методы радиолокационного распознавания и их моделирование / Я.Д. Ширман, С.А. Горшков, С.П. Лещенко, Г.Д. Братчеко // Зарубежная радиоэлектроника. – 1996. – № 11. – С. 3 – 64.

3. Селекция и распознавание на основе локационной информации / Я.Л. Горелик, Ю.Л. Барабаш, О.В. Кривошеев, С.С. Эпштейн. Под ред. Я.Л. Горелика. – М.: Радио и связь, 1990. – 240 с.

4. Распознавание радиолокационных целей по сигнальной информации / Е.Л. Казаков, Д.Г. Васильев, А.Е. Казаков, Д.Н. Рыжов, А.В. Коломийцев. Под ред. Е.Л. Казакова, - Х.: КП «Городская типография», 2010. – 231 с.

5. Адаптивная обработка сигналов в многопозиционных локаторах при определении признаков распознавания целей / Казаков Е.Л., Батурин О.В., Васильев Д.Г., Казаков А.Е., Коломийцев А.В. Под ред. Е.Л. Казакова. Монография – Х.: КП «Міська друкарня». 2012. – 133 с.

6. Казаков Е.Л. Распознавание радиолокационных целей по некоординатной информации при использовании простых сигналов / Е.Л. Казаков, В.Б. Бзот // Прикладная радиоэлектроника. – Х.: ХНУРЭ, 2002. – Т. 1, № 2. – С. 155 – 164.

Надійшла до редколегії 23.01.2017

Рецензент: д-р техн наук, с.н.с. В.М. Биков, Національний технічний університет імені В.Н. Каразіна, Харків.

МОЖЛИВОСТІ ВРАХУВАННЯ ВПЛИВУ ЧАСОВИХ ФЛУКТУАЦІЙ ИНТЕНСИНОСТЕЙ ВІДОБРАЖЕНИХ БАГАТОЧАСТОТНИХ СИГНАЛІВ І ОСОБЛИВОСТЕЙ РЛС КРУГОВОГО ОГЛЯДУ ПРИ ВИЗНАЧЕННІ ОЗНАК РОЗПІЗНАВАННЯ ЦІЛЕЙ

Є.Л. Казаков, О.Є. Казаков

Розглянуті основні методи та розроблений пристрій компенсації помилок отримання ознак розпізнавання цілей, які виникають за рахунок впливу характеристик трактів різних класів РЛС при використанні багаточастотних сигналів.

Ключові слова: *радіолокаційний сигнал, радіолокаційна мета, модуляція, коефіцієнт кореляції, амплітудні флуктуації, діаграма спрямованості антени, багаточастотний сигнал.*

THE POSSIBILITY OF ACCOUNTING FOR THE EFFECT OF TEMPORARY FLUCTUATIONS INTENSITIES OF THE REFLECTED MULTI-FREQUENCY SIGNALS AND FEATURES THE RADAR OF THE CIRCULAR REVIEW WHEN DEFINING THE CHARACTERISTICS OF TARGET RECOGNITION

E.L. Kazakov, A.E. Kazakov

The basic techniques and developed a compensation device error obtaining characteristics of target recognition that occurs due to the influence of the characteristics of paths of different classes of radar when using multi-frequency signals.

Keywords: *radar signal radar target, modulation, correlation coefficient, amplitude fluctuations, antenna pattern, multi-frequency signal.*

УДК 629.429.3:621.313

О.М. Петренко

Харківський університет міського господарства імені О.М. Бекетова, Харків

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ ВЕНТИЛЯТОРА АСИНХРОННОГО ТЯГОВОГО ДВИГУНА ТРАМВАЙНОГО ВАГОНУ

В статті розроблено методику оптимізації параметрів вентилятора тягового асинхронного двигуна трамвайного вагону, що рухається на ділянці колії с заданим профілем та графіком , яка основана на вирішенні задачі умовної мінімізації за критерієм економічної ефективності системи охолодження методом Вейля за узагальненим золотим перетином.

Ключові слова: *трамвайний вагон, критерій оптимізації, параметри оптимізації, тяговий асинхронний двигун, еквівалентна теплова схема заміщення, рух на ділянці колії, перегрівання над температурою охолоджувального середовища.*

Вступ

Для охолодження асинхронних тягових двигунів (АТД) зі ступенем захисту IP44 та IP54, які застосовуються для сучасних трамвайних вагонів використовуються двоконтурна система самовентиляції до якої входить вентилятор, що безпосередньо встановлений на свобідному кінці валу двигуна та забезпечує потік повітря який охолоджує станину двигуна, а також внутрішній вентилятор, що забезпечує внутрішню циркуляцію внутрішнього повітря. Загальна потужність цих систем становить близько 0,1-1,5% від часової потужності двигуна.

Аналіз останніх досліджень. Режими роботи тягового приводу трамваю залежать від комплексу факторів таких як: ваги потягу; профілю шляху, графіку руху, кліматичних явиш (швидкості вітру, опадів та інші), режимів роботи системи керування тяговим приводом, системи електропостачання та інші [1-6]. Теплові процеси у тягових двигунах характеризуються великими значеннями постійної часу, що може становити 10..30 хв. [1-6]. Нагрів двигуна до постійної температури може тривати 35…100 хв. [1-6]. Однак електромеханічні процеси при русі електрорухомого складу більш динамічні. Режим роботи тягового приводу може змінюватися кілька разів за одну хвилину. Тому для визначення теплового стану тягового двигуна необхідно врахування теплового навантаження за весь час роботи [1,2]. В зв'язку з тим, що при роботі тягового приводу поширені режими вибігу та механічного (пневматичного) гальмування при яких перетворення енергії у тяговому двигуні не відбувається і він перебуває в процесі охолодження, максимальна температура тягового двигуна може бути значно нижче за температуру, що встановилася, та вимагати значно менш потужнішої системи охолодження.

Таким чином оптимізація параметрів вентилятора АТД є актуальною науково-технічною задачею для міського електротранспорту, яку можливо вирішити на основі застосуванням методів оптимізації, як режимів роботи тягового приводу з АТД, так і трамвайного вагону на ділянці колії за оптимальною траєкторією руху, а також з використанням системи охолодження АТД з оптимальними геометричними параметрами.

Для вирішення цієї проблеми можливі наступні шляхи [1, 7-12]. Перший, застосування режимів роботи АТД на електрорухомому складі (ЕРС), який рухається з різною швидкістю та при різних навантаженнях, значно знижують загальний ККД електрорухомого складу [1, 7-12]. Визначення оптимальних за енергоспоживанням режимів руху дозволяє підвищити ефективність системи охолодження тягових двигунів [1, 7-12]. Другим шляхом є підвищення системи охолодження та створення оптимальних за геометрією вентиляторів тягових двигунів. В роботі розглядається оптимізація лише зовнішнього вентилятора тому, як внутрішній вентилятор двигуна є складовою частиною коротко замикаючих кілець ротору і виконує подвійну функцію.

Мета статті: розробка методики оптимізації оптимізація параметрів вентилятора асинхронного тягового двигуна трамвайного вагону.

Результати досліджень

Для вирішення поставленої мети запропоновано застосування методів умовної оптимізації параметрів системи охолодження та вентиляції АТД трамвайного вагона.

В якості критерію у досліджені було обрано критерій економічної ефективності $k_{e,\,e}$, в зв'язку з тим що основні витратами при роботі ЕРС е витрати на його експлуатацію, що пов'язано з досить тривалим строком життєвого циклу транспортних засобів (від 10 до 50 років.), який визначається за виразом [13, 14]:

$$k_{e,e} = Q_{охол} / Q_a, \qquad (1)$$

де $Q_{охол}$ — витрати енергії на охолодження, Q_a — втрати енергії в активних частинах АТД.

Ефективність роботи вентилятора охолодження обумовлюється його розмірами тобто: зовнішній діаметр (D_l) та ширина лопатки (b_l), які можливо обрати у якості параметрів. Усі інші розміри можливо залишити такими як у базовій конструкції двигуна. Обмеження, що накладаються при вирішенні задачі оптимізації параметрів системи охолодження та вентиляції можливо розділити на такі групи.

1. Обмеження у вигляді нерівностей, що накладаються на параметри оптимізації:

$$b_{min} < b_l < b_{max}, \quad (2)$$

$$D_{min} < D_l < D_{max}, \quad (3)$$

де b_{min}, b_{max} – мінімальний та максимальна допустимий розмір лопатки вентилятора, D_{min}, D_{max} – мінімальний та максимальна допустимий розмір лопатки вентилятора. Ці параметри обумовлені конструкцією АТД.

2. Обмеження, що накладаються на максимальний перегрів над температурою охолоджувального середовища елементів конструкції тягових двигунів, що виникає при русі локомотиву з составом на ділянці колії с заданим профілем та графіком руху

$$u_{max} < u_{dop}, \quad (4)$$

де u_{max}, u_{dop} – вектори стовбці перегрівань елементів АТД та допустимих значень цих перегрівань.

Рішення задачі оптимізації проводиться на прикладі руху трамвайного вагона Т-3ВПА з тяговим двигуном АД931 на ділянках колії від трамвайного депо «Салтівське» до розворотного коло 602 мр/н м. Харків та в зворотному, що повторювався чотири рази.

Основні технічні характеристики тягових приводів приведені та результати визначення оптимальних траєкторій руху трамваю приведено у роботі [15].

Далі визначити втрати у елементах АТД трамваю на підставі методики, що наведена у роботах [10-12, 16] результати яких наведено на рис. 1.

За результатам цих залежностей визначаємо витрати енергії в активних частинах АТД можливо визначити за виразом

$$Q_a = \sum_{n=1}^{5} \int_T P_n, \quad (5)$$

де P_1 – втрати у сталі статора; P_2 – втрати у роторі, P_3 – втрати у пазу обмотки статора, P_4 – лобовій частині обмотки статора, P_5 – механічні втрати.

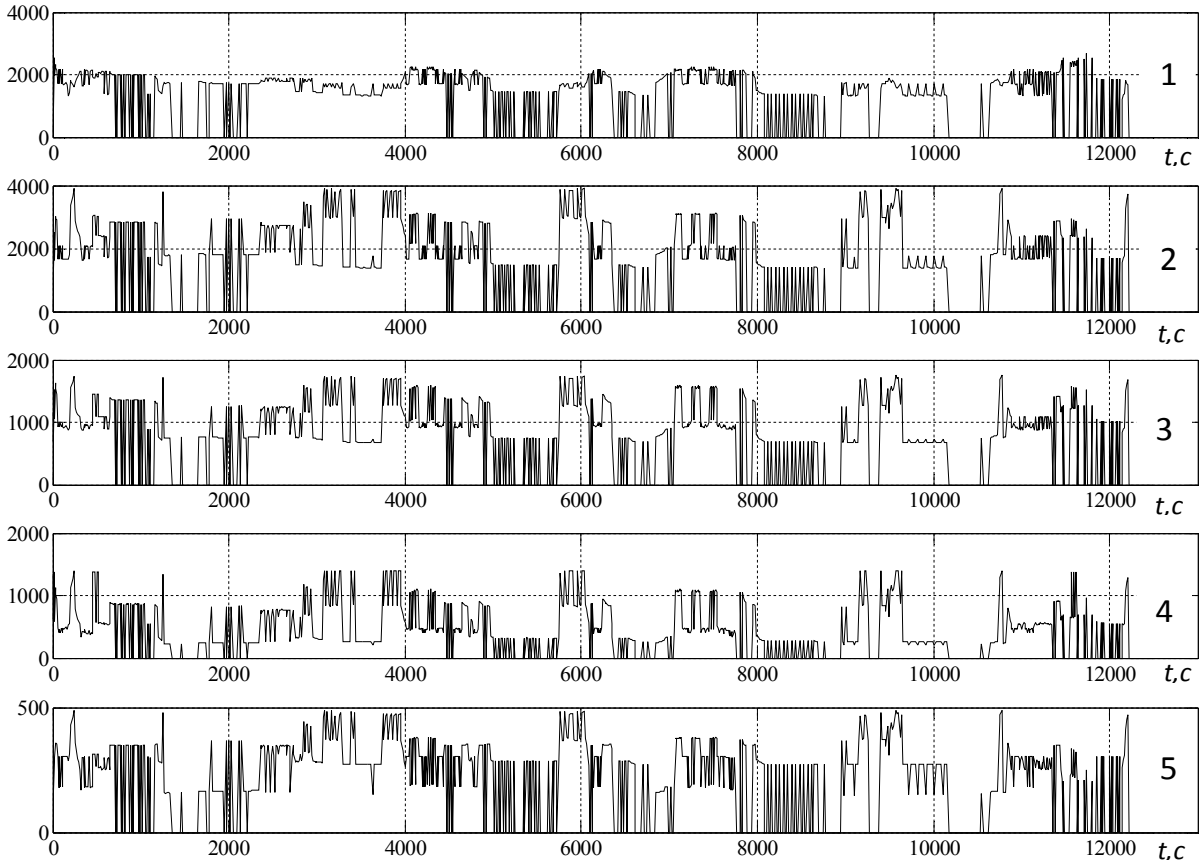


Рис. 1. Втрати у тяговим двигуном: 1 – втрати у сталі статора P_1, Вт ; 2 – втрати у роторі P_2, Вт, 3 –пазової частині обмотки статора P_3, Вт, 4 – лобовій частині обмотки статора P_4, Вт, 5 – механічні втрати P_5, Вт

Ці результати є вхідними даними для вирішення задачі аналізу яка базується на методиці моделювання теплових режимів яка наведена в роботах [10-12]. Відповідно до цієї методики пропонується застосування універсальної еквівалентної теплової схеми, що дозволяє виконувати теплові розрахунки нестаціонарних режимів роботи АТД за різних систем охолодження. В роботах [10-12,16] розглянуто використання універсальної теплової схеми для теплових розрахунків асинхронних двигунів регульованих електроприводів для двигунів зі ступенем захисту IP44, IP54 до яких належить АД 931. Його еквівалентна теплова схема зображена на рис.2. Для розрахунку еквівалентної теплової схеми пропонується використати метод вузлових потенціалів для електричних кіл.

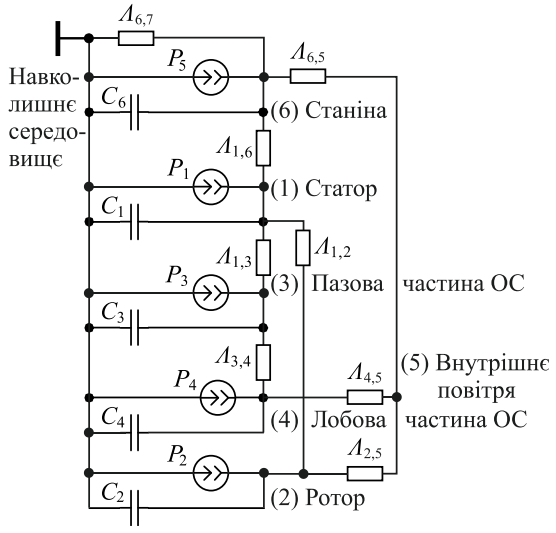


Рис. 2. Еквівалентна теплова схема для АТД з ступенем захисту IP44, IP54

На його підставі для запропонованої універсальної еквівалентної теплової схеми може бути складена система диференціальних рівнянь теплового балансу.

У матричному виді система представляється системою рівнянь:

$$\frac{d}{dt}u = [C]^{-1} \cdot [ДР + Л \times u], \qquad (6)$$

де u – матриці-стовпці середніх перегрівань над температурою охолоджувального середовища у відповідних конструктивних елементах електричної машини, С – матриця теплоємкостей відповідних конструктивних елементів, на які умовно розбивається АТД, ДР – матриця-стовпець потужностей тепловиділення у відповідних конструктивних елементах АТД, Л – матриця теплових провідністей.

Величини потужностей тепловиділення розраховуються за втратами в елементах АТД, які змінюються за часом. в залежності від режиму роботи тягового приводу, що наведені на рис. 1 та в роботі [15] Також змінюються і провідності схеми заміщення в залежності від потоку повітря, що створює вентилятор та залежать від параметрів які прийняті для вирішення задачі аналізу.

Для визначення обмеження (4) проводиться аналіз змін перегрівань елементів АТД за весь час моделювання теплових режимів за виразом

$$u_{max} = MAX(u). \qquad (7)$$

Потужність, що втрачається при роботі вентилятора визначається за виразом [17, 18]

$$P_{вен} = \frac{\Delta p \, Q_v}{\eta_v}, \qquad (8)$$

де Δp – тиск повітря в вентиляторі, Q_v – потік повітря у вентиляторі, η_v – ККД вентилятора, які визначаються за результатами вентиляційного розрахунку за методикою наведеною в [17,18] та залежать від геометрії вентилятора та частоти його обертання.

Втрати потужності на охолодження знаходяться за виразом

$$Q_{вен} = \int_T P_{вен}, \qquad (9)$$

де T – інтервал часу руху ЕРС.

Результатом вирішення задачі аналізу є знаходження критерію оптимізації за виразом (1).

За результатами вирішення тестових задач оптимізації параметрів вентилятора АТД найкращій результат показав метод Вейля за узагальненим золотим перетином.

Хід вирішення задачі наведено на рис. 3 (ромбом позначена оптимальна точка, круг – стартова.).

Отримані наступні оптимальні значення зовнішній діаметр вентилятора $D_l = 308{,}2$ *мм*, а ширина лопатки вентилятора b_l – 15,7 *мм*.

Критерій оптимальності у розглянутій задачі становив значення 0,0408. Порівняно з базовою конструкцією він знизився на 27,6%. (0,052).

Результати моделювання теплових режимів АТД при оптимальних значеннях параметрів вентилятора приведені на рис. 4.

Як видно з графіків найбільше перегрівання має лобова частина обмотки статору АТД, що складає 139,6 °С на 3363с з початку руху і не перевищує допустиме значення у 140 °С.

Висновки

Розроблено методику оптимізації параметрів вентилятора тягового асинхронного двигуна, що рухається на ділянці колії с заданим профілем та графіком особливості якої є наступне:

– методика основана на вирішенні задачі умовної мінімізації за критерієм економічної ефективності системи охолодження методом Вейля за узагальненим золотим перетином;

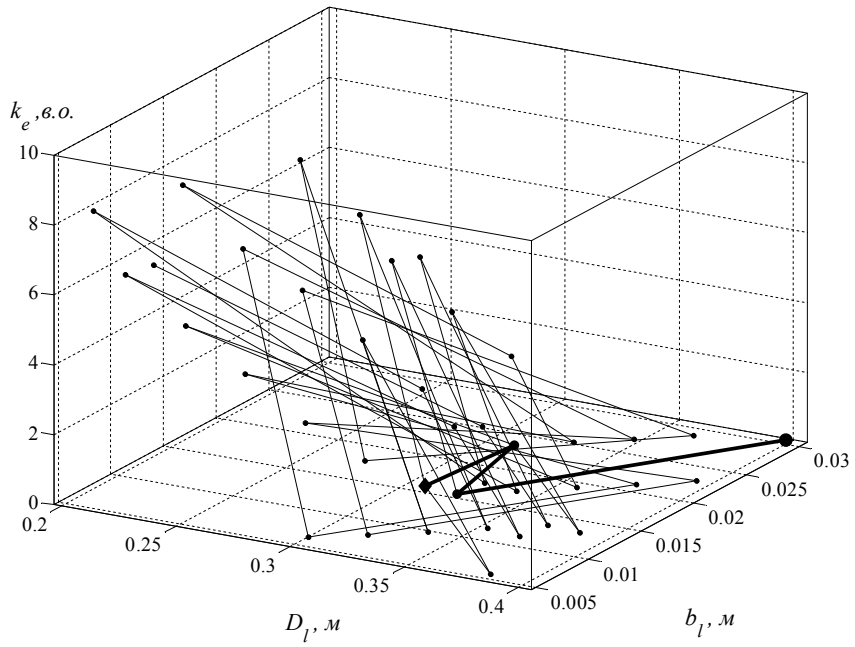


Рис. 3. Хід вирішення задачі мінімізації

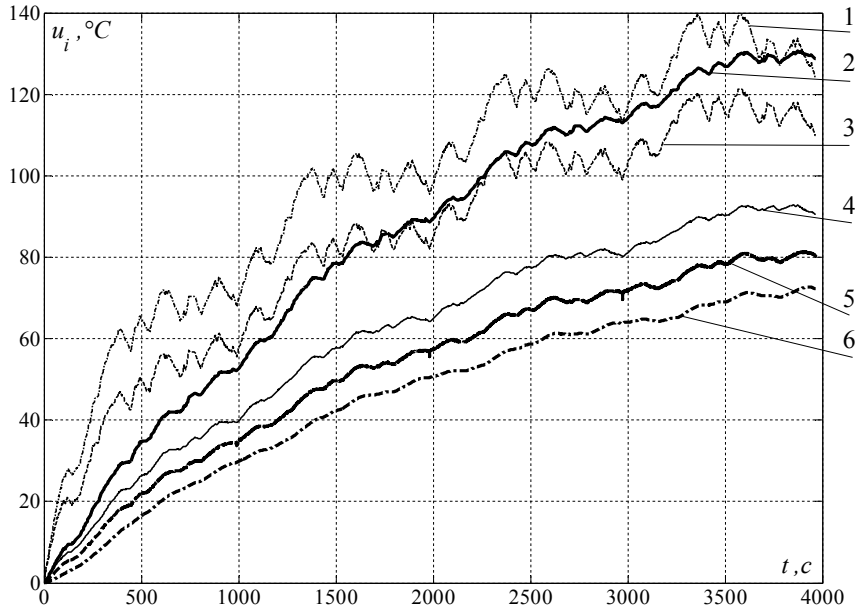


Рис. 4. Результати моделювання теплового стану тягового двигуна АД931 встановленого у трамвайному вагоні Т-3ВПА, який рухається на ділянках колії від трамвайного депо «Салтівське» до розворотного коло 602 мр/н м. Харків та в зворотному напрямі, що повторювався чотири рази. Залежності перегрівань над температурою охолоджувального середовища °С від часу: 1 – лобової частини обмотки статора, 2 – ротору; 3 – пазової частини обмотки статора; 4 – осердя статора, 5 – внутрішнє повітря, 6 – станини

– в якості параметрів оптимізації обрані наступні величини: зовнішній діаметр та ширина лопатки;

– задача аналізу системи охолодження тягових двигунів основана на моделюванні теплових режимів АТД за узагальненою еквівалентною тепловою схемою.

Вирішення тестової задачі проведено на прикладі тягового двигуна АД931 встановленого у трамвайному вагоні Т-3ВПА, який рухається на ділянках колії від трамвайного депо «Салтівське» до розворотного коло 602 мр/н м. Харків та в зворотному напрямі, що повторювався чотири рази отримані такі оптимальні значення:

– діаметр вентилятора D_l = 308,2 мм,

– ширина лопатки вентилятора b_l – 15,7 мм,

– критерій оптимальності у розглянутій задачі становив значення 0,0408.

Встановлено, що порівняно з базовою конструкцією критерій ефективності знизився на 27,6%. (0,052).

За результатами моделювання АТД з оптимальним вентилятором встановлено, що найбільше пере-

грівання має лобова частина обмотки статору АТД, що складає 139,6 °С на 3363с з початку руху і не перевищує допустиме значення у 140 °С.

Список літератури

1. Любарський Б.Г. Теоретичні основи для вибору та оцінки перспективних систем електромеханічного перетворення енергії електрорухомого складу. – Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.22.09. - «Електротранспорт». Національний технічний університет «Харківський політехнічний інститут». Харків, - 2014. – 368 с.

2. Гетьман Г.К. Научные основы определения рационального мощностного ряда тяговых средств железнодорожного транспорта [Текст]: монография / Г.К. Гетьман. – Д.: Изд. Днепр. нац. ун-та ж/д трансп. им. акад. В. Лазаряна, 2008. – 444 с.

3. Мокін О.Б. Моделювання та оптимізація руху багатомасових електричних транспортних засобів поверхнями зі складним рельєфом : монографія / О. Б. Мокін, Б. І. Мокін. – Вінниця : ВНТУ, 2013 . – 192 с.

4. Дмитриенко В.Д. Моделирование и оптимизация процессов управления движением дизель-поездов / В.Д. Дмитриенко, А.Ю. Заковоротный. - Х.: Изд. центр "НТМТ", 2013. – 248 с.

5. Петренко О.М. Визначення ефективності електрорухомого складу. Основні положення та підходи / О.М. Петренко, Б.Г. Любарський // Інформаційно-керуючі системи на залізничному транспорті. – 2015. № 6 – С. 8-13.

6. Todorov, Emanuel. "Optimal control theory." Bayesian brain: probabilistic approaches to neural coding (2006): 269-298.

7. Kappen, Hilbert J. "Optimal control theory and the linear bellman equation."Inference and Learning in Dynamic Models (2011): 363-387.

8. Петренко О. М. Алгоритм синтезу експертної системи управління рухом електрорухомого складу на основі рішення рівняння Гамільтона-Якобі-Беллмана / О. М. Петренко, Б. Г. Любарський, М. Л. Глєбова // Вісник Нац. техн. ун-ту "ХПІ" : зб. наук. пр. Темат. вип.: Математичне моделювання в техніці та технологіях– Харків : НТУ "ХПІ", 2016. – № 6 (1178). – С. 89-95.

9. Петренко О.М. Методика оптимізації режимів роботи асинхронного тягового приводу рухомого складу/ О.М. Петренко, І.В. Доманський, Б.Г. Любарський // Механіка та машинобудування. – 2016.– №1. – С.59-67

10. Петренко О. М. Алгоритм синтезу експертної системи управління рухом електрорухомого складу на основі рішення рівняння Гамільтона-Якобі-Беллмана / О. М. Петренко, Б. Г. Любарський, М. Л. Глєбова // Вісник Нац. техн. ун-ту "ХПІ" : зб. наук. пр. Темат. вип. : Математичне моделювання в техніці та технологіях– Харків : НТУ "ХПІ", 2016. – № 6 (1178). – С. 89-95.

11. Петренко О.М. Математична модель оптимального керування рухом електрорухомого складу на підставі вирішення рівнянь Гамільтона-Якобі-Беллмана/ О.М. Петренко, Б.Г. Любарський // Інформаційно-керуючі системи на залізничному транспорті. – 2016. – № 2. – С. 19-24

12. Петренко О.М. Методика оптимізації режимів роботи асинхронного тягового приводу рухомого складу/ О.М. Петренко, І.В. Доманський, Б.Г. Любарський // Механіка та машинобудування. – 2016.– №1. – С. 59-67.

13. Борисенко А.И. Аэродинамика и теплопередача в электрических машинах / А.И. Борисенко, В.Г. Данько, А.И. Яковлев. – М.: Энергия, 1974. – 560 с.

14. Борисенко А.И. Охлаждение промышленных электрических машин / А.И. Борисенко, О.Н. Костиков, А.И. Яковлев. – М.: Энергоатомиздат, 1983. – 296 с.

15. Петренко О.М. Оптимізація режимів руху трамвайного вагону з асинхронними тяговими двигунами на ділянці колії з встановленим графіком руху та профілем / О.М. Петренко, Б.Г. Любарський // Системи управління, навігації та зв'язку. – 2016. – № 4(40). – С. 36-40.

16. Петрушин В.С. Расчет температур конструктивных элементов асинхронных двигателей в динамических режимах/ В.С. Петрушин, С.В. Рябинин, А.М. Якимец // Вісник Національного університету «Львівська политехніка», – 2000. – № 403. – С. 145 – 149.

17. Филиппов И.Ф. Теплообмен в электрических машинах./ И.Ф. Филиппов. - Л.: Энергоатомиздат. Ленингр. отд-ние, 1986. – 256 с.

18. Сипайлов Г. А., Тепловые, гидравлические и аэродинамические расчеты в электрических машинах./ Г.А.Сипайлов, Д.И.Санников, В. А. Жадан. – М.: Высш. шк., 1989. – 239 с.

Надійшла до редколегії 18.12.2016

Рецензент: д-р техн. наук, проф. В.Т. Доманський, Національний технічний університет «Харківський політехнічний інститут», Харків.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ ВЕНТИЛЯТОРА АСИНХРОННОГО ТЯГОВОГО ДВИГАТЕЛЯ ТРАМВАЙНОГО ВАГОНА

А.Н. Петренко

В статье разработана методика оптимизации параметров вентилятора тягового асинхронного двигателя трамвайного вагона, движущегося на участке пути с заданным профилем и графиком, основанная на решении задачи условной минимизации по критерию экономической эффективности системы охлаждения методом Вейля по обобщенному золотому сечению.

Ключевые слова: *трамвайный вагон, критерий оптимизации, параметры оптимизации, тяговый асинхронный двигатель, эквивалентная тепловая схема замещения, движение на участке пути, превышение температуры над температурой охлаждающей среды.*

OPTIMIZATION OF PARAMETERS OF THE FAN OF THE ASYNCHRONOUS TRACTION ENGINE OF A TRAW WAGON

O.M. Petrenko

In the article the technique of optimization of the fan parameters of a traction asynchronous motor of a tram car moving on a section of a path with a given profile and schedule is developed based on solving the problem of conditional minimization by the criterion of the economic efficiency of the cooling system by the Weyl method over the generalized golden section.

Keywords: *Tram car, optimization criterion, optimization parameters, traction asynchronous motor, equivalent thermal replacement circuit, movement on the section of the track, excess of temperature above the temperature of the cooling medium.*

УДК.621.396.62.33

В.В. Печенин, К.А. Щербина, М.А. Вонсович, Ю.В. Съедина

Национальный аэрокосмический университет имени Н. Е. Жуковского «ХАИ», Харьков

ОЦЕНКА КАЧЕСТВА ФИЛЬТРАЦИИ СПЕКТРА ДОПЛЕРОВСКОГО СИГНАЛА, ОТРАЖЕННОГО ОТ ПОДСТИЛАЮЩЕЙ ПОВЕРХНОСТИ, СЛЕДЯЩИМ МОДУЛИРОВАННЫМ ФИЛЬТРОМ

Цель выполненных в работе исследований состояла в улучшении показателей качества приема и обработки доплеровского сигнала с детерминированной основой спектра, обусловленной скоростью движения летательного аппарата, наличием аддитивных помех и влиянием радиофизических свойств подстилающей поверхности. В работе разработан метод основанный на использовании резонансного фильтра с модулируемой емкостью, что обеспечило увеличение помехоустойчивости по сравнению с методом следящего гетеродина в пределах 2…3 дБ.

Ключевые слова: *следящий доплеровский фильтр, фильтрация, показатели качества, следящий прием, частота.*

Введение

Становление и развитие автономных радиотехнических систем, как самостоятельного класса систем, способных решать весьма широкий круг экономических и иных задач в интересах Украины, является важной научно-технической проблемой, требующей постоянного внимания.

Наиболее распространенными и широко применяемыми на практике, являются автономные радиотехнические системы, предназначенные для измерения вектора воздушной скорости летательных аппаратов различного назначения.

Успешное выполнение самых разных задач автономными радиотехническими системами возможно только на основе дальнейшего совершенствования методов и устройств приема и обработки доплеровской информации, осуществляемой с помощью следящих радиолокационных измерителей скорости движущихся объектов [1]. В практически реализуемых следящих измерителях особое внимание уделяется резонансным трактам следящего приема и обработки доплеровского сигнала, формируемого протяженной отражающей поверхностью в присутствии аддитивного шума [1, 2].

Основным элементом резонансного тракта следящего приема является следящий узкополосный фильтр (УПФ) с фиксированной полосой и резонансной частотой настройки [3]. При этом процесс слежения за изменяющейся средней частотой доплеровского спектра осуществляется гетеродинным методом при обязательном наличии отдельной системы поиска и захвата доплеровского сигнала [4], поиска и захвата средней частоты спектра.

Традиционные следящие УПФ реализуются на основе известных схем фазовой и частотной автоподстройки частоты управляемого генератора (ФАПЧ и ЧАП), а также комбинированных схем, улучшающих по некоторым показателям качества работы существующие УПФ, построенные на основе традиционных следящих систем. Известны комбинированные следящие УПФ, осуществляющие автоподстройку частоты и фазы синхронизированного управляемого генератора [5]. Системы данного класса, по ряду показателей качества работы превосходят известные схемы ФАПЧ, ЧАП и комбинированные системы, построенные на простом генераторе с одним управляющим входом [6].

Интересным направлением дальнейшего развития следящих УПФ, является отказ от существующих схем, построенных на управляемых генераторах путем их замены следящим модулированным фильтром (МФ) [7].

Однако, здесь остается нерешенной, как в теоретическом, так и особенно в экспериментальном направлениях, задача оценки качества фильтрации спектра доплеровского сигнала в условиях влияния аддитивных помех с известными статистическими характеристиками.

Цель выполненных в работе исследований состояла в теоретическом анализе показателя качества фильтрации спектра доплеровского сигнала следящим модулированным фильтром и экспериментальным исследованием фильтрующих свойств следящего МФ методом имитационного моделирования динамических систем при воздействии аддитивной нормальной с учетом влияния радиофизических свойств подстилающей поверхности.

Изложение основного материала

Статистическая модель доплеровского сигнала, отраженного протяженной поверхностью.

Специфика функционирования реальных доплеровских измерителей скорости (ДИС) летательного аппарата предполагает наличие на отражающей поверхности “светящихся” точек, количество кото-

рых ограничено размерами площади поверхности [8]. При этом "светящиеся" точки порождают статистически "независимые" элементарные сигналы, так что наблюдаемый на входе приемного тракта ДИС результирующий сигнал представляется в виде аддитивной суммы элементарных сигналов. Опираясь на результаты исследований, выполненных в [9, 10] статистическую модель наблюдаемого в точке приема, то есть на борту летательного аппарата (ЛА), можно представить в аналитической форме следующим образом:

$$S(\lambda_a(t),\lambda_ч(t),\omega_Д,t)=E_0[1+M_{AM}\lambda_a(t)]\times \\ \times\sin[\omega_0 t+M_{ЧМ}\int_0^t\lambda_ч(\tau)d\tau+\omega_Д t+\varphi(t)], \quad (1)$$

где E_0, ω_0 - априорно известные амплитуда и частота; $\omega_Д t$ - составляющая полной фазы полезного сигнала, которая является медленно меняющейся "регулярной" функцией обусловленной эффектом Доплера, возникающим за счёт движения ЛА с радиальной скоростью Vr; $\varphi(t)$ - случайная начальная фаза; M_{AM} - коэффициент амплитудной модуляции; $M_{ЧМ}$ - индекс частотной модуляции.

Функции $\lambda_a(t)$ и $\lambda_ч(t)$ представляют собой случайные функции, порождаемые радиофизической структурой отражающей поверхности, модулируют амплитуду и частоту сигнала $S(\cdot)$, где частота $\omega_Д$ - медленно изменяющаяся регулярная функция, связанная с радиальной скоростью движения ЛА простым соотношением:

$$\omega_Д=\frac{4\pi Vr}{\lambda_0}=\frac{4W_П}{\lambda_0}\cos\beta_0, \quad (2)$$

где β_0 - угол между направлением вектора путевой скорости ЛА и направлением приема (излучения) сигнала, определяемым угловым положением диаграммы направленности антенной системы ДИС относительно отражающей поверхности. Ширина спектра доплеровского сигнала принимаемого на борту ЛА определяется соотношением:

$$\Delta\omega_Д=\frac{4\pi W_П}{\lambda_0}\sin\beta\Delta\beta_{0.5}, \quad (3)$$

где $\beta_{0.5}$ - ширина двухсторонней на (прием и передачу) диаграммы направленности i-го луча ДИС.

При конкретизации статистического описания случайных модулирующих процессов $\lambda_a(t)$ и $\lambda_ч(t)$, в частности, при релеевских флуктуациях амплитуды и равномерном распределении фазы сигналов, формируемых "светящимися" точками (12), случайные процессы $\lambda_a(t)$ и $\lambda_ч(t)$ удобно писать в виде стохастических дифференциальных уравнений марковских случайных процессов:

$$\dot{\lambda}_a(t)=\alpha_1\lambda_1+N_{01}/(4\lambda_1)+n_{01}(t), \quad (4)$$

$$\dot{\lambda}_ч(t)=-\alpha_2\lambda_2+n_{02}(t), \quad (5)$$

где α_1 и α_2 - величины, обратные интервалу корреляции амплитудных τ_a и частотных флуктуаций; $n_{01}(t)$, $n_{02}(t)$ - нормальные "белые" шумы с нулевым средним и дельта функцией корреляции; N_{01} - спектральная плотность мощности амплитудной флуктуации; $\lambda_1=E_0$ - амплитуда; $\lambda_2=\varphi$ - фаза сигнала.

Как следует из (1), процесс формирования отраженного от подстилающей поверхности доплеровского сигнала при ее зондировании непрерывным гармоническим сигналом, сопровождается преобразованием непрерывного сигнала в амплитудно-частотно модулированный сигнал. (АМ-ЧМ сигнал), что определяет в дальнейшем построение и анализ фильтрующих схем спектра допплеровского сигнала, принимаемого на фоне аддитивного гауссовского шума.

Анализ статистической структуры спектра доплеровского сигнала, отраженного подстилающей поверхностью

Детальный анализ статистической структуры спектра доплеровского сигнала при случайном характере модулирующей функции $\lambda_ч(t)$ практически невозможен (10). Здесь естественен переход от поэлементного анализа и построению более общих корреляционных характеристик, а затем к исследованию статистической структуры спектра.

В общем случае угловой модуляции при $E_0=1$ и $M_{AM}=0$ сигнал (1) запишем в виде

$$S[\lambda_ч(t),\Delta\omega_Д,t]=\cos[\omega_0 t+\Delta\psi(t)], \quad (6)$$

где $\Delta\psi(t)=\int\Delta\omega_Д(t)dt.$.

При $\Delta\psi(t)=M_{ЧМ}=\Delta\omega_Д/\Omega$, невозможно отличить фазовую модуляцию (ФМ) от частотной модуляции (ЧМ). Под Ω следует понимать характеристическую частоту случайного процесса $\xi(t)$:

$$\Omega=\sqrt{8\alpha_1\alpha_2-(\alpha_1+\alpha_2)^2+4\alpha_2\sqrt{\alpha_1(2\alpha_1-\alpha_2)}}. \quad (7)$$

Выражение (7) представляет интерес с точки зрения возможности представления модулирующей функции $\lambda_ч(t)\equiv\xi(t)$, обладающей характеристической частотой, определяемой выражением (7).

Выражение (6) можно преобразовать к виду

$$S[\cdot]=\cos\Delta\psi(t)\cos\omega_0 t-\sin\Delta\psi(t)\sin\omega_0 t. \quad (8)$$

То есть ЧМ-колебания (7) можно представить в виде суммы двух ортогональных АМ-колебаний $S_c(t)$ и $S_s(t)$ с огибающими $\cos\Delta\psi(t)$ и $\sin\Delta\psi(t)$ соответственно.

Опуская промежуточные преобразования при вычислении функции корреляции можно получить

$$R(\tau)=\frac{1}{2}\cos\omega_0\tau\overline{\cos x}, \quad (9)$$

$$X=\Delta\psi(t+\tau)-\psi(t). \quad (10)$$

Черта сверху $\overline{\cos x}$ – временное усреднение.

По формуле (9) для конкретных модулирующих процессов с известным законом распределения вероятностей можно получить $R(\tau)$, а затем использовав преобразование Винера-Хинчина, вычислить энергетический спектр ЧМ колебаний

$$G(\omega)=4\int_0^\infty R(\tau)\cos\omega\tau d\tau. \quad (11)$$

При ЧМ-модуляции гармонической несущей случайной моделирующие функцией $\lambda_Ч(t)\approx\Omega$ выражение для энергетического спектра имеет вид:

$$G(\omega)=\int_0^\infty\cos(\omega-\omega_0)\tau e^{-\Delta\psi_{эф}^2[1-r_x(\tau)]}dt, \quad (12)$$

где $r_x(\tau)$ - коэффициент корреляции $\Delta\psi(t)$,

$\Delta\psi_{эф}^2$ - средний квадрат девиации фазы.

При $\omega=\omega_0$ интеграл (12) расходится. Это говорит о наличии в спектре на частоте ω_0 дискретной линии. Однако, для доплеровского сигнала, отраженного от подстилающей поверхности $\omega_Д$ входит в гармоническую несущую, излучаемую с борта ЛА.

Чтобы обойти эту трудность, необходимо представить $G(\omega_0)$ в виде суммы дискретной несущей и непрерывных боковых полос. При этом энергетический спектр модулирующей функции Ω должен быть известен, поскольку он определяет вид коэффициента $r_x(\tau)$. Тогда при широкополосной ЧМ-модуляции ($\Delta\psi_{эф}>>1$), спектр имеет вид

$$G(\omega)=\sqrt{\frac{\pi}{2}}\frac{1}{\Delta\omega_{эф}}\exp\left(-\pi\cdot(\omega-\omega_0)^2\Big/\left(2\Delta\omega_{эф}^2\right)\right). \quad (13)$$

Если положить $\Delta\omega_{эф}=\Delta\omega_Д$, то выражение (13) с точностью до энергетического множителя P равного мощности отраженного от протяженной поверхности доплеровского сигнала совпадает с выражением для $G(\omega)$, полученным в (16) для равномерного прямолинейного движения ЛА на постоянной высоте H со скоростью $W_П$.

При узкополосной ЧМ-модуляции ($\Delta\psi_{эф}^2<<1$) интенсивность несущей максимальна и от модулирующей функции не зависит. Тогда

$$G(\omega)=\pi\delta(\omega-\omega_0)+\frac{1}{2}\Delta\psi_{эф}^2G_\Omega(\omega-\omega_0), \quad (14)$$

где $G_\Omega(\omega-\omega_0)=4\int_0^\infty r_x(\tau)\cos\omega\tau d\tau$ - безразмерный энергетический спектр модулирующего процесса; $\delta(\omega-\omega_0)$ - дельта функция.

Если заменить ω_0 на $\omega_Д$, а $\Delta\omega_{эф}$ на $\Delta\omega_Д$, то с точностью до P получим выражение для энергетического спектра отраженного сигнала

$$G_{отр}(\omega)=P\frac{1}{\Delta\omega_Д}\exp\left(-\pi(\omega-\omega_Д)^2\Big/\left(2\Delta\omega_Д^2\right)\right). \quad (15)$$

Таким образом, можно полагать, что при широкополосной ЧМ выражения (13) и (15) полностью эквивалентны. Но с другой стороны нельзя игнорировать отсутствие в (15) дискретной компоненты $\pi\delta(\omega_Д)$. Тогда на физическом уровне можно записать следующее выражение для спектра доплеровского сигнала, отраженного от подстилающей поверхности

$$G^*(\omega)=\pi\delta(\omega-\omega_Д)+P\frac{1}{\Delta\omega_Д}e^{-\pi(\omega-\omega_Д)^2\Big/\left(2\Delta\omega_Д^2\right)} \quad (16)$$

и считать энергетический спектр доплеровского сигнала представленного формулой (1) широкополосным, а сам доплеровский сигнал считать широкополосным ЧМ сигналом и с учетом АМ модуляции АМ-ЧМ сигналом.

Следящий модулированный фильтр с самосинфазированием

Единая теория модулированных фильтров, и в первую очередь следящих фильтров ЧМ сигналов и родственных им систем оптимального приема ЧМ сигнала, нашедших широкое применение в системах связи, радиолокации, радионавигации и радиоуправления изложено в [9]. Однако теория приема и обработки сигналов следящими доплеровскими измерителями, обладающих частотным спектром с детерминированной основой (регулярной медленно меняющейся частотой Доплера) отнесена в [9] к перспективному направлению теоретических и экспериментальных исследований. Согласно существующей терминологии термин “следящий” подразумевает “мгновенную” перестройку рабочей частоты резонансного фильтра, именуемого модулированным фильтром с полезными компонентами спектра ЧМ сигнала синфазно. В нашем случае термин “следящий” включает в себя возможность отслеживания кроме смысла, изложенного в [9], отслеживание детерминированной компоненты с медленно изменяющейся частотой. Функциональная схема такого следящего модулированного фильтра приведена на рис. 1.

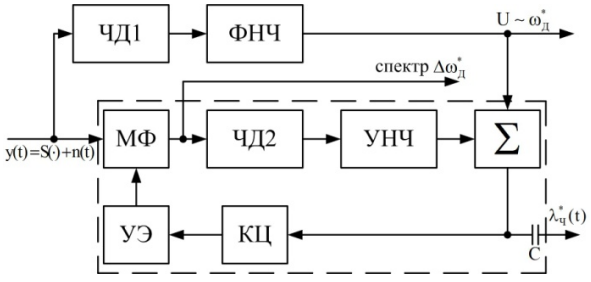


Рис. 1. Функциональная схема следящего МФ с самосинфазированием

В схеме, показанной на рис. 1, введены следующие обозначения: ЧД1, ЧД2 - частотные дискриминаторы; ФНЧ - фильтр нижних частот; УНЧ - усилитель низкой частоты; КЦ - корректирующая цепь; УЭ - управляющий элемент; Σ - сумматор; С - разделительная емкость. Теоретические и экспериментальные исследования классической схемы модулированного фильтра с самосинфазированием МФС, содержащей блоки функциональной схемы, обведены штриховой линией, достаточно подробно изложены в [9]. Режим слежения за средней частотой $\Delta\omega_{Д}^{*}$ в схеме рис. 1 обеспечивается трактом, состоящим из блоков ЧД и ФНЧ с большой постоянной времени $T_{Ф}$, которая зависит от динамики движения ЛА. При сравнении помехоустойчивости обычного ЧМ приемника со следящим гетеродином и ЧМ приемника со следящим фильтром в тракте промежуточной частоты может быть достигнуто уменьшение синфазной составляющей мощности шумов, а с ней и надпороговой мощности полезного сигнала $\frac{(P_{Ш\,синф})_{ПЧ}}{(P_{Ш\,синф})_{СМФ}} \simeq \frac{\Delta\omega_{ПЧ.Ш}}{\Delta\omega_{СМФ.Ш}} \simeq M_{ЧМ} = \frac{\Delta\omega_{Д}}{\Omega}$, или надпорогового напряжения полезного сигнала в $\sqrt{\beta}$ раз.

Выбор показателя качества фильтрации следящего МФ с самосинфазированием и методика его оценки по спектральным измерениям

Из приведенного выше достаточно упрощенного рассмотрения следящего МФ с самосинфазированием (СМФС) следует, что основным показателем качества работы СМФС является помехоустойчивость приема ЧМ сигнала, зависящая от соотношения шумовой полосы резонансного тракта приемника до частотного дискриминатора к шумовой полосе после частотного дискриминатора в надпороговой области.

Как следует из теории работы МФС, как системы с замкнутой петлей управления [9], основой оценки помехоустойчивости МФС, а следовательно, и СМФС является эквивалентная частотная характеристика (ЭЧХ) управляемого контура

$$K_{\Sigma}(j\Omega) = 1\Big/\Big(1+\big(j\Omega/\Delta\omega_{эф}\big)\cdot\big[1-K_{\Sigma}(j\Omega)\big]\Big). \quad (17)$$

ЭЧХ дает возможность рассчитать частотные искажения ЧМ сигнала и нелинейные искажения модулирующей функции. Воспользуемся на формальном уровне таким же определением качества работы, а именно, фильтрации СМФС как и для обычного ЧМ приемника с той лишь разницей, что соответствующие соотношения сигнал/шум по мощности будем оценивать (измерять) на входе и выходе МФ считая, что центральная частота, настройки МФ является постоянной $f_{О.МФ} = \omega_{Д}^{*}/(2\pi)$, а полоса пропускания $\Delta\omega_{эф} \geq \Delta\omega_{Д}$.

Запишем выражение для оценки качества фильтрации спектра (т.е. качества работы МФ) доплеровского сигнала при наличии шума

$$A = \big(\overline{P}_{с.вых}/\overline{P}_{ш.вых}\big)\Big/\big(\overline{P}_{с.вх}/\overline{P}_{ш.вх}\big), \quad (18)$$

где $\overline{P}_{с.вых}$, $\overline{P}_{с.вх}$ - средние значения мощностей сигнала на входе и выходе МФ; $\overline{P}_{ш.вых}$, $\overline{P}_{ш.вх}$ - средние значения мощностей шума на входе и выходе МФ. Черта сверху означает усреднение по спектральным компонентам ЧМ сигнала и шума.

Из теории спектрального анализа [9] известно, что средняя мощность сигнала x(t), прошедшего узкополосный фильтр F (по предположению идеальный) с полосой пропускания $\Delta\omega$, центральной частотой ω_0 и коэффициентом усиления внутри полосы $(\omega_0 - \Delta\omega/2,\ \omega_0 + \Delta\omega/2)$ равным 1, будет определяться выражением

$$\overline{P}_{с.вых} = \lim_{T\to\infty}\int_{-T/2}^{T/2}\Big|x_F(t)^2\,dt\Big|. \quad (19)$$

Так как фильтр пропускает только часть спектра сигнала, заключенную в полосе $\Delta\omega$, то средняя мощность сигнала на выходе

$$\overline{P}_{с.вых} = \int_{\omega_0-\Delta\omega/2}^{\omega_0+\Delta\omega/2} S_x(\omega)\,d\omega. \quad (20)$$

Величину $S_x(\omega)$, входящую в (20) именуют спектральной плотностью.

Сравнивая (19) и (20) получим

$$\int_{-\infty}^{\infty} S_x(\omega)\,d\omega = \lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2}\Big|x(t)^2\,dt\Big| = \overline{P}_{с.вых}. \quad (21)$$

Для определения $S_x(\omega)$ нужно устремить $\Delta\omega \to 0$. Но это означает, что на выходе фильтра будет очень слабый сигнал, который трудно измерить (кроме случая при котором спектр содержит дискретную компоненту т.е. $\omega_{Д}^{*}$)

На практике для вычисления $\overline{P}_{с.вых}$, $\overline{P}_{с.вх}$ необходим спектроанализатор, вычисляющий спектры сигнала и шума на входе и выходе МФ в заданной полосе частот $(\omega_0 - \Delta\omega/2, \omega_0 + \Delta\omega/2)$. Далее необходимо выполнить возведение в квадрат и усреднение по количеству M вычисленных значений. Тогда

$$\overline{P}_{c} = \frac{1}{M}\sum_{q=1}^{M} S_q^2(m);\ \text{мВт/Гц}.$$

Обычно значение M не более 1024для цифровых спектроанализаторов.

Результаты экспериментальных исследований

Экспериментальные исследования фильтрующих свойств СМФС выполнялось на основе цифро-

вой имитационной модели фильтра, синтезированной в среде имитационного моделирования динамических систем на основе использования функциональной схемы, представленной на рис. 1.

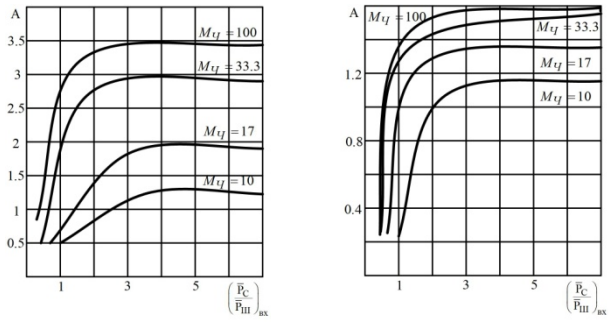
В качестве МФ, примененного в имитационной динамической модели, использовался колебательный контур с перестраиваемой емкостью C_0 каналом управления, состоящим из ЧД2, УНЧ, Σ, КЦ и УЭ (см. рис. 1). В состав имитационной модели СМФС входил источник модулирующего сигнала, который обеспечивал формирование модулирующей функции Ω в виде низкочастотной гармонической функции вида $\lambda_ч(t) \approx \sin\Omega t$ и случайной моделирующей функции (7) без учета коэффициента корреляции амплитудных флуктуаций ЧМ сигнала (1).

Генератор шума имитировал "белый" шум n(t) с заданной спектральной плотностью N_0 и корреляционной функцией $K(\tau) = N_0\delta(t)/2$ в виде случайных чисел с нормальным распределением.

Контроль спектров ЧМ сигнала на входе и выходе МФ осуществлялся встроенным в имитационную модель цифровым спектроанализатором в виде некоторого программного продукта.

Остальные элементы имитационной модели СМФС выполнены на основе стандартных цифровых блоков с известной программной реализацией (модулятор ЧМ сигнала, сумматоры, ФНЧ фильтры, блоки сохранения данных и т.д.).

Результаты имитационного моделирования представлены на рис. 2-4.



а б

Рис. 2. Зависимость коэффициента фильтрации от $\left(P_C / P_Ш\right)_{вх}$ при гармонической (а) и случайной Х (б) модулирующей функции λЧ(t)

Исходные данные моделирования:

$F_0 = F_Д^* = 10$ кГц - резонансная частота МФ (эквивалентна $W_П^* \simeq 900$ км/ч);

$\Delta F = \Delta F_Д^* = 1$ кГц - ширина полосы пропускания МФ;

$F_M = \Omega/(2\pi)$ - гармоническая и характеристическая частота модулирующей функции равнялась $10 \div 100$ Гц,

полоса УНЧ составляла $0 \div 200$ Гц с дискретами 10, 30, 60, 90, 100 Гц;

девиация частоты ЧМ модулятора составляла ± 500 Гц и ± 100 Гц,

индекс частотной модуляции $M_ч = \Delta F/F_M$ составлял 10, 30, 17, 11, 10; спектральная плотность мощности шума $N_0 = 5\cdot10^{-5} \div 100\cdot10^{-5}$ Вт/Гц.

На рис. 5 жирной линией нанесена условно спектральная линия S^2 на частоте 10 кГц, соответствующая $\delta(f)$ для $f_0 = 10$ кГц.

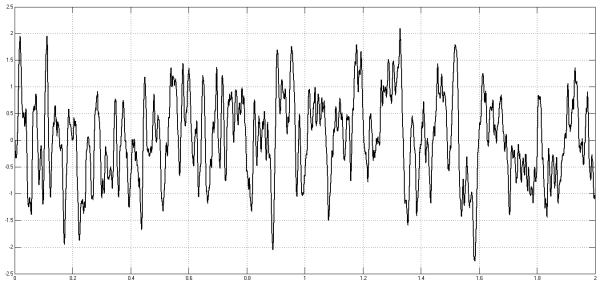
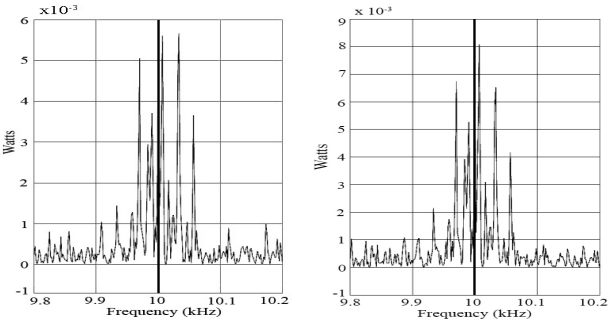


Рис. 4. Вид случайной модулирующей функции ЧМ сигнала при частоте среза ФНЧ FM = Ω/(2π) =30 Гц



а б

Рис. 5. Спектр ЧМ сигнала $S^2(t)$ на входе (а) и выходе (б) модулированного фильтра при $\left(P_C / P_Ш\right)_{вх} = 14$ и $\beta = \pm 100$ Гц

Заключение

В работе исследована задача оценки качества фильтрации спектра доплеровского сигнала, отраженного от подстилающей поверхности следящим модулированным фильтром.

Полагается, что в процессе зондирования подстилающей поверхности непрерывным гармоническим сигналом, происходит его преобразование в амплитудно-частотно модулированный сигнал, который принимается в виде аддитивной смеси с "белым" гауссовским шумом.

При выбранном показателе качества фильтрации спектра доплеровского сигнала СМФС, формально совпадающем с известным показателем помехоустойчивости приема ЧМ сигнала в канале передачи непрерывных сообщений, отличающимся расчетом средних мощностей сигнала и шума на входе и выходе МФ, получены такие результаты.

Максимальное значение коэффициента фильтрации при гармонической модулирующей функции ЧМ сигнала не превышает $3 \div 3,5$ раз или примерно 5 дБ по мощности для индекса ЧМ модуляции стремящемуся к максимуму при $F_Д$, стремящейся к минимуму.

Область пороговых значений коэффициента фильтрации примерно одинакова для различных значений индекса модуляции ЧМ сигнала и находится в пределах $3 \div 5$ дБ по отношению средних мощностей сигнала и шума на входе МФ, рассчитанных по их спектрам.

Аналогичные выводы можно сделать и для случайной модулирующей функции ЧМ сигнала на входе МФ. Отличие состоит лишь в том, что максимальное значение коэффициента фильтрации не превышает $1,2 \div 1,4$ раз, или примерно 1,5 дБ по отношению средних мощностей сигнала и шума на входе МФ, рассчитанных по их спектрам.

При этом область пороговых значений коэффициента фильтрации для различных значений индекса модуляции находится в пределах $0,8 \div 1,5$ дБ по отношению средних мощностей сигнала и шума на входе МФ.

Таким образом, замена резонансных узкополосных фильтров с фиксированными параметрами, которые применяются в существующих трактах приема и обработки доплеровской информации следящим модулированным фильтром с самосинфазированием для реальных условий формирования модулирующей функции в виде случайного процесса, даст улучшение помехоустойчивости до $1,5 \div 2$ дБ.

Список литературы

1. Ярлыков М.С. Статистическая теория радионавигации [Текст] / М.С. Ярлыков. - М.: Радио и связь, 1985 - 344 с.

2. Печенин В.В. Узкополосная фильтрация и измерение частоты сигналов в доплеровских системах навигации летательных аппаратов [Текст] учеб. пособие / В.В. Печенин, К.А. Щербина, М.А. Вонсович и др. - Х.: Нац. аэрокосм. ун-т им Н.Е. Жуковского "ХАИ" 2016. – 56 с.

3. Виницкий А.С. Автономные радиосистемы. Учеб. пособие для вузов [Текст] /А.С. Виницкий. - М.: Радио и связь, 1986. - 336 с.

4. Колчинский В.Е. Автономные доплеровские системы и устройства навигации летательных аппаратов [Текст] / В.Е. Колчинский, И.А. Мандуровский, М.И. Константиновский - М.: Сов. радио, 1975. - 432 с.

5. Печенин В.В. Синтез структурно-физической модели следящего фильтра с принудительной перестройкой частоты синхронизированного автогенератора [Текст] / В.В. Печенин, К.А. Щербина, О.В. Войтенко // Системи управління, навігації та зв'язку. - 2012. - №3(23). С. 94-98.

6. Зайцев Г.Ф. Радиотехнические системы автоматического управления высокой точности [Текст] / Г.Ф. Зайцев, В.К. Стеклов. - К.: Техника, 1998 - 208 с.

7. Печенин В.В. Классы следящих систем на модулированном фильтре [Текст] / В.В. Печенин, К.А. Щербина, М.А. Вонсович // Труды 8-й Международной конференции Акустические и радиолокационные методы измерений и обработки информации 20-23 сентября 2015, Суздаль, Россия. - С 161-163.

8. Печенин В.В. Статистическая модель доплеровского сигнала автономного измерителя скорости летательного аппарата [Текст] / В.В. Печенин, Щербина К.А., Войтенко О.В. // Всеукраинский межведомственный научно-технический сборник "Радиотехника". – Вып. 177. - Х.; 2014 - С. 64-70.

9. Виницкий А.С. Модулированные фильтры и следящий прием ЧМ сигналов [Текст] / А.С. Виницкий - М.: изд. Советское радио, 1969, 548 с.

10. Печенин В.В. Взаимная корреляция уровня и фазы гармонического сигнала при распространении электромагнитных волн в тропосфере [Текст] / В.В. Печенин, С.А. Дейкало // Радиоэлектроника и информатика №3(12) 2000. С 15-17.

Надійшла до редколегії 1.02.2017

Рецензент: д-р техн. наук, с.н.с. В.В. Павліков, Національний аерокосмічний університет імені М.Є. Жуковського «Харківський авіаційний інститут», Харків.

ОЦІНКА ЯКОСТІ ФІЛЬТРАЦІЇ СПЕКТРА ДОПЛЕРІВСЬКОГО СИГНАЛА ВІДБИТОГО ВІД ПІДСТИЛЬНОЇ ПОВЕРХНІ СЛІДКУЮЧИМ МОДУЛЬОВАНИМ ФІЛЬТРОМ

В.В. Печенін, К.О. Щербина, М.А. Вонсович, Ю.В. С'єдіна

Мета виконаних у роботі досліджень полягала в поліпшенні показників якості прийому і обробки доплерівського сигналу з детермінованою основою спектру, обумовленою швидкістю руху ЛА, наявністю адитивних перешкод і впливом радіофізичних властивостей підстилаючої поверхні. Розроблений метод заснований на використанні резонансного фільтра з модульованою ємністю, яка забезпечує збільшення завадостійкості порівняно з методом слідкуючого гетеродина в межах 2…3 дБ.

Ключові слова: *слідкуючий доплерівський фільтр, фільтрація, модульований фільтр, показники якості,слідкуючий прийом, частота.*

MODULATED TRACKING FILTER QUALITY ASSESSMENT OF SPECTRUM FILTRATION OF DOPPLER SIGNAL GENERATED BY UNDERLYING SURFACE

V.V. Pechenin, K.A. Shcherbina, M.A. Vonsovich, J.V. Syedina

The purpose of the carried out research was to improve quality indicators upon transmitting and receiving the Doppler signal with deterministic spectrum predetermined by the aircraft speed, the presence of additive noise and the influence of radiophysical properties of the underlying surface. The developed method is based on the use of a resonant filter with modulated capacity, which provides enhanced noise immunity in comparison with the tracking heterodyne method within 2…3 dB.

Keywords: *doppler tracking filter, filtration, modulated filter, quality indicators, tracking, frequency.*

УДК 681.518.2

О.В. Шульга, О.В. Шефер

Полтавський національний технічний університет імені Юрія Кондратюка, Полтава

ГЕОМЕТРИЧНИЙ ЧИННИК ТА ЙОГО ВПЛИВ НА ПОХИБКУ ВИЗНАЧЕННЯ НАВІГАЦІЙНИХ ПАРАМЕТРІВ У ПСЕВДОСУПУТНИКОВІЙ РАДІОСИСТЕМІ

Доведено, що співвідношення між похибками визначення первинних та вторинних навігаційних параметрів залежить тільки від вигляду матриці градієнтів споживача (С), тобто від геометрії взаємного розташування псевдосупутників (ПС) та споживача С. Проведений аналіз показав, що у загальному вигляді вираз для геометричного чинника (ГЧ) може бути записано як відношення GDOP = σ_q/σ_D, *де* σ_q *– середньо – квадратична похибка (СКП) визначення вектора стану споживача С;* σ_D *– СКП визначення псевдодалекостей до ПС. Визначено, що на практиці споживачів цікавить ступінь погіршення точності місцевизначення окремо у горизонтальній та вертикальній площинах відносно поверхні Землі, а також ступінь погіршення точності визначення поправок часу.*

Ключові слова: *геометричний чинник, псевдосупутник, споживач, псевдо далекість, стільникова структура, кут височіння, елементарна чарунка, пряма видимість, геодезична віддаль.*

Вступ

Навігаційна задача, яка вирішується у апаратурі споживачів (С) псевдосупутникової радіонавігаційної системи (ПС РНС), у найпростішому випадку полягає у визначенні просторово-часових координат $\Pi = ||x\ y\ z\ D'||^T$.

На точність визначення споживачем ПС РС координат місцезнаходження, висоти, швидкості, часу та інших параметрів впливає велика кількість факторів. Вони пов'язані з особливостями первинних та вторинних навігаційних вимірювань, з характеристиками сигналів, які використовуються, середовища розповсюдження та ін.

Розглянемо основні джерела похибок стосовно до псевдодалекомірного метода навігаційних вимірювань.

У ПС РС як і в супутникових радіонавігаційних системах (СРНС) реалізується псевдодалекомірний метод визначення точки знаходження С зі збереженням точки початку відліку на борту навігаційного супутника (НС), який відрізняється від далекомірного на величину

$$w = cT',$$

де с – швидкість розповсюдження радіохвиль, T' – різниця між часом навігаційної апаратури споживача (НАС) та системним часом РНС).

Мета статті. Вивчення загальних закономірностей структури ПС РНС, яку доцільно подати у вигляді сукупності тетраедрів, для чого побудувати стільникову структуру, обравши у якості елементарної чарунки «трикутник з центральною точкою», в якій для наземного С дальність прямої видимості ПС обумовлюється також мінімальним кутом височіння ПС.

Основна частина

Для переходу від геоцентричної системи координат (ГСК) до топоцентричної системи координат (ТСК) застосовується афінний перехід:

$$A_k = \begin{Vmatrix} \cos\lambda\sin\phi & \sin\lambda\sin\phi & -\cos\phi \\ -\sin\lambda & \cos\lambda & 0 \\ \cos\lambda\cos\phi & \sin\lambda\cos\phi & \sin\phi \end{Vmatrix},$$

де φ та λ – геодезичні координати споживача С [1].

Кореляційна матриця K_q перераховується у ТСК за допомогою формули

$$K_{qTCK} = A_K \Gamma_{KK} A^T_K,$$

де Γ_{KK} – блок матриці K_q, який відповідає похибкам координат

$$K_q = \begin{Vmatrix} \Gamma_{KK} & \Gamma_{Kt} \\ \Gamma_{Kt} & \Gamma_{tt} \end{Vmatrix}.$$

Таким чином, геометричні чинники погіршення точності при визначенні місця у просторі – PDOP, у плані (горизонтальній площині) – HDOP, по висоті – VDOP та часу – TDOP запишуться відповідно у вигляді.

$$PDOP = (y_{11} + y_{22} - y_{33})^{1|2};$$

$$HDOP = (y_{11} + y_{22})^{1|2};$$

$$VDOP = (y_{33})^{1|2};$$

$$TDOP = (y_{44})^{1|2},$$

де y_{ij} є елементами матриці $K_q = A^{-1}$.

У багатьох джерелах, зокрема у [2, 3], показано, що мінімальних значень ГЧ можна досягти, коли С знаходиться у центрі правильного тетраедра. Для наземного С мінімальне значення досягається тоді, коли один НС знаходиться у зеніті, а

три інших НС рівномірно розташовані у горизонтальній площині.

Таким чином, для мінімізації GDOP необхідно максимізувати об'єм тетраедра.

Виходячи з цього, структуру ПС РС доцільно подати у вигляді сукупності тетраедрів, для чого побудувати стільникову структуру, обравши у якості елементарної чарунки "трикутник з центральною точкою" (рис. 1).

Розміри такого трикутника обумовлюються висотою ПС, яка, у свою чергу, обумовлює радіус (R) зони прямої видимості С – ПС. Для наземного С дальність прямої видимості ПС обумовлюється також мінімальним кутом височіння ПС. Як правило, для СРНС цей кут складає 5-15° і обумовлюється кривизною земної поверхні та наявним на ній рельєфом. Залежність кута височіння ПС (θ), який знаходиться на висоті 8 км, від геодезичної віддалі наземного С до його опорної точки (L) при припущенні відсутності рельєфу місцевості було проілюстровано на рис. 2.

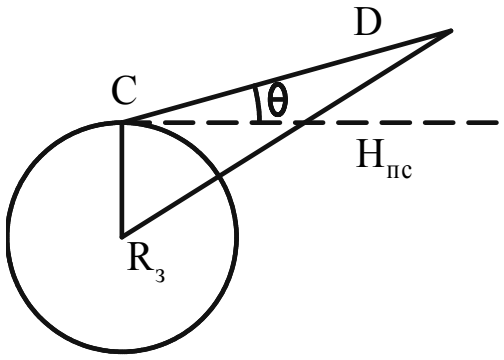


Рис. 1. Визначення дальності прямої видимості ПС з урахуванням кута височіння θ

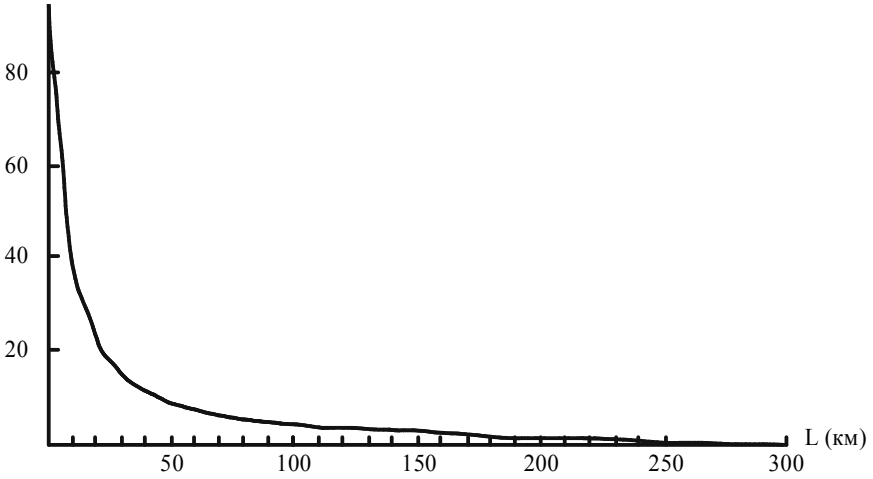


Рис. 2. Залежність кута височіння ПС від відстані С до опорної точки

З метою аналізу поля точності ПС РНС, побудованої на основі елементарної чарунки "трикутник з центральною точкою", було обрано структуру, у якій усі ПС знаходяться на висоті 8000 м. У такому випадку довжина боків трикутника становить 70–80 км. Центр чарунки знаходиться у точці з координатами 50,2° пн.ш., 25,5° сх.д.

Результати проведених розрахунків свідчать, що горизонтальний ГЧ (HDOP) для наземних С у межах робочої зони не перевищує 2 (рис. 3, а).

Вертикальний ГЧ (VDOP) у центрі дорівнює 1,9, а до краю зони підвищується до 12, що цілком обумовлюється співвідношенням горизонтальних та вертикальних розмірів системи.

На висоті 100 м зона прямої видимості збільшується до 250 км. HDOP у радіусі 60-80 км від центра чарунки не перевищує 10, а VDOP змінюється від 1,9 до 37 (рис. 3,б).

На перший погляд центральну РНТ у елементарній чарунці можна було б розташувати дещо нижче решти ПС, оскільки необхідний радіус дії цієї точки менший решти радіусів. Розглянемо як зміниться поле точності у цьому випадку. Для цього розташуємо елементарну чарунку, як і раніше, трикутником, і підрахуємо значення ГЧ довкола неї. На рис.3 а,б показано поле ГЧ при розташуванні ПС на одній висоті (8 км). Рис.3, в ілюструє поле ГЧ при зменшенні висоти центрального ПС до 4,5 км, а на рис.3, г – при збільшенні висоти центрального ПС до 12 км. Як бачимо, при зміні висоти центрального ПС поле ГЧ є дуже неоднорідним, що пояснюється співвісним розташуванням деяких ПС та С, які знаходяться на окраїнах зони.

Висновки

Проведене у рамках даної статті моделювання дає змогу зробити висновок, що при проектуванні ПС РНС характеристики її точності може бути оцінено за допомогою ГЧ, оскільки саме ГЧ є найбільш впливовим фактором, який зменшує точність вимірювань у ПС РС, тому виявляється необхідним провести дослідження неконтрольованого випромінювання джерел світла, що використовуються у якості наземної мережі псевдосупутників ПС.

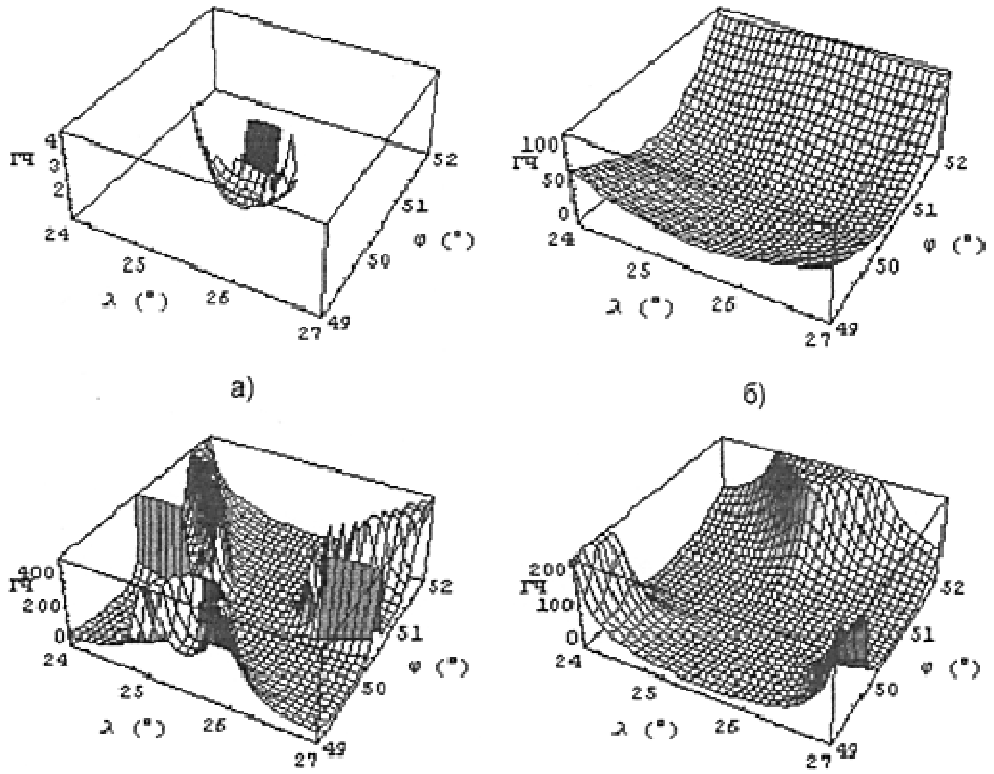


Рис. 3. Поле значень горизонтального ГЧ
при різних висотах С та геометрії елементарної чарунки ПС

Список літератури

1. Шебшаевич В.С. Введение в теорию космической навигации / В.С. Шебшаевич. – М: Сов. радио, 1971. – 296 с.

2. Соловьев Ю.А. Системы спутниковой навигации / Ю.А. Соловьев. – М: Эко-трендз, 2000. – 270 с.

3. Глобальная спутниковая радионавигационная система ГЛОНАСС / Под ред. В.Н.Харисова, А.И.Перова, В.А.Болдина. – М: ИПРЖР, 1999. – 560 с.

Надійшла до редколегії 1.12.2016

Рецензент: д-р техн. наук, проф. С.В. Козелков, Державний університет телекомунікацій, Київ.

ГЕОМЕТРИЧЕСКИЙ ФАКТОР И ЕГО ВЛИЯНИЕ НА ПОГРЕШНОСТЬ ОПРЕДЕЛЕНИЯ НАВИГАЦИОННЫХ ПАРАМЕТРОВ В ПСЕВДОСПУТНИКОВОЙ РАДИОСИСТЕМЕ

О.В. Шульга, О.В. Шефер

Доказано, что соотношение между погрешностями определения первичных и вторичных навигационных параметров зависит только от вида матрицы градиентов потребителя (С), то есть от геометрии взаимного расположения псевдоспутников (ПС) и потребителя С. Проведенный анализ показал, что в общем виде выражение для геометрического фактора (ГЧ) может быть записано как отношение GDOP = σ_q/σ_D, где σ_q – среднеквадратичная погрешность (СКП) определения вектора состояния потребителя С; σ_D – СКП определения псевдодальностей к ПС. Определено, что на практике потребителей интересует степень ухудшения точности местоопределения отдельно в горизонтальной и вертикальной плоскостях относительно поверхности Земли, а также степень ухудшения точности определения поправок времени.

Ключевые слова: *геометрический фактор, псевдоспутник, потребитель, псевдоудаленность, сотовая структура, угол возвышения, элементарная ячейка, прямая видимость, геодезическое расстояние.*

GEOMETRIC FACTOR AND ITS INFLUENCE ON NAVIGATION PARAMETERS DETERMINING ERROR IN PSEUDOSATELLITE RADIO SYSTEM

O.V. Shulga, O.V. Shefer

It is proved that the relation between errors definition of primary and secondary navigation parameters depends on the type of matrix consumer gradients (C), that is, the geometry of the mutual position of pseudosatellites (PS) and the consumer C. The analysis showed that in the general expression for the geometrical factor (MS) can be written as the ratio of GDOR = = σ_q/σ_D, where σ_q – mean square error (MSE) of the consumer C state vector definition; σ_D – MSE to determine pseudorange to PS. It is determined that the practice of consumers interested in the degree of deterioration in the accuracy of positioning separate horizontal and vertical planes relative to the Earth's surface, as well as the degree of time corrections determining accuracy deterioration.

Keywords: *geometric factor, pseudosatellite, consumer pseudorange, honeycomb structure, elevation angle, unit cell, line of sight, geodesic distance.*

УДК 629.1.07

М.Л. Шуляк

Харьковский национальный технический университет сельского хозяйства им. П. Василенка

ОПРЕДЕЛЕНИЕ КОМПОНЕНТ УСКОРЕНИЯ АГРЕГАТА ОТНОСИТЕЛЬНО ОСЕЙ ПОВОРОТА, ПРОХОДЯЩИХ ЧЕРЕЗ НЕПОДВИЖНЫЙ АКСОИД СИСТЕМЫ

В работе рассмотрено сложное движение транспортного агрегата, как системы твердых тел закрепленных на некотором расстоянии друг от друга стационарной связью. Предложена теоретическая модель определения компонент ускорения любой точки тракторного агрегата в ее поступательном движении и трех вращательных движений относительно мгновенных осей поворота. Для экспериментального исследования определены условия расположения акселерометров, относительно центра тяжести трактора (сельскохозяйственной машины).

***Ключевые слова**: динамика агрегата, сложное движение, центр масс, ускорение.*

Вступление

Изучение динамической составляющей движения транспортного агрегата (ТА) представляет большой научный интерес и требует дальнейшего развития. Одним из наиболее информативных параметров такого движения, является ускорение агрегата, так как его определение экспериментальным путем упрощается, вследствие применения акселерометров. В тоже время отсутствие методик переноса, полученных ускорений отдельно выбранных точек (мест установки датчиков) к центру масс агрегата снижает возможности применения полученных результатов для серии агрегатов, так как каждый опыт становиться не воспроизводимым в других условиях.

Анализ источников информации. В работе [1] определено необходимое число датчиков и рассмотрены различные принципы их установки, однако это сделано для плоскости и не позволяет оценить динамику ТА в пространстве. Для реализации методики предложенной в работах [2 – 4] необходимым условием является определение ускорения центра масс всего агрегата (вне зависимости от количества составных звеньев) при его движении в трехмерном пространстве. Это делает необходимым дальнейшее развитие модели определения ускорения агрегата, предложенной в работе [5].

Цель и постановка задачи. Целью работы является дальнейшее развитие модели теоретического определения вектора полного ускорения агрегата на основе полученных экспериментальным путем ускорений контрольных точек его составных звеньев при свободном расположении акселерометров.

Основная часть

Рассмотрим движение агрегата как движение системы двух абсолютно твердых тел, закрепленных на некотором расстоянии друг от друга стационарной связью. Тогда, при выполнении технологического процесса, и при нарушении прямолинейного движения агрегата, каждая i точка трактора ($i = 1,2$) будет иметь ускорение [5]:

$$\vec{a}_1 = \vec{a}_{01} + \vec{a}_1^{\,n} + \vec{a}_1^{\,\tau} + \vec{a}_1^{\,b}; \quad (1)$$

$$\vec{a}_2 = \vec{a}_{02} + \vec{a}_2^{\,n} + \vec{a}_2^{\,\tau} + \vec{a}_2^{\,b}, \quad (2)$$

где $\vec{a}_0 = \vec{a}_{01} = \vec{a}_{02}$ – ускорение поступательного движения центра вращения трактора – ускорение в поступательном движении точки неподвижного аксоида соответствующего датчика, являющейся мгновенным центром поворота трактора (точка O_1 для датчика 1 и точка O_1 для датчика 2). В неподвижной системе координат $Oxyz$ компоненты данного вектора определятся из таких зависимостей:

$$\vec{a}_{0x} = \frac{dv_{ц.т.}}{dt}\vec{\eta}; \ \vec{a}_{0y} = \frac{dv_{ц.т.}}{dt}\vec{\lambda}; \ \vec{a}_{0z} = \frac{dv_{ц.т.}}{dt}\vec{\chi}, \quad (3)$$

где $v_{ц.т.}$ – скорость поступательного движения центра тяжести трактора относительно неподвижной системы координат $Oxyz$.

Для определения остальных слагаемых, рассмотрим движение каждого датчика в пространстве по некоторой кривой как совокупность поступательного движения с ускорением $\vec{a}_{0i}$ (здесь i – номер датчика) и вращательного движения с центром вращения в точке O_i в трех ортогональных плоскостях, определенных ортонормированным подвижным базисом $O'i'j'k'$, связанным с центром тяжести.

Таким образом, рассматривая суперпозицию рассмотренных вращений можно говорить о том, что трактор совершает в пространстве сложное движение, которое является совокупностью поступательного движения его центра тяжести и вращательного движения всего трактора вокруг мгновенной неподвижной оси вращения или вокруг одной неподвижной точки [5]. Каждую вращательную компоненту вектора ускорения из зависимостей (1) и (2) можно представить в следующем виде:

$$\vec{a}_1^{\,n} = \vec{a}_{п1}^{\,сопр} + \vec{a}_{п1}^{\,норм},\ \ \vec{a}_2^{\,n} = \vec{a}_{п2}^{\,сопр} + \vec{a}_{п2}^{\,норм};\qquad (4)$$

$$\vec{a}_1^{\,\tau} = \vec{a}_{\tau1}^{\,сопр} + \vec{a}_{\tau1}^{\,спр},\ \ \vec{a}_2^{\,\tau} = \vec{a}_{\tau2}^{\,сопр} + \vec{a}_{\tau2}^{\,спр};\qquad (5)$$

$$\vec{a}_1^{\,b} = \vec{a}_{b1}^{\,спр} + \vec{a}_{b1}^{\,норм},\ \ \vec{a}_2^{\,b} = \vec{a}_{b2}^{\,спр} + \vec{a}_{b2}^{\,норм}.\qquad (6)$$

Необходимо отметить, что зависимости (4) – (6) описывают именно те величины, значения которых определяются акселерометрами, установленными на тракторе. Таким образом, полное ускорение датчиков определится из таких зависимостей:

$$\vec{a}_1 = \vec{a}_{01} + \vec{a}_{п1}^{\,сопр} + \vec{a}_{п1}^{\,норм} + \vec{a}_{\tau1}^{\,сопр} + \\ + \vec{a}_{\tau1}^{\,спр} + \vec{a}_{b1}^{\,спр} + \vec{a}_{b1}^{\,норм};\qquad (7)$$

$$\vec{a}_2 = \vec{a}_{02} + \vec{a}_{п2}^{\,сопр} + \vec{a}_{п2}^{\,норм} + \vec{a}_{\tau2}^{\,сопр} + \\ + \vec{a}_{\tau2}^{\,спр} + \vec{a}_{b2}^{\,спр} + \vec{a}_{b2}^{\,норм}.\qquad (8)$$

Спроектируем векторные зависимости (7) и (8) на оси неподвижной системы координат. Получим:

$$a_{iX} = a_{0iX} + a_{пiX}^{сопр} + a_{пiX}^{норм} + a_{\tau iX}^{сопр} + \\ + a_{\tau iX}^{спр} + a_{biX}^{спр} + a_{biX}^{норм};\qquad (9)$$

$$a_{iY} = a_{0iY} + a_{пiY}^{сопр} + a_{пiY}^{норм} + a_{\tau iY}^{сопр} + \\ + a_{\tau iY}^{спр} + a_{biY}^{спр} + a_{biY}^{норм};\qquad (10)$$

$$a_{iZ} = a_{0iZ} + a_{пiZ}^{сопр} + a_{пiZ}^{норм} + a_{\tau iZ}^{сопр} + \\ + a_{\tau iZ}^{спр} + a_{biZ}^{спр} + a_{biZ}^{норм};\qquad (11)$$

Учитывая особенность движения естественного трехгранника, связанного с каждым датчиком, можно говорить о том, что все проекции в зависимостях (9) – (11) определяются при помощи умножения соответствующего вектора, заданного естественным способом при помощи базиса $O_i i_i j_i k_i$, на матрицу поворота в трехмерном пространстве с учетом угла, описывающего движение трактора. Получим:

$$M_x(\theta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix};\qquad (12)$$

$$M_y(\gamma) = \begin{pmatrix} \cos\gamma & 0 & \sin\gamma \\ 0 & 1 & 0 \\ -\sin\gamma & 0 & \cos\gamma \end{pmatrix};\qquad (13)$$

$$M_z(\psi) = \begin{pmatrix} \cos\psi & -\sin\psi & 0 \\ \sin\psi & \cos\psi & 0 \\ 0 & 0 & 1 \end{pmatrix},\qquad (14)$$

где индекс матрицы указывает соответствующую ось поворота, вокруг которой совершается поворот на угол, указанный в скобках.

Таким образом, суммарное значение ускорений точек трактора, вдоль координатных осей неподвижной системы координат, может быть определено из зависимостей вида:

$$a_{\Sigma X}^{тр} = \sum_{i=1}^{k} a_{0iX}^{тр} + a_{пiX}^{тр} + a_{\tau iX}^{тр} + a_{biX}^{тр};\qquad (15)$$

$$a_{\Sigma Y}^{тр} = \sum_{i=1}^{k} a_{0iY}^{тр} + a_{пiY}^{тр} + a_{\tau iY}^{тр} + a_{biY}^{тр};\qquad (16)$$

$$a_{\Sigma Z}^{тр} = \sum_{i=1}^{k} a_{0iZ}^{тр} + a_{пiZ}^{тр} + a_{\tau iZ}^{тр} + a_{biZ}^{тр},\qquad (17)$$

где k – количество датчиков, установленных на трактор; $a_{0iX}^{тр}$, $a_{0iY}^{тр}$, $a_{0iZ}^{тр}$ – проекции ускорения центра вращения трактора на неподвижные оси координат; $a_{\tau iX}^{тр}$, $a_{\tau iY}^{тр}$, $a_{\tau iZ}^{тр}$ – проекции показаний датчика, установленного на тракторе, по «внутренней» оси X на оси неподвижной системы координат; $a_{пiX}^{тр}$, $a_{пiY}^{тр}$, $a_{пiZ}^{тр}$ – проекции показаний датчика, установленного на тракторе, по «внутренней» оси Y на оси неподвижной системы координат; $a_{biX}^{тр}$, $a_{biY}^{тр}$, $a_{biZ}^{тр}$ – проекции показаний датчика, установленного на тракторе, по «внутренней» оси Z на оси неподвижной системы координат.

При рассмотрении сельскохозяйственной машины (рис. 1) по аналогичному алгоритму, можно прийти к выводу, что установка двух датчиков на последней в произвольном положении позволяет определить такие же компоненты ускорений, величины которых определяются из зависимостей вида:

$$a_{\Sigma X}^{маш} = \sum_{i=1}^{k} a_{0iX}^{маш} + a_{пiX}^{маш} + a_{\tau iX}^{маш} + a_{biX}^{маш};\qquad (18)$$

$$a_{\Sigma Y}^{маш} = \sum_{i=1}^{k} a_{0iY}^{маш} + a_{пiY}^{маш} + a_{\tau iY}^{маш} + a_{biY}^{маш};\qquad (19)$$

$$a_{\Sigma Z}^{маш} = \sum_{i=1}^{k} a_{0iZ}^{маш} + a_{пiZ}^{маш} + a_{\tau iZ}^{маш} + a_{biZ}^{маш},\qquad (20)$$

где k – количество датчиков, установленных на сельскохозяйственную машину; $a_{0iX}^{маш}$, $a_{0iY}^{маш}$, $a_{0iZ}^{маш}$ – проекции ускорения центра вращения сельскохозяйственной машины на неподвижные оси координат; $a_{\tau iX}^{маш}$, $a_{\tau iY}^{маш}$, $a_{\tau iZ}^{маш}$ – проекции показаний датчика, установленного на сельскохозяйственной машине, по «внутренней» оси X на оси неподвижной системы координат; $a_{пiX}^{маш}$, $a_{пiY}^{маш}$, $a_{пiZ}^{маш}$ – проекции показаний датчика, установленного на сельскохозяйственной машине, по «внутренней» оси Y на оси неподвижной системы координат; $a_{biX}^{маш}$, $a_{biY}^{маш}$, $a_{biZ}^{маш}$ – проекции показаний датчика, установленного на сельскохозяйственной машине по «внутренней» оси Z на оси неподвижной системы координат.

Таким образом, кинематика рассматриваемой динамической системы относительно ортогональной системы координат $Oxyz$, определяется векторной суммой ускорений всех составных частей механической системы.

Рассмотрим динамику каждого элемента данной системы с точки зрения второго закона динамики.

Так, для трактора сумма проекций всех сил, действующих на последний, на оси неподвижной системы координат Oxyz определяется из зависимостей:

$$\sum_{i=1}^{n} F_{Xi}^{тр} = M^{тр} a_{\Sigma X}^{тр}; \quad (21)$$

$$\sum_{i=1}^{n} F_{Yi}^{тр} = M^{тр} a_{\Sigma Y}^{тр}; \quad (22)$$

$$\sum_{i=1}^{n} F_{Zi}^{тр} = M^{тр} a_{\Sigma Z}^{тр}, \quad (23)$$

где $F_{Xi}^{тр}$, $F_{Yi}^{тр}$, $F_{Zi}^{тр}$ – проекции всех внешних сил, действующих на трактор, на оси неподвижной системы координат $Oxyz$; $M^{тр}$ – масса трактора; n – количество внешних сил, действующих на трактор.

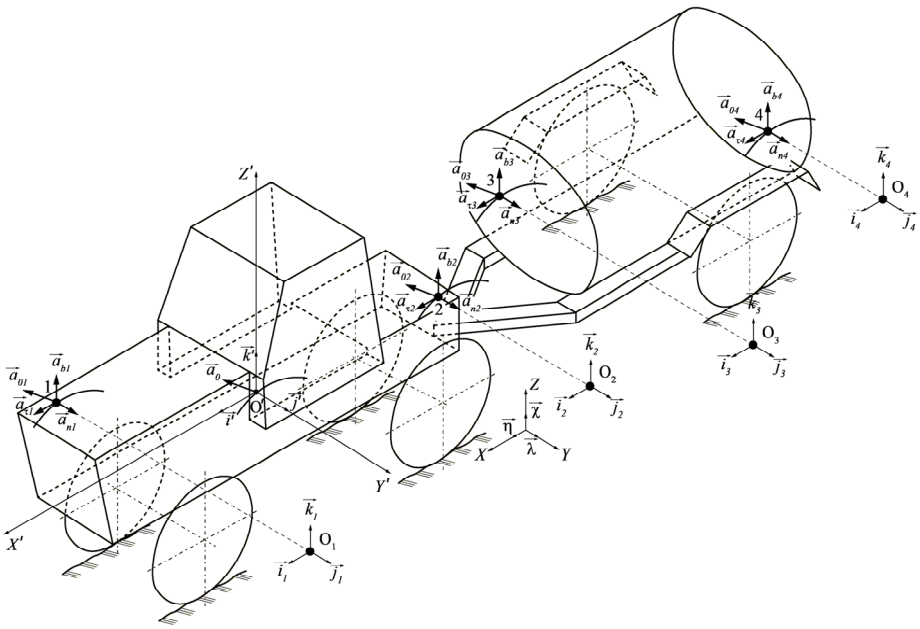


Рис. 1. Кинематическая модель движения тракторного агрегата

Тогда, для сельскохозяйственной машины, получим такие выражения:

$$\sum_{i=1}^{m} F_{Xi}^{маш} = M^{маш} a_{\Sigma X}^{маш}; \quad (24)$$

$$\sum_{i=1}^{m} F_{Yi}^{маш} = M^{маш} a_{\Sigma Y}^{маш}; \quad (25)$$

$$\sum_{i=1}^{m} F_{Zi}^{маш} = M^{маш} a_{\Sigma Z}^{маш}, \quad (26)$$

где $F_{Xi}^{маш}$, $F_{Yi}^{маш}$, $F_{Zi}^{маш}$ – проекции всех внешних сил, действующих на сельскохозяйственную машину, на оси неподвижной системы координат $Oxyz$; $M^{маш}$ – масса сельскохозяйственной машины; m – количество внешних сил, действующих на трактор.

Учитывая факт движения энергетического средства вместе с сельскохозяйственной машиной в качестве динамической системы, запишем условие движения последней с учетом теоремы о движении центра масс системы. Получим:

$$\sum_{i=1}^{s} F_{Xi}^{агр} = M^{агр} a_{X}^{агр}; \quad (27)$$

$$\sum_{i=1}^{s} F_{Yi}^{агр} = M^{агр} a_{Y}^{агр}; \quad (28)$$

$$\sum_{i=1}^{s} F_{Zi}^{агр} = M^{агр} a_{Z}^{агр}, \quad (29)$$

где $F_{Xi}^{агр}$, $F_{Yi}^{агр}$, $F_{Zi}^{агр}$ – проекции всех внешних сил, действующих на агрегат, на оси неподвижной системы координат $Oxyz$; $M^{агр}$ – масса машинно-тракторного агрегата; S – количество внешних сил, действующих на машинно-тракторный агрегат; $a_{X}^{агр}$, $a_{Y}^{агр}$, $a_{Z}^{агр}$ – проекции вектора полного ускорения, центра масс динамической системы на оси неподвижной системы координат $Oxyz$.

Учитывая зависимости (21) – (29), получим:

$$\sum_{i=1}^{n} F_{Xi}^{тр} + \sum_{i=1}^{т} F_{Xi}^{маш} = M^{тр} a_{\Sigma X}^{тр} + M^{маш} a_{\Sigma X}^{маш}; \quad (30)$$

$$\sum_{i=1}^{n} F_{Yi}^{тр} + \sum_{i=1}^{т} F_{Yi}^{маш} = M^{тр} a_{\Sigma Y}^{тр} + M^{маш} a_{\Sigma Y}^{маш}; \quad (31)$$

$$\sum_{i=1}^{n} F_{Zi}^{тр} + \sum_{i=1}^{т} F_{Zi}^{маш} = M^{тр} a_{\Sigma Z}^{тр} + M^{маш} a_{\Sigma Z}^{маш}, \quad (32)$$

Если учесть, что сумма сил, действующих на трактор и сельскохозяйственную машину представляет собой сумму всех внешних сил, действующих на динамическую систему, т.е.:

$$\sum_{i=1}^{n} F_{Xi}^{тр} + \sum_{i=1}^{т} F_{Xi}^{маш} = \sum_{i=1}^{s} F_{Xi}^{агр}; \quad (33)$$

$$\sum_{i=1}^{n} F_{Yi}^{тр} + \sum_{i=1}^{т} F_{Yi}^{маш} = \sum_{i=1}^{s} F_{Yi}^{агр}; \quad (34)$$

$$\sum_{i=1}^{n} F_{Zi}^{тр} + \sum_{i=1}^{т} F_{Zi}^{маш} = \sum_{i=1}^{s} F_{Zi}^{агр}, \quad (35)$$

то приравнивая уравнения (27) – (32) получим:

$$M^{агр} a_{X}^{агр} = M^{тр} a_{\Sigma X}^{тр} + M^{маш} a_{\Sigma X}^{маш}; \quad (36)$$

$$M^{агр} a_{Y}^{агр} = M^{тр} a_{\Sigma Y}^{тр} + M^{маш} a_{\Sigma Y}^{маш}; \quad (37)$$

$$M^{агр} a_{Z}^{агр} = M^{тр} a_{\Sigma Z}^{тр} + M^{маш} a_{\Sigma Z}^{маш}. \quad (38)$$

Если учесть, что сумма $M^{тр} + M^{маш} = M^{агр}$, то, сокращая массы системы в зависимостях (36) – (38), получим формулы определения проекций ускорения центра масс машинно-тракторного агрегата через проекции ускорений трактора и сельскохозяйственной машины:

$$a_X^{агр} = a_{\Sigma X}^{тр} + a_{\Sigma X}^{маш};\ \ a_Y^{агр} = a_{\Sigma Y}^{тр} + a_{\Sigma Y}^{маш}; \quad (39)$$

$$a_Z^{агр} = a_{\Sigma Z}^{тр} + a_{\Sigma Z}^{маш}. \quad (40)$$

Либо, окончательно:

$$a_X^{агр} = \sum_{i=1}^{k}\left(a_{0iX}^{тр} + a_{пiX}^{тр} + a_{\tau iX}^{тр} + a_{biX}^{тр}\right) + \sum_{i=1}^{k}\left(a_{0iX}^{маш} + a_{пiX}^{маш} + a_{\tau iX}^{маш} + a_{biX}^{маш}\right); \quad (41)$$

$$a_Y^{агр} = \sum_{i=1}^{k}\left(a_{0iY}^{тр} + a_{пiY}^{тр} + a_{\tau iY}^{тр} + a_{biY}^{тр}\right) + \sum_{i=1}^{k}\left(a_{0iY}^{маш} + a_{пiY}^{маш} + a_{\tau iY}^{маш} + a_{biY}^{маш}\right); \quad (42)$$

$$a_Z^{агр} = \sum_{i=1}^{k}\left(a_{0iZ}^{тр} + a_{пiZ}^{тр} + a_{\tau iZ}^{тр} + a_{biZ}^{тр}\right) + \sum_{i=1}^{k}\left(a_{0iZ}^{маш} + a_{пiZ}^{маш} + a_{\tau iZ}^{маш} + a_{biZ}^{маш}\right). \quad (43)$$

Зная проекции вектора полного ускорения центра масс системы, можно получить модуль данного вектора из зависимости вида:

$$a^{агр} = \sqrt{\left(a_X^{агр}\right)^2 + \left(a_Y^{агр}\right)^2 + \left(a_Z^{агр}\right)^2}. \quad (44)$$

Зная модуль вектора $a^{агр}$ можно определить его основные характеристики – направляющие косинусы относительно неподвижной системы координат Oxyz, которые позволят наиболее полно охарактеризовать расположение данного вектора в пространстве и распределение его годографа в виде дискретных точек:

$$\cos\Delta = \frac{a_X^{агр}}{a^{агр}};\ \ \cos\Theta = \frac{a_Y^{агр}}{a^{агр}};\ \ \cos\Omega = \frac{a_Z^{агр}}{a^{агр}}, \quad (45)$$

где Δ – угол между направлением вектора полного ускорения центра масс динамической системы и осью x неподвижной системы Oxyz; Θ – угол между направлением вектора полного ускорения центра масс динамической системы и осью y неподвижной системы Oxyz; Ω – угол между направлением вектора полного ускорения центра масс динамической системы и осью Z неподвижной системы Oxyz.

Вывод

Таким образом, располагая датчики ускорений, чтобы их «внутренние» оси координат совпадали с базисом, определенным относительно центра тяжести трактора (сельскохозяйственной машины), можно определить компоненты ускорений любой точки тракторного агрегата в ее поступательном движении и трех вращательных движений относительно мгновенных осей поворота, проходящих через точки неподвижного аксоида системы.

Список літератури

1. Артемов Н.П. Метод парциальных ускорений и его приложения в динамике мобильных машин / Н.П. Артемов, А.Т. Лебедев, М.А. Подригало, А.С. Полянский, Д.М. Клец, А.И. Коробко, В.В. Задорожняя – Х.: Міськдрук, 2012. – 220 с.

2. Подригало М.А. Оценка дополнительных энергетических потерь при установившемся режиме движения транспортно тяговых машин / М.А. Подригало, Н.П. Артемов, Д.В. Абрамов, М.Л. Шуляк // Механіка та машинобудування. – Х.: НТУ «ХПІ», 2015. – Вип. № 9. – С. 98 – 107.

3. *Шуляк М.Л. Оцінка функціонування сільськогосподарського агрегату за динамічними критеріями / М.Л. Шуляк, А.Т. Лебедєв, М.П. Артьомов, Є.І. Калінін // Технічний сервіс агропромислового, лісового та транспортного комплексів – 2016. – № 4. – С. 218 – 226.*

4. *Шуляк М.Л. Область функціонування машинотракторного агрегату, що апроксимована поверхнею другого порядку / М.Л. Шуляк // Зб. наук. праць ВНАУ. – Вінниця: ВНАУ, 2016. – Вип. 1(93), т. 1. – С. 28 – 31.*

5. *Шуляк М.Л. Определение вектора полного ускорения агрегата на основе экспериментальных ускорений его составных звеньев / М.Л. Шуляк // Системи управління, навігації та зв'язку – 2016. – Вип. 2(38) – С. 53 – 56.*

Надійшла до редколегії 11.01.2017

Рецензент: д-р техн. наук, проф. А.Т. Лебедєв, Харківський національний технічний університет сільського господарства ім. П. Василенка, Харків.

ВИЗНАЧЕННЯ КОМПОНЕНТ ПРИСКОРЕННЯ АГРЕГАТУ ЩОДО ОСЕЙ ПОВОРОТУ, ЩО ПРОХОДИТЬ ЧЕРЕЗ НЕРУХОМУ АКСОІД СИСТЕМИ

М.Л. Шуляк

В роботі розглянуто складний рух транспортного агрегату, як системи твердих тіл закріплених на деякій відстані один від одного стаціонарним зв'язком. Запропоновано теоретичну модель визначення компонент прискорення будь-якої точки тракторного агрегату в її поступальному русі і трьох обертальних рухів щодо миттєвих осей повороту. Для експериментального дослідження визначено умови розташування акселерометрів, щодо центра ваги трактора (сільськогосподарської машини).

Ключові слова: *динаміка агрегату, складний рух, центр мас, прискорення.*

DETERMINING THE ACCELERATION COMPONENT OF THE TRACTOR UNIT, RELATIVELY THE ROTATIONAL AXIS THAT PASSES THROUGH STATIONARY AKSOID OF THE SYSTEM

M.L. Shulyak

In this work considered a complicated movement of the transport unit, a system of rigid bodies fixed at a certain distance from each other by a stationary connection. A theoretical model for determining the acceleration component of any point of the tractor unit in its translational motion and three rotational movements relatively instantaneous axis of rotation. For an experimental research defined the conditions location of accelerometers relative to the vehicle's center of gravity (agricultural machinery).

Keywords: *dynamics unit, complicated movement, center of mass, acceleration.*

УДК 510.635

Н.В. Голян

Харьковский национальный университет радиоэлектроники, Харьков

ИЗОМОРФИЗМ И ИНТЕРПРЕТАЦИИ АЛГЕБР ПОНЯТИЙ

В работе сформулирована и доказана теорема о том, что алгебры понятий одинаковой размерности изоморфны друг другу. Вместе с теоремой о существовании алгебр понятий теорема об изоморфизме позволяет утверждать, что алгебра понятий каждой размерности существует и единственна с точностью до изоморфизма.

Ключевые слова: *алгебра конечных предикатов, алгебра понятий, каноническая алгебра, изоморфизм, интерпретации алгебры.*

Введение

Работа является логическим продолжением статей [1, 2]. В статье [1] аксиоматически построена алгебра понятий - алгебраическая система, элементы множества-носителя которой интерпретируются как понятия интеллекта, а ее операции над этими элементами – как действия интеллекта над понятиями. Доказана теорема о существовании алгебры понятий любой размерности. В статье [2] проанализированы множества элементов канонической алгебры понятий. Показано, что алгебра большей размерности является расширением алгебры меньшей размерности. Иначе говоря, алгебра меньшей размерности является подалгеброй алгебры большей размерности. Введены правила построения формул алгебр понятий и показано, что язык формул алгебры понятий любой размерности полон. Доказана теорема о существовании и единственности стандартной формы алгебры понятий.

В статье сформулирована и доказана теорема о том, что алгебры понятий одинаковой размерности изоморфны друг другу. Вместе с теоремой о существовании алгебр понятий можно утверждать, что алгебра понятий каждой размерности существует и единственна с точностью до изоморфизма.

Рассмотрены некоторые возможные интерпретации алгебры понятий - алгебры множеств, двоичных наборов, одноместных и многоместных предикатов первого порядка, булевых функций.

1. Изоморфизм алгебр понятий

Ниже формулируется и доказывается теорема об изоморфизме алгебр понятий.

Теорема. Все алгебры понятий размерности n $(n \in \{1,2,...\})$ изоморфны друг другу.

Доказательство. В [2] было доказано, что каждой стандартной форме и ее ядру соответствует свое понятие алгебры L_n. Следовательно, каждому понятию $x \in L_n$ соответствует свое подмножество E_x базиса B_n. Множество E_x будем называть ядром понятия x. Обозначим через C_n систему всех подмножеств базиса B_n. Существует биекция

$$\Omega : S_n \to C_n,$$

которая ставит в соответствие каждому понятию $x \in L_n$ его ядро $E_x \in C_x$, так что $E_x = \Omega(x)$.

Докажем, что любая алгебра понятий L_n размерности n изоморфна канонической алгебре понятий $\mathbf{L}_n$ той же размерности. Все символы, относящиеся к алгебре L_n, будем записывать тонким шрифтом, а символы относящиеся к алгебре $\mathbf{L}_n$ – жирным. Введем биекцию

$$\Phi : S_n \to \mathbf{S}_n,$$

определив ее следующим образом:

$$\Phi(0) = \mathbf{0},$$

$$\Phi(e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}) = \mathbf{e}_{i_1}\mathbf{e}_{i_2}...\mathbf{e}_{i_p}.$$

Имеем:

$$\Phi(0 \vee 0) = \Phi(0) = \mathbf{0} = \mathbf{0} \vee \mathbf{0} = \Phi(0) \vee \Phi(0),$$

$$\Phi(0 \vee (e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p})) = \Phi(e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}) =$$

$$= \mathbf{e}_{i_1}\mathbf{e}_{i_2}...\mathbf{e}_{i_p} = 0 \vee \mathbf{e}_{i_1}\mathbf{e}_{i_2}...\mathbf{e}_{i_p} =$$

$$= \Phi(0) \vee \Phi(e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}),$$

$$\Phi((e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}) \vee 0) = \Phi(e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}) =$$

$$= \mathbf{e}_{i_1}\mathbf{e}_{i_2}...\mathbf{e}_{i_p} = \mathbf{e}_{i_1}\mathbf{e}_{i_2}...\mathbf{e}_{i_p} \vee \mathbf{0} =$$

$$= \Phi(e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}) \vee \Phi(0).$$

В алгебре L_n логическая сумма

$$z = e_{k_1} \vee e_{k_2} \vee ... \vee e_{k_r}$$

любых ненулевых понятий

$$x = e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p} \text{ и } y = e_{j_1} \vee e_{j_2} \vee ... \vee e_{j_q}$$

может быть определена, согласно аксиомам идемпотентности, коммутативности и ассоциативности, следующим правилом:

$$\{e_{k_1} \vee e_{k_2} \vee ... \vee e_{k_r}\} = \{e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}\} \cup$$
$$\cup \{e_{j_1} \vee e_{j_2} \vee ... \vee e_{j_q}\}.$$

Для получения логической суммы y по этому правилу нужно выбрать из стандартных форм обоих слагаемых

$$x = e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p} \text{ и } y = e_{j_1} \vee e_{j_2} \vee ... \vee e_{j_q}$$

все входящие в них базисные символы

$$e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p},\ e_{j_1} \vee e_{j_2} \vee ... \vee e_{j_q}$$

и составить из них стандартную форму

$$z = e_{k_1} \vee e_{k_2} \vee ... \vee e_{k_r},$$

не допуская повторений базисных символов и располагая последние в порядке возрастания их номеров. Как мы знаем, аналогичное правило используется и для образования логической суммы в алгебре L_n .мВ силу сказанного имеем:

$$\Phi((e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}) \vee (e_{j_1} \vee e_{j_2} \vee ... \vee e_{j_q})) =$$
$$= \Phi(e_{k_1} \vee e_{k_2} \vee ... \vee e_{k_r}) = \mathbf{e}_{i_p}\mathbf{e}_{k_1}...\mathbf{e}_{k_p}\mathbf{e}_{k_1}\mathbf{e}_{k_2}...\mathbf{e}_{k_r} =$$
$$= \mathbf{e}_{i_1}\mathbf{e}_{i_2}...\mathbf{e}_{i_p} \vee \mathbf{e}_{j_1}\mathbf{e}_{j_2}...\mathbf{e}_{j_q} = \Phi(e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}) \vee$$
$$\vee \Phi(e_{j_1} \vee e_{j_2} \vee ... \vee e_{j_q}).$$

Итак, при любых $x, y \in S_n$ имеем:

$$\Phi(x \vee y) = \Phi(x) \vee \Phi(y).$$

Это означает, что любая алгебра понятий L_n изоморфна [3] канонической алгебре понятий $\mathbf{L}_n$. Отсюда непосредственно следует, что все алгебры понятий размерности n изоморфны друг другу. Теорема доказана.

Смысл теоремы сводится к тому, что ранее введенному понятию алгебры понятий размерности n удовлетворяет единственный абстрактный математический объект. Это означает, что все возможности алгебры понятий размерности n отличаются друг от друга лишь используемыми в них обозначениями. По существу же, т.е. в абстрактном смысле, все такие алгебры неразличимы.

Объединяя теоремы о существовании и изоморфизме алгебр понятий, мы можем утверждать что алгебра понятий каждой размерности n ($n \in \{1,2,...\}$) существует и единственна (с точностью до изоморфизма).

2. Интерпретации алгебры понятий

Рассмотрим некоторые из возможных интерпретаций алгебры понятий размерности n.

А. Алгебра множеств. В качестве носителя S_n алгебры понятий L_n при теоретико-множественной интерпретации берем систему T_n всех подмножеств множества

$$R_n = \{a_1, a_2, ..., a_n\}$$

каких-нибудь символов $a_1, a_2, ..., a_n$. В роли элементов множества S_n выступают подмножества системы T_n. В роли нулевого понятия алгебры L_n берем пустое множество $\varnothing$. В роли базисных понятий

$$e_1, e_2, ..., e_n$$

в алгебре множеств берем одноэлементные множества

$$\{a_1\}, \{a_2\}, ..., \{a_n\}.$$

Под элементом

$$e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}$$

в алгебре множеств понимается множество

$$\{a_{i_1}, a_{i_2}, ..., a_{i_p}\}.$$

Роль операции дизъюнкции в алгебре множеств выполняет операция объединения множеств. Легко проверить, что все аксиомы алгебры понятий L_n в алгебре множеств выполняются.

Б. Алгебра двоичных наборов. В роли понятий алгебры при двоично-кодовой интерпретации берем n-компонентные наборы

$$(\alpha_1, \alpha_2, ..., \alpha_n)$$

двоичных цифр $\alpha_1, \alpha_2, ..., \alpha_n$. В роли носителя S_n алгебры L_n в алгебре двоичных кодов принимаем n-ную декартову степень множества $\{0, 1\}$. Нулевым понятием алгебры L_n при такой интерпретации служит набор $(0,0,...,0)$, составленный из одних нулей. В роли базисных понятий используются всевозможные двоичные наборы, в состав которых входит по одной единице $(1,0,0,...,0)$, $(0,1,0,...,0)$, ..., $(0,0,0,...,1)$. Под элементом

$$e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}$$

в алгебре двоичных наборов понимается набор, у которого на $i_1, i_2, ..., i_p$-том местах стоят единицы, а на остальных местах – нули. Дизъюнкция понятий при двоично-кодовой интерпретации определяется как дизъюнкция двоичных наборов:

$$(\alpha_1, \alpha_2, ..., \alpha_n) \vee (\beta_1, \beta_2, ..., \beta_n) =$$
$$= (\alpha_1 \vee \beta_1 \vee, \alpha_2 \vee \beta_2, ..., \alpha_n \vee \beta_n).$$

Нетрудно убедиться, что все аксиомы алгебры понятий L_n в алгебре n-компонентных двоичных наборов выполняются.

Между алгеброй множеств и алгеброй двоичных наборов существует взаимно однозначная связь. Пусть A – произвольно выбранный элемент алгебры множеств, а $(\alpha_1, \alpha_2, ..., \alpha_n)$ – соответствующий ему элемент алгебры двоичных наборов. Тогда: если $a_i \in A$, то $\alpha_i = 1$; если $a_i \notin A$, то $\alpha_i = 0$; если

$\alpha_i = 1$, то $a_i \in A$; если $\alpha_i = 0$, то $a_i \notin A$ $(i \in \{1,2,...,n\})$. Например, элементу (a_2, a_3, a_5) шестимерной алгебры множеств соответствует элемент $(0,1,1,0,1,0)$ шестимерной алгебры двоичных наборов. Элементу $(1,0,0,0,1,1)$ алгебры двоичных наборов соответствует элемент (a_1, a_5, a_6) алгебры множеств.

В. Алгебра одноместных предикатов первого порядка [4]. Понятиями в n-мерной алгебре одноместных предикатов первого порядка служат всевозможные предикаты $P(x)$, заданные на множестве

$$R_n = (a_1, a_2, ..., a_n)$$

букв $a_1, a_2, ..., a_n$. Нулевым понятием здесь служит тождественно ложный предикат. В роли базисных понятий используются предикаты узнавания букв

$$x^{a_1}, x^{a_2}, ..., x^{a_n},$$

обращающиеся в 1 соответственно при

$$x = a_1, x = a_2, ..., x = a_n$$

и в 0 – при остальных значениях переменной x. Понятием

$$e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_p}$$

в алгебре одноместных предикатов первого порядка служит предикат $P(x)$, обращающийся в 1 при

$$x \in \{a_{i_1}, a_{i_2}, ..., a_{i_p}\}$$

и в 0 – при всех других значениях переменной x. Роль дизъюнкции понятий выполняет операция предикатов. Аксиомы 1) - 5) в алгебре одноместных предикатов первого порядка выполняются. Всего имеется 2^n одноместных предикатов первого порядка.

Между алгеброй множеств и алгеброй двоичных наборов, с одной стороны, и алгеброй одноместных предикатов первого порядка, с другой, имеют место следующие связи. Пусть

$$\{a_{i_1}, a_{i_2}, ..., a_{i_p}\} -$$

произвольно выбранный элемент алгебры множеств. Ему взаимно однозначно соответствует элемент

$$x^{a_{i_1}}, x^{a_{i_2}}, ..., x^{a_{i_p}}$$

алгебры одноместных предикатов первого порядка. Нулевому элементу $\varnothing$ алгебры множеств соответствует тождественно ложный предикат 0. Элементу

$$(\alpha_1, \alpha_2, ..., \alpha_n)$$

алгебры двоичных наборов взаимно однозначно соответствует элемент

$$\alpha_1 \cdot x^{a_1}, \alpha_2 \cdot x^{a_2}, ..., \alpha_n \cdot x^{a_n}$$

алгебры одноместных предикатов.

Г. Алгебра многоместных предикатов первого порядка. Рассмотрим множество N всевозможных предикатов вида

$$P(x_1, x_2, ..., x_m),$$

заданных на декартовом произведении

$$M = M_1 \times M_2 \times ... \times M_m$$

множеств

$$M_i = \{a_{i_1}, a_{i_2}, ..., a_{i_i}\},$$

где $i \in \{1,2,...,m\}$.

Множество N принимаем в роли носителя алгебры понятий L_n. Всего в области M имеется

$$n = n_1 n_2 ... n_m$$

наборов, в множестве N содержится всего

$$2^{n_1 n_2 ... n_m}$$

предикатов. Размерностью алгебры многоместных предикатов первого порядка служит число n. Дизъюнкцией понятий в алгебре многоместных предикатов первого порядка служит операция дизъюнкции предикатов. Нулевым понятием служит предикат 0, тождественно равный нулю. В алгебре многоместных предикатов первого порядка имеется n базисных понятий. В их роли выступают всевозможные предикаты

$$P_j \ (j = 1,2,...,n),$$

обращающиеся в единицу на единственном наборе значений аргументов $(s_1, s_2, ..., s_m)$:

$$P_j(x_1, x_2, ..., x_m) =$$

$$= \begin{cases} 1, & \text{если } (x_1, x_2, ..., x_m) = (s_1, s_2, ..., s_m), \\ 0, & \text{если } (x_1, x_2, ..., x_m) \neq (s_1, s_2, ..., s_m). \end{cases} \quad (1)$$

Нетрудно проверить, что все аксиомы алгебры понятий размерности n в алгебре многоместных предикатов первого порядка выполняются.

В теоретико-множественной интерпретации алгебре многоместных предикатов первого порядка соответствует алгебра всех подмножеств декартова произведения

$$M_1 \times M_2 \times ... \times M_m.$$

Если P и $(s_1, s_2, ..., s_m)$ – соответствующие друг другу элементы алгебры многоместных предикатов первого порядка и алгебры подмножеств декартова произведения $M_1 \times M_2 \times ... \times M_m$, то взаимно однозначная связь между ними определяется правилом:

$$P(x_1, x_2, ..., x_m) = 1$$

в том и только в том случае, когда

$$(s_1, s_2, ..., s_m) \in M_1 \times M_2 \times ... \times M_m.$$

В двоично-кодовой интерпретации алгебре многоместных предикатов первого порядка соответствует алгебра двоичных кодов длины

$$n = n_1, n_2, ..., n_m.$$

Связь между многоместным предикатом первого порядка и соответствующим ему двоичным кодом длины n может быть установлена таким образом.

Двоичному коду

$$x_1, x_2, ..., x_m$$

взаимно однозначно соответствует предикат

$$P(x_1, x_2, ..., x_m) = \bigvee_{a_1, a_2, ..., a_m} \alpha_i x_1^{a_1} x_2^{a_2} ... x_m^{a_m}, \quad (2)$$

где i – номер набора [5] $(s_1, s_2, ..., s_m)$.

д) Алгебра предикатов произвольного порядка [3]. В ней роль идей алгебры L_n выполняют всевозможные предикаты p-го порядка вида

$$f(x_{01}, x_{02}, ..., x_{0m_2}, x_{11}, x_{12}, ..., x_{1m_1}, \ldots,$$

$$x_{p-1,1}, x_{p-1,2}, ..., x_{p-1m_{p-1}}),$$

заданные на декартовом произведении

$$M = M_0^{m_0} \times M_1^{m_1} \times ... \times M_{p-1}^{m_{p-1}}. \quad (3)$$

Множество M_i $(i = 1, 2, ..., p-1)$ образовано из предикатов i-порядка. Алгебра предикатов p-го порядка имеет размерность

$$n = n_0^{m_0} n_1^{m_1} ... n_{p-1}^{m_{p-1}}. \quad (4)$$

Числа $n_1, n_2, ..., n_{p-1}$ определяются по следующей рекуррентной формуле

$$n_i = 2^{n_0^{m_0} n_1^{m_1} ... n_{p-1}^{m_{p-1}}}. \quad (5)$$

где n_0 – число элементов в множестве M_0. В остальном алгебра предикатов произвольного порядка рассматривается аналогично алгебре многоместных предикатов первого порядка.

е) Алгебра булевых функций [4]. К алгебре булевых функций приходим, принимая в алгебре понятий L_n в роли S_n множество всех m-местных булевых функций. Размерностью алгебры понятий в этом случае служит число $n = 2^m$. Всего в множестве S_n содержится $n = 2^{2^m}$ векторов. Нулевым понятием служит m-местная булева функция, тождественно равная нулю. В роли базисных понятий выступают всевозможные булевы функции, обращающиеся в единицу лишь на одном наборе значений аргументов. Всего в алгебре m-местных булевых функций имеется 2^m различных базисных понятий. В роли операции дизъюнкции понятий в данном случае выступает операция дизъюнкции m-местных булевых функций. При $m=1$ приходим к алгебре логики. В этом случае в роли операции дизъюнкции понятий выступает дизъюнкция двоичных знаков: $0 \vee 0 = 0$, $0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1$. Нулевым понятием служит знак 0, единственным базисным понятием– знак 1.

Выводы

В работе сформулирована и доказана теорема о том, что алгебры понятий одинаковой размерности изоморфны друг другу. Вместе с теоремой о существовании алгебр понятий теорема об изоморфизме позволяет утверждать, что алгебра понятий каждой размерности существует и единственна с точностью до изоморфизма.

Рассмотрены некоторые возможные интерпретации алгебры понятий - алгебры множеств, двоичных наборов, одноместных и многоместных предикатов первого порядка, булевых функций.

Список литературы

1. Голян Н.В. Алгебра понятий как формальный аппарат моделирования действий интеллекта над понятиями / Н.В. Голян, В.В. Голян, Л.Д. Самофалов // Системи управління, навігації та зв'язку. – П.: ПНТУ, 2016. – Вип. 3(39). – С. 38-41.

2. Голян Н.В. О свойствах канонической алгебры понятий / Н.В. Голян // Системи управління, навігації та зв'язку. – П.: ПНТУ, 2016. – Вип. 4(40). – С. 44-47.

3. Гильберт Д. Основания геометрии / Д. Гильберт. – М.; Л.: Гостехиздат. 1948. – 364 с.

4. Бондаренко М.Ф. Теория интеллекта. Учебник / М.Ф. Бондаренко, Ю.П. Шабанов-Кушнаренко. – Харьков: СМИТ, 2007 – 576 с.

5. Гильберт Д., Основания математики. Логические исчисления и формализация арифметики / Д. Гильберт, П. Бернайс . – М.: Наука, 1979. – 557 с.

Надійшла до редколегії 26.12.2016

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет імені М.Є. Жуковського «ХАІ», Харків.

ІЗОМОРФІЗМ І ІНТЕРПРЕТАЦІЇ АЛГЕБРИ ПОНЯТЬ

Н.В. Голян

У роботі сформульована і доведена теорема про те, що алгебра понять однакової розмірності ізоморфні між собою. Разом з теоремою про існування алгебри понять теорема про ізоморфізм дозволяє стверджувати, що алгебра понять кожної розмірності існує і єдина з точністю до ізоморфізму.

Ключові слова: *алгебра скінченних предикатів, алгебра понять, канонічна алгебра, изоморфизм, интерпретации алгебры.*

THE CONCEPTS ALGEBRAS ISOMORPHISM AND INTERPRETATIONS

N.V. Golian

In the article is set forth and well-proven a theorem that identical dimension concepts algebras are isomorphic each other. Together with a theorem about concepts algebras existence a theorem about an isomorphism allows to assert that every dimension concepts algebra exists and only within an isomorphism.

Keywords: *finite predicates algebra, algebra of concepts, canonical algebra, isomorphism, algebra interpretations.*

УДК 519.6:311.214

В.Ю. Дубницкий[1], А.М. Кобылин[1], О.А. Кобылин[2]

[1] *Харьковский учебно-научный институт ГВУЗ «Университет банковского дела», Харьков*
[2] *Харьковский национальный университет радиоэлектроники, Харьков*

ВЛИЯНИЕ ОСОБЕННОСТЕЙ ПОДГОТОВКИ ДАННЫХ НА ШИРИНУ ИНТЕРВАЛА НЕОПРЕДЕЛЕННОСТИ ТИПА В ПРИ ВЫЧИСЛЕНИИ ОСНОВНЫХ ВИДОВ ЭКОНОМИЧЕСКИХ ИНДЕКСОВ

В работе рассмотрены основные сводные индексы, используемые в экономической статистике. Приведены выражения для вычисления значений основных типов сводных индексов, используемых в экономической статистике, при условии их определения в виде интервальных чисел, заданных в системе центр-радиус. Проведен численный пример, иллюстрирующий полученные результаты. В результате численного эксперимента проверено влияние условий вычислений основных типов экономических индексов на величину получаемого интервала неопределённости типа В. Проверена гипотеза о неустойчивости величины интервала неопределённости типа В по отношению к виду вычисляемого индекса и количеству слагаемых, используемых при его определении. Проверена гипотеза о корректности применения выборочных методов при вычислении экономических индексов.

Ключевые слова. *экономические индексы, индексный метод в статистике, интервальные вычисления, система центр-радиус, выборочный метод в статистике, непараметрические методы статистики, тесты Краскалла-Уоллеса, медиан Муда.*

Введение

В экономической статистике индексный метод служит одним из основных методов экономического анализа. Основы этого метода и особенности его применения рассмотрены, например, в работах [1…3]. В работе [1] дано такое определение: «Индексы - это относительные системные показатели, которые характеризуют изменения экономических, социальных и других явлений во времени, в пространстве или в сопоставлении с любой базой сравнении (стандартными, плановыми или средними величинами, показателями прошлых периодов, лучших предприятий, организаций, учреждений и т.д.)». При вычислении индексов, характеризующих локальные хозяйственные предприятия, в которых возможен сплошной бухгалтерский учет всех видов затрат, точность вычислений индексов гарантирована выполнением требований соответствующих нормативных документов. В том случае, когда элементы индексов определены по результатам выборочных наблюдений, возникает проблема оценки погрешности полученных результатов. Естественным способом уменьшения погрешности выборочного метода может быть увеличение объёма обследуемой выборки, что сопряжено с увеличением затрат на проведение исследования. Поэтому предварительное определение погрешности получаемых результатов может существенно сократить затраты на проведение исследований.

Анализ литературы. Одной из первых работ, в которых была рассмотрена задача определения погрешности экономических показателей, была работа [4]. В ней рассмотрены три взаимосвязанные проблемы: достоверность в связи с построением экономических показателей; методы ее оценки; чувствительность и устойчивость показателей. Для оценки погрешности определения экономических показателей автор работы [4] использовал методы теории погрешностей вычислений и методы математической статистики. В работе [5] методами имитационного моделирования было изучено влияние случайных погрешностей на изменение индексов, характеризующих динамику экономических показателей. Аналогичный приём использован и в работе [6]. В работе [7], используя метод линеаризации неслучайных функций случайных аргументов, в явном виде получены выражения необходимые для оценки дисперсии результатов вычисленных значений индексов. Приведены способы определения абсолютной и относительной погрешности численных значений индексов товарооборота, объёма реализации, индексов цен в форме Пааше и в форме Ласпейроса. Получены выражения для определения предельной относительной ошибки при вычислении этих индексов.

Так, как исходные данные для вычисления индексов, по предположения, получают по результатам выборочных исследований, то окончательному результату будет присуща некоторая неопределённость, которая должна быть учтена при анализе полученных результатов.

Для этого используем концепцию неопределённости измерений [8…10]. В соответствии с ней неопределённость делят на две группы. Неопределённость типа А, оцениваемая по результатам статистического анализа повторных наблюдений и неопределённость типа **В**, оцениваемая нестатистиче-

скими методами. В работе [7] решена задача определения интервала неопределённости типа **A**, которая возникает при применении индексного метода экономической статистики. Эта же задача при неопределённости типа **B**, насколько нам известно, в литературе не рассмотрена. В работе [11] показано, что при выполнении экономических расчётов в условиях неопределённости типа B целесообразно использовать методы интервальной арифметики. Наименьший интервал неопределённости результата вычислений в этом случае будет при использовании интервальных чисел, заданных в системе центр-радиус. Правила вычисления, используемые в этом случае, подробно описаны в работах [12, 13]

В данной работе будут рассмотрены следующие индексы, приведенные в работах [1…3] и представленные в форме, приведенной в работе [7]. В силу сложившейся традиции в индексном методе форма записи формул, несколько отличающаяся от принятой в математике. Примем в качестве исходных данных не только символику, но и названия индексов и способы их определения.

Сводный индекс товарооборота представим в виде:

$$I_{pq} = \frac{\sum p_1 q_1}{\sum p_0 q_0} = \sum_{i=1}^{n} p_{1i} q_{1i} \Big/ \sum_{i=1}^{n} p_{0i} q_{0i} \ , \ i = \overline{1,n} \ . \quad (1)$$

В этом и последующих выражениях индекс i=1, 2, …, n и соответствует строке в таблице рис. 1, обозначающей вид продукции.

Сводный индекс физического объёма реализации представим в виде:

$$I_p = \frac{\sum p_0 q_1}{\sum p_0 q_0} = \sum_{i=1}^{n} p_{0i} q_{1i} \Big/ \sum_{i=1}^{n} p_{0i} q_{0i} \ , \ i = \overline{1,n} \ . \quad (2)$$

Сводный индекс цен (по методу Пааше) представим в виде:

$$\Pi_q = \frac{\sum p_1 q_1}{\sum p_0 q_1} = \sum_{i=1}^{n} p_{1i} q_{1i} \Big/ \sum_{i=1}^{n} p_{0i} q_{1i} \ , \ i = \overline{1,n} \ . \quad (3)$$

Сводный индекс цен (по методу Ласпейреса) представим в виде:

$$L_p = \frac{\sum p_1 q_0}{\sum p_0 q_0} = \sum_{i=1}^{n} p_{1i} q_{0i} \Big/ \sum_{i=1}^{n} p_{0i} q_{0i} \ , \ i = \overline{1,n} \ . \quad (4)$$

В этих и последующих выражениях первый нижний индекс в соответствии с работой [2] обозначает соответственно данные, полученные в отчетном периоде, если он равен единице и данные, полученные в базисном периоде, если он равен нулю. Второй индекс i=1, 2, …, n обозначает наименование вида продукции.

В работах [1]…[3] подробно рассмотрено экономическое содержание основных экономических индексов и техника их вычисления. Неопределённость результатов вычислений в них не рассмотрена.

Постановка задачи

Так как в нашем случае структура формул и особенности вычислений будут важнее конкретной предметной области, то рассмотрим выражение вида:

$$Z = \frac{\sum ab}{\sum cd} = \sum_{i=1}^{n} a_i b_i \Big/ \sum_{i=1}^{n} c_i d_i \ . \quad (5)$$

Рассматривая это выражение как некий обобщённый индекс, представим его в интервальном виде, используя систему центр-радиус:

$$\tilde{Z} = \langle z; r_z \rangle = \tilde{U} / \tilde{W} = \langle u; r_u \rangle / \langle w; r_w \rangle \ . \quad (6)$$

Числитель выражения (6) представим в виде

$$\langle u; r_u \rangle = \sum_{i=1}^{n} \langle a_i ; r_{ai} \rangle \cdot \langle b_i ; r_{bi} \rangle \ , \quad (7)$$

знаменатель выражения (6) представим в виде

$$\langle w; r_w \rangle = \sum_{i=1}^{n} \langle c_i ; r_{ci} \rangle \cdot \langle d_i ; r_{di} \rangle \ . \quad (8)$$

Представим слагаемое в (8) в таком виде:

$$\langle a_i ; r_{ai} \rangle \cdot \langle b_i ; r_{bi} \rangle = \left\langle \sum_{i=1}^{n} (a_i b_i + r_{ai} r_{bi}) ; \sum_{i=1}^{n} (a_i r_{bi} + b_i r_{ai}) \right\rangle . \quad (9)$$

Используя доказанное в работе [13] свойство ассоциативности для интервальных чисел, определённых в системе центр-радиус, условие (9) представим в виде:

$$\langle u; r_u \rangle = \left\langle \sum_{i=1}^{n} (a_i b_i + r_{ai} r_{bi}) ; \sum_{i=1}^{n} (a_i r_{bi} + b_i r_{ai}) \right\rangle . \quad (10)$$

Знаменатель условия (6) используя равенство (9) представим в виде:

$$\langle w; r_w \rangle = \left\langle \sum_{i=1}^{n} (c_i d_i + r_{ci} r_{di}) ; \sum_{i=1}^{n} (c_i r_{di} + d_i r_{ci}) \right\rangle . \quad (11)$$

Используя выражение (6) получим, что:

$$\frac{\langle u, r_u \rangle}{\langle w, r_w \rangle} = \left\langle \frac{uw + r_u r_w}{w^2 - r_w^2}, \frac{ar_b + br_a}{w^2 - r_w^2} \right\rangle . \quad (12)$$

Из условий (6) и (7) следует, что:

$$u = \sum_{i=1}^{n} (a_i b_i + r_{ai} r_{bi}) \ ; \quad (13)$$

$$r_u = \sum_{i=1}^{n} (a_i r_{bi} + b_i r_{ai}) \ ; \quad (14)$$

$$w = \sum_{i=1}^{n} (c_i d_i + r_{ci} r_{di}) \ ; \quad (15)$$

$$r_w = \sum_{i=1}^{n} (c_i r_{di} + d_i r_{ci}) \ . \quad (16)$$

Рассмотрим пример, основанный на данных, приведенных в работе [7].

Исходные данные для расчета индексов в интервальном виде приведены на рис. 1.

Вид продукции	Базисный период				Отчетный период			
	Цена единицы, грн, в интервале p_0		Продано единиц, q_0 (в интервале)		Цена единицы, грн, p_1		Продано единиц, q_1	
	Базовая цена-центр	Отклонение цены в % -радиус	Количество проданной продукции-центр	Отклонение количество проданной продукции в % -радиус	Базовая цена-центр	Отклонение цены в % -радиус	Количество проданной продукции - центр	Отклонение количества проданной продукции в % -радиус
Продукция 1	12	10	18	5	12	5	15	8
Продукция 2	11	5	22	6	10	4	27	7
Продукция 3	9	5	20	7	7	5	24	9

Рис. 1. Исходные данные для расчета индексов в интервальном виде

Результаты расчета сводных индексов по традиционной методике, изложенной в работах [1]…[3], и в интервальном виде в форме «центр-радиус», изложенном в работах [11]…[13] представлены в табл. 1.

Таблица 1

Результаты вычислений индексов в евклидовом и интервальном, в системе центр-радиус, виде

Наименование индекса	Классическая, Евклидова, форма	Интервальные значения	
		Нижняя граница	Верхняя граница
Сводный индекс товарооборота, Ipq	0,969	0,754	1,245
Сводный индекс объёма реализации, Ip	1,086	0,829	1,420
Сводный индекс цен по методу Паше, Пq	0,892	0,684	1,165
Сводный индекс цен по методу Ласпейреса, Lp	0,903	0,717	1,140

Следует обратить внимание на то, что на этом, примере уже видно, что интервал неопределенности, то есть разность значений верхней и нижней границы индексов, дает возможность с равным успехом утверждать, что в генеральной совокупности наблюдений мы наблюдаем спад экономики или её подъём. Причём оба эти вывода математически корректны. Заголовок работы [14] дает исчерпывающее объяснение этому обстоятельству.

Исходя из условий (6) – (16) предложена гипотеза о том, что на величину итогового интервала неопределённости типа **B** могут оказывать влияние следующие факторы, связанные с процессом организации вычислений:

- -порядок чисел сомножителей в каждом из слагаемых, входящих в тот или иной тип индекса;
- -наличие или отсутствие изменений, произошедших в изучаемой системе за анализируемый промежуток времени.
- -количество слагаемых, учитываемых при определении каждого из типов индексов.

Цель работы: проведение численного эксперимента для проверки сформулированной гипотезы.

Методика проведения численного эксперимента и полученные результаты

Обоснования для выбранных факторов, влияющих, по предположению авторов данного сообщения, на результат вычислений следующие. Например, при продаже товаров повседневного спроса цена каждого вида товара небольшая, количество единиц проданного товара велико и, следовательно, порядки чисел, входящих в сомножители в формулах вычисления индексов могут отличаться в разы. При изучении изменений, произошедших в экономических системах за заданный интервал времени итоговые интервалы неопределённости могут пересекаться, что затруднит корректные выводы о наличии или отсутствии изменений в развитии системы. При проведении выборочных наблюдений на результат вычислений может оказать влияние фактор объёма выборки. Вычислительный эксперимент был организован следующим образом.

На первом этапе моделировали данные для системы, в которой предполагали отсутствие изменений, схема «Роста нет». Для этого получали сто равномерно распределённых чисел в заданных интервалах. Эти данные имитировали данные, полученные в начале наблюдения за системой. Порядок соотношения сомножителей и результаты вычислений показаны в табл. 2. На втором шаге эксперимента эту процедуру повторяли, при этом интервалы, в которых моделировали данные, совпадали с интервалами первого этапа, что соответствовало схеме «Роста нет».

На втором этапе моделировали данные для системы, в которой предполагали наличие изменений, схема «Рост есть». Для этого на первом шаге получали сто равномерно распределённых чисел в заданных интервалах. Эти данные имитировали данные, полученные в начале наблюдения за системой.

Порядок соотношения сомножителей и результаты вычислений показаны в табл. 2 (схема «Роста нет»). На втором шаге эксперимента эту процедуру повторяли, но каждую пару данных умножали на увеличивающие коэффициенты, равномерно распределённые в заданных интервалах для каждой пары данных. Этот приём реализовывал схему «Рост есть». Для величины p_1 этот коэффициент составил 1,05…1,15; для величины q_1 этот коэффициент составил 1,20…1,30. Результаты приведены в табл. 2 (схема «Рост есть»).

Данные для изучения влияния на ширину интервала неопределённости типа индекса, соотношения порядка сомножителей и наличия или отсутствия динамики в процессе функционирования рассматриваемых систем представлены в табл. 3.

Таблица 2

Величина интервала неопределённости при вычислении основных типов экономических индексов

Вид индекса	Соотношение порядка сомножителей в каждом из слагаемых											
	1:1			1:2			1:3			1:4		
	НГ[1)]	Ц	ВГ	НГ	Ц	ВГ	НГ	Ц	ВГ	НГ	Ц	ВГ
Схема «Роста нет»												
Ipq	0,989	0,990	0,991	1,028	1,033	1,038	1,184	1,184	1,185	0,947	0,948	0,949
Ip	0,960	0,963	0,965	0,999	1,000	1,001	0,993	0,993	0,993	0,968	0,972	0,977
Пq	1,025	1,029	1,032	1,028	1,033	1,039	1,193	1,193	1,194	0,971	0,975	0,978
Lp	1,005	1,005	1,006	1,002	1,004	1,005	1,168	1,170	1,171	0,926	0,928	0,930
Схема «Рост есть»												
Ipq	1,363	1,363	1,363	1,363	1,363	1,363	1,363	1,363	1,363	1,363	1,363	1,363
Ip	1,199	1,199	1,199	1,199	1,199	1,199	1,199	1,199	1,199	1,199	1,199	1,199
Пq	1,131	1,131	1,131	1,131	1,131	1,131	1,131	1,131	1,131	1,131	1,131	1,131
Lp	1,105	1,105	1,105	1,105	1,105	1,105	1,105	1,105	1,105	1,105	1,105	1,105

Примечание: НГ –нижняя граница, Ц –центр, ВГ- верхняя граница интервала неопределенности

Таблица 3

Влияние на ширину интервала неопределённости при вычислении основных типов экономических индексов, соотношения порядка сомножителей и типа индекса

Соотношение порядков сомножителей	Границы интервала неопределённости	Ipq	Ip	Пq	Lp	min	max	Δ
Схема «Роста нет»								
1:1	НГ	0,989	0,960	1,025	1,005	0,960	1,025	0,065
	Ц	0,990	0,963	1,029	1,005	0,963	1,029	0,066
	ВГ	0,991	0,965	1,032	1,006	0,965	1,032	0,067
1:2	НГ	1,028	0,999	1,028	1,002	0,999	1,028	0,029
	Ц	1,033	1,000	1,033	1,004	1,000	1,033	0,034
	ВГ	1,038	1,001	1,039	1,005	1,001	1,039	0,039
1:3	НГ	1,184	0,993	1,193	1,168	0,993	1,193	0,200
	Ц	1,184	0,993	1,193	1,170	0,993	1,193	0,201
	ВГ	1,185	0,993	1,194	1,171	0,993	1,194	0,201
1:4	НГ	0,947	0,968	0,971	0,926	0,926	0,971	0,045
	Ц	0,948	0,972	0,975	0,928	0,928	0,975	0,047
	ВГ	0,949	0,977	0,978	0,930	0,930	0,978	0,048
min		0,947	0,960	0,971	0,926			
max		1,185	1,001	1,194	1,171			
Δ		0,238	0,040	0,223	0,245			
Схема «Рост есть»								
1:1	НГ	1,363	1,199	1,131	1,105	1,105	1,363	0,258
	Ц	1,364	1,202	1,135	1,106	1,106	1,364	0,259
	ВГ	1,366	1,205	1,139	1,106	1,106	1,366	0,259
1:2	НГ	1,417	1,250	1,131	1,106	1,106	1,417	0,311
	Ц	1,423	1,251	1,138	1,108	1,108	1,423	0,316
	ВГ	1,430	1,252	1,144	1,109	1,109	1,430	0,321
1:3	НГ	1,626	1,239	1,312	1,280	1,239	1,626	0,387
	Ц	1,627	1,239	1,313	1,282	1,239	1,627	0,388
	ВГ	1,628	1,239	1,314	1,283	1,239	1,628	0,388
1:4	НГ	1,297	1,209	1,064	1,017	1,017	1,297	0,280
	Ц	1,298	1,215	1,068	1,019	1,019	1,298	0,279
	ВГ	1,299	1,221	1,072	1,021	1,021	1,299	0,278
min		1,297	1,199	1,064	1,017			
max		1,628	1,252	1,314	1,283			
Δ		0,331	0,053	0,249	0,266			

Влияние исследуемых факторов на наименьшую и наибольшую ширину интервалов определения индексов показано в табл. 4.

Таблица 4

Влияние
на наименьшую и наибольшую ширину интервала неопределённости при вычислении основных типов экономических индексов, соотношения порядка сомножителей и типа индекса

Ширина интервала	Соотношения порядка сомножителей	Тип индекса
Схема «Роста нет»		
Наименьшая	0,029	0,040
Наибольшая	0,201	0,245
Схема «Рост есть»		
Наименьшая	0,258	0,053
Наибольшая	0,388	0,331

Приведенные данные дают основание предположить, что процесс вычисления индексов неустойчив по отношению к изучаемым факторам.

Для сравнения результатов определений значений индексов сплошным и выборочным методом был выполнен экономический анализ, проведенный по следующей схеме.

Определению подлежал индекс Ipq для данных полученных по схеме «Роста нет».

Соотношение порядка сомножителей было принято 1:1.

Сплошной (исходной) выборке соответствовали сто данных, результаты обработки которых приведены в табл. 2, 3.

Из исходной выборки было сформировано десять выборок по десять результатов вычислений индексов. Для каждой из этих выборок ширина интервала (удвоенный радиус) показана в табл. 5.

Таблица 5

Ширина интервала неопределённости полученного при определении индекса Ipq

Соотношение порядка сомножителей			
1:1	1:2	1:3	1:4
0,03628	0,036951	0,011807	0,012425
0,02026	0,013371	0,008266	0,011174
0,017747	0,018756	0,004039	0,002121
0,005485	0,02158	0,011428	0,018228
0,015232	0,029416	0,010929	0,022903
0,009176	0,000361	0,006012	0,008928
0,009176	0,000361	0,00601	0,008928
0,006636	0,003453	0,00475	0,010321
0,013263	0,008104	0,023915	0,047052
0,00624	0,012614	0,018677	0,014333

Для проверки нестатистической гипотезы о совпадении результатов выборочных исследований между собой были сформулированы следующие статистические гипотезы: нулевая гипотеза о том, что медианы полученных выборок совпадают и альтернативная - медианы полученных выборок не совпадают.

Для проверки этих гипотез использованы непараметрические тесты Краскалла-Уоллеса и медиан Муда в том виде, в котором они реализован в системе STATGRAPHICS XV.1. Результаты вычислений приведены в табл. 6. Так как полученные величины Pv превышают величину Pv=0,05, следует принять нулевую гипотезу.

Таблица 6

Результаты проверки нестатистической гипотезы
о совпадении результатов выборочных исследований при определении индекса Ipq

Тип теста	Значение критерия	Величина Pv
Краскалла-Уоллеса	1,2450	0,7351
медиан Муда	0,8000	0,8449

Выводы

1. В работе использованы основные сводные индексы, используемые в экономической статистике.

2. Приведены выражения для вычисления значений основных типов сводных индексов, используемых в экономической статистике, при условии их определения в виде интервальных чисел, заданных в системе центр-радиус. Приведен численный пример, иллюстрирующий полученные результаты.

3. В результате численного эксперимента проверено влияние условий вычислений основных типов экономических индексов на величину получаемого интервала неопределённости типа B.

4. Проверена гипотеза о неустойчивости величины интервала неопределённости типа В по отношению к виду вычисляемого индекса и количеству слагаемых, используемых при его определении.

5. Проверена гипотеза о корректности применения выборочных методов при вычислении экономических индексов.

Список литературы

1. Ковалевский Г.В. Статистика: учебник [Текст] / Г.В. Ковалевский; Харьк. нац. акад. гор. хоз-ва. – Х.: ХНАГХ, 2012. – 445 с.

2. Практикум по теории статистики: Учеб. пособие. [Текст] / Под ред. Р.А. Шмойловой. – М.: Финансы и статистика, 2003. – 416 с.

3. Эконометрия [Текст] / В.И. Суслов, Н.М. Ибрагимов, Л.П. Талышева, А.А. Цыплаков. – Н-ск : Изд.-во СО РАН, 2005. –744 с.

4. Эдельгауз Г.Е. Достоверность статистических показателей. [Текст] / Г.Е. Эдельгауз. М.: Статистика, 1977. – 278 с.

5. Абрамова Ю.С. Исследование проблемы точности планирования финансовых показателей предприятия с помощью имитационно-статистического моделирования: дис. канд. экон. наук: 08. 00. 05 [Текст] / Абрамова Юлия Сергеевна. – Москва, 2005. – 229 с.

6. Сильченко Т.Ю. Точность экономических расчётов при обосновании управленческих решений в производственных системах промышленных предприятий. [Текст] / Т.Ю. Сильченко // TERRA ECONOMICUS. –2009. – Т. 7, № 3. – С. 86-90.

7. Дубницкий В.Ю. Определение интервала неопределённости при применении индексного метода экономической статистики [Текст] / В.Ю. Дубницкий // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 8(115). – С. 171-175.

8. Guide to the Expression of Uncertainty in Measurement: First edition. [Текст] / ISO, Switzerland,1993.

9. ДСТУ-Н РМГ 43:2006 Метрологія. Застосування «Руководства по выражению неопределенности измерений» (РМГ 43:2001).

10. Поджаренко В.О. Опрацювання результатів вимірювань на основі концепції невизначеності. Навчальний посібник. [Текст] / В.О. Поджаренко, О.М. Василевський, В.Ю.Кучерук. – Вінниця: ВНТУ, 2008. – 158 с.

11. Дубницький В.Ю. Порівняльний аналіз результатів планування нормативів банківської безпеки засобами класичної та нестандартної інтервальної математики. [Текст] / В.Ю. Дубницький, А.М. Кобилін // Радіоелектронні і комп'ютерні системи. – Х., 2014. – №5 (69). – С. 29-33.

12. Дубницький В.Ю. Вычисление значений элементарных функций с интервально заданным аргументом, определённым в системе центр-радиус [Текст] / В.Ю. Дубницкий, А.М. Кобылин, О.А. Кобылин. // Системи обробки інформації. – Х.: ХУПС, 2016. – Вип. 7(144). – С. 107-112.

13. Жуковська О.А. Основи інтервального аналізу. [Текст] / О.А. Жуковська. – К.: Освіта України 2009. – 136 с.

14. Селюнин В. Лукавая цифра / В. Селюнин, Г. Ханин // Новый мир. – 1987. – № 2. – С. 181-201.

Надійшла до редколегії 26.12.2016

Рецензент: д-р екон. наук, доц. С.В. Кавун, Харківського навчально-наукового інституту ДВНЗ «Університет банківської справи», Харків.

ВПЛИВ ОСОБЛИВОСТЕЙ ПІДГОТОВКИ ДАНИХ НА ШИРИНУ ІНТЕРВАЛУ НЕВИЗНАЧЕНОСТІ ТИПУ В ПРИ ОБЧИСЛЕННІ ОСНОВНИХ ВИДІВ ЕКОНОМІЧНИХ ІНДЕКСІВ

В.Ю. Дубницький, А.М. Кобилін, ОА. Кобилін

У роботі використано основні зведені індекси, які використовують в економічній статистиці. Наведено вирази для обчислення значень основних типів зведених індексів, що використовують в економічній статистиці, за умови їх визначення у вигляді інтервальних чисел, заданих в системі центр-радіус. Наведено чисельний приклад, що ілюструє отримані результати. В чисельному експерименті перевірено вплив умов обчислень основних типів економічних індексів на величину отриманого інтервалу невизначеності типа В. Перевірена гіпотеза про нестійкість величини інтервалу невизначеності типу В по відношенню до виду обчислюваного індексу і кількості доданків, що використовано при його визначенні. Перевірена гіпотеза про коректність застосування вибіркових методів при обчисленні економічних індексів.

Ключові слова: *економічні індекси, індексний метод в статистиці, інтервальні обчислення, система центр-радіус, вибірковий метод в статистиці, непараметричні методи статистики, тести Краскалла-Уоллеса, медіан Муда.*

EFFECT OF DATA PREPARATION PECULIARITIES ON B TYPE INTERVAL OF UNCERTANTY WIDTH IN CALCULATION OF BASIC KINDS OF ECONOMIC INDICES

V.Yu. Dubnitskiy, A.M. Kobylin, O.A. Kobylin

The work operates with basic composite indices as used in economic statistics. Expressions are specified for calculation of values of basic economic indices as used in economic statistics under the proviso that they were determined in the form of interval numbers set in center-radius system. A numeric example is given that illustrates the obtained results. By way of numeric experiment the effect of conditions for calculation of basic economic indices types on the value of obtained B type interval of uncertainty was checked. A hypothesis was tested of instability of B type interval of uncertainty value in relation to the type of calculated index and to the number of summands used in its definition. A hypothesis was tested of correctness of sampling methods application in calculation of economic indices.

Keywords*: economic induces, index method in statistics, interval calculations, center-radius system, sampling method in statistics, non-parametric methods of statistics, Kruskal-Wallis test, Mood's median test.*

УДК 510.635

И.А. Лещинская

Харьковский национальный университет радиоэлектроники, Харьков

О СВОЙСТВАХ ПРЕДИКАТА РАВЕНСТВА ПОНЯТИЙ

В работе развивается алгебра понятий. Найдены и доказаны свойства предиката равенства понятий. Эти свойства проанализированы с точки зрения практического применения для идентификации интеллектуальной деятельности человека.

Ключевые слова: *алгебра конечных предикатов, алгебра понятий, интеллект, высказывание.*

Введение

В работе [1] был рассмотрен абстрактный эквивалент алгебры конечных предикатов - алгебра понятий. С помощью алгебры понятий формально описываются закономерности интеллектуальной деятельности человека. Это сложный объект для идентификации, поскольку интеллектуальная деятельность человека субъективна. Восприятие, понимание, мысли, образы, формируемые интеллектом человека, надо формализовать на основе объективных научных методов. Обсуждаются требования к экспериментам с испытуемым – однозначность, повторяемость; к подбору физических сигналов, выполняющих роль имен понятий, информационной подготовке испытуемого, обеспечению учета контекста эксперимента. Введен предикат равенства понятий и проанализирована его роль в механизме интеллекта.

В статье развивается алгебра понятий. Найдены и доказаны свойства предиката равенства понятий. Эти свойства проанализированы с точки зрения практического применения для идентификации интеллектуальной деятельности человека.

1. Свойства предиката равенства понятий

Найдем свойства предиката D_k, введенного в [1]. Предикат D_k подчиняется закону рефлексивности: для $\forall P \in M_k$ $D_k(P, P) = 1$. Действительно, согласно определению (1) из [1], для каждого предиката $P \in M_k$ имеем:

$$D_k(P, P) = \forall x\,(P(x) \sim P(x)) = \forall x\,(1) = 1.$$

Предикат D_k подчиняется также закону, который называют законом подстановки: для $\forall P, Q \in M_k$, если $R(P) = 1$ и $D_k(P, Q) = 1$, то $R(Q) = 1$. Здесь $R(P)$ - произвольно выбранный предикат, заданный на множестве предикатов M_k.

Доказательство закона подстановочности: если $P, Q \in M_k$ таковы, что $P = Q$, то

$$R(P) \wedge D_k(P,Q) \supset R(Q) = R(P) \wedge D_k(P,P) \supset$$
$$\supset R(P) = R(P) \cdot 1 \supset R(P) = R(P) \supset R(P) = 1.$$

Если же $P \neq Q$, то

$$R(P) \wedge D_k(P, Q) \supset R(Q) = R(P) \wedge \forall x(P(x) \sim$$
$$\sim Q(x)) \supset R(Q) = R(P) \cdot 0 \supset R(Q) = 0 \supset R(Q) = 1.$$

Предикат D_k удовлетворяет закону симметричности: для $\forall P, Q \in M_k$ если $D_k(P,Q) = 1$, то $D_k(Q,P) = 1$. Действительно,

$$D_k(P,Q) \supset D_k(Q,P) = \forall x(P(x) \sim Q(x)) \supset \forall x(Q(x) \sim$$
$$\sim P(x)) = \forall x(P(x) \sim Q(x)) \supset \forall x(P(x) \sim Q(x)) = 1.$$

Предикат D_k подчиняется закону транзитивности: для $\forall P, Q, R \in M_k$ если

$$D_k(P,Q) = D_k(Q,R) = 1,$$

то $D_k(P,R) = 1$. В самом деле, для $\forall P, Q, R \in M_k$ по закону подстановочности выводим:

если $R(Q) = D_k(P,R) = 1$ и $D_k(Q,R) = 1$, то $R(P) = D_k(P,R) = 1$.

Предикат равенства идей D_k подчиняется закону рефлексивности: для $\forall x \in S_k$ имеет место равенство $D_k(x,x) = 1$. Действительно, согласно определению (2) из [1], имеем:

$$D_k(x,x) = D_k(\Phi(x), \Phi(x)) = 1.$$

Предикат D_k подчиняется также закону подстановочности: для любого предиката R, заданного на множестве S_k, и для $\forall x, y \in S_k$ если $R(x) = 1$ и $D_k(x,y) = 1$, то $R(y) = 1$. В самом деле, пусть

$$P = \Phi(x),\ Q = \Phi(y),\ R(P) = R(\Phi^{-1}(P)),$$

$$D_k(P,Q) = D_k(\Phi^{-1}(P), \Phi^{-1}(Q)).$$

Тогда по закону подстановочности предиката равенства предикатов имеем: $R(P) = 1$ и $D_k(P, Q) = 1$ влечет $R(Q) = 1$. Иными словами, $R(\Phi^{-1}(P)) = 1$ и $D_k(\Phi^{-1}(P), \Phi^{-1}(Q))$ влечет $R(\Phi^{-1}(Q)) = 1$. Учитывая, что $\Phi^{-1}(P) = x$, $\Phi^{-1}(Q) = y$, приходим к закону подстановочности

для предиката равенства идей. Аналогично выводятся для предиката D_k закон симметричности: для $\forall x, y \in S_k$ если $D_k(x,y) = 1$, то $D_k(y,x) = 1$, и закон транзитивности: для $\forall x, y, z \in S_k$ если $D_k(x,y) = D_k(y,z) = 1$, то $D_k(x,z) = 1$.

2. Экспериментальная проверка свойств предиката равенства понятий

Сначала рассмотрим психологическую интерпретацию закона симметричности. В содержательной формулировке закон симметричности гласит: если испытуемый признал понятия x и y идентичными, то он обязательно признает идентичными также и понятия y и x. Мы затрудняемся привести какой-нибудь конкретный случай, в котором при ясном и четком восприятии двух понятий и при выполнении условия повторяемости результат сравнения понятий зависел бы от того, в каком порядке они предъявлены человеку. Таким образом, факты, которые бы опровергали закон симметричности, не удается обнаружить. Из закона симметричности следует, что области задания для переменных x и y предиката $D_k(x,y)$ совпадают, а это означает, что множество T, на котором определен предикат D_k, можно представить, причем единственным образом, в виде декартова квадрата некоторого множества Q, т.е. $T=Q\times Q$. Множество Q мы примем в роли носителя алгебры понятий S_k.

Несколько сложнее будет обстоять дело с выполнением закона симметричности, если мы захотим распространить термин «понятие» не только на мысли, но и на ощущения. Известны такие опыты из области психофизики ощущений, которые, казалось бы, опровергают закон симметричности для предиката D_k. Опишем один из таких опытов. Испытуемому предъявляются два коротких звука, имеющих специально подобранные спектры и следующих друг за другом с секундным интервалом. Предлагается установить, равны ли они по громкости. Для тех случаев, когда громкости оказываются одинаковыми, звуки меняют местами и снова предъявляют испытуемому. Оказывается, что теперь первый звук слышится громче, чем второй.

Описанный эффект, однако, легко объясняется маскирующим действием первого звука на второй, снижающим слышимую громкость последнего. Стало быть, здесь мы имеем неконтролируемый побочный фактор, нарушающий условие повторяемости. Громкость одного и того же физического звука меняется в зависимости от наличия или отсутствия предшествующего звука. К закону симметричности это не имеет никакого отношения.

Переходим к психологической интерпретации закона рефлексивности. В содержательной формулировке закон рефлексивности гласит: равные понятия должны восприниматься испытуемым как равные. Иными словами, на равные понятия испытуемый всегда должен реагировать положительным ответом. В такой формулировке закон рефлексивности выглядит как довольно бессодержательное утверждение. Действительно, если с самого начала два понятия принимаются равными, то как они после этого могут оказаться неравными? И все же, в законе рефлексивности содержится нечто такое, что требует экспериментального подтверждения. Дело в том, что понятия фактически могут быть равными, однако испытуемый недоброкачественно их проанализирует и в результате вместо положительного выработает отрицательный ответ.

Закон рефлексивности, по существу, представляет собой требование корректности проведения эксперимента: при выработке двоичного ответа, сигнализирующего о равенстве или неравенстве понятий, испытуемый не должен ошибиться. При фактическом равенстве понятий он обязан отреагировать положительным ответом. Ясно, что из-за невнимательности или по злому умыслу испытуемый это требование вполне может нарушить. Отметим, что закон рефлексивности весьма близок к закону тождества, который рассматривается в курсах формальной логики. Закон тождества требует, чтобы в процессе рассуждения все понятия оставались равными самим себе, нельзя производить подмены понятий. Закон тождества в формальной логике расценивается как одно из важнейших требований, без выполнения которого интеллектуальная деятельность человека становится невозможной.

Рассмотрим, далее, психологическую интерпретацию закона транзитивности. В содержательной формулировке закон транзитивности гласит: если для некоторого испытуемого понятие x равно понятию y, а понятие y равно понятию z, то понятие x тем же испытуемым должно восприниматься как равное понятию z. В применении к смыслам фраз закон транзитивности выполняется на практике безупречно. Когда люди замечают, что кто-то из них нарушает закон транзитивности, то это неизменно квалифицируется ими как сбой в мыслительной деятельности. В практике математических доказательств встречаются длинные ряды равносильных друг другу высказываний, и при этом всегда оказывается, что первое высказывание в ряду равносильно последнему. Если же это не так, то всегда может быть обнаружена ошибка в доказательстве.

Несколько сложнее обстоит дело с выполнением закона транзитивности в случае с ощущениями. Известен следующий опыт, который обычно приводится для опровержения закона транзитивности.

Испытуемому предъявляется световое излучение красного цвета определенной мощности. К красному цвету предлагается подравнять по видимой яркости (светлоте) оранжевый цвет путем регулирования мощности вызывающего его светового излучения. Далее, к оранжевому цвету подравнивается по светлоте желтый цвет, а затем то же самое проделывается с салатным, зеленым, лазурным, голубым, синим, фиолетовым и сиреневым цветами. Наконец, к сиреневому цвету подравнивается по светлоте исходный красный цвет. В итоге оказывается, что мощность исходного светового излучения, как правило, не совпадает с мощностью излучения, полученного в конце процесса подравнивания.

Опровергает ли этот опыт закон транзитивности? Мы полагаем, что нет. Если описанный опыт выполнить многократно с одними и теми же цветами и одной и той же исходной мощностью излучения, то результирующая мощность светового излучения не получается в разных опытах одной и той же, но меняется случайным образом от опыта к опыту. При этом она колеблется вокруг первоначальной мощности излучения, то приближаясь к ней, то удаляясь от нее в сторону увеличения или уменьшения. И чем больше опытов проведено, тем более среднее значение результирующей мощности, вычисленное по всем опытам, будет приближаться к исходной мощности светового излучения. Этот факт можно истолковать таким образом, что светлота световых излучений, предъявляемых испытуемому, не остается стабильной и испытывает небольшие случайные колебания. При движении по длинному ряду цветов эти колебания светлоты накапливаются (опять-таки случайным образом), и в результате появляется заметное различие начальной и конечной светлот. Так что в этом и в любых других подобных опытах нарушается не закон транзитивности, а условие повторяемости.

Переходим к психологической интерпретации закона подстановочности. В содержательной формулировке закон подстановочности гласит: если какое-нибудь понятие x для некоторого испытуемого обладает свойством R_k, то тем же свойством для этого испытуемого будет обладать и любое понятие y, равное понятию x. Рассмотрим пример, иллюстрирующий содержание закона подстановочности. Предикат $R_k(x)$ задаем условием «Из высказывания x логически следует высказывание «Идет дождь»». В роли x берем смысл высказывания «Идет дождь, и светит солнце», в роли y - смысл высказывания «Светит солнце, и идет дождь». Последние два высказывания логически равносильны, так что $x = y$. Производя подстановку в исходное условие вместо x высказывания «Идет дождь, и светит солнце», получаем тавтологию «Из высказывания «Идет дождь, и светит солнце» логически следует высказывание «Идет дождь»», при этом $R_k(x) = 1$. Заменяя в исходном условии x на y и подставляя вместо y высказывание «Светит солнце, и идет дождь», получаем высказывание «Из высказывания «Светит солнце, и идет дождь» логически следует высказывание «Идет дождь»». В строгом соответствии с требованием закона подстановочности оно также является тавтологией, при этом $R_k(x) = 1$.

Как в повседневной речи, так и особенно в математике люди постоянно пользуются законом подстановочности, и нет никаких свидетельств, чтобы это приводило к каким-либо сбоям в мышлении. Отметим, что закон подстановочности родственен правилу подстановки, которое рассматривается в курсах исчисления высказываний. Это правило формулируют следующим образом: «Пусть A - формула, содержащая букву A. Тогда, если A - истинная формула в исчислении высказываний, то, заменяя в ней букву A всюду, где она входит, произвольной формулой B, мы также получим истинную формулу».

Множество S_k можно образовать только из имен понятий. Но одно и то же понятие можно представить в виде различных по виду, но тождественных по смыслу высказываний. Таким образом, в зависимости от выбора способа обозначения одних и тех же понятий, мы приходим к тому или иному множеству высказываний. Поэтому и предикаты равенства понятий получаются разными. Более точно можно сказать, что предикат равенства понятий задается единственным образом с точностью до обозначений или изоморфизма. Изоморфизм моделей $\langle S'_k, D'_k \rangle$ и $\langle S''_k, D''_k \rangle$ означает, что существует биекция

$$\Omega : S'_k \to S''_k,$$

для которой предикат D'_k совпадет с предикатом D''_k.

3. Операции над понятиями

Для дальнейшего развития алгебры понятий необходимо ввести достаточный набор операций над понятиями. Для экспериментальной работы с испытуемым и формализации его понятий введем операции отрицания, конъюнкции, дизъюнкции и следования.

Операции практически реализуются соответствующими предикатами.

Операцию отрицания понятий зададим с помощью бинарного предиката $\text{ОТР}(x, y)$, определенного на множестве $S_k \times S_k$. Его значения определяются правилом:

$$\text{ОТР}(x,y)=\begin{cases}1, \text{ если } y=\overline{x},\\ 0, \text{ если } y\neq\overline{x}.\end{cases}$$

Операцию конъюнкции понятий вводим с помощью тернарного предиката $\text{КОН}(x,y,z)$, определенного на множестве $S_k\times S_k\times S_k$.

Его значения определяются правилом:

$$\text{КОН}(x,y,z)=\begin{cases}1, \text{ если } z=x\wedge y,\\ 0, \text{ если } z\neq x\wedge y.\end{cases}$$

Операцию дизъюнкции понятий задаем с помощью тернарного предиката $\text{ДИЗ}(x,y,z)$, определенного на множестве $S_k\times S_k\times S_k$. Его значения определяются правилом:

$$\text{ДИЗ}(x,y,z)=\begin{cases}1, \text{ если } z=x\vee y,\\ 0, \text{ если } z\neq x\vee y.\end{cases}$$

Говоря о переменных, мы обязаны ввести их области определения. Т.е. существуют конечный универсум переменных $B=\{x_1,x_2,..,x_n\}$ и конечный универсум букв $A=\{a_1,a_2,...a_k\}$, на котором заданы переменные из B. Предполагается, что множества A и B настолько обширны и неопределенны, что в них содержатся все нужные нам буквы и переменные. Поэтому при практическом задании конкретных моделей множества A и B остаются как бы за кадром, они присутствуют лишь потенциально.

Именно благодаря их существованию мы можем ввести буквы $a_1,a_2,...\in A$ и переменные $x_1,x_2,...\in B$ и оперировать ими.

Под буквами множества A будем понимать понятия, которые могут быть предъявлены исследователем испытуемому в процессе изучения закономерностей его интеллектуальной деятельности. Будем предполагать, что число k понятий, содержащихся в множестве A, достаточно велико, а их состав достаточно разнообразен.

Сказанное означает, что каждый исследователь, вне зависимости от степени обширности и сложности решаемых им задач, всегда найдет в множестве A любые понятия, нужные ему для работы с испытуемым. Напомним, что под понятиями понимаются лишь субъективные состояния испытуемого, в роли которых могут выступать ощущения, восприятия, представления, мысли, эмоции, намерения.

Кроме того, нуждается в пояснении запись предиката D в виде $D(x_1,y_2)$, где указаны только две переменные x_1,x_2, а не все те переменные $x_1,x_2,..,x_n$, которые содержатся в универсуме B.

Запись $D(x_1,y_2)$, в отличие от записи $D(x_1,x_2,..,x_n)$, не полная, а сокращенная, в ней несущественные переменные не указаны. Несущественными будем считать те из переменных $x_1,x_2,..,x_n$, от значений которых значение предиката $D(x_1,x_2,..,x_n)$ не зависит.

Необходимость такой записи определяется невозможностью перечислить все переменные $x_1,x_2,..,x_n$.

Выводы

В работе развивается формальный аппарат для описания закономерностей интеллектуальной деятельности человека - алгебра понятий. Это абстрактный эквивалент алгебры конечных предикатов.

Основной инструмент метода сравнения в алгебре понятий для изучения интеллекта человека - предикат равенства понятий.

В работе проанализированы свойства предиката равенства понятий и особенности их применения для формализации понятий.

Список литературы

1. Лещинский В.А. О теоремах исчисления высказываний / В.А. Лещинский // Системи обробки інформації. — 2016. — № 9. — С. 97-100.

2. Лещинский В.А. О формульном описании переменных сложных высказываний / В.А. Лещинский, И.А. Лещинская // Збірник наукових праць Харківського національного університету Повітряних Сил. — 2016. — № 3. — С. 92-95.

Надійшла до редколегії 26.12.2016

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет імені М.Є. Жуковського «ХАІ», Харків.

О СВОЙСТВАХ ПРЕДИКАТА РАВЕНСТВА ПОНЯТИЙ

І.О. Лещинська

У роботі розвивається алгебра понять. Знайдені і доведені властивості предиката рівності понять. Ці властивості проаналізовані з точки зору практичного застосування для ідентифікації інтелектуальної діяльності людини.

Ключові слова: *алгебра скінченних предикатів, алгебра понять, інтелект, висловлювання.*

О СВОЙСТВАХ ПРЕДИКАТА РАВЕНСТВА ПОНЯТИЙ

I.O. Leshchynska

Algebra of concepts develops in-process. The properties of concepts equality predicate are found and well-proven. These properties are analyzed from the point of view of practical application for authentication of intellectual activity of man.

Keywords: *finite predicates algebra, algebra of concepts, intellect, utterance.*

УДК 510.635

В.А. Лещинский

Харьковский национальный университет радиоэлектроники, Харьков

О МОДЕЛИ РАВЕНСТВА ПОНЯТИЙ

В работе вводится абстрактный эквивалент алгебры конечных предикатов - алгебра понятий. С помощью алгебры понятий формально описываются закономерности интеллектуальной деятельности человека.

Ключевые слова: *алгебра конечных предикатов, алгебра понятий, интеллект, высказывание.*

Введение

В публикации [1] была разработана алгебра конечных предикатов (АКП), предназначенная для целей математического описания интеллектуальной деятельности человека и ее закономерностей. В процессе развития формального описания закономерностей интеллектуальной деятельности на языке АКП было обнаружено, что кроме этой алгебры, для теории интеллекта необходим еще и некий абстрактный эквивалент этой алгебры, названный алгеброй понятий.

Выбор такого названия обусловлен тем, что элементы множества – носителя алгебры понятий, как будет показано ниже, естественным образом интерпретируется как понятия интеллекта, вообще – как любые субъективные состояния человека, а операции алгебры понятий над этими элементами – как действия интеллекта над понятиями.

1. Формальное представление понятий

Развивая алгебру понятий, одновременно с этим будем формально описывать закономерности интеллектуальной деятельности человека [2]. Это будет достигаться посредством психологической интерпретации законов алгебры понятий. Правомерность такой интерпретации будет обосновываться в каждом конкретном случае путем экспериментального изучения соответствующих свойств поведения испытуемого. Под испытуемым мы подразумеваем того конкретного человека, интеллектуальная деятельность которого подвергается формализации. В этой работе вводится носитель алгебры понятий. С содержательной точки зрения он представляет собой множество всех понятий испытуемого с заданным на нем предикатом равенства.

В роли прототипа алгебры понятий примем частный случай АКП - алгебру одноместных k-ичных предикатов первого порядка [1]. Дело в том, что при переходе от конкретной алгебры к ее абстрактному эквиваленту частное и общее меняются местами. Поэтому наиболее частный вариант АКП порождает алгебру понятий самого общего вида.

Рассмотрим, к примеру, троичные предикаты $(k=3)$, заданные на множестве $A_3=\{a, b, c\}$. Всевозможные такие предикаты $P_0 \div P_7$ представлены в табл. 1. Всего имеется $N_0(3)=2^3=8$ троичных предикатов. Если читать снизу вверх колонку логических констант, соответствующую в табл. 1 предикату $P_i (i\in\{0, 1, 2,..., 7\})$, интерпретируя логические константы как двоичные цифры, то каждому предикату можно поставить в соответствие некоторый двоичный код. Число i, соответствующее этому коду, принимаем в качестве *номера предиката* P_i. Например, предикату P_3 соответствует код 001, представляющий собой число 3. В данном случае в роли множества всех предикатов выступает множество $M_3=\{P_0, P_1,..., P_7\}$.

Таблица 1

Троичные предикаты

x	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7
a	0	1	0	1	0	1	0	1
b	0	0	1	1	0	0	1	1
c	0	0	0	0	1	1	1	1

Введем биекцию $\Phi: S_k \to M_k$, устанавливающую взаимно однозначное соответствие между всеми понятиями размерности k и всеми одноместными k-ичными предикатами первого порядка, заданными на множестве A_k. Биекцию Φ можно выбрать многими способами. Всего существует $2^k!$ различных вариантов выбора биекций Φ, заданных на множестве S_k, что соответствует числу всех перестановок из 2^k различных элементов. Например, при $k=3$ существует $2^3!=40320$ различных вариантов выбора биекции Φ. Предикат $P=\Phi(x)$ будем называть предикатом, соответствующим понятию x, а понятие $x=\Phi^{-1}(P)$ - понятием, соответствующим предикату P.

Под элементами множества S_k будем понимать понятия какого-нибудь конкретного человека, которого в дальнейшем будем именовать испытуе-

мым. Человека, изучающего интеллектуальную деятельность испытуемого, будем называть исследователем. Проводя опыты, исследователь по своему желанию формирует в уме испытуемого ту или иную мысль. Это невозможно сделать непосредственно, поэтому испытуемому для восприятия предъявляется специально подобранный физический сигнал, выполняющий роль имени понятия. Мысль, порождаемую каким-либо именем, будем называть смыслом этого имени.

Мысли от одного человека к другому передается с помощью высказываний. Любое высказывание имеет вид повествовательного предложения или последовательности повествовательных предложений – текста. Мысль, заключенную в том или ином высказывании, будем называть смыслом высказывания. Высказывание выполняет роль имени мысли. Именем мысли может быть не только высказывание, но и любой другой физический сигнал. Например, красный свет семафора передает машинисту электровоза мысль «Путь закрыт». И, тем не менее, высказывания как средства передачи мыслей в некотором смысле незаменимы: человек не сможет понять смысл неречевого сигнала до тех пор, пока ему не объяснят его с помощью высказываний. Так, машинист электровоза должен быть предварительно обучен тому, что красный свет семафора означает запрещение проезда. Если этого не сделать, то красный свет семафора не будет возбуждать в уме машиниста нужной мысли. Как средство передачи мыслей высказывания универсальны. Любую мысль каждый психически здоровый человек может сформулировать в виде высказывания. Если человек этого сделать не может, то у окружающих его лиц может возникнуть убеждение, что данной мысли у него попросту нет. Высказываний больше, чем мыслей. Одну и ту же мысль можно выразить различными высказываниями. Высказывания, выражающие одну и ту же мысль, будем называть тождественными.

Не каждое повествовательное предложение может быть высказыванием. Например, фраза, написанная на непонятном для испытуемого языке, не несет ему никакой мысли. Чтобы повествовательное предложение могло возбудить в уме испытуемого какую-то мысль, оно должно быть им понято. Одно и то же предложение для одного испытуемого может быть понятным, а для другого непонятным. Предложение может оказаться непонятным, даже будучи записанным или произнесенным на языке, которым владеет испытуемый. Это может случиться, если предложение имеет неправильную грамматическую структуру или в нем встречаются непонятные для испытуемого слова. Текст, взятый из руководства по незнакомой области знаний, будет испытуемому непонятен. Но после того, как испытуемый освоит эту область знаний, тот же самый текст станет ему понятным. Таким образом, вопрос о том, признать ли данную фразу высказыванием или нет, решается только применительно к конкретному испытуемому, причем на находящемуся на вполне определенной стадии своего развития. Вместе с тем, можно говорить, что данное предложение является высказыванием относительно целой группы лиц, но только в том случае, если все они понимают смысл этого предложения, причем одинаково.

У исследователя нет прямого способа удостовериться в том, что мысль испытуемого совпадает с его собственной мыслью. Это обстоятельство может послужить причиной неправильного понимания исследователя испытуемым. Предъявляя фразу, исследователь рассчитывает, что она возбудит в уме испытуемого именно ту мысль, которую он в нее вложил. Но испытуемый может расшифровать фразу как совершенно иную мысль или мысль, не вполне совпадающую с той, которую имел ввиду исследователь. О том, что такое возможно, свидетельствует постоянно встречающиеся в жизни случаи неточной передачи мыслей от человека к человеку и проистекающие от этого недоразумения. Одна и та же фраза, в зависимости от меняющихся побочных обстоятельств, может быть воспринята испытуемым поразному. Так, цитата, вырванная из контекста и вставленная в другой текст, зачастую приобретает совершенно иной смысл. Это явление может нарушить стабильность формирования исследователем мыслей в уме испытуемого.

Проводя эксперименты на испытуемом, исследователь обязан позаботиться о том, чтобы возбуждаемые в уме испытуемого мысли всегда однозначно определялись предъявленным ему высказываниями. Смысл имени всегда должен однозначно соответствовать имени. Выполнение этого требования, назовем его условием повторяемости, совершенно обязательно для доброкачественности опытов. Эксперимент не пострадает, если исследователь вызовет в уме испытуемого не ту мысль, которую намеревался получить, лишь бы повторное предъявление высказывания порождало в сознании испытуемого ту же самую мысль. Но опыт не удастся, если при его проведении не будет обеспечена повторяемость при формировании мыслей, т.е. если при различных предъявленьях одного и того же высказывания в сознании испытуемого будут возникать различные мысли. Требование повторяемости предъявляется не только к описываемым здесь психофизическим экспериментам, его выполнение необходимо также и в любом грамотном физическом эксперименте. Если условие повторяемости в экспериментах нарушается, то мысли, предъявляемые испытуемому, становятся неконтролируемыми, а результаты опытов – неопределенными.

Для борьбы с нестабильностью мыслей исследователь должен тщательно учитывать все обстоятельства, сопутствующие высказываниям в момент их предъявления испытуемому, и выяснить те из них, которые приводят к искажению мыслей. Помощь исследователю в этом деле может оказать сам испытуемый, указывая случаи изменения смысла высказывания при появлении того или иного обстоятельства. Например, испытуемый легко обнаруживает изменение смысла фразы, вызванное сменой контекста, сопутствующего этой фразе. Факторы, влияющие на смысл высказывания, должны исключаться из условий опыта или же стабилизироваться. Так, например, фразу можно предъявить, не связывая ее ни с каким контекстом. Если же это по каким-либо причинам неприемлемо, то каждое предъявление данной фразы следует сопровождать одним и тем же контекстом. Стабилизируемые в опыте обстоятельства необходимо включать в характеристику высказывания, которому эти обстоятельства сопутствуют.

Рассмотрим предикат равенства $D_k(P,Q)$, определенный на $M_k \times M_k$. Его можно представить в виде [1]:

$$D_k(P,\ Q)=\forall x(P(x)\sim Q(x)), \qquad (1)$$

справедливым для $\forall P,Q\in M_k$. Здесь выражение $\forall x$ означает квантор общности, который берется по переменной $x\in A_k$. Символ $\sim$ обозначает операцию эквивалентности логических констант. Предикат D_k ставит в соответствие равным предикатам P и Q логическую константу 1, не равным – 0.

В табл. 2 в виде примера приведен предикат равенства предикатов $D_3(P,\ Q)$, заданный на декартовом квадрате множества $M_3=\{P_0,P_1,...,P_7\}$ всех троичных одноместных предикатов первого порядка. Под символами 0 и 1 понимаются логические константы. Для примера табл. 3 и 4 заданы предикаты равенства понятий D'_3 и D''_3 и биекций Φ' и Φ''. Предикат $D'_3(x',y')$ определен на множестве $S'_3\times S'_3$, а предикат $D''_3(x'',y'')$ - на множестве $S''_3\times S''_3$.

Таблица 2

Предикат равенства предикатов $D_3(P,\ Q)$

P	Q_0	Q_1	Q_2	Q_3	Q_4	Q_5	Q_6	Q_7
P_0	1	0	0	0	0	0	0	0
P_1	0	1	0	0	0	0	0	0
P_2	0	0	1	0	0	0	0	0
P_3	0	0	0	1	0	0	0	0
P_4	0	0	0	0	1	0	0	0
P_5	0	0	0	0	0	1	0	0
P_6	0	0	0	0	0	0	1	0
P_7	0	0	0	0	0	0	0	1

Таблица 3

Предикат равенства понятий D'_3 и биекций Φ'

x'	s'_0	s'_1	s'_2	s'_3	s'_4	s'_5	s'_6	s'_7
s'_0	1	0	0	0	0	0	0	0
s'_1	0	1	0	0	0	0	0	0
s'_2	0	0	1	0	0	0	0	0
s'_3	0	0	0	1	0	0	0	0
s'_4	0	0	0	0	1	0	0	0
s'_5	0	0	0	0	0	1	0	0
s'_6	0	0	0	0	0	0	1	0
s'_7	0	0	0	0	0	0	0	1

Отношение равенства $x=y$ понятий x и y определяем следующим образом: $x=y$ в том и только в том случае, если $\Phi(x)=\Phi(y)$. Можно сказать иначе: отношение $x=y$ задается уравнением $D_k(x,y)=1$. Отношение неравенства понятий $x\neq y$ имеет место в том и только в том случае, когда $\Phi(x)\neq\Phi(y)$. Иными словами, отношение $x\neq y$ задается уравнением $D_k(x,y)=0$.

Таким образом, для $\forall x,y\in S_k$ можно записать:

$$D_k(x,y)=\begin{cases}0, & \text{если } \Phi(x)\neq\Phi(y),\\ 1, & \text{если } \Phi(x)=\Phi(y).\end{cases} \qquad (2)$$

Таблица 4

Предикат равенства понятий D''_3 и биекций Φ''

x''	s''_0	s''_1	s''_2	s''_3	s''_4	s''_5	s''_6	s''_7
s''_0	1	0	0	0	0	0	0	0
s''_1	0	1	0	0	0	0	0	0
s''_2	0	0	1	0	0	0	0	0
s''_3	0	0	0	1	0	0	0	0
s''_4	0	0	0	0	1	0	0	0
s''_5	0	0	0	0	0	1	0	0
s''_6	0	0	0	0	0	0	1	0
s''_7	0	0	0	0	0	0	0	1

Предикатам D'_3 и D''_3, рассмотренным в ранее приведенном примере, соответствуют разные отношения равенства понятий:

$$\{(s'_0,s'_0),\ (s'_1,s'_1),...,\ (s'_7,s'_7)\},$$

$$\{(s''_0,s''_0),\ (s''_1,s''_1),...,\ (s''_7,s''_7)\},$$

поскольку эти предикаты заданы на различных множествах $S'_k\times S'_k$ и $S''_k\times S''_k$.

В рассмотренном выше примере предикат D'_3 переводится в предикат D''_3 при помощи биекции Ω, указанной в табл. 4. Биекция Ω выражается через биекции Φ' и Φ'', введенные ранее, следующим образом: $\Omega(x)=\Phi''^{-1}(\Phi'(x))$.

Встречаются случаи, когда два высказывания с точки зрения исследователя являются логически равносильными, а испытуемый не может установить равенство мыслей, предъявленных этими высказываниями. Так, для испытуемого может быть непосредственно неочевидной логическая равносильность двух достаточно сложных математических утверждений. Неочевидность равенства мыслей может сохраниться даже после того, как испытуемый изучил доказательство логической равносильности соответствующих высказываний.

Итак, наличие доказательства равносильности двух высказываний еще не означает равенства соответствующих мыслей для данного испытуемого. Заключение о равенстве мыслей в конечном счете основывается на ясном и непосредственном свидетельстве сознания испытуемого, удостоверяющего идентичность двух мыслей. Доказательство логической равносильности соответствующих высказываний, конечно, необходимы, но оно может оказаться недостаточным, если испытуемый не способен его осмыслить и усвоить в совершенстве. Математик, владеющий своим предметом, непосредственно, без каких бы то ни было доказательств, «чувствует» логическую равносильность даже самых сложных из относящихся к его компетенции математических утверждений.

Неспособность испытуемого установить идентичность равных (с точки зрения исследователя) мыслей свидетельствует не о неравенстве мыслей, а лишь о том, что эти мысли (по крайней мере, одна из них) не сформировались в его уме достаточно ясно и четко. Иными словами, испытуемый в полной мере не владеет этими понятиями.

Выводы

В заключение обсудим ту роль, которую играет предикат равенства понятий в механизме интеллекта. Роль эта нам представляется фундаментальной и весьма значительной. Тот факт, что человек может удостовериться в равенстве каких-либо двух понятий, означает, что он имеет доступ к мельчайшим деталям этих понятий, способен сравнивать эти детали друг с другом и устанавливать их идентичность.

Таким образом, эффективное действие предиката равенства предполагает полный анализ структуры понятий.

Никакие другие операции над понятиями, сколь бы сложными они ни были, не смогут проникнуть в структуру понятий глубже, чем это способен сделать предикат равенства понятий.

Возможность сравнивать между собой все понятия человека и устанавливать их равенство и неравенство лежит в основании механизма, обеспечивающего единство человеческой личности, единство того, что называют нашим «Я». Представим, что множество всех понятий какой-то личности распалось на две не связанные друг с другом части, и теперь независимо на каждой из них действует свой собственный, предикат равенства. Ясно, что единство этих двух частей нарушится и произойдет то, что в психиатрии называют расщеплением или раздвоением личности. Две различные человеческие личности разделены психологическим барьером именно вследствие того, что каждая из них имеет непосредственный доступ только к своим собственным субъективным состояниям, их понятия не объединяет единый предикат равенства. Допустим, что такой, общий для двух личностей, предикат равенства понятий каким-то образом удалось практически ввести. Наличие такого предиката явилось бы предпосылкой к слиянию двух личностей в одну.

Можно ожидать, что единая в двух телах личность смотрела бы на мир «в четыре глаза», имела бы единую волю и общие мысли.

Список литературы

1. Бондаренко М.Ф. Теория интеллекта. Учебник / М.Ф. Бондаренко, Ю.П. Шабанов-Кушнаренко. – Харьков: СМИТ, 2007 – 576 с.

2. Гильберт Д., Основания математики. Логические исчисления и формализация арифметики / Д. Гильберт, П. Бернайс . – М.: Наука, 1979. – 557 с.

Надійшла до редколегії 26.12.2016

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет імені М.Є. Жуковського «ХАІ», Харків.

ПРО МОДЕЛЬ РІВНОСТІ ПОНЯТЬ

В.О. Лещинський

У роботі вводиться абстрактний еквівалент алгебри скінченних предикатів – алгебра понять. За допомогою алгебри понять формально описуються закономірності інтелектуальної діяльності людини.

Ключові слова: *алгебра скінченних предикатів, алгебра понять, інтелект, висловлювання.*

ABOUT CONCEPTS EQUALITY MODEL

V.O. Leshchynskyi

The abstract equivalent of finite predicates algebra - algebra of concepts is in-process entered. By means of concepts algebra conformities to law of intellectual activity of man are formally described.

Keywords: *finite predicates algebra, algebra of concepts, intellect, utterance.*

УДК 529.85

Л.Г. Раскин, В.В. Карпенко

Национальный технический университет «ХПИ», Харьков

НЕЧЕТКАЯ ЗАДАЧА МАРШРУТИЗАЦИИ

Рассмотрена задача маршрутизации высокой размерности в условиях, когда исходные данные заданы нечетко. Предложен декомпозиционный алгоритм решения задачи, использующий кластеризацию исходного множества пунктов. Основой алгоритма является технология сравнения нечетких чисел с целью выбора минимального из них, обеспечивающая возможность кластеризации. Проведен анализ двух альтернативных методов сравнения. Приведен пример.

Ключевые слова: *маршрутизация, задача коммивояжера высокой размерности, декомпозиция, нечеткие исходные данные.*

Введение

Задача маршрутизации входит в широкий класс проблем логистики и состоит в отыскании маршрута, соединяющего два заданных пункта с учетом имеющихся магистралей. Традиционные критерии для выбора наилучшего маршрута: длина пути или затраты (временные, стоимости и т.п.) на его преодоление. Частный случай этой задачи возникает, если маршрут обязательно должен проходить через заданное множество пунктов. Такая задача носит специальное название – задача коммивояжера [1, 2]. Трудности решения этой задачи зависят от её размерности, а также от уровня качества исходной информации. Приведем краткий анализ известных методов решения задачи коммивояжера.

Анализ литературных данных

Функциональная постановка задачи коммивояжера имеет вид [1, 2]: найти булеву матрицу $X = (x_{ij}),$ доставляющую минимум линейной форме

$$L(X) = \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}x_{ij},,$$

компоненты которой удовлетворяют ограничениям:

$$\sum_{i=1}^{n} x_{ij} = 1,\ \ j = \overline{1,n};\quad \sum_{j=1}^{n} x_{ij} = b_j,\ \ i = \overline{1,n};$$

$$u_i - u_j + nx_{ij} \le n-1,\quad i = \overline{1,n},\ j = \overline{1,n},$$

где n – число пунктов, c_{ij} – расстояние между пунктами $(i, j),$; x_{ij} – булев индикатор, равный единице, если в маршруте имеется звено, соединяющее непосредственно пункты $(i, j),$ и равный нулю в противном случае. Выполнение ограничений обеспечивает получение замкнутого маршрута без петель [3].

Эта задача принадлежит к классу трудных комбинаторных, так называемых NP-полных задач. Эффективность известных алгоритмы её решения невелика – решение может быть получено только для задач сравнительно небольшой размерности ($n > 20$). Однако, на практике возникает необходимость решения этой задачи существенно более высокой размерности. Эффективное решение задачи возможно с использованием генетического алгоритма (ГА) [4, 6]. Результаты экспериментального решения задачи коммивояжера различной размерности этим алгоритмом представлены в табл. 1 [7].

Таблица 1

Зависимость времени поиска кратчайшего маршрута (в условных единицах) от количества пунктов при использовании ГА

Количество пунктов	10	18	26	34	42
Время решения	1	8	23	50	90

Количество пунктов	50	58	66	74	80
Время решения	195	285	401	597	780

Для аналитического описания этой зависимости в [7] введена модель

$$T(n) = an^b. \qquad (1)$$

Параметры модели найдены методом наименьших квадратов.

После логарифмирования (1):

$$\ln T(n) = \ln a + b\ln n\,.$$

С использованием обозначений $y = \ln T(n),$ $b_0 = \ln a,$ $b_1 = b,$ $x = \ln n$ получено линейное относительно параметров b_0 и b_1 уравнение регрессии $y = b_0 + b_1 x.$ Далее, для m вариантов исходных данных имеем

$$H = \begin{pmatrix} 1 & \ln n_1 \\ 1 & \ln n_2 \\ \dots & \dots \\ 1 & \ln n_m \end{pmatrix},\quad B = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix},\quad Y = \begin{pmatrix} \ln T(n_1) \\ \ln T(n_2) \\ \dots \\ \ln T(n_m) \end{pmatrix}.$$

При этом функционал наименьших квадратов имеет вид $I=(AB-Y)^T(AB-Y)$, а минимизирующий этот функционал вектор $\hat{B}$ определяется соотношением

$$\hat{B}=\left(H^TH\right)^{-1}H^TY=\begin{pmatrix}\hat{b}_0\\ \hat{b}_1\end{pmatrix},\ a=e^{\hat{b}_0},\ b=\hat{b}_1.$$

После выполнения расчетов по данным из табл. 1 получена искомая зависимость: $T=0,0009n^{3,1332}$.

Таким образом, генетический алгоритм решения задачи коммивояжера существенно более эффективен, нежели любой другой известный алгоритм решения *NP*-полных задач. Предельная размерность задачи для этого алгоритма составляет 80-100 пунктов назначения [7]. Однако, решение этой задачи возможно получить приближенно даже для случая существенно более высокой размерности с использованием декомпозиции [8].

Предлагаемая при этом технология решения задачи коммивояжера является четырехэтапной. На первом этапе все множество пунктов обхода с использованием какого-либо алгоритма кластеризации разделяется на совокупность кластеров. Для каждого кластера отыскиваются координаты центров тяжести. На втором этапе для этих точек строится кратчайший маршрут их обхода. На следующем этапе для каждой пары "соседних" кластеров отыскивается пункт выхода из предыдущего кластера и пункт входа в последующий. Наконец, на последнем этапе решается последовательность задач коммивояжера для каждого из кластеров с учетом полученных на предыдущем этапе начального и конечного пунктов. В результате будет получена последовательность маршрутов, объединение которых образует искомый маршрут.

Применение декомпозиционной процедуры существенно снижает размерность решаемых на этапе 2 и 4 частных задач по сравнению с исходной. Это обстоятельство расширяет возможности генетического алгоритма для решения задачи коммивояжера до 500-600 пунктов.

Реализация описанной технологии существенно усложняется, если исходные данные (расстояния между пунктами) заданы нечетко. Сформулируем задачи, порождаемые этой особенностью исходных данных.

Постановка задачи

Важнейшим конструктивным элементом процедуры кластеризации является сравнение расстояний между точками, соответствующими объектам кластеризации и центрами группирования [9]. Расчет расстояний усложняется, если они заданы нечетко своими функциями принадлежности. Известны различные способы сравнения нечетких чисел с целью выбора минимального из них [10]. Общий недостаток – сложность программной реализации, которая быстро растет с увеличением размерности задачи. В связи с этим поставим задачу построения простых, но достаточно эффективных приемов решения задачи сравнения нечетких чисел.

Основные результаты

Пусть два нечетких числа x_1 и x_2 заданы, например, треугольными функциями принадлежности.

$$M_1(x_1)=\begin{cases}0, & x_1<a_1,\\ \dfrac{x_1-a_1}{c_1-a_1}, & a_1\le x_1<c_1,\\ \dfrac{b_1-x_1}{b_1-c_1}, & c_1\le x_1<b_1,\\ 0, & x_1\ge b_1,\end{cases}$$

$$M_2(x_2)=\begin{cases}0, & x_2<a_2,\\ \dfrac{x_2-a_2}{c_2-a_2}, & a_2\le x_2<c_2,\\ \dfrac{b_2-x_2}{b_2-c_2}, & c_2\le x_2<b_2,\\ 0, & x_2\ge b_2.\end{cases}\qquad(2)$$

Зададим набор уровней принадлежности $\alpha_1,\alpha_2,...,\alpha_m$. Рассчитаем значения нечетких переменных x_1 и x_2 соответствующие выбранным уровням принадлежности. С этой целью решим уравнения:

$$M_1(x_1)=\alpha_k,\quad M_2(x_2)=\alpha_k,\quad k=1,2,...,m.$$

Имеем

$$\frac{x_1-a_1}{c_1-a_1}=\alpha_k,\quad x_{1k}^{(1)}=a_1+\alpha_k(c_1-a_1),$$

$$\frac{b_1-x_1}{b_1-c_1}=\alpha_k,\quad x_{1k}^{(2)}=b_1-\alpha_k(b_1-c_1),$$

$$\frac{x_2-a_2}{c_2-a_2}=\alpha_k,\quad x_{2k}^{(1)}=a_2+\alpha_k(c_2-a_2),$$

$$\frac{b_2-x_2}{b_2-c_2}=\alpha_k,\quad x_{2k}^{(2)}=b_2-\alpha_k(b_2-c_2).$$

Далее определим значения середин отрезков:

$$[x_{1k}^{(1)},x_{1k}^{(2)}],\ [x_{2k}^{(1)},x_{2k}^{(2)}],\ k=1,2,...,m.$$

Получим

$$\bar{x}_{1k}=\frac{1}{2}\left(x_{1k}^{(1)}+x_{1k}^{(2)}\right)=\frac{a_1+b_1}{2}+\frac{\alpha_k}{2}\left(-a_1-b_1+2c_1\right),$$

$$\bar{x}_{2k}=\frac{1}{2}\left(x_{2k}^{(1)}+x_{2k}^{(2)}\right)=\frac{a_2+b_2}{2}+\frac{\alpha_k}{2}\left(-a_2-b_2+2c_2\right).$$

Теперь уровень предпочтения нечеткого числа x_2 перед нечетким числом x_1 можно определить значением критерия

$$\eta = \sum_{k=1}^{m} \alpha_k (\overline{x}_{2k} - \overline{x}_{1k}). \quad (3)$$

Естественно считать, что число x_2 "больше" числа x_1 если $\eta > 0$, и "меньше" – в противном случае. Понятно, что уровень достоверности получаемого при этом вывода зависит от того, на каких уровнях выбраны сечения $\alpha_k, k = 1,...,m$, и каково их число. Более точным является результат сравнения нечетких чисел, получаемый путем построения теоретико-вероятностных аналогов функций принадлежности нечетких чисел [7]. Для функции принадлежности нечеткого числа $M(x)$ введем функцию

$$\phi(x) = M(x) \Big/ \int_{-\infty}^{\infty} M(x)dx. \quad (4)$$

Понятно, что определенная таким образом неотрицательная функция $\phi(x)$ обладает всеми свойствами плотности распределения случайно величины. Теперь для функций принадлежности $M_1(x_1)$ и $M_2(x_2)$ введем, используя (4), функции

$$\phi_1(x_1) = \frac{M_1(x_1)}{\int_{-\infty}^{\infty} M_1(x_1)dx}, \quad \phi_2(x_2) = \frac{M_2(x_2)}{\int_{-\infty}^{\infty} M_2(x_2)dx}.$$

Тогда "вероятность" того, что нечеткое число x_2 будет больше нечеткого числа x_1 задается так:

$$P(x_2 > x_1) = \int_{-\infty}^{\infty} \left(\int_{-\infty}^{\infty} \phi_2(x_2)dx_2 \right) \phi_1(x_1)dx_1. \quad (5)$$

Запишем (4) для случая, когда $M_1(x_1)$ и $M_2(x_2)$ определены формулами (2). При этом

$$\phi_1(x_1) = M_1(x_1) \Big/ \int_{-\infty}^{\infty} M_1(x_1)dx = \frac{2M_1(x_1)}{b_1 - a_1},$$

$$\phi_2(x_2) = \frac{2M_2(x_2)}{b_2 - a_2}.$$

Далее

$$\int_{-\infty}^{\infty} \phi_2(x_2)dx_2 =$$

$$= \begin{cases} 1, & x_2 < a_2 \\ \int_{x_1}^{c_2} \phi_2(x_2)dx_2 + \int_{c_2}^{b_2} \phi_2(x_2)dx_2, & a_2 \le x_1 < c_2, \\ \int_{x_1}^{b_2} \phi_2(x_2)dx_2, & c_2 \le x_1 < b_2, \\ 0, & x_1 > b_2. \end{cases} \quad (6)$$

Подставляя (2) в (6), после несложных вычислений, получим

$$J_1(x_1) = \int_{x_1}^{c_2} \phi_2(x_2)dx_2 + \int_{c_2}^{b_2} \phi_2(x_2)dx_2 =$$

$$= \frac{-x_1^2 - a_2c_2 + 2a_2x_1 + b_2c_2 - b_2a_2}{(b_2 - c_2)(c_2 - a_2)}, \quad (7)$$

$$J_2(x_1) = \int_{x_1}^{b_2} \phi_2(x_2)dx_2 = \frac{(b_2 - x_1)^2}{(b_2 - a_2)(b_2 - c_2)}. \quad (8)$$

Теперь, с учетом (5)–(8), имеем

$$P(x_2 > x_1) = \int_{a_1}^{a_2} \phi_1(x_1)dx_1 + \int_{a_2}^{c_2} J_1(x_1)\phi_1(x_1)dx_1 +$$

$$+ \int_{c_2}^{b_2} J_2(x_1)\phi_1(x_1)dx_1 = M_0 + M_1 + M_2. \quad (9)$$

Далее

$$M_0 = \int_{a_1}^{c_1} \frac{2}{b_1 - a_1} \frac{x_1 - a_1}{c_1 - a_1} dx_1 + \int_{c_1}^{a_2} \frac{2}{b_1 - a_1} \frac{b_1 - x_1}{b_1 - c_1} dx_1 =$$

$$= \frac{-c_1b_1 - a_1b_1 + a_1c_1 + 2b_1a_2 - a_2^2}{(b_1 - a_1)(b_1 - c_1)}, \quad (10)$$

$$M_1 = \frac{1}{(b_1 - c_1)(b_2 - c_2)(c_2 - a_2)(b_1 - a_1)} \cdot$$

$$\cdot \int_{a_2}^{c_2} (-x_1^2 - a_2c_2 + 2a_2x_1 + b_2c_2 - b_2a_2)(b_1 - x_1)dx_1 =$$

$$= \frac{1}{(b_1 - c_1)(b_2 - a_2)(b_1 - a_1)} \cdot$$

$$\cdot \left[\frac{1}{4}(c_2^2 + a_2^2)(c_2 + a_2) - \frac{d_{11}}{3}(c_2^2 + c_2a_2 + a_2^2) + \right.$$

$$\left. + \frac{d_{12}}{2}(c_2 + a_2) + d_{13} \right], \quad d_{11} = (b_1 + 2a_2),$$

$$d_{12} = 2b_1a_2 + a_2c_2 - b_2c_2 + a_2b_2,$$

$$d_{13} = b_1b_2c_2 - b_1a_2c_2 - b_1b_2a_2. \quad (11)$$

$$M_2 = \frac{1}{(b_1 - c_1)(b_2 - a_2)(b_2 - c_2)(b_1 - a_1)} \cdot$$

$$\cdot \int_{c_2}^{b_2} (b_2 - x_1)^2 (b_1 - x_1)dx_1 =$$

$$= \frac{1}{(b_1 - c_1)(b_2 - a_2)(b_1 - a_1)} \left[-\frac{1}{4}(b_2^2 + c_2^2)(b_2 + c_2) + \right.$$

$$\left. + \frac{d_{21}}{3}(b_2^2 + b_2c_2 + c_2^2) - \frac{d_{22}}{2}(b_2 + c_2) + b_2^2b_1 \right],$$

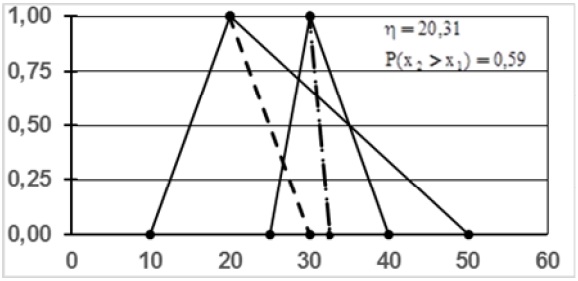
$$d_{21} = b_1 + 2b_2, \; d_{22} = b_2^2 + 2b_1b_2. \quad (12)$$

Рассмотрим примеры использования полученных соотношений (3) и (4) для сравнения нечетких чисел. Зададим в (2) следующие значения параметров функций принадлежности:

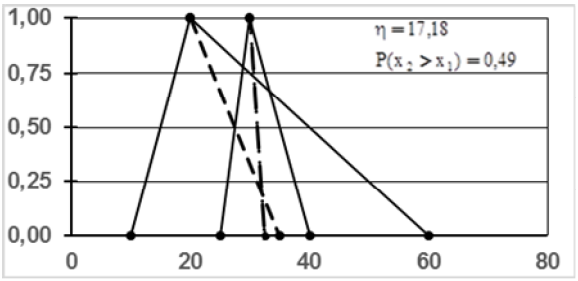
$$a_1 = 10, \quad c_1 = 20, \quad b_1 = 50, 60, 80, 120,$$

$$a_2 = 25, \quad c_2 = 30, \quad b_2 = 40.$$

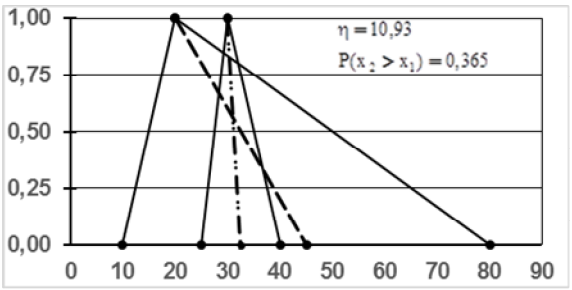
Соответствующие графики и результаты приведены на рис. 1.



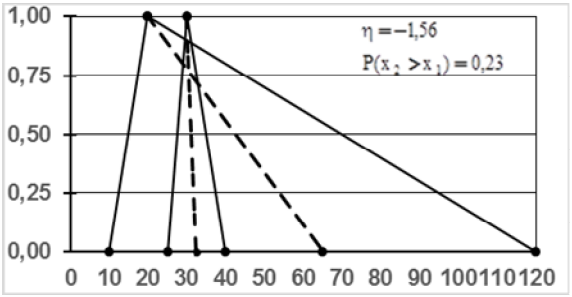
а – $a_1 = 10, c_1 = 20, b_1 = 50,\ a_2 = 25, c_2 = 30, b_2 = 40.$



б – $a_1 = 10, c_1 = 20, b_1 = 60,\ a_2 = 25, c_2 = 30, b_2 = 40.$



в – $a_1 = 10, c_1 = 20, b_1 = 80,\ a_2 = 25, c_2 = 30, b_2 = 40.$



г – $a_1 = 10, c_1 = 20, b_1 = 120,\ a_2 = 25, c_2 = 30, b_2 = 40.$

Рис. 1. Результаты сравнения нечетких чисел

Выводы

Рассмотрена задача коммивояжера высокой размерности в условиях нечетких исходных данных.

Стержневой элемент технологии решения задачи – декомпозиция, реализуемая путем кластеризации множества пунктов обхода.

Предложены два альтернативных метода сравнения нечетких расстояний между пунктами, используемые при решении задачи кластеризации.

Приведен пример реализации этих методов.

Список литературы

1. Flood M.M. The Traveling Salesman Problem / M.M. Flood // Operations Research, 1958. – N 6. – P.791–814.

2. Groes G. Method for Solving of Traveling Salesman Problem / G. Groes // Operations Research, 1958. – N6. – P. 791–814.

3. Раскин Л.Г. Анализ сложных систем и элементы теории оптимального управления. / Л.Г. Раскин. – М.: Сов. радио, 1976. – 344 с.

4. Goldberg D. Genetic Algorithms / D. Goldberg. – MA: Addison Wesley, 1989. – 210 p.

5. Holland D. Adaptation in Natural and Artificial Systems / D. Holland. – N.Y.: MIT Press, 1992. – 340 p.

6. Лысенко Ю.Г. Нейронные сети и генетические алгоритмы / Ю.Г. Лысенко, Н.Н. Иванов, А.Ю. Минц. – Донецк: Юго-Восток, 2003. – 230 с.

7. Серая О.В. Многомерные модели логистики в условиях неопределённости. / О.В. Серая. – Х.: ФОП Стеценко, 2010. – 512 с.

8. Серая О.В. Применение процедуры кластеризации при решении задачи коммивояжера высокой размерности с использованием генетического алгоритма / О.В. Серая // Вестник НТУ "ХПИ", 2006. – № 23 – С. 164–169.

9. Раскин Л.Г. Математические методы исследования операций и анализа сложных систем / Л.Г. Раскин. – Х.: ВИРТА ПВО, 1988. – 178 с.

10. Раскин Л.Г. Нечеткая математика / Л.Г. Раскин, О.В. Серая. – Х.: Парус, 2008. – 352 с.

Поступила в редколлегию 29.03.2017

Рецензент: д-р техн. наук, проф. О.В. Серая, Национальный технический университет «ХПИ», Харьков.

НЕЧІТКА ЗАДАЧА МАРШРУТИЗАЦІЇ

Л.Г. Раскін, В.В. Карпенко

Розглянуто задачу маршрутизації високої розмірності в умовах нечіткого задання вхідних даних. Запропоновано декомпозиційний алгоритм вирішення задачі, який використовує кластеризацію вхідної множини пунктів. Основою алгоритму є технологія порівняння нечітких чисел з метою вибору мінімального з них, що забезпечує можливість кластеризації. Виконаний аналіз двох альтернативних методів порівняння. Наведено приклад.

Ключові слова: *маршрутизація, задача комівояжера високої розмірності, декомпозиція, нечіткі вхідні дані.*

FUZZY ROUTING PROBLEM

L.G. Raskin, V.V. Karpenko

The high-dimensional routing problem is considered under conditions where the initial data are not clearly defined. A decomposition algorithm for solving a problem using clustering of the initial set of points is proposed. The basis of the algorithm is the technology of comparing fuzzy numbers in order to select the minimum of them, which provides the possibility of clustering. Two alternative comparison methods are compared. An example is given.

Keywords: *routing, the task of a traveling salesman of high dimension, decomposition, fuzzy initial data.*

УДК 621.311

А.М. Сільвестров, В.А. Святненко, О.М. Скринник

Національний технічний університет України «КПІ ім. Ігоря Сікорського», Київ

ПРЕДСТАВЛЕННЯ КУСКОВО-АНАЛІТИЧНИХ МОДЕЛЕЙ ЄДИНОЮ АНАЛІТИЧНОЮ МОДЕЛЛЮ

Дослідження, результати яких наведено у публікації, підтверджують можливість розробки запропонованим методом достатньо простої аналітичної моделі, яка за точністю апроксимації відповідає вимогам сучасних методів математичного та об'єктно-орієнтованого моделювання. Розроблені даним методом моделі можуть бути застосовані для аналітичних розрахунків оптимальних режимів роботи нестаціонарних стохастичних об'єктів, діагностики їх стану, інтерполяції та екстраполяції змінних об'єкта та для інших цілей шляхом ідентифікації локальних математичних моделей та об'єднання їх у повну аналітичну.

Ключові слова: *нелінійна модель, об'єкт ідентифікації, апроксимація, аналітична модель, транзистор, коефіцієнт нелінійних спотворень.*

Вступ

Останнім часом все більшу увагу приділяють чисельним методам комп'ютерного моделювання об'єктів ідентифікації ([1 – 3] та ін.). Це обгрунтовано складністю процесів у об'єкті, що досліджується (кусково-нелінійні залежності між змінними, логіка переключення від однієї моделі до іншої) та майже необмеженими можливостями сучасних електронно-обчислювальних машин (ЕОМ). Однак заміна теоретичних досліджень чисельними на ЕОМ призводить до втрати загальності рішення. Множина рішень чисельним моделюванням завжди обмежена. Існує ймовірність не змодельованої ситуації на об'єкті, яка може бути небажаною. Це стосується кусково-аналітичних моделей, заміни диференційних залежностей різницевими (особливо для нестійких об'єктів), апроксимації багатомірних нелінійних залежностей на кінцевій множинні експериментальних даних поліномами високого порядку та ін. Тому доцільно використовувати аналітичні рішення, користуючись чисельними методами і ЕОМ лише, як допоміжними засобами. Розглянемо задачу отримання єдиної аналітичної залежності для моделі, яку подано кусково-аналітичними частковими моделями з логікою переключення від однієї до іншої залежно від координат об'єкта.

Основна частина

Більшість нелінійних елементів реальних об'єктів мають кусково-аналітичну залежність y(x) Під час аналізу і синтезу систем з такими елементами виникають незручності, пов'язані з врахуванням граничних умов переходу від однієї області змінних x, y до сусідньої, за якого можуть виникати розриви y(x) та її похідних. В той час, як в реальній системі ці явища відсутні. Бажано мати аналітичну модель y(x) в усій області зміни x, y, щоб виключити складну логіку зміни структури y(x) та некоректності диференціювання dy/dx, d^2y/dx^2, … в точках стиковки. Таку умову можна забезпечити, якщо залежність y(x) подати зваженою аналітичними в усьому діапазоні функціями ваги $\eta_i(x)$ сумою:

$$y(x)=\sum_{i=1}^{n}\eta_i(x)\cdot y_i(x), \qquad (1)$$

де для виділення області x від 0 до $x=a$,

$$\eta_1(x)=\left(1\Big/\sqrt{1+a^{-2}x^2}\right)^m,\ x\in[0,a],\ a>0;$$

для області *x* від $x=a$ до $x\to\infty$,

$$\eta_2(x)=\left(\left|a^{-1}x\right|\Big/\sqrt{1+a^{-2}x^2}\right)^m,$$
$$x\in[0,\infty],\ x\in[-a,-\infty];$$

для області $x\in[a,b]$:

$$\eta_3(x)=\left(1\Big/\sqrt{1+b^{-2}x^2}\right)^m-\left(1\Big/\sqrt{1+a^{-2}x^2}\right)^m.$$

Значення m береться за умови близькості з точністю до ε моделі $\hat{y}(x)$ до реальної залежності $y(x)$. Тобто m збільшується до значення m^*, за якого похибка близькості $y(x)$ до $\hat{y}(x)$ буде близька до ε. Аналітична залежність (1) дозволяє (якщо x функція часу $x(t)$), обчислити аналітичні вирази похідних

$$\frac{dy}{dt}=\frac{dy}{dx}\frac{dx}{dt},\quad \frac{d^2y}{dt^2}=\frac{d}{dt}\left(\frac{dy}{dt}\right)=\frac{d^2y}{dx^2}\cdot\frac{dx}{dt}+\frac{dy}{dx}\cdot\frac{d^2x}{dt^2}$$

і т.і. Для кінцевого значення m похідні будуть гладкими функціями часу, які можна обчислити за допомогою відповідних програм (Mathcad, MATLAB та ін.) на ЕОМ.

Якщо нелінійність $y(x_1,\ldots,x_n)$ багатовимірна кусково-поліноміальна, то її об'єднання в єдину аналітичну досягається аналогічно одномірній (1),

тільки функції ваги багатомірні $\eta_i(x_1,\dots,x_k,x_n)$, де x_k – незалежні змінні, наприклад, у вигляді добутків часткових одномірних функцій $\eta_{ij}=\eta_i(x_j)$:

$$\eta_i(x_1,\dots,x_n)=\eta_{i1}(x_1)\cdot\eta_{i2}(x_2)\cdot\ldots\cdot\eta_{in}(x_n). \quad (2)$$

Для прикладу розглянемо вольт-амперну характеристику (ВАХ) $I_K(U_{KE})$ біполярного транзистора МП25 (рис. 1).

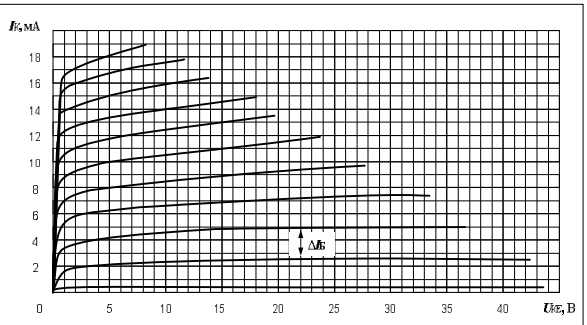


Рис. 1. ВАХ транзистора МП25, $\Delta I_Б = 0{,}1$ мА

Кусково-лінійна залежність $I_K(U_{KE})$ (рис.2) для фіксованого значення струму $I_Б$ транзистора МП25 дорівнює:

$$\hat{I}_K(U_{KE},I_{Бi})=\begin{cases}\beta_{1i}\cdot U_{KE}, \text{якщо } U_{KE}<0.8\text{ V}, i=\overline{1,n}\\ \beta_{2i}+\beta_{3i}\cdot U_{KE}, \text{якщо } U_{KE}\ge 0.8\text{ V},\end{cases} \quad (3)$$

Щоб позбавитися логічних складових опису (3) замінимо логічні складові аналітичними для всього діапазону зміни відповідних аргументів. Тоді, замість (3), отримаємо аналітичну на всьому інтервалі U_{KE} модель:

$$\hat{I}_K=(\beta_{1i}\cdot U_{KE})\cdot\eta_1+(\beta_{2i}+\beta_{3i}\cdot U_{KE})\cdot\eta_2, \quad (4)$$

де $$\eta_1(U_{KE})=\left(1+(U_{KE}/0{,}8)^m\right)^{-1},$$

$$\eta_2(U_{KE})=\left(1+(0{,}8/U_{KE})^m\right)^{-1},\ m\gg 1.$$

При описі цієї залежності, за обмеженою кількістю вимірів, єдиним в цьому діапазоні степеневим поліномом матимемо наближену апроксимацію з небажаною пульсацією між вимірами (рис. 2, пунктир).

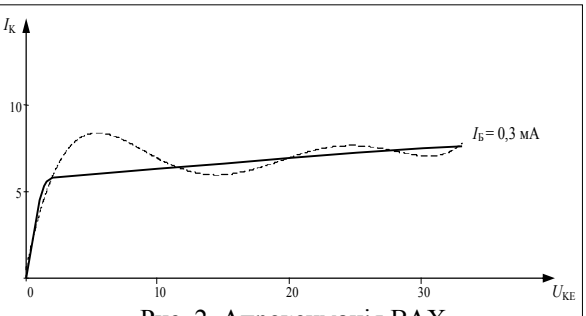


Рис. 2. Апроксимація ВАХ транзистора поліномом п’ятої степені

ВАХ транзистора двовимірна $y(x_1,\ x_2)$ кусково-поліноміальна. Її об’єднання в єдину аналітичну досягається аналогічно одномірній, тільки функції ваги $\eta_i(x_1,\ x_2)$, задаються у вигляді добутків часткових функцій $\eta_{ij}=\eta_i(x_j)$, де x_k – незалежні змінні U_{KE}, I_K ,тобто

$$\eta_i(x_1,\ x_2)=\eta_{i1}(x_1)\cdot\eta_{i2}(x_2).$$

За допомогою функції $\eta_3(I_Б)=\left(1+(I_Б/1.1)^m\right)^{-1}$ обмежимо модель (2) діапазоном $I_Б$ від 0 до 1,1 мА і апроксимуємо залежність коефіцієнтів β_i $(i=1,2,3)$ від другої змінної $I_Б$, лінійною моделлю:

$$\hat{\beta}_i(I_Б)=\gamma_{i0}+\gamma_{i1}\cdot I_Б.$$

В результаті отримуємо єдину для всього діапазону аналітичну модель

$$\hat{I}_K=(\beta_1(\gamma)\cdot U_{KE}\cdot\eta_3)\cdot\eta_1+ +\left((\beta_2(\gamma)+\beta_3(\gamma)\cdot U_{KE})\cdot\eta_3\right)\cdot\eta_2, \quad (4)$$

графік якої (рис. 3) співпадає з наданим графіком (рис. 1) із середньо квадратичною похибкою 2,6%, а для робочої зони вона менше 1%.

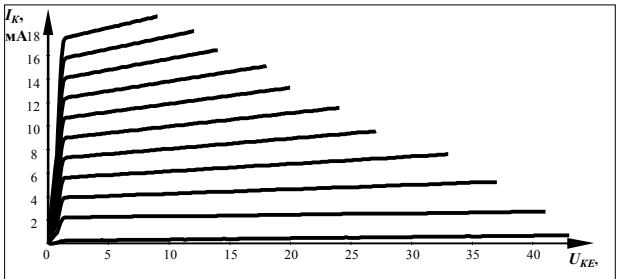


Рис. 3. Графік аналітичної моделі ВАХ транзистора

Враховуючи значення β_i, η_1, η_2, маємо аналітичну модель (4) вихідних характеристик транзистора, увімкненого за схемою зі спільним емітером (СЕ):

$$\hat{I}_K(U_{KE},I_Б)=\frac{(10.227\cdot I_Б+0.204)\cdot U_{KE}}{9.313\cdot U_{KE}^{10}+1}+ +\frac{16.652\cdot I_Б+(0.252\cdot I_Б)\cdot U_{KE}+0.511}{0.107\cdot U_{KE}^{-10}+1}. \quad (5)$$

Вхідні характеристики (рис. 4) для схеми з СЕ апроксимуються виразом $I_Б(U_{БЕ})=10\cdot U_{БЕ}^2$.

Режими роботи підсилювального каскаду знаходяться за рівнянням навантаження. Напруга колектора $U_{KE}=U_{вих}$ за наявності навантаження R_K в його колі, відповідно до другого закону Кірхгофа, дорівнює

$$U_{KE}=E_K-R_K\cdot I_K=30-10\cdot I_K, \quad (6)$$

де I_K пов’язане з $I_Б$ та U_{KE} рівнянням (5).

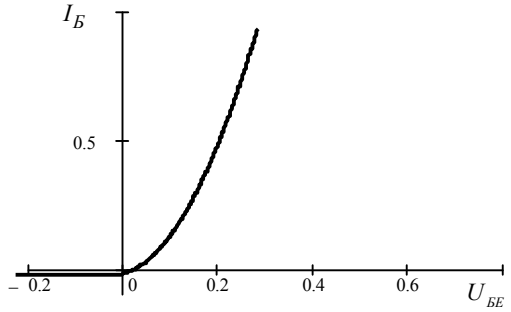


Рис. 4. Графік
вхідної характеристики транзистора

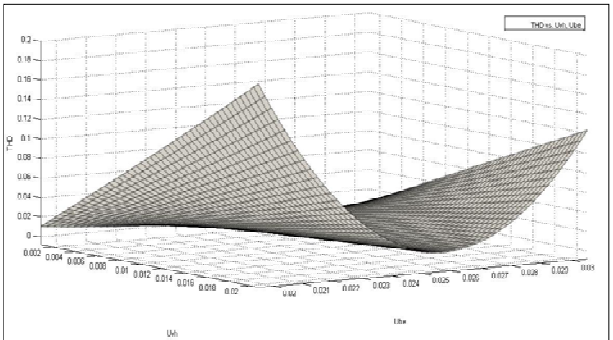


Рис. 5. Графік залежність коефіцієнта
нелінійних спотворень

Однією з основних характеристик якості підсилювача є коефіцієнт нелінійних спотворень. Цей показник характеризує ступінь відмінності форми сигналу від синусоїдальної і дорівнює відношенню середньоквадратичного значення всіх вищих гармонік сигналу до напруги першої гармоніки.

Маючи аналітичні вирази $U_{KE}(U_{вх}, U_{БЕ0})$ та враховуючи, що $U_{KE}(I_Б) = -0{,}36 \cdot e^{-3.43 \cdot I_Б} - 0.016$, використовуємо МАТКАД для знаходження значення 30-и гармонік і визначаємо залежності коефіцієнта нелінійних спотворень (КНС) від величини вхідного синусоїдального сигналу $U_{вх}$ та напруги спокою бази $U_{БЕ0}$:

$$КНС(U_{вх}, U_{БЕ0}) = 527{,}0 \cdot U_{вх}^3 - 2{,}387 \cdot U_{вх}^2 \cdot U_{БЕ0} + \\ + 49{,}1 \cdot U_{вх}^2 + 2{,}33 \cdot 10^5 \cdot U_{вх} \cdot U_{БЕ0}^2 - 1{,}91 \cdot 10^4 \cdot U_{вх} \times \quad (6) \\ \times U_{БЕ0} + 153 \cdot U_{вх} - 3{,}83 \cdot U_{БЕ0}^2 + 0{,}124 \cdot U_{БЕ0} - 0{,}0008.$$

Рівняння (7) дає можливість ще на етапі проектування мати уявлення щодо граничних меж використання підсилювача, а також вибирати оптимальний режим його роботи. Поверхня, що ілюструє цю залежність, зображена на рис. 5.

Висновок

Дослідження, результати яких наведено у публікації, підтверджують можливість розробки запропонованим методом достатньо простої аналітичної моделі складних нелінійностей. Розроблені даним методом моделі можуть бути застосовані для аналітичних розрахунків оптимальних режимів роботи нелінійних об'єктів та для інших цілей шляхом ідентифікації локальних математичних моделей та об'єднання їх у повну аналітичну без суттєвого ускладнення моделі. Також доцільно використання даного методу для стискування інформації шляхом заміни табличних та графічних довідкових даних про об'єкти різної природи нескладними аналітичними моделями.

Список літератури

1. Зеленський К.Х., Ігнатенко В.М., Коц О.П. Комп'ютерні методи прикладної математики. – К.: Академперіодика, 2002. – 480 с.

2. Методи теории автоматического управления / под. ред. Н.Д.. Егунова. – М.: МГТУ им. Баумана, 2000. – 748 с.

3. Бідюк П.І., Меняйленко О.С., Половцев О.В. Методи прогнозування. – Луганськ: Альма-матер, 2008. – 607 с.

Надійшла до редколегії 20.01.2017

Рецензент: д-р техн. наук, проф. В.І. Сінько. Національний технічний університет України «КПІ ім. Ігоря Сікорського», Київ.

ПРЕДСТАВЛЕНИЕ КУСОЧНО-АНАЛИТИЧЕСКИХ МОДЕЛЕЙ ЕДИНОЙ АНАЛИТИЧЕСКОЙ МОДЕЛЬЮ

А.Н. Сильвестров, В.А. Святненко, А.Н. Скрынник

Исследования, результаты которых приведены в публикации, подтверждают возможность разработки предложенным методом достаточно простой аналитической модели, которая по точности аппроксимации соответствует требованиям современных методов математического и объектно-ориентированного моделирования. Разработанные данным методом модели могут быть применены для аналитических расчетов оптимальных режимов работы нестационарных стохастических объектов, диагностики их состояния, интерполяции и экстраполяции переменных объекта и для других целей путем идентификации локальных математических моделей и объединение их в полную аналитическую.

Ключевые слова: *нелинейная модель, объект идентификации, аппроксимация, аналитическая модель, транзистор, коэффициент нелинейных искажений.*

REPRESENTATION OF PIECEWISE-ANALYTICAL MODELS UNIFIED ANALYTICAL

A.M. Silvestrov, V.A. Svyatnenko, O.M. Skrynnyk

The research results are presented in the publication confirm the possibility of developing quite simple analytical model with the proposed method. The accuracy of the approximation meets the requirements of modern mathematical methods and object-oriented modeling. The developed model by this method can be used for analytical calculation of optimal modes of stochastic non-stationary objects, diagnosis of their condition, interpolation and extrapolation variable object. Also for other purposes by identifying local mathematical models and combining them into a full analytical.

Keywords: *nonlinear model, object identification, approximation, analytical model, transistor, total harmonic distortion.*

УДК 004.728 : 519.87

А.А. Коваленко, Г.А. Кучук

Харьковский национальный университет радиоэлектроники, Харьков

МЕТОД УПРАВЛЕНИЯ РЕКОНФИГУРАЦИЕЙ ИНФОРМАЦИОННОЙ СТРУКТУРЫ КОМПЬЮТЕРНОЙ СИСТЕМЫ ОБЪЕКТА КРИТИЧЕСКОГО ПРИМЕНЕНИЯ ПРИ ВКЛЮЧЕНИИ ОПЕРАТИВНЫХ ЗАДАЧ В СИСТЕМУ УПРАВЛЕНИЯ

В статье предложен метод управления реконфигурацией информационной структуры компьютерной системы объекта критического применения при включении оперативных задач в систему управления. Проведен анализ особенностей, возникающих при реконфигурации таких систем без ограничений и с ограничениями на ресурсы. Предложены выражения, позволяющие определить параметры оптимальной информационной структуры системы относительно количества средних потерь в единицу времени.

Ключевые слова: *информационная структура, система управления, иерархический уровень управления, компонент, оперативная задача.*

Введение

Эволюция и реконфигурация компьютерных систем (КС) на сегодняшний день представляют собой плохо формализованные задачи, вследствие динамичекого характера изменений потребностей абонентов КС, разнообразных характеристик компонентов КС и принципов управления, реализованных в них [1 – 4]. Кроме того обширный спектр задач, связанных с активностями жизненного цикла систем управления (СУ) объектами критического применения (КП), являются слабо изученными, поскольку уже существует и еще разрабатывается множество факторов, подходов и соответствующих критериев.

С точки зрения синтеза различных структур систем управления, одной из актуальных задач является оценка качества варианта такой структуры, и, в свою очередь, соответствующая динамика функционирования составляющих ее компонент.

К важным подзадачам, подлежащим решению в процессе синтеза структуры СУ, относятся определение оптимального числа уровней иерархии, оптимальное распределение решаемых задач по таким уровням, а также выбор конкретных компонент уровней для решения поставленных задач [5 – 8]. Такие подзадачи подлежат решению при множестве наложенных совместимых ограничений. Таким образом, основная задача состоит в обеспечении такого функционирования СУ, которое позволит минимизировать технические потери и экономические затраты для всей иерархической структуры СУ.

Целью данной статьи является разработка метода управления реконфигурацией информационной структуры компьютерной системы объекта критического применения при включении оперативных задач в систему управления.

1. Особенности реконфигурации информационной структуры компьютерной системы объекта критического применения при включении оперативных задач в систему управления

Требованием к иерархической структуре СУ является ее полнота – должна быть реализована полная функциональность, от получения заявок от объекта КП до их обработки конечным компонентом СУ и выдачи соответствующего результата.

При формализации связей между множествами компонент и уровней СУ объектом КП удобно использовать вероятностный подход, когда факт окончания обслуживания заявки некоторым компонентом приводит к появлению заявки на одном или определенном множестве других компонент с заданной вероятностью. Таким образом, становится возможным использовать следующие модели для представления СУ:

– системы сбора и предварительной обработки информации: на нижних уровнях содержат компоненты, позволяющие собирать и обрабатывать информацию, при этом на более высокие уровни иерархии передается лишь незначительная часть информации;

– СУ с вертикалью управления: сбор и обработка информации производится исключительно компонентами нижних уровней, не оказывая влияния на загрузку верхних уровней; при этом последние управляют загрузкой нижних уровней;

– сложные СУ сбора и обработки информации: сбор и обработка информации может производиться компонентами каждого из уровней иерархии СУ.

Выбор структуры СУ объектом КП на сегодняшний день может осуществляться с использова-

нием множества моделей и методов, основанных на теории массового и имитационном моделировании. Исследование таких СУ, в свою очередь, производится посредством методов статистического моделирования.

В общем случае, каждый компонент более высокого уровня иерархии СУ получает меньшее количество заявок, причем такой поток можно рассматривать как простейший. Это приводит к возможности анализа функционирования каждого из компонент определенного уровня независимо от функционирования компонент более низкого уровня.

В стационарном режиме работы СУ, удобно выбрать критерием функционирования i-го ее компонента количество средних потерь в единицу времени, описываемое линейной зависимостью с коэффициентами c_i и d_i [9]:

$$\Im_i = c_i n_i + d_i, \qquad (1)$$

где n_i – среднее количество задач в i-м компоненте, а коэффициент c_i – среднее значение потерь в единицу времени вследствие пребывания задачи в системе обслуживания компонента.

Таким образом, выражение (1) представляет собой сумму потерь в единицу времени вследствие задержек передачи команд по вертикали управления и расходов в единицу времени на эксплуатацию компонента СУ. Сумму всех издержек СУ несложно получить суммированием потерь, описанных выражением (1), по всем компонентам рассматриваемой СУ. При однородности структуры СУ объектом КП в рамках каждого из уровней, величина общего критерия функционирования такой СУ, состоящей из ξ иерархических уровней, может быть вычислена достаточно просто, используя следующее рекуррентное выражение:

$$\Im(\xi) = z_{\xi-1}\Im(\xi-1) + \Im_\xi,$$

где $\Im(\xi)$ – оценка критерия функционирования для ξ-уровневой системы, $\Im(\xi-1)$ – соответствующая средняя оценка критерия функционирования в узлах предшествующего уровня, причем количество таких подсистем равно $z_{\xi-1}$, $\Im_\xi$ – оценка критерия функционирования в узле высшего уровня.

На основании вышеприведенного рекуррентного выражения можно записать что

$$\Im(\xi) = \sum_{i=1}^{\xi} \Im_i \prod_{j=1}^{\xi} z_j, \qquad (2)$$

где z_j – количество компонент уровня j, связанных с одним компонентом уровня j+1.

При условии наличия в СУ исключительно простейших потоков, распределение длительностей их обслуживания можно описать, используя показательные законы, компоненты являются надежными, каждая из заявок равновероятно может поступить на следующий уровень иерархии и допускается пренебрегать длиной очереди в компонентах. Это позволяет использовать выражение (2) для оценивания различных вариантов построения СУ с целью выявления наиболее перспективных. В таком случае интенсивность входного потока заявок для каждого из компонент СУ уровня i может быть вычислена с использованием следующего выражения:

$$\lambda_i = \Lambda \cdot \left(\prod_{j=1}^{i-1} k_j \prod_{j=1}^{\xi} z_j \right)^{-1},$$

где Λ – суммарная интенсивность потока заявок от объекта КП к СУ, k_j – коэффициент обратный вероятности передачи заявки на следующий уровень иерархии внутри СУ.

Принимая во внимание выражения (1) и (2), получим:

$$\Im(\xi) = \sum_{i=1}^{\xi} c_i \Lambda \left(d_i + \left(\mu_i \prod_{j=1}^{i-1} k_j \prod_{j=1}^{\xi} z_j - \Lambda \right)^{-1} \right) \cdot \prod_{j=1}^{\xi} z_j.$$

При дальнейшей детализации структуры и состава СУ, в терминах уровней и компонент (c_i, μ_i, k_i), используя вышеприведенное выражение, становится возможным определение оптимальных параметров структуры СУ объектом КП. Таким образом, можно записать следующую структуру системы уравнений относительно оптимальных значений z_i^*:

$$c_i \Lambda \left(\mu_i \prod_{j=1}^{i-1} k_j \prod_{j=1}^{\xi} z_j - \Lambda \right)^{-1} = d_i, \; i = \overline{1, \xi - 1},$$

решением которой есть следующее рекуррентное соотношение:

$$z_i^* = \Lambda \cdot \left(1 + \sqrt{c_i / d_i}\right) \Bigg/ \left(\mu_i \prod_{j=1}^{i-1} k_j \prod_{j=i+1}^{\xi} z_j^* \right).$$

Если дополнительно задать условие, что стоимость эксплуатации компонент уровня i пропорциональна их интенсивности обслуживания заявок с коэффициентами γ_i и δ_i ($d_i = \gamma_i \mu_i + \delta_i$) [9], то соответствующее оптимальное значение последнего может быть вычислено следующим образом:

$$\mu_i^* = \Lambda \Bigg/ \prod_{j=1}^{i-1} k_j \prod_{j=1}^{\xi} z_j + \sqrt{c_i \cdot \Lambda \Bigg/ \left(\gamma_i \prod_{j=1}^{i-1} k_j \prod_{j=1}^{\xi} z_j \right)}.$$

С целью дальнейшего описания, предположим, что имеет место типовой случай с моделью СУ с вертикалью управления, когда сбор и обработка ин-

формации производится исключительно компонентами нижних уровней, не оказывая влияния на загрузку верхних уровней. Таким образом, на каждый уровень иерархии СУ поступает поток заявок Λ_1, где $i=\overline{1,\xi}$. В результате их обслуживания компонентами уровня иерархии генерируются сигналы управления и соответствующие заявки для низлежащих (либо подчиненных) уровней. Пусть, интенсивность такого потока заявок для компонента уровня i равна

$$\lambda_i=\left(\sum_{j=1}^{\xi}\Lambda_j\right)\cdot\left(\prod_{j=i}^{\xi-1}z_i\right)^{-1},$$

где $i=\overline{1,\xi}$, z_j – число управляемых компонент низлежащего уровня, ξ – общее число уровней.

В таком случае, в единицу времени, суммарные издержки в СУ можно вычислить таким образом:

$$W(\xi)=\sum_{i=1}^{\xi}\left[\frac{c_i\sum_{j=1}^{\xi}\Lambda_j}{\mu_i\prod_{j=1}^{\xi-1}z_j-\sum_{j=1}^{\xi}\Lambda_j+d_i}\right]\cdot\prod_{j=1}^{\xi}z_j.$$

При дальнейшей детализации структуры и состава СУ, в терминах уровней и компонент (c_i,d_i,μ_i,Λ_i), становится возможным определение оптимальных параметров структуры СУ объектом КП для минимизации $\Im(\xi)$. Таким образом, можно записать следующую структуры системы уравнений относительно оптимальных значений z_i^*:

$$\alpha_i\sum_{j=1}^{m}\Lambda_j\left(\mu_i\prod_{j=i}^{m}x_j^*-\sum_{j=1}^{m}\Lambda_j\right)^{-1}=\beta_i,\ i=\overline{1,m-1},$$

решением которой есть следующее рекуррентное соотношение:

$$z_i^*=\sum_{j=1}^{\xi}\Lambda_j\cdot\left(1+\sqrt{\frac{c_i}{d_i}}\right)\cdot\left(\mu_i\prod_{j=i+1}^{\xi}z_j^*\right)^{-1},\ i=\overline{1,\xi-1}.$$

2. Особенности реконфигурации информационной структуры при наличии ограничений

При наличии ограничений на количество компонент СУ ($\aleph$), имеем следующее:

$$\sum_{i=1}^{\xi}\prod_{j=1}^{\xi}z_j\le\aleph. \qquad (3)$$

Если полученное множество оптимальных значений z_i^* не удовлетворяет такому соотношению, то необходимо вычислить новое множество $\{\overline{z_i}\}$, обеспечивающих минимизацию $\Im(\xi)$ при выполнении соотношения (3). Это становится возможным, например, при использовании метода множителей Лагранжа. Получим:

$$F(x_1,...,x_{\xi-1},f)=\Im(\xi+fg),$$

где $g=\sum_{i=1}^{\xi}\prod_{j=1}^{\xi}z_j-\aleph$, f – множитель Лагранжа.

Тогда:

$$\overline{z_i}=\Lambda\left(\mu_i\prod_{j=1}^{i-1}k_j\prod_{j=i+1}^{\xi}\overline{z}_j\right)^{-1}\cdot\left(1+\sqrt{c_i(d_i+f)^{-1}}\right),$$

при этом $i=\overline{1,\xi-1}$, а f можно найти используя следующее выражение:

$$\sum_{i=1}^{\xi-1}\Lambda\left(\mu_i\prod_{j=1}^{i-1}z_j\right)\left(1+\sqrt{\frac{c_i}{d_i+f}}\right)=\aleph-1.$$

При ограничении, равном Ξ, для расходов g на эксплуатацию СУ в единицу времени, можно записать следующее выражение:

$$g=\sum_{i=1}^{\xi}d_i\prod_{j=i}^{\xi}d_j-\Xi=0. \qquad (4)$$

Теперь становится возможным определить параметры оптимальной структуры СУ:

$$\overline{z_i}=\Lambda\left(\mu_i\prod_{j=1}^{i-1}k_j\prod_{j=i+1}^{\xi}\overline{z}_j\right)^{-1}\cdot\left(1+\sqrt{\frac{c_i}{d_i\cdot(1+f)}}\right);$$

$$\sum_{i=1}^{\xi}d_i\Lambda\left(1+\sqrt{\frac{c_i}{d_i\cdot(1+f)}}\right)\cdot\left(\mu_i\prod_{j=1}^{i-1}k_j\right)^{-1}=\Xi-\beta_\xi.$$

При одновременном соблюдении равенств (3) и (4) имеем:

$$F(x_1,...,x_{\xi-1},f_1,f_2)=\Im(\xi)+f_1g_1+f_2g_2;$$

$$g_1=\sum_{i=1}^{\xi}c_i\prod_{j=1}^{\xi}z_j-\Xi;$$

$$g_2=\sum_{i=1}^{\xi}d_i\prod_{j=1}^{\xi}z_j-\aleph$$

и искомое число управляемых компонент каждого из низлежащих уровней иерархии системы управления объектом критического применения одним компонентом вышестоящего уровня может быть получено следующим образом:

$$\overline{z_i}=\frac{\Lambda\cdot\left(1+\sqrt{\frac{c_i}{d_i(1+f_1)+f_2}}\right)}{\mu_i\prod_{j=1}^{i-1}k_j\prod_{j=i+1}^{\xi}\overline{z}_j};\quad i=\overline{1,m-1};\ m\ge4.$$

Для нахождения значений f_1 и f_2, в свою очередь, можно использовать следующую систему:

$$\sum_{i=1}^{\xi-1} d_i \Lambda\left(1+\sqrt{\frac{c_i}{d_i(1+f_1)+f_2}}\right)\cdot\left(\mu_i\prod_{j=1}^{i-1}k_j\right)^{-1}=\Xi-\beta_\xi;$$

$$\sum_{i=1}^{\xi-1} \Lambda\left(1+\sqrt{\frac{c_i}{d_i(1+f_1)+f_2}}\right)\cdot\left(\mu_i\prod_{j=1}^{i-1}x_j\right)^{-1}=\Xi-1.$$

Выводы

В статье рассмотрен метод управления реконфигурацией информационной структуры компьютерной системы объекта критического применения при включении оперативных задач в систему управления. Проведен анализ особенностей, возникающих при реконфигурации таких систем без ограничений и с ограничениями на ресурсы. Предложены и обоснованы выражения, позволяющие определить параметры оптимальной информационной структуры системы относительно количества средних потерь в единицу времени.

Ближайшим направлением дальнейших исследований является разработка алгоритма, реализующего предложенный метод.

Список литературы

1. Коваленко, А.А. Подходы к синтезу информационной структуры системы управления объектом критического применения / А.А. Коваленко // Системы обработки информации: сборник научных трудов. – Х.: ХУ ВС, 2014. – Вып. 1 (117). – С. 180 – 184.

2. Коваленко, А.А. Подходы к синтезу технической структуры компьютерной системы, образующей систему управления объектом критического применения / А.А. Коваленко // Сборник научных трудов Харьковского университета Воздушных Сил. – Х.: ХУ ВС, 2014. – Вып. 1(38). – С. 116 – 119.

3. Коваленко, А.А. Подходы к оптимизации распределения задач управления по компонентам компьютерной системы, образующей систему управления объектом критического применения / А.А. Коваленко // Наука у техніка Повітряних Сил Збройних Сил України: науково-технічний журнал. – Х.: ХУ ПС, 2014. – Вип. 2(15). – С. 158 – 160.

4. Кучук, Г.А. Модель процесса эволюции топологической структуры компьютерной сети системы управления объектом критического применения / Г.А. Кучук, А.А. Коваленко, А.А. Янковский // Системы обработки информации: сборник научных трудов. – Х.: ХУ ВС, 2014. – Вып. 7 (123). – С. 93 – 96.

5. Кучук, Г.А. Інформаційні технології управління інтегральними потоками даних в інформаційно-телекомунікаційних мережах систем критичного призначення / Г.А. Кучук. – Х.: ХУПС, 2013. – 264 с..

6. Кучук, Г.А. Синтез структуры вычислительной сети для иерархической системы управления / Г.А. Кучук, А.В. Королев, О.В. Муравьев, О.Ю. Набока // Сб. научн. трудов. Информационные системы. Вып. 2. – Х.:НАНУ, ПАНИ, ХВУ, 1994. – С. 90 – 93.

7. Кучук, Г.А. Концептуальний підхід до синтезу структури інформаційно-телекомунікаційної мережі / Г.А. Кучук, І.В. Рубан, О.П. Давікоза // Системи обробки інформації : збірник наукових праць. – Х.: ХУ ПС, 2013. – Вип. 7 (114). – С. 106 – 112.

8. Кучук, Г.А. Синтез стратифікованої інформаційної структури інтеграційної компоненти гетерогенної складової Єдиної АСУ Збройними Силами України / Г.А. Кучук, О.П. Давікоза // Наука і техніка Повітряних Сил Збройних Сил України : науково-технічний журнал. – Х.: ХУ ПС, 2013. – № 3(12). – С. 154-158.

9. Мамиконов, А.Г. Математическая модель и алгоритм выбора оптимальной структуры типового контура управления ЛА / А.Г. Мамиконов, А.Д. Цвиркун, В.Н. Новиков, В.К. Атинфиев // Сб. трудов ИПУ. – М.: ИПУ, 1975. – Вып. 6. – С. 80 – 84.

Надійшла до редколегії 1.02.2017

Рецензент: д-р техн. наук, проф. С.Г. Удовенко, Харківський національний економічний університет імені Саймона Кузнеця, Харків.

МЕТОД УПРАВЛІННЯ РЕКОНФІГУРАЦІЄЮ ІНФОРМАЦІЙНОЇ СТРУКТУРИ КОМП'ЮТЕРНОЇ СИСТЕМИ ОБ'ЄКТА КРИТИЧНОГО ЗАСТОСУВАННЯ ПРИ ВКЛЮЧЕННІ ОПЕРАТИВНИХ ЗАВДАНЬ В СИСТЕМУ УПРАВЛІННЯ

А.А. Коваленко, Г.А. Кучук

У статті запропоновано метод управління реконфігурацією інформаційної структури комп'ютерної системи об'єкта критичного застосування при включенні оперативних завдань в систему управління. Проведено аналіз особливостей, що виникають при реконфігурації таких систем без обмежень і з обмеженнями на ресурси. Запропоновано вирази, що дозволяють визначити параметри оптимальної інформаційної структури системи щодо кількості середніх втрат в одиницю часу.

Ключові слова: *інформаційна структура, система управління, ієрархічний рівень управління, компонент, оперативне завдання.*

CONTROL METHOD FOR RECONFIGURATION OF INFORMATIONAL STRUCTURE OF A CRITICAL APPLICATION OBJECT'S CONTROL SYSTEM CONTAINING OPERATIONAL TASKS

A.A. Kovalenko, G.A. Kuchuk

The paper proposes control method for reconfiguration of informational structure of a critical application object's control system containing operational tasks. It was performed an analysis concerning features related to reconfiguration of such systems Considering both cases: presence and absence of restrictions on resources. Expressions are proposed that allow to determine the parameters of the optimal informational structure of the system relative to the number of average losses per time unit.

Keywords: *information structure, control system, hierarchical level of control, component, operational task.*

УДК 004.932.721

О.А. Мокрінцев

Державний університет телекомунікацій, Київ

ПОПЕРЕДНЯ ОБРОБКА ЗОБРАЖЕНЬ ДЛЯ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ОДНОВИМІРНИХ ШТРИХ-КОДІВ

Одновимірні або лінійні штрих-коди отримали широке розповсюдження у логістиці, медицині, торговій сфері та інших областях. У статті розглянуто сучасні тенденції та підходи до розробки методики та алгоритмів попередньої обробки зображень для автоматичного розпізнавання одновимірних штрих-кодів. Попередня підготовка потрібна для поліпшення умов зчитування кодів та дозволяє привести зображення до уніфікованого вигляду, необхідного для подальшого декодування. Також наведені методи локалізації штрих-кодів у зображеннях.

Ключові слова: *одновимірний штрих-код, цифрова обробка зображень, конвертація у відтінки сірого, методика розпізнавання штрих-кодів.*

Вступ

Штрих-код є оптичним представленням даних, що пристосоване до розпізнавання автоматичними пристроями. Історично, спочатку штрих-коди кодувалися шляхом варіювання ширини і інтервалу у послідовності паралельних ліній (штрихів). Такі штрих-коди називаються лінійними або одновимірними [1]. Пізніше вони еволюціонували в прямокутники, точки, шестикутники та інші геометричні двовимірні форми (2D). Не зважаючи на те що 2D системи можуть складатися з різних геометричних фігур, не тільки ліній, зазвичай вони також мають назву штрих-кодів. Двовимірні коди є найбільш сучасним напрямком бурхливого розвитку оптичного кодування даних. Але все ж найбільш поширеними і найчастіше вживаними є класичні одновимірні або лінійні штрих-коди. Далі ми будемо розглядати методи та алгоритми розпізнавання саме таких методів оптичної репрезентації даних.

Результати досліджень

1. Проблематика розпізнавання штрих-кодів. Спочатку одновимірні штрих-коди можна було сканувати переважно лише за допомогою лазерних сканерів. На фізичному рівні у якості первинних даних такі сканери дозволяли отримувати відбиток лінії (або ж сукупність різнонаправлених ліній). Пізніше, з розвитком та широким розповсюдженням кишенькових комп'ютерів і смартфонів постала проблема розпізнавання кодів знятих за допомогою цифрових камер, якими зазвичай комплектувалися ці пристрої. На відміну від розпізнавання ліній, стало потрібно знаходити та розпізнавати коди у двовимірному фотозображенні. До того ж, завдяки вадам освітлення, фокусування та загальної технічної недосконалості бюджетних мінікамер, ця задача отримала додаткові складнощі. Зазвичай, найбільш узагальнений процес розпізнавання одновимірних штрих-кодів складається з наступних кроків:

- попередня обробка зображення
- локалізація областей, що містять штрих-код, визначення його орієнтації
- сегментація або виділення (сканування) меж ліній штрих-кодів
- декодування і перевірка коду

У різних програмних реалізаціях деякі з цих кроків можуть бути скасовані. Але у найбільш загальних випадках ми маємо застосовувати усі пункти. Також слід зазначити, що наведена послідовність може бути змінена та/або деякі операції можуть бути застосовані у довільному порядку. Але перші два етапи можна виділити як підготовку зображення до сканування.

2. Попередня обробка зображення. Попередня обробка зображень може включати різні методи перетворень для поліпшення умов зчитування кодів та фільтраційних заходів для видалення шумів. На виході ми маємо отримати теж картинку, але в дещо удосконаленій для розпізнавання формі.

Наведемо основні види перетворень що можуть бути застосовані на даному етапі:

- конвертація кольорового зображення у чорно-біле (або у відтінки сірого)

Найбільш простим і поширеним рішенням є застосування формули згідно з рівнями освітлюваності по кожній базовій кольоровій компоненті [2]. Отже, беручи кольорове вхідне зображення, маємо:

$$i[m,n] = 0.299 \times r[m,n] + 0.587 \times g[m,n] + 0.114 \times b[m,n],$$

де r, g і b - червоні, зелені і сині компоненти вхідного сигналу, відповідно і $[m, n]$ є інтенсивністю яскравості в точці зображення $[m, n]$. Також у деяких спрощених випадках або як фінальна операція попередньої обробки використовується «бінарізація» або пряма конвертація зображення у чорно біле. Але слід зауважити що у загальному випадку при цьому втрачається частка вхідної графічної інформації, що може негативно позначитися на процесі розпізнавання коду в цілому.

- **інвертування зображення**

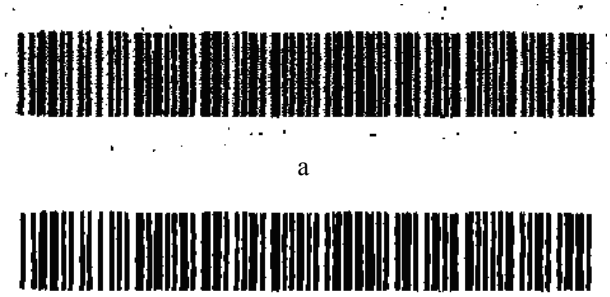
Інвертування кольорів зображення допомагає розпізнавати не тільки штрих-коди, що нанесені чорним по білому, але й ті коди, в яких стовпчики мають відносно світліший колір ніж колір фону (білі штрихи по чорному полю).

- **усунення перекосів**

Внаслідок перекосу камери або нанесення штрих-кодів на профільовані поверхні можуть виникати перекоси та інші візуальні деформації вихідної області штрих-кодів. У таких випадках може бути застосовано аналіз деформації контуру областей що містять штрих-код або внесення «ручних» поправок ззовні користувачем.

- **видалення «пилу»**

На цьому етапі здійснюється фільтрація дрібних шумових явищ (або «пилу») перед подальшою обробкою зображення. Усуваються усі чорні плями, розмір яких меншій деякого порогового значення [3] (рис. 1).



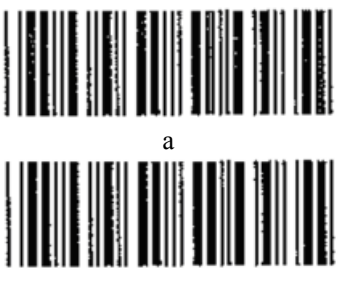
а

б

Рис. 1. Приклад зображення штрих-коду, спотвореного дрібним «пилом» до (а) та після (б) обробки

- **згладжування (видалення дрібних проміжків)**

За допомогою зазначеної операції розмиваються усі чорні об’єкти у горизонтальному та вертикальному напрямку на задану глибину. Тобто видаляються плями аналогічно видаленню пилу, але цього разу білого кольору. Таким чином усуваються похибки сканування і потертості вихідного зображення та відновлюється візуальна структура стовпчиків штрих-коду (рис. 2).



а

б

Рис. 2. Приклад видалення дрібних проміжків у зображенні до (а) та після (б) обробки

3. Локалізація областей що містять штрих-код. У деяких системах розпізнавання цей етап може бути пропущений. Можна просто сканувати зображення уздовж ліній що розташовані паралельно у деякому напрямку з однаковим відступом. Такий підхід може бути виправданим якщо:

- потрібно розпізнавати лише один-два типу штрих-коду
- зображення, що містить штрих-код відносно невелике за розміром

Якщо ці критерії не виконуються, доцільно попередньо визначити області, що потенційно містять код. Можуть бути застосовані такі методи:

- **виділення у зображенні набору штрихів**

Спочатку, за допомогою, наприклад, рандомізованого перетворення Хафа [4] на зображенні виділяються усі можливі лінії (рис. 3). Далі потрібно їх проаналізувати. Для покращення процесу локалізації можна вжити додаткові заходи. Наприклад, якщо два відрізки розташовані на одній лінії з невеликим розривом, їх потрібно «склеїти». Після кожної склейки усі лінії потрібно проаналізувати заново.

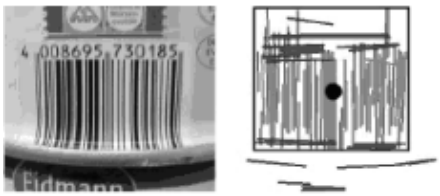


Рис. 3. Застосування рандомізованого перетворення Хафа до зображення з штрих-кодом

Далі потрібно виділити набори штрихів що розташовані паралельно, та без суттєвих проміжків у деякій обмеженій компактній області. Відкинувши невеликі області з малим числом штрихів остаточно отримаємо потрібний результат.

Хоча цей метод і має деякі плюси (так, одночасно ми отримаємо направлення штрих-коду), в цілому цей підхід потребує значних обчислювальних ресурсів. Крім цього, він відносно складний алгоритмічно та у площині практичної реалізації.

- **градієнтний аналіз**

Штрих-код утворює зображення у якому фактор освітлення є таким, що різко та багатократно змінюється у обмежених за розміром областях. Зазначимо, що такі ж самі властивості має, наприклад, і звичайний текст, але на відміну від тексту ця зміна має досить чітку монотонність направлення уздовж штрихів.

Це дає змогу локально аналізуючи властивості текстури зображення виділяти штрих-коди згідно односпрямованості градієнтів яскравості у обмеженій області. [5, 6, 7].

Величина і фаза градієнта зображення у кожній точці зображення обчислюється за допомогою маски Собеля 3 × 3:

$$S_h = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} S_v = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}; \quad \begin{matrix} G_h = I \otimes S_h; \\ G_v = I \otimes S_v, \end{matrix}$$

де S_h і S_v, є горизонтальні і вертикальні маски Собеля, відповідно G_h і G_v є горизонтальні і вертикальні градієнтні карти, а $\otimes$ є оператором згортки.

Як варіант можуть бути використані альтернативні матриці обчислень, наприклад, оператор Щарра:

$$S_h = \begin{bmatrix} 3 & 10 & 3 \\ 0 & 0 & 0 \\ -3 & -10 & -3 \end{bmatrix} \; S_v = \begin{bmatrix} 3 & 0 & -3 \\ 10 & 0 & -10 \\ 3 & 0 & -3 \end{bmatrix}.$$

Для аналізу штрих-кодів що розташовані під кутом приблизно 45 та 135 градусів можуть бути використані такі матриці:

$$S_{d1} = \begin{bmatrix} 0 & -\frac{1}{4} & 0 \\ \frac{1}{4} & 0 & -\frac{1}{4} \\ 0 & \frac{1}{4} & 0 \end{bmatrix}; \; S_{d2} = \begin{bmatrix} 0 & \frac{1}{4} & 0 \\ \frac{1}{4} & 0 & \frac{1}{4} \\ 0 & -\frac{1}{4} & 0 \end{bmatrix}.$$

Продукт фільтрації вихідного зображення з фільтруючими матрицями являє собою контурний малюнок з контурними лініями, що перпендикулярні напрямку диференціювання. Щоб отримати цілісну область треба «розмити» отриману градієнтну карту, наприклад, шляхом усереднення значень градієнтів на деякій площі, значно меншій розмірів штрих-коду та дещо більшої за розміром його елементів. Або можна використати алгоритм зворотної тесселяції. Відкинувши області, що не задовольняють мінімальним розмірам або містять забагато проміжків, врешті отримаємо результат.

Висновки

Для підвищення надійності розпізнавання штрих-кодів у сканованих зображеннях потрібна попередня цифрова обробка, до якої відносять конвертацію кольорового зображення у відтінки сірого, інвертування зображення, усунення перекосів видалення пилу та згладжування (видалення дрібних проміжків). Звичайно, використання кожного з методів залежить від специфіки ситуації з вхідними даними.

Для подальшого прискорення процесу розпізнавання доречно використовувати локалізацію областей зайнятих штрих-кодами. Для цього можуть бути використані виділення у зображенні набору штрихів (методом Хафа) або градієнтний аналіз.

Список літератури

1. T. Pavlidis, J. Swartz, and Y. P. Wang, "Fundamentals of bar code information theory," Computer, vol. 23, no. 4, pp. 74-86, Apr. 1990.

2. C. Saravanan, "Color Image to Grayscale Image Conversion," Computer Engineering and Applications (ICCEA), 2010 Second International Conference on, Bali Island, 2010, pp. 196-199.

3. Kumawat, Deepika; Singh, Ranjeet Kumar; Gupta, Deepak; Gupta, Shikha. "Impact of Denoising using Various Filters on QR Code" International Journal of Computer Applications 63.5 (2013).

4. Muniz R, Junco L, Otero A. A. "A robust software barcode reader using the Hough transform". International Conference on Information Intelligence and Systems; 1999. pp. 313–319.

5. N. Normand, and C. Viard-Gaudin, "A Two-Dimensional Bar Code Reader," Pattern Recognition, Vol. 3, pp. 201 03, 1994.

6. C. Viard-Gaudin, N. Normand, and D. Barba, "Algorithm Using a Two-Dimensional Approach," Proc. of the Second Int. Conf. on Document Analysis and Recognition, No. 20-22, pp. 45-48, October 1993.

7. A.A. Krasnobaev, "Barcodes Recognition Algorithms", Inst. Appl. Math., The Russian Academy of Science, Moscow 2004.

Надійшла до редколегії 22.12.2016

Рецензент: д-р техн. наук, проф. С.В. Козелков, Державний університет телекомунікацій, Київ.

ПРЕДВАРИТЕЛЬНАЯ ОБРАБОТКА ИЗОБРАЖЕНИЙ ДЛЯ АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ ОДНОМЕРНЫХ ШТРИХ-КОДОВ

А.А. Мокринцев

Одномерные или линейные штрих-коды получили широкое распространение в логистике, медицине, сфере торговли и других областях. В статье рассматриваются современные тенденции и подходы в разработке методики и алгоритмов предварительной обработки изображений для автоматического распознавания одномерных штрих-кодов. Предварительная подготовка необходима для улучшения условий считывания кодов и позволяет привести изображение к унифицированному виду, необходимого для дальнейшего декодирования. Также, приводятся методы локализации штрих-кодов в изображениях.

Ключевые слова: *одномерный штрих-код, цифровая обработка изображений, сегментация изображений, декодирование штрих-кодов.*

DIGITAL IMAGE PREPROCESSING IN AUTOMATIC LINEAR BARCODE RECOGNITION

O.A. Mokrintsev

One-dimensional or linear barcodes are widely utilized in logistics, medical diagnostic, retail and other areas. The work covers latest tendencies and approaches in development of methods and algorithms for digital image preprocessing for linear barcodes recognition. Preprocessing is necessary to improve the code reading conditions and allows transforming images to a unified state, required for further decoding. Also, covered some methods of barcodes localization in digital images.

Keywords: *one-dimensional barcode, digital image processing, image grayscale conversion, barcode-decoding methods.*

УДК 681.3

Л.В. Морозова

Національна академія Національної гвардії України, Харків

ФОРМУВАННЯ СИСТЕМИ ЛОГІСТИЧНИХ ОРГАНІВ ДЛЯ ОБСЛУГОВУВАННЯ РОЗГАЛУЖЕНИХ СПОЖИВАЧІВ

Пропонується алгоритм рішення задачі з формування системи логістичних органів для обслуговування розгалужених споживачів. Рішення включає розбивку вихідної множини розгалужених споживачів на щільні підмножини і розміщення в цих підмножинах логістичних органів.

Ключові слова: *розгалужені споживачі, логістичний орган, система логістичних органів, щільні множини розгалужених споживачів, координатна площина.*

Вступ

Постановка проблеми. Для виконання завдань з обслуговування розгалужених споживачів (РС), наприклад, постачання матеріально-товарних засобів до мережі магазинів, сервісне обслуговування споживачів на певній території, складське обслуговування тощо необхідно створювати систему логістичних органів (ЛОр). Такими органами можуть бути склади мережі магазинів, майстерні з обслуговування техніки, склади вищого рівня і т.п. Під системою ЛОр будемо розуміти їх кількість, закріплення за ними РС та територіальне розміщення відносно цих споживачів.

Основними вимогами до таких систем є, по-перше, необхідність обслуговування територіально розгалужених споживачів, по-друге, своєчасне обслуговування РС у місцях їх розміщення і, по-третє, обслуговуванні об'єктів раціональним (наявним) складом ЛОр.

Розгалужені споживачі мають "прив'язку" до місцевості, тобто координати, розташовані на певній відстані один від одного, територія їх розміщення має транспортну інфраструктуру. Тому для виконання означених вимог потребує вирішення задач формування груп (підмножини) РС, виділення для їх обслуговування ЛОр та визначення (або призначення) місця розташування таких органів для кожної з підмножин логістичних органів. Або для відомого складу ЛОр визначити групи РС, що будуть за ними закріплені.

Для формування таких груп РС і визначення місць розміщення в цих групах логістичних органів необхідно визначати показник та критерій сформованості таких груп, мати алгоритми рішення таких задач.

Аналіз останніх досліджень і публікацій. Аналіз розв'язання сформульованої задачі в різних постановках показав, що більшість з їх належить до класу комбінаторних, а методи їх вирішення розділяються на точні (комбінаторні) та наближені (включаючи евристичні) [1-4].

Комбінаторні методи передбачають повний або напрямків перебір усіляких варіантів формування груп РС. Методи відсікання можуть бути використані тільки в тих випадках, коли цільова функція та функції обмежень лінійні. Тоді задача може розглядатися як окремий випадок задачі цілочисельного лінійного програмування, що істотно звужує область їх практичного застосування [2, 3].

Можливість застосування комбінаторних методів з'являється при використанні підходу, заснованого на виключенні ізоморфних варіантів [5].

Серед наближених методів, що знаходять широке застосування при вирішенні задач великої розмірності, виділяються методи, що використають випадковий пошук, методи, що використають випадковий пошук з локальною оптимізацією і методи, схеми яких враховують специфіку задач. До числа найбільш ефективних методів цієї групи можуть бути віднесені методи еволюційного синтезу, реалізовані за допомогою генетичних алгоритмів [7, 8] і методи, що використають схеми покоординатної оптимізації [1, 6]. При цьому методи еволюційного синтезу добрі пристосовані для вирішення багатокритеріальних задач, але поступаються методам на основі покоординатної оптимізації за комплексним показником "точність-складність" при вирішенні задач за показником витрат. Методи на основі покоординатної оптимізації мають відносно низьку часову складність, однак не гарантують одержання точних рішень.

При вирішенні задач оптимізації множин РС з регулярним розподілом ЛОр отримані оцінки оптимальної кількості елементів вищого рівня в них на основі аналітичної моделі Нокера і попередньої оцінки витрат для систем з радіально-вузловими структурами [9]. При цьому територіальне розміщення таких органів не визначається.

Метою статті є розроблення алгоритму розв'язання задачі формування системи логістичних органів, які забезпечать обслуговування розгалужених споживачів.

Виклад основного матеріалу

Множину РС з урахуванням того, що відомо їх географічні координати, можна представити зваженим графом $G=(Q, R)$ із множиною вершин $Q=\{q_i\}$, $i=\overline{1,n}$, кожна з яких відповідає певному споживачу, і множиною ребер $R=\{r_{ij}\}$, $i, j=\overline{1,n}$, з вагами r_{ij}, що визначають відстані між вершинами q_i і q_j.

Даний граф відрізняється від звичайного зваженого графа [10] тим, що його вершини мають фіксовані, задані координатами місця розташування на координатній площині, а кожна пара вершин q_i і q_j зв'язана ребром з вагою r_{ij}, що дорівнює відстані між відповідними точками площини. На координатній площині граф G візуально представляється множиною вершин $q_i \in Q$ із завданням координат (x_i, y_i). Граф G може бути представлений також матрицею відстаней $R=\|r_{ij}\|_{n\times m}$, яка виходить на основі візуального подання графа. Матриця R є симетричною, а діагональні елементи $r_{ij}=0$.

При формуванні системи ЛОр, як правило, виникає задача розбивки множини РС на задане число підмножин так, щоб сума відстаней між ними в підмножинах була мінімальною. Тобто, необхідно одержати щільні підмножини РС.

З урахуванням позначень, прийнятих при визначенні графа G, розглянуту задачу можна сформулювати в такий спосіб.

Множину Q необхідно розбити на сукупність підмножин $\{Q_k\}$, $k=\overline{1,m}$, таких, що:

$$\sum_k \sum_{q_i, q_j \in Q_k} r_{ij} \to \min, \qquad (1)$$

$$\bigcup_k Q_k = Q, \quad Q_k \cap Q_s = \varnothing, \quad k, s=\overline{1,m}, \qquad (2)$$

$$|Q_k| \cong [n/m], \quad \sum_k |Q_k| = n. \qquad (3)$$

Умова (3) означає, що потужність множини Q_k приймається рівній величині n/m, округленій в більшу або меншу сторону так, щоб сума $|Q_k|$ становила величину n. Величини $|Q_k|$ можуть призначатися при дотриманні другої частини умови (3).

Умови (2) і (3) задають на множині Q множину W припустимих варіантів розбивки $\{Q_k\}$. Сукупність множин $\{Q\}_w$, що задовольняють умовам (2) і (3), відповідає деякому варіанту розбивки $w \in W$.

Розбивку $\{Q_k^*\}_w$ назвемо щільною розбивкою (ЩР) множини вершин Q графа G, якщо дана розбивка задовольняє критерію (1). Суму відстаней r_{ij} між вершинами q_i і q_j у множині Q_k позначимо величиною L_k, тобто $L_k = \sum_{q_i, q_j \in Q_k} r_{ij}$, а сумарну оцінку щільності для розбивки $\{Q\}_w$ позначимо величиною $L_w^* = \sum_k L_k$. Тоді щільній розбивці $\{Q_k^*\}_w$ буде відповідати оцінка щільності $L_w^* = \min_{w\in W} L_w$.

Варто мати на увазі, що оцінка щільності L_w відноситься до розбивки $\{Q_k\}_w$ в цілому, а не до її окремих множин Q_k. Інакше кажучи, не можна сказати, що множини Q_k^* з оцінками L_k^* в ЩР $\{Q_k^*\}_w$ є щільними, а множини Q_k з оцінками L_k в розбивці $\{Q_k\}_w$ ні. Множина Q_k має певну оцінку щільності L_k незалежно від того, входить Q_k у ЩР чи ні.

При формуванні системи ЛОр задачу (1)–(3) треба вирішувати не тільки з метою одержання ЩР, але і для розміщення на координатній площині розташування вершин множини Q_k деякого ЛОр, для взаємодії з вершинами $q_i \in Q_k$. У цьому випадку як оцінку щільності множини Q_k можна використовувати сумарну відстань від вершин множини до ЛОр.

У множині Q_k логістичний орган будемо розглядати як додаткову вершину q_k з координатами (x_k, y_k). Тоді оцінка щільності R_k множини Q_k відносно ЛОр q_k визначається виразом $R_k = \sum_{q_i \in Q_k} r_{ik}$, де r_{ik} – відстань від вершини q_i до ЛОр q_k. Аналогічно оцінкам L_w і L_w^* вводяться оцінки $R_w = \sum_k R_k$ для розбивок $\{Q_k\}_w$ і оцінки $R_w^* = \min_{w\in W} R_w$ для ЩР $\{Q_k^*\}_w$.

Приймемо, що координати (x_k, y_k) ЛОр q_k для множини Q_k приблизно визначаються як центри мас, тобто

$$x_k = 1/\mu_k \sum_{q_i \in Q_k} x_i, \quad y_k = 1/\mu_k \sum_{q_i \in Q_k} y_i, \qquad (4)$$

де μ_k – число вершин у множині Q_k.

Якщо за умовами задачі ЛОр можуть або повинні бути розміщені тільки в одній з вершин відповідної множини Q_k, то при використанні оцінок R_w критерій вирішення задачі запишеться у вигляді:

$$\sum_k \sum_{q_i \in Q_k} r_{ik} \to \min. \qquad (5)$$

Щодо використання оцінок L і R варто відмітити, що вони не суперечать одна одній, тобто мінімізація оцінки L відповідає мінімізації оцінки R і навпаки. Надалі будемо розглядати задачу в постановці (5), (2), (3) з обчисленням координат ЛОр за виразом (4).

Розглянемо одну з можливих розбивок $\{Q_k\}_w$. У множинах Q_k згідно (4) визначені координати ЛОр q_k. Вирішимо задачу закріплення вершин множини Q за ЛОр так, щоб за кожним логістичним органом q_k було закріплено μ_k вершин, а сума від-

станей, що зв'язують ЛОр із закріпленими на ними вершинами, була б мінімальною.

Введемо змінну $x_{ik} = 1$, якщо вершина q_i закріплена за ЛОр q_k, $x_{ik} = 0$, у противному випадку. Задачу закріплення вершин за ЛОр запишемо як задачу математичного програмування:

$$\min R = \sum_{i=1}^{n}\sum_{k=1}^{m} r_{ik} x_{ik}\,, \qquad (6)$$

$$\sum_{i=1}^{n} x_{ik} = \mu_k\,, \quad k = \overline{1,m}\,, \qquad (7)$$

$$\sum_{k=1}^{m} x_{ik} = 1\,, \quad i = \overline{1,n}\,. \qquad (8)$$

Умова (7) забезпечує закріплення за кожним ЛОр q_k рівно μ_k вершин. За умовою (8) кожна вершина закріплюється за одним із обраних ЛОр. Критерій (6) відповідає мінімальній оцінці R_w деякої розбивки, отриманій в результаті вирішення задачі (6)-(8), виходячи із заданого варіанта розміщення ОПЕ. Задача (6)-(8) займає проміжне положення між задачею лінійного програмування транспортного типу і задачею про призначення [11].

Вирішення задачі (6)-(8) приводить до одного із двох результатів, що принципово відрізняються. В одному з них закріплення вершин за ЛОр повністю відповідає розбивці $\{Q_k\}_w$. У цьому випадку за кожним логістичним органом q_k закріпилися вершини множини Q_k. Дане рішення відповідає ситуації, коли в розбивці $\{Q_k\}_w$ вершини множини Q відносно ЛОр q_k, $k = \overline{1,m}$, закріпилися найкращим чином і при цьому розбивка $\{Q_k\}_w$ виявилася найкращою щодо прийнятого розташування ЛОр q_k на координатній площині. Таке розташування ЛОр варто вважати стійким. Слід відмітити, що стійке розташування сукупності ЛОр $\{q_k\}$ завжди зв'язується із сукупністю значень $\{\mu_k\}$. При цьому взаємно однозначна відповідність між $\{q_k\}$ і $\{\mu_k\}$ може встановлюватися довільно.

Інший результат вирішення задачі (6)-(8) відповідає ситуації, коли відбувається зміна деяких або всіх множин Q_k, тобто має місце перерозподіл вершин між даними множинами. Нові множини, позначимо їх Q'_k, очевидно утворять розбивку з більш високою оцінкою щільності, тобто $R'_{w'} \le R_w$. Дійсно, оцінка $R'_{w'}$, отримана в результаті вирішення задачі (6)-(8), не може бути більше оцінки R_w, тому що це означало б, що рішення задачі (6)-(8) не є оптимальним, тобто гірше вихідної розбивки $\{Q_k\}_w$. Отже, між оцінками щільності розбивок $\{Q'_k\}_{w'}$ і $\{Q_k\}_w$ повинне виконуватися одне зі співвідношень – $R'_{w'} < R_w$ або $R'_{w'} = R_w$. Співвідношення $R'_{w'} = R_w$ відповідає розглянутій вище ситуації, при якій перерозподіл вершин між множинами Q_k не відбувся, або має місце дві різних розбивки $\{Q'_k\}_{w'}$ і $\{Q_k\}_w$ з рівними оцінками щільності. Співвідношення $R'_{w'} < R_w$ однозначно вказує на те, що вершини між множинами Q_k перерозподілилися, і це привело до покращання оцінки щільності нової розбивки.

У множинах Q'_k нової розбивки залишилися ЛОр, встановлені для множин Q_k вихідної розбивки. Ці ЛОр не відповідають реальним виконавчим елементам множин Q'_k. Тому з'являється можливість обчислити нові місця розташування ЛОр і покращати оцінку щільності $R'_{w'}$. З огляду на перенос ЛОр на нові місця, розбивка $\{Q'_k\}_{w'}$ розглядається як вихідна, а задача (6)-(8) вирішується щодо нових логістичних органів в надії одержати розбивку $\{Q''_k\}_{w''}$ з оцінкою щільності $R''_{w''} < R'_{w'}$.

Перенос ЛОр і вирішення задачі (6)-(8) доцільно повторювати доти, поки знов отримана розбивка не збіжиться з попередньою, прийнятою в якості вихідної. Це буде означати, що отримане стійке розташування ЛОр, що відповідає стійкій розбивці, яку будемо називати локальною щільною розбивкою (ЛЩР). Знайдена стійка розбивка названа локальною, тому що немає підстав вважати, що серед множини розбивок W вона має найкращу оцінку щільності R^*_w, тобто є щільною розбивкою.

Алгоритм вирішення задачі (5), (2), (3) зводиться до одержання ЛЩР. Для цього використовується метод послідовного поліпшення розбивок. Для застосування методу необхідно сформувати вихідну розбивку та визначити ЛОр в її множинах.

В [12] запропоновано як вихідну сукупність ЛОр використовувати m вершин $q_i \in Q$. Такі вершини названі полюсами. В якості полюсів будемо приймати довільну сукупність із m вершин. Зокрема, це можуть бути вершини множини Q з першими m номерами.

Вихідна розбивка отримується шляхом вирішення задачі (6)-(8) відносно прийнятої сукупності полюсів. При цьому в умові (7) значення μ_k зменшується на 1, тому що полюси входять у відповідні множини Q_k. Алгоритм одержання ЛЩР буде включати наступні операції.

1. Задається координатна площина і на ній фіксується розташування вершин множини Q. Координати вершин формуються автоматично за місцем фіксації вершин. Нумерація вершин здійснюється відповідно до послідовності їх фіксації.

2. Обчислюються відстані r_{ij} між вершинами q_i і q_j, формується матриця відстаней R.

3. Задається значення m і відповідно до умови (3) обчислюються величини μ_k, $k = \overline{1,m}$. Величини

μ_k можуть призначатися з дотриманням співвідношення $\sum_k \mu_k = n$.

4. У множині Q виділяється сукупність полюсів, які приймаються в якості вихідних ЛОр і відносно них формується матриця відстаней для вирішення задачі (6)-(8). Для виділення полюсів використовується одне з простих формальних правил [12], або в множині Q вибирається m вершин довільним образом. При необхідності сукупність полюсів може призначатися користувачем.

5. Відносно полюсів вирішується задача (6)-(8) і визначаються множини Q_k вихідної розбивки.

6. Для кожної множини Q_k за виразом (4) визначаються координати ЛОр q_k і формується нова матриця відстаней для вирішення задачі (6)-(8).

7. Відносно ЛОр, отриманих у п.6, вирішується задача (6)-(8), формується нова розбивка.

8. Аналізується результат вирішення задачі (6)-(8). Якщо нова розбивка відрізняється від вихідної, то нова розбивка приймається в якості вихідної і виконуються п. 6 і 7. Якщо нова і вихідна розбивки збігаються, то це означає, що отримана локальна щільна розбивка.

Висновки

1. Розроблений алгоритм рішення шуканої задачі за умови визначеної кількості ЛОр дозволяє формувати таку ж кількість локальних щільних підмножин РС або на підставі визначеної кількості локальних щільних підмножин РС визначати кількість ЛОр.

2. Розроблено алгоритм одержання локальних компактних розбивок множини РС, в основу якого покладений метод послідовного поліпшення розбивок.

3. Алгоритм є ефективним інструментом для наближеного рішення задачі розбивки множини розгалужених споживачів на підмножини рівної потужності з мінімальною сумарною оцінкою щільності.

Список літератури

1. Петров, Э.Г. Территориально распределенные системы обслуживания / Э.Г. Петров, В.П. Писклакова, В.В. Бескоровайный. – К.: Техника, 1992. – 208 с.

2. Комяк, В.М. Алгоритм оптимізації розміщення пожежних депо при проектуванні нових районів міст (реконструкції існуючих) [Текст] / В.М. Комяк, А.Г. Косе, О.К. Пандорін, О.В. Панкратов // Прикладна геометрія та інженерна графіка. – К.: КНУБА, 2000. – Вип. 68. – С. 62-64.

3. Годлевский, М.Д. Принципы структурно-параметрического синтеза модели транспортно-складской системы транснациональной логистической компании [Текст] / В.В. Дыбская // Вестник НТУ "ХПИ".- 2009.- №10.- С. 23-30.

4. Годлевский, М.Д. Модель статической задачи структурного синтеза корпоративной информационно-вычислительной системы [Текст] / М.Д. Годлевский, В.Ю. Воловщиков // Восточно-европейский журнал передовых технологий. – 2006. – № 2/2 (20). – С. 110-113.

5. Свирщева, Э.А. Структурный синтез неизоморфных систем с однородными компонентами / Э.А. Свирщева. – Х.: ХТУРЭ, 1998. – 256 с.

6. Бескоровайный, В.В. Модификация метода направленного перебора для синтеза топологии систем с радиально-узловыми структурами [Текст] / В.В. Бескоровайный // АСУ и приборы автоматики. – 2003. – Вып. 123. – С. 110-116.

7. Бескоровайный, В.В. Генетический алгоритм структурной оптимизации централизованных многоуровневых ИВС [Текст] / В.В. Бескоровайный, З.А. Имангулова // Вестник ХГПУ: Новые решения в современных технологиях. – 2000. – Вып. 83. – С. 4-7.

8. Годлевский, М.Д. СППР управления развитием корпоративной информационно-вычислительной системы при нечеткой исходной информации [Текст] / М.Д. Годлевский, В.Ю. Воловщиков // Восточно-европейский журнал передовых технологий. – 2006. – № 2/2 (26). – С. 3-6.

9. Бескоровайный, В.В. Оценка оптимального количества подсистем при проектировании систем с регулярно распределенными элементами [Текст] / В.В. Бескоровайный // АСУ и приборы автоматики. – 2003. – Вып. 122. – С. 141-144.

10. Кристофидес Н. Теория графов. Алгоритмический подход. – М.: Мир, 1978. – 432 с.

11. Дегтярев, Ю.И. Методы оптимизации. – М.: Советское радио, 1980. – 272 с.

12. Морозова, Л.В. Формування топології логістичної системи [Текст] / Л.В. Морозова // Системи управління, навігації та зв'язку. - 2016. - Вип. 1(37). – С. 32-37.

Надійшла до редколегії 1.02.2017

Рецензент: д-р екон. наук, доц. К.А. Фісун, Національна академія Національної гвардії України, Харків.

.

ФОРМИРОВАНИЕ СИСТЕМЫ ЛОГИСТИЧЕСКИХ ОРГАНОВ ДЛЯ ОБСЛУЖИВАНИЯ РАЗВЕТВЛЕННЫХ ПОТРЕБИТЕЛЕЙ

Л.В. Морозова

Предлагается алгоритм решения задачи по формированию системы логистических органов для обслуживания разветвленных потребителей. Решение включает разбивку исходного множества разветвленных потребителей на плотные подмножества и размещение в этих подмножествах логистических органов.

***Ключевые слова**: разветвленные потребители, логистический орган, система логистических органов, плотные множества разветвленных потребителей, координатная плоскость.*

FORMATION OF SYSTEM OF LOGISTICAL SERVICE BODIES FOR EXTENSIVE CONSUMERS

L.V. Morozova

The algorithm of solution to the problem of formation of system of logistical agencies for the maintenance of extensive consumers. The solution includes a breakdown of the initial set of branched consumers on a dense subset and placement in these pameginam logistics bodies.

***Keywords:** branched-chain consumers, on logistics, system logistics bodies, dense many branched consumers coordinate plane.*

УДК 621.391

O.L. Nedashkivskiy

State University of Telecommunications, Kiev

ESTIMATION OF QUALITY OF INTERNET ACCESS SERVICES IN UKRAINE

A leading role in the grant of information to the users is occupied by a global network - Internet, based on IP protocol. The attempt of estimation of quality of Internet services in Ukraine is carried, and also the tasks of researches that will show out our country into deserving place in rating of leading countries of the world on Internet services are set. The solution of these problems will allow the Ukrainian segment of Internet to occupy a leading provision in all rating, and national IT industry will become like that magic stick that will revive all our economy.

Keywords: *Internet, access, quality of services, rating.*

Introduction

Rapid development of science and technique, successes in information technologies, openness of borders, between the states and people resulted in all greater globalization. In these terms success of any country, as well as separately any man depends on availability, timeliness, plenitude and rightness of necessary information. Thus it should be noted that formal this rule is not newly - a man that owned greater information at all times was let in on the ground as compared to all other. Changed, and more correct to say added, only methods of collection, storage and information transfer.

Obviously, that a leading role in the grant of information to the users is occupied by a global network - Internet, based on IP protocol. Thus most dynamic is a segment mobile the Internet.

Statement of the problem and its solution

It is known that IP protocol corresponds to the third level of OSI model [1] with the performance of basic objective are routing and transmissions of IP packages. We will conduct a clear border between "Internet services" and by "services base on Internet".

Internet services we will name the transmission of packages by mean or through the Internet, here clients are levels from fourth and higher of OSI model.

By services base on Internet we will count services that get to eventual application. Thus any services base on Internet is formed from a set of protocols of levels from fourth till the seventh of OSI model and has two interfaces: one with eventual application, second with an Internet network. Generally known, that an Internet does not have single administrator and single compatible basis (base) it is possible to name the first two levels of OSI model that.

Quality of Internet services it is possible in the first approaching to estimate on by large-sized global criteria:

a) index of availability, that will be formed coming from potential (zone of coverage) and real (amount of users) penetration;

b) minimum, middle and peak values access to the Internet speed, that will be formed coming from the potentially attainable (theoretical features of concrete technology of access and communication of data) and really attainable (practical realization is in the concrete terms of surroundings) values of the got results.

Structure and dynamics of Internet market in Ukraine

On the state on the end of September, 2015 from data of Government service of statistics of Ukraine [2] volume of profits from the grant of access to the Internet, IP-telephony and mobile communication is almost 73% from all telecom and mail services profits.

As be obvious from a Table 1, during five last years the total volume of profits grows insignificantly. It is expedient to analyze the dynamics of separate constituents.

A stake of mobile telephony is dominant (60,3%), although during this period diminished from 61,7% to 60,3%, that talks both about a market saturation and about absence of fresh drivers of height in the conditions of the present crisis phenomena.

The stake of IP-telephony diminished headily from 0,3% to 0,04%. It is possible to explain by, that IP-telephony as independent service stops to exist, it becomes technological component part of other complex services or dissolves in other services, for example in Internet access both mobile and fixed.

Most interesting is a dynamics of Internet access raise: the stake of Internet access increases on 1% annually. As be obvious from a Table 1, this service compensates falling of profits both from IP-telephony and from the being sated market of mobile communication.

The analysis of official statistical data allows to do next conclusions:

a) raise of profits from the Internet access for the last five years, even in the conditions of the crisis phenomena, increased on 9,3%, while indexes on industry increased only on 4,2%, and an economy showed a negative dynamics on the whole;

Table 1

Structure of earnings from mail and communication services in Ukraine

Year	Prof. all, mill. hrn	Internet access		IP-telephony		Mobile		Total %
		mill. hrn	%	mill. hrn	%	mill. hrn	%	
2015	41377	5193	12,5	16,9	0,04	24957,3	60,3	72,9
2014	52434	6190	11,8	92,6	0,2	31566,3	60,2	72,2
2013	52492	5697	10,9	136,3	0,3	31405,8	59,8	70,9
2012	52271	5402	10,3	135,8	0,3	31535,2	60,3	70,9
2011	50281	4749	9,4	161,2	0,3	31027,9	61,7	71,5

б) if the dynamics of receipt of profits from communication services will be saved, in what it is possible to express a confidence, then in the nearest 3-5 years the locomotive of increase of profits from the connection services there will be Internet access services.

Features of development of Internet services in Ukraine

For the estimation of current status, potential and ways of development of Internet network in Ukraine we will analyze the most known rating.

According to data of Internet Live Stats [3] for 2014 Ukraine is on 32 places on the amount of users. An annual increment was 9% while a mean value in the whole World was 6,6%, that talks that Internet in Ukraine develops passing ahead rates.

A maximal height is observed in developing countries (Burundi, Eritrea for 17%), and minimum in Sweden, Iceland for 1%.

A rise in the United States of America, the motherland the Internet, is 7%.

A part of Internet Live Stats rating is driven in Table 2.

From the Table 2 evidently, that the Ukrainian segment of Internet develops quickly enough, limit of satiation yet far.

Thus, if to notice that even in the USA and South Korea, where penetration (relation of Internet users from the general population of country) makes about 90%, ready a rise makes about 7-8%, that can be done conclusion, that in the near future satiations in Ukraine is not expected and it will be necessary to decide many tasks and problems, related to the height and development the Internet in Ukraine.

Table 2

Internet users by country (2014)

Rank	Country	Internet Users	1 Year Growth %	Total Country Population	Penetration (% of Pop. with Internet)
1	China	641601070	4%	1393783836	46,03%
2	United States	279834232	7%	322583006	86,75%
.....	.....	.....	.....	.....	.....
12	South Korea	45314248	8%	49512026	91,52%
.....	.....	.....	.....	.....	.....
32	**Ukraine**	**16849008**	**9%**	**44941303**	**37,49%**
.....	.....	.....	.....	.....	.....
47	Sweden	8581261	1%	9631261	89,10%
.....	.....	.....	.....	.....	.....
60	Hong Kong SAR	5751357	9%	7259569	79,22%
.....	.....	.....	.....	.....	.....
95	Lithuania	2113393	2%	3008287	70,25%
.....	.....	.....	.....	.....	.....
135	Iceland	321475	1%	333135	96,50%
.....	.....	.....	.....	.....	.....
159	Burundi	146219	17%	10482752	1,39%
.....	.....	.....	.....	.....	.....
173	Eritrea	59784	17%	6536176	0,91%
.....	.....	.....	.....	.....	.....
198	Niue	617	5%	28	47,2%
-	МИР	2817874294	6,6%	7096625556	39,71%

Comparative estimation of connection speed to Internet

Another known way of estimation of rating of Internet quality, used by the Akamai Technologies company, there is Internet access speed [4]. In the report of State of the Internet it is talked for the first quarter of 2014, that middle Internet access speed (under middle Internet access speed will understood meddle value of great number of the individual independent measuring produced during the investigated period by plenty of end user in the direction of different test servers in by the help of WEB-application like Speedtest [5] and grouped on directions) in the world is 3,9 Mbps, that on 1,8% more as compared to the result of previous quarter and on 24% more than by a year before (Table 3).

The first five countries with the most rapid Internet looked like the following: South Korea (68,5 Mbps), Hong Kong (66,0 Mbps), Singapore (57,7 Mbps), Israel (57,6 Mbps) and Japan (Mbps). Estonia, Russia, Ukraine, Armenia, Kazakhstan and Georgia, occupied in the world rating 31, 35, 36, 54, 57 and 58 places accordingly. Kyrgyzstan, Tajikistan and Belarus, a bit fell behind, appearing on 71, 74 and 75 places.

It is also possible to mark the active height of the so-called high broadband (>10 Mbps) Internet access in the with values from 10 Mbps and higher (Table 4). Penetration of high broadband in the world overcame a border in 20% general stake of all connections, showing a height at the level of 9,4 %.

In speed connections of mobile devices (including Wi-Fi) (Table 5) leadership in the world market belongs to South Korea. A middle index in country is estimated by experts in 14,7 Mbps.

It is should especially mark pleasant fact, that according to the results in Europe Ukraine (Table 5) leads on the index of the highest middle speed of mobile connection (networks of the second and third generation, Wi-Fi) - 7,3 Mbps. Middle peak speed of mobile connection in Ukraine is 28,4 Mbps. In addition, in Ukraine the stake of >4 Mbps connections is 89%% of all connections - again the highest index in Europe.

Table 3

Average connection speed by country/region (first ten)

Rank	Country/Region	Q1 14 Avg. Mbps	QoQ Change	YoY Change
-	Global	3,9	1,8%	24%
1	South Korea	23,6	8%	145%
2	Japan	14,6	12%	29%
3	Hong Kong	13,3	8,5%	24%
4	Switzerland	12,7	5,8%	26%
5	Netherlands	12,4	0,3%	28%
6	Latvia	12	15%	26%
7	Sweden	11,6	6,6%	30%
8	Czech Republic	11,2	-1,9%	24%
9	Finland	10,7	18%	37%
10	Ireland	10,7	4,3%	47%

Table 4

High broadband (>10 mbps) connectivity (first ten)

Rank	Country/Region	% above 10 Mbps	QoQ Change	YoY Change
-	Global	21%	9,4%	65%
1	South Korea	77%	8,2%	146%
2	Japan	54%	11%	32%
3	Hong Kong	45%	7,3%	49%
4	Switzerland	44%	-3%	52%
5	Netherlands	43%	14%	30%
6	Latvia	37%	15%	26%
7	Sweden	36%	10%	62%
8	Czech Republic	35%	7,6%	81%
9	Finland	35%	-0,5%	73%
10	Ireland	34%	-9,3%	54%

Table 5

Average and average peek connection speeds, broadband (>4 mbps) connectivity for mobile connections by country/region

Country/Region	Q1 14 Avg. Mbps	Q1 14 Peak Mbps	% above 4 Mbps
AFRICA			
Egypt	2	11,6	2,5%
Morocco	1,8	14,6	1,1%
South Africa	1,7	6	4,8%
ASIA			
China	4,8	12,2	57%
Hong Kong	4,9	23,4	42%
India	1,3	8,7	2,7%
Indonesia	2	10,8	3,5%
Iran	2	5	3,9%
Japan	5,7	47,3	61%
Kazakhstan	2	7,8	1,7%
Kuwait	3,5	33,1	17%
Malaysia	2,3	19,8	7,6%
Pakistan	1,5	14,7	2,8%
Singapore	3,6	23,2	19%
South Korea	14,7	41,3	78%
Sri Lanka	2,3	23,7	3,6%
Taiwan	3,4	27,8	13%
Thailand	2	35,1	4,6%
Vietnam	1,1	6,5	0,1%
EUROPE			
Austria	6,1	32,2	63%
Belgium	3,2	9,2	17%
Croatia	2,2	9,1	1,8%
Czech Republic	4,9	18,6	58%
Denmark	7	30,4	84%
France	5,9	34	66%
Germany	2,9	14,8	11%
Hungary	2,9	16,6	10%
Ireland	5,1	27,6	40%
Italy	4,6	36,6	47%
Lithuania	3,4	24,4	20%
Moldova	3,8	17,9	26%
Netherlands	3,3	16	17%
Norway	4,3	17,9	36%
Poland	3,9	24,7	35%
Romania	3,2	24,5	13%
Russia	6,1	35,1	63%
Slovakia	7	37	71%
Slovenia	3,5	13,9	26%
Spain	4,8	27,3	46%
Sweden	6,6	34,3	81%
Turkey	2,7	21,1	5,3%
Ukraine	**7,3**	**28,4**	**89%**
United Kingdom	5,6	34,6	53%
NORTH AMERICA			
Canada	6,3	21,5	60%
El Salvador	2,3	12,8	3,4%
United States	5,5	15,1	33%
OCEANIA			
Australia	4,6	14,2	40%
New Zealand	3	14,3	25,0%

End of table 5

SOUTH AMERICA			
Argentina	1	6,6	1,6%
Bolivia	1,2	7,1	0,1%
Brazil	1,2	9,3	0,4%
Chile	1,4	11,2	1,4%
Colombia	1,7	9,1	0,2%
Paraguay	1,4	8,5	0,1%
Uruguay	1,6	11,1	3,2%
Venezuela	4,3	19,9	69%

High evaluation indexes on access speed and the subzero indexes of penetration can be explained by that at the construction of new networks for Internet access the newest technologies are used in Ukraine, and part of out-of-date or low-speed technologies is extremely insignificant.

In addition in the conditions of the crisis phenomena as a rule choice done: a) on highly profitable projects; b) on the real effective demand; c) on withholding of existent clients, that together results in that speeds of tariff plans grow, profits fall, networks do not develop in breadth (expansion in regions).

Thus, looking on the quite good results of level of development the Internet in Ukraine, we should consider necessary to distinguish the chain of problems:

a) digital divide of territories;

b) unbalanced of capital investments;

c) unfair competition or her complete absence.

The solution of these problems will allow the Ukrainian segment of Internet to occupy a leading provision in all rating, and national IT industry will become like that magic stick that will revive all our economy.

Conclusion

1. The market of Internet access in Ukraine (9,3%) grows quicker, than other communication services (4,2%), but yet it far to prevailing (12,5%). Mobile communication (exactly due to the mobile Internet that in official statistics in any way is not distinguished) continues (60,3%) to lead.

2. In spite of sure height there is the Internet of audience in Ukraine (9%), passing ahead a middle World index (6,6%), penetration remains very poor (37,49%), that can be explained by the large unevenness of both development of territories (cities/village) and level of real solvency of corresponding population.

3. According to rating of Internet access speed, Ukraine occupies 36 place in a general rank-list among the countries of the World and first in Europe on speed of mobile Internet, that can be considered an unexpected surprise creating the real pre-conditions for the achievement of the high world rating of Internet services of our country.

References

1. ISO/ IEC7498-1: 1994, available to: http://www.iso.org/iso/catalogue_detail.htm?csnumber=20269.

2. Revenues from services provided by post and communication, I HY, 2015, available to: www.ukrstat.gov.ua.

3. Internet Users by Country (2014), available to: http://www.internetlivestats.com./internet-users-by-country.

4. Average Global Connection Speed Up 14% According to Akamai's 'Third Quarter, 2015, State of the Internet Report', available to: https://www.akamai.com/us/en/about/ news/press/2015-press/akamai-releases-third-quarter-2015-state-of-the-internet-report.jsp.

5. The Global Broadband Speed Test, available to: http://www.speedtest.net.

Надійшла до редколегії 1.12.2016

Рецензент: д-р техн. наук, проф. А.І. Семенко, Державний університет телекомунікацій, Київ.

ОЦІНКА ЯКОСТІ НАДАННЯ ПОСЛУГ МЕРЕЖІ ІНТЕРНЕТ В УКРАЇНІ

О.Л. Недашківський

Все більш провідну роль у наданні інформації користувачам займає глобальна мережа - Інтернет, яка базується на основі протоколу IP. У статті виконано спроба оцінки якість Інтернет послуг в Україні, а також вказані проблеми майбутніх досліджень, проведення яких виведуть нашу країну на гідне місце в рейтингах провідних країн світу по послугах мережі Інтернет. Вирішення вказаних проблем дозволить українському сегменту мережі Інтернету не тільки зайняти лідируюче положення у всіх рейтингах, а й перетворити національну IT індустрію в ту чарівну паличку, яка оживить всю нашу економіку.

Ключові слова: *Інтернет, доступ, якість послуг, рейтинг.*

ОЦЕНКА КАЧЕСТВА ПРЕДОСТАВЛЕНИЯ УСЛУГ СЕТИ ИНТЕРНЕТ В УКРАИНЕ

А.Л. Недашковский

Все более ведущую роль в предоставлении информации пользователям занимает глобальная сеть - Интернет, которая базируется на основе протокола IP. В статье выполнена попытка оценки качества Интернет услуг в Украине, а также указаны проблемы будущих исследований, проведение которых выведут нашу страну на достойное место в рейтингах ведущих стран мира по услугам сети Интернет. Решение указанных проблем позволит украинскому сегменту сети Интернета не только занять лидирующее положение во всех рейтингах, но и превратить национальную ИТ индустрию в ту волшебную палочку, которая оживит всю нашу экономику.

Ключевые слова: *Интернет, доступ, качество услуг, рейтинг.*

УДК 681.324

І.П. Саланда[1], О.В. Барабаш[2], А.П. Мусієнко[2]

[1] *Східноєвропейський національний університет імені Лесі Українки, Луцьк*
[2] *Київський національний університет імені Тараса Шевченка, Київ*

СИСТЕМА ПОКАЗНИКІВ ТА КРИТЕРІЇВ ФОРМАЛІЗАЦІЇ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ ЛОКАЛЬНОЇ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ РОЗГАЛУЖЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖ

Запропоновано показники та критерії синтезу функціонально стійкої розгалуженої інформаційної мережі на основі графових моделей. За допомогою запропонованих показників та критеріїв можна оцінювати та порівнювати різні структури мереж з високим рівнем зв'язності, а також застосовувати їх для формування методики оптимального використання надмірності системи при парируванні наслідків позаштатних ситуацій. Дані показники доцільно використовувати для сучасних та перспективних мереж 5 покоління(5G), які є безпровідними, динамічними, самоорганізуючими, оскільки вони дозволяють під час реструктуризації враховувати елементи, пошкодження яких не впливає на локальну функціональну стійкість мережі.

Ключові слова: *інформаційні мережі, функціональна стійкість, тотальна зв'язність, мережі 5G.*

Вступ

Дослідження існуючих науково-обґрунтованих підходів підвищення ефективності складних технічних систем, до яких повною мірою відносяться й розгалужені інформаційні мережі (РІМ) дозволили зробити висновок про формування за останні роки нового пріоритетного підходу, пов'язаного із забезпеченням системі властивості функціональної стійкості.

Постановка проблеми в загальному вигляді. Аналіз функціонування розгалужених інформаційних мереж показав, що елементи мереж, до яких відносяться вузли комутації та лінії зв'язку між ними, піддаються безлічі внутрішніх (відмови, збої, помилки обслуговуючого персоналу) і зовнішніх (пошкодження, перешкоди, несанкціонований доступ) дестабілізуючих факторів.

Відомі властивості інформаційних мереж, такі як стійкість, надійність, живучість, відмовостійкість характеризують функціонування мереж при впливі відмов і пошкоджень, але не дозволяють в повній мірі описати процеси функціонування в умовах значних руйнувань, впливу потоків відмов і несправностей , можливих навмисних впливів, в тому числі і терористичних.

Тому, доцільно розглянути нову властивість РІМ – функціональну стійкість.

Під функціональною стійкістю (ФС) об'єкта будемо розуміти його властивість зберігати протягом заданого часу виконання своїх основних функцій в межах, встановлених нормативними вимогами, в умовах протидії, а також впливу потоків відмов, несправностей і збоїв [1].

Об'єктивне дослідження функціональної стійкості розгалуженої інформаційної мережі неможливе без кількісної оцінки цієї властивості. Різноманітність інформаційних мереж, процесів руйнування та відновлення, складність найбільш повних моделей мереж зв'язку та інші обставини дозволяють зробити висновок про неможливість створення єдиного показника ФС для всіх мереж і їх елементів.

Математична формалізація функціональної стійкості мереж є першим науково-обґрунтованим кроком створення методологічних основ забезпечення функціональної стійкості РІМ. Для наукового обґрунтування та математичної формалізації функціональної стійкості необхідно дослідити формалізацію стійкості взагалі.

Більш перспективним щодо цього є підхід до розгляду стійкості, що використовує внутрішні резерви системи на основі існуючої апаратної, програмної, часової та інформаційної надмірності.

Разом з тим, нечисленні роботи у галузі забезпечення функціональної стійкості складних технічних систем не дають змоги виробити єдині підходи та започаткувати теоретичні основи забезпечення функціональної стійкості для РІМ. Проблема полягає у відсутності стандартизованого понятійного апарату функціональної стійкості.

Аналіз основних публікацій. Поняття функціональної стійкості вперше було введено Машковим О. А., який запропонував підхід щодо забезпечення цієї властивості в динамічних системах на основі перерозподілу наявної надмірності [2]. Запропонований підхід базується на принципах комплексного забезпечення спостережливості, керованості та ідентифікації динамічних об'єктів. Однак для складних організаційних систем даний апарат неприйнятний.

В роботах Кравченка Ю. В. [3] пропонується дещо інший підхід щодо визначення та забезпечення

функціональної стійкості для систем спеціального призначення, заснований на вирішенні оптимізаційної задачі з застосуванням матроїдних структур. Проте, такий підхід є вузькоспеціалізованим і надто складним для реалізації внаслідок труднощів повного опису елементів та параметрів РІМ у термінах матроїдів.

Більш близьким можна вважати підхід, запропонований у роботах Барабаша О. В., зокрема у [1, 6, 7, 8], у яких пропонуються показники та критерії для побудови стійких розподілених інформаційних систем. Даний підхід базується на оцінках зв'язності графів мережі.

Поняття зв'язності графів грає фундаментальну роль в аналізі та синтезі структур функціонально стійких інформаційних мереж. Проте аналіз відомих характеристик зв'язності показав, що ці характеристики в деяких випадках є малоефективними в задачах синтезу ФС мереж [9, 10]. У зв'язку з цим виникла необхідність розробки нових характеристик зв'язності, які б дозволили синтезувати графи структур інформаційних мереж з високим рівнем функціональної стійкості.

Отже, проблема визначення показників та критеріїв функціональної стійкості розгалуженої інформаційної мережі потребує обґрунтування відповідних залежностей і підходів та залишається актуальною.

Метою статті є розробка системи показників і критеріїв для формалізації процесів забезпечення функціональної стійкості розгалуженої інформаційної мережі.

Основна частина

Обравши за основу підхід, запропонований у [1] відзначимо, що особливий інтерес в теорії функціональної стійкості РІМ представляє показник зв'язності – ω(λ), тобто найменше число вершин (ребер), видалення яких призводить до незв'язності або одновершинного графа.

В результаті аналізу існуючих характеристик зв'язності розроблено класифікацію характеристик зв'язності, яка максимально враховує усі обмеження та вимоги до структури мережі (рис. 1).

Проте, при пошкоджені деяких вузлів або ліній комутації мережі важливо знати локальну зв'язність між вузлами, які знаходяться на певній відстані від пошкоджених елементів. Великий інтерес становлять графи мережі, в яких пошкодження окремих елементів не впливають на локальну зв'язність між іншими вузлами.

Вибір нижче наведених характеристик зв'язності визначався двома обставинами:

- існуючими показниками функціональної стійкості [6, 7];
- класифікацією характеристик зв'язності [1, 4] (рис. 1).

1. Тотальна зв'язність.

У зв'язку з цим доцільно ввести в розгляд новий показник функціональної стійкості – тотальну (k, ω)-зв'язність [4], де kчисло елементів оптимального руйнування ω-зв'язного графа.

Вперше поняття «тотальнозв'язного» графа зустрічається в роботі [4].

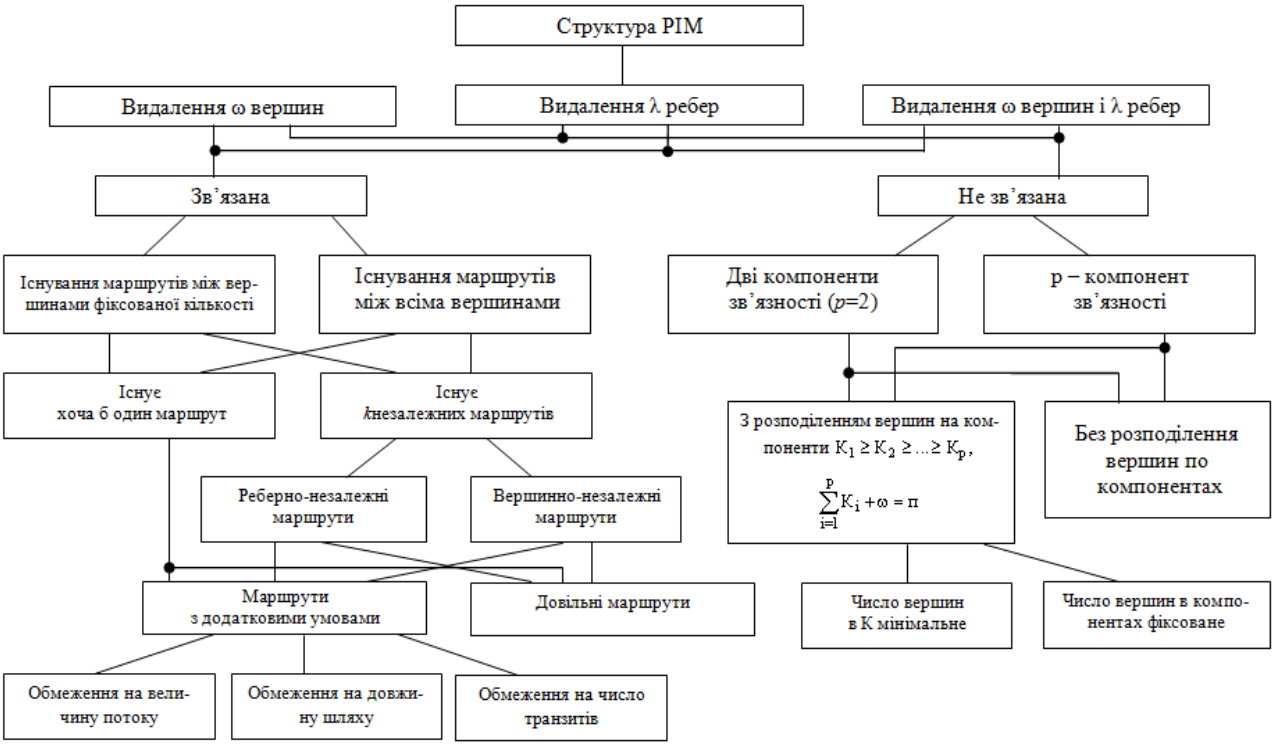


Рис. 1. Класифікація характеристик зв'язності структури РІМ

Введемо деякі означення та позначення:

ω-поєднаність – максимальне число вершино незалежних маршрутів між будь-якою парою вершин графа[5];

λ-сплетеність – максимальне число реберно незалежних маршрутів між будь-якою парою вершин графа[5];

$G[v_x]$ – множина вершин, суміжних з v_x в графі G;

$G^z[v_x]$ – множина вершин, які знаходяться на відстані z від вершини v_x.

Граф G(V, L) ω-зв'язний – називається (k, ω)-тотально зв'язним, якщо при видалені будь-яких k ($k < \omega$)вершин $\{v_i\}$ з графа будь-яка пара вершин із множини $V \setminus (\{v_i\} \cup G[\{v_i\}])$ ω-поєднана в підграфі $G'(V-\{v_i\}, L^i)$ [4].

Тобто, нас цікавитимуть мережі, які після видалення k вузлів комутації зберігають задану зв'язність, крім одиничного околу видалених вузлів.

2. Тотальна реберна зв'язність.

При синтезі структури мережі ненадійними елементами можуть бути не лише вузли комутації, а й лінії зв'язку.

Тому становлять цікавість мережі, які зберігають заданий рівень ФС при видалені ребер.

Граф G(V, L) ω-зв'язний – називається (k, λ)-тотально реберно зв'язним, якщо при видалені будь-яких k ($k < \lambda$) ребер $\{l_{ij}\}$ в суграфі $G'(V, L \setminus \{l_{ij}\})$ будь-які дві вершини із множини $V\setminus(\{v_i\}U\{v_j\})$ λ-сплетені, тобто λ-реберно зв'язні [4].

Іншими словами, розглядатимемо мережі, вузли яких після видаленняk ліній зв'язку залишаються λ-сплетеними, крім інцидентних видаленим лініям.

3. Показники локальної функціональної стійкості структури.

1.Число (k, ω) тотальної зв'язності – максимальне число вершин, видалення яких разом з інцидентними ребрами не змінює локальної ω-зв'язності вершин не суміжних з видаленими.

2. Число (k, λ) реберної тотальної зв'язності – оптимальне число ребер, видалення яких не впливає на локальну λ-зв'язність вершин неінцидентних видаленим ребрам.

Для розгалужених інформаційних мереж важко встановити тотальну зв'язність, оскільки необхідно перевірити на локальну зв'язність безліч вершин. Щоб уникнути цієї проблеми досить скористуватись наступними критеріями.

4. Критерії тотальної зв'язності:

1) структура буде (k, ω)-тотально зв'язною тоді і лише тоді, якщо для будь-якої множини вершин $V'=(v_1, v_2,\ldots,v_k)\subset V$ ($k<\omega$) в підграфі $G'(V- V', L')$ будь-яка пара вершин із підмножини $G^2[V']$ ω-поєднана в G'[4];

2) структура буде (k, λ)-тотально реберно зв'язною тоді і лише тоді, якщо для будь-якої множини ребер $L'=\{l_{ij}\}\subset L$, $|L'|=k$, ($k<\lambda$) в суграфі G'(V, L\L') будь-яка пара вершин із підмножини $G[\bigcup_{i,j=1}^{k}(v_i U v_j)]$ λ-сплетена в G[4].

5. Обґрунтування даних показників.

Тотальна зв'язність (k, ω) характеризує максимально можливе число відмов вузлів комутації, при якому мережа залишається ω-локально зв'язною.

Тотальна реберна зв'язність (k, λ) характеризує максимально можливе число ліній зв'язку, після відмови яких, мережа залишається λ-локально зв'язною.

Іншими словами, дані показники дозволяють врахувати елементи, пошкодження яких не впливає на локальну зв'язність між іншими елементами, не суміжними з видаленими.

Врахувавши понятійний апарат ФС та проаналізувавши сказане вище можна сформулювати критерій ФС.

6. Критерій локальної функціональної стійкості.

Структура буде локально функціонально стійкою, якщо показники зв'язності задовольняють наступним умовам:

$$\{\omega(G) \geq 2 \bigcap k > 1\} \bigcup \{\lambda(G) \geq 2 \bigcap k > 1\}.$$

Розглянуті критерії не дозволяють створити ефективні алгоритми для перевірки тотальної зв'язності. Однак в більшості випадків достатньо отримати нижню оцінку для k при заданій вершинній та реберній зв'язності.

Наведемо алгоритми отриманнянижньої оцінки тотальної зв'язності.

7. Алгоритм знаходження нижньої оцінки числа видалених вершин.

Нехай заданий ω-зв'язний граф G(V, L). Виділимо в цьому графа пару несуміжних вершин v_x, v_y і перевіримо їх ω-з'єднаність при умові, що видалені вершини не суміжні з v_x іv_y.

Алгоритм I.

Крок 1. Для вершин v_x іv_y знайдемо $G^2[v_x]$ і $G^2[v_y]$.

Крок 2. Якщо v_x належить $G^2[v_y]$ (v_y відповідно $G^2[v_x]$), то

$$\tau := |G[x] \cap G[y]|,$$

із графа G видалити вершини

$$G[v_x] \bigcap G[v_y].$$

Переходимо на крок 1, інакше на крок 3.

Крок 3. Між вершинами $G^2[v_x]$ і $G^2[v_y]$ знайдемо максимальне число вершино незалежних ланцюгів, які з'єднують ці множини, причому ланцюги не повинні перетинатися і по кінцевих вершинах.

Крок 4. В $G^2[v_x]$ і $G^2[v_y]$ виберемо підмножини вершин V_x і V_y, в яких починається і закінчується побудова незалежних ланцюгів.

Крок 5. Для кожної вершини

$$v_i \in G[v_x] \ (v_j \in G[v_y])$$

знайдемо значення

$$d_{v_i} = \tau_{V_x}(v_i) - 1;$$

$$d_{v_j} = \tau_{V_y}(v_j) - 1,$$

де $\tau_{V_x}(v_i)$ – число вершин із V_x, суміжних з v_i,

$$k_x := \min(\min(d_{v_i}), |V_x| - (\omega - \tau)),$$

$$k_y := \min(\min(d_{v_j}), |V_y| - (\omega - \tau)),$$

$$k' := \min(k_x, k_y).$$

Крок 6. Знайдемо локальну зв'язність $\delta(v_x,v_y)$ між вершинами v_x іv_y.

Обчислимо кінцеві значення kпри заданій зв'язності ω між вершинами v_x і v_y:

$$k_{x,y}=k'+(\delta(v_x,v_y) - (\omega-\tau)).$$

Нижня оцінка для числа видалених вершин між вершинами v_x,v_y в умовах збереження ω-зв'язності цих вершин знайдена.

Крок 7. $k \le \min\limits_{v_x,v_y \in V} k_{x,y}$.

8. Обґрунтування алгоритму.

Якщо $\tau \ge \omega$, то видалення будь-яких вершин, не суміжних з v_x іv_y, не знижує ω-поєднаність цих вершин.

Нехай $\tau<\omega$, тоді очевидно, що можливе число видалених вершин не більше $|V_x| - (\omega - \tau)$.

З іншого боку при видалені $\tau_{V_x}(v_i)$ вершин із V_x може порушитися зв'язність вершин v_i з v_x і, відповідно

$$d_{v_i} = \tau_{V_x}(v_i) - 1.$$

Таким чином, k_xне більше $\min\limits_i d_{v_i}$.

Відповідно, $k \le \min(k_x, k_y)$, і якщо локальна зв'язність $\delta(v_x,v_y)$ більша ω, то очевидно

$$k_{x,y}=k'+(\delta(v_x,v_y) - (\omega-\tau)).$$

Звідси випливає, що нижня оцінка kдля (k, ω)-тотальної зв'язності не перевищує $\min\limits_{v_x,v_y \in V} k_{x,y}$.

Аналогічним чином можна знайти нижню оцінку k для (k, λ)-тотальної реберної зв'язності.

9. Алгоритм знаходження нижньої оцінки числа видалених ребер.

Нехай заданий λ-реберно-зв'язний граф G(V, L).

Виділимо в цьому графа пару несуміжних вершин v_x,v_y і перевіримо їх λ-сплетеність.

Алгоритм II.

Крок 1. Для несуміжних вершин v_x іv_y знайдемо $G[v_x]$ і $G[v_y]$.

Крок 2. Між вершинами $G[v_x]$ і $G[v_y]$ знайдемо максимальне число λ-реберно-незалежних ланцюгів, які з'єднують ці множини.

Крок 3. Для кожної вершини $v_i \in G[v_x]$ $(v_j \in G[v_y])$ знайдемо значення

$$l_{v_i} = \sigma_{V_x}(v_i) - 1$$

$$l_{v_j} = \sigma_{V_y}(v_j) - 1,$$

де $\sigma_{V_x}(v_i)$ $(\sigma_{V_y}(v_j))$ – число незалежних ланцюгів, з кінцем у вершині v_i (v_j), суміжних з v_i,

$$k_x := \min_i(l_{v_i}),$$

$$k_y := \min_j(l_{v_j}),$$

$$k' := \min(k_x, k_y).$$

Крок 4. Знайдемо локальну реберну зв'язність $\gamma(v_x,v_y)$ між вершинами v_x іv_y. Тоді

$$k_{x,y}=k'+(\gamma(v_x,v_y) - \lambda).$$

Крок 5. Оцінка k для всього графа G обчислюється за формулою

$$\min_{v_x,v_y \in V} k_{x,y}.$$

Обґрунтування запропонованого алгоритму аналогічне попередньому.

Дослідження розроблених показників і критеріїв показали, що основним методом підвищення локальної функціональної стійкості структури розгалуженої інформаційної мережі є підвищення зв'язності структури за рахунок введення надлишкових ліній зв'язку.

Висновки

В роботі наведена найбільш повна класифікація характеристик зв'язності інформаційних мереж, що враховує різні особливості та обмеження.

Введено в розгляд нові показники та критерії оцінки локальної функціональної стійкості розгалуженої інформаційної мережі.

Запропонований підхід комплексно використовує зв'язність структури і пропонує алгоритми розрахунку оптимального руйнування заданого числа елементів.

Дані показники та критерії доцільно використовувати для сучасних та перспективних мереж 5 покоління (5G), які є безпровідними, динамічними, самоорганізуючими. До них постійно підключаються та вводяться абонентські пристрої, які не лише є кінцевими, а й виконують функції маршрутизаторів. Такі мережі функціонують під впливом перешкод та завад. Тому увесь час зникають та з'являються лінії зв'язку, підключаються та відключаються вузли. В таких умовах мережа має автоматично реструктуруватись, самостійно налаштовуватись та забезпечувати стійке функціонування.

Разом з тим, коли більшість вузлів є мобільними, то енергетичні характеристики таких вузлів не є незалежними. Вони можуть зв'язуватись (налагоджувати лінії зв'язку) тільки з найближчими (в межах радіуса дії), а не з усіма вузлами.

Список літератури

1. Барабаш О. В. Построение функционально устойчивых распределенных информационных систем / О. В. Барабаш. – К.: НАОУ, 2004. – 226 с.

2. Машков О. А. Оптимизация цифровых автоматических систем, устойчивых к отказам / Л. М. Артюшин, О. А. Машков. – К.: КВВАИУ, 1991. – 89 с

3. Кравченко Ю. В. Применение метода последовательного увеличения ранга k-однородного матроида в задаче синтеза структуры псевдоспутниковой радионавигационной системы / Ю. В. Кравченко // Сучасні інформаційні технології у сфері безпеки та оборони. – К.: 2008. – №2(2). – С. 19 – 22.

4. Попков В.К. Математические модели живучести сетей связи/В.К. Попков. – Новосибирск: Вычислительный центр СО АН СССР, 1990. – 235 с.

5. Нечепуренко М.И. Алгоритмы и программы решения задач на графах и сетях/ М.И. Нечепуренко, В.К. Попков, С.М. Майнагашев и др. –Новосибирск: Наука. Сиб. Отд-ние, 1990. – 515 с.

6. Саланда І.П. Методи пошуку оптимальних маршрутів графа структури розгалуженої інформаційної мережі за заданим критерієм оптимальності при різних обмеженнях / І.П. Саланда, О.В. Барабаш, А.П. Мусієнко// Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – №2(42). – С. 99–106.

7. Barabash O. Methods of self-diagnosis of telecommunication networks based on flexible structures of test connections / O/Barabash, N. Lukova-Chuiko, A. Musiyenko // Zborník príspevkov z medzinárodného vedeckého seminára „Riadenie bezpečnosti zložitých systémov". 23 – 27 februára 2015. – Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2015. – Str. 226 – 231.

8. Обідін Д. М. Ознаки та критерії функціональної стійкості інтелектуалізованої системи автоматичного управління польотом літака. / Д. М. Обідін, О. В. Барабаш // Системи озброєння і військова техніка: Науковий журнал. – Х.: ХУПС, 2012. – № 1 (29). – С. 133 – 136.

9. Кучук Г.А. Управление ресурсами инфотелекоммуникаций: монография / Г.А. Кучук, Р.П. Гахов, А.А. Пашнев. – М.: Физматлит, 2006. – 220 с.

10. Кучук Г.А. Інформаційні технології управління інтегральними потоками даних в інформаційно-телекомунікаційних мережах систем критичного призначення: монографія / Г.А. Кучук. – Х.: Харківський університет Повітряних Сил, 2013. – 264 с.

Надійшла до редколегії 2.02.2017

Рецензент: д-р техн. наук, проф. В.В. Вишнівський, Державний університет телекомунікацій, Київ.

СИСТЕМА ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ФОРМАЛИЗАЦИИ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ЛОКАЛЬНОЙ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ

И.П. Саланда, О.В. Барабаш, А.П. Мусиенко

Предложены показатели и критерии синтеза функционально устойчивой распределенной информационной сети на основе графовых моделей. С помощью предложенных показателей и критериев можно оценивать и сравнивать различные структуры сетей с высоким уровнем связности, а также применять их для формирования методики оптимального использования избыточности системы при парирования последствий внештатных ситуаций. Данные показатели целесообразно использовать для современных и перспективных сетей 5 поколения (5G), которые являются беспроводными, динамичными, самоорганизующиеся, поскольку они позволяют при реструктуризации учитывать элементы, повреждение которых не влияет на локальную функциональную устойчивость сети.

Ключевое слова: *информационные сети, функциональная устойчивость, тотальная связность, сети 5G, реструктуризация.*

SYSTEM OF INDICATORS AND CRITERIA FOR THE FORMALIZATION OF PROCESSES OF PROVIDING LOCAL FUNCTIONAL STABILITY OF DISTRIBUTED INFORMATION NETWORKS

I.P. Salanda, O.V. Barabash, A.P. Musienko

The indicators and criteria for the synthesis of a functionally stable distributed information network based on graph models are proposed. With the help of the proposed indicators and criteria, it is possible to evaluate and compare the various structures of networks with a high level of connectivity, and also apply them to formulate a methodology for the optimal use of system redundancy when parrying the consequences of extraordinary events. These indicators should be used for modern and prospective 5G generation networks (5G), which are wireless, dynamic, self-organizing, as they allow the restructuring to take into account the elements, the damage of which does not affect the local functional stability of the network.

Keywords: *information networks, functional stability, total connectivity, 5G networks, restructuring.*

Запобігання та ліквідація надзвичайних ситуацій

УДК 614.8

Р.І. Шевченко

Національний університет цивільного захисту України, Харків

ФОРМУВАННЯ СТРУКТУРИ ТА ОКРЕМИХ ОРГАНІЗАЦІЙНИХ РІШЕНЬ З РОЗБУДОВИ СИСТЕМИ ЕШЕЛОНОВАНОГО МОНІТОРИНГУ У ПЕРЕДУМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Спираючись на теоретико-методологічні засади інформаційно-комунікативного підходу до розбудови системи моніторингу у передумовах надзвичайних ситуацій, запропонована сучасна структура останньої та окремі організаційні рішення з її реалізації як системи матеріально-інформаційно-розумного типу.

Ключові слова: *моніторинг, інформаційно-комунікативний підхід, надзвичайна ситуація, організаційні рішення.*

Вступ

Постановка проблеми. Аналіз результатів [1, 2] багаторічної практичної реалізації комплексу питань пов'язаних з розбудовою вітчизняної системи моніторингу надзвичайних ситуацій дозволяє впевнено констатувати наявність цілої низки невирішених, на цей час, системних проблем, починаючи як з відсутності сучасної концепції та теоретико-методологічних основ розвитку системи моніторингу у передумовах надзвичайних ситуацій, так теоретичних і практичних рішень з її реалізації. Вирішенню саме похідної частини проблемного поля, організаційним та структурним питанням розбудови системи моніторингу у передумовах надзвичайних ситуацій і присвячена дана робота.

Аналіз останніх досліджень і публікацій. Шляхами вирішення проблеми створення сучасної системи моніторингу у передумовах надзвичайних ситуацій є застосування можливостей [3] інформаційно-комунікативного підходу до її розбудови. Комплексному вирішенню базової частини визначеної складної проблеми присвячена низка робіт [4-8], яка дозволяє надалі сформувати мету дослідження та запропонувати нижче наведені організаційні рішення.

Постановка завдання та його вирішення

Від так метою дослідження є розробка, на базі раніше створених матеріально-інформаційно-розумної концепції [5] та теоретико-методологічного апарату [3 – 7] інформаційного-комунікативного підходу до формування функціонального поля моніторингу у передумовах надзвичайних ситуацій, структури останнього та низки організаційних рішень щодо її подальшої практичної реалізації.

Виконання складного завдання щодо забезпечення безперебійного надходження інформаційно-комунікативного потоку моніторингу у передумовах надзвичайних ситуацій пропонується здійснити за рахунок створення організаційної структури системи моніторингу у передумовах надзвичайних ситуацій з урахуванням двох базових принципів: багато ешелонованого резервування та децентралізації процесу обробки інформаційно-комунікативного потоку моніторингу стану об'єктів контролю.

На виконання першого принципу пропонується утворити три ешелони моніторингу у передумовах НС (рис. 1) у складі: І (ІКР) інформаційно-комунікативний рівень (базовий); ІІ ІКР (резервний); ІІІ ІКР (додатковий).

Підрівні кожного ІКР визначаються за рівнем охвату інформаційного простору та складаються наступним чином. Так базовий ІКР містить чотири підрівні охвату інформаційного простору, а саме: державний, який базується на ІКП отриманому зі супутникових носіїв (AVHRR, MODIS) не комерційного призначення низької та середньої роздільної здатності NOAA, Terra, Aqua; регіонального, який базується на ІКП отриманому зі супутників комерційного призначення високої роздільної здатності (наприклад Landsat – TM/ETM) та (/або) безпілотних аеростатів; місцевого, який складається з базових інформацій модулів (БІМ), що розміщуються на матеріальній базі мережі стільникового зв'язку та відповідно покривають майже 100 % територію держави. Врахування особливостей місцевості (як-то зміщення вектору виникнення НС в бік природної або техногенної складової, наявність особливостей об'єкту контролю: ландшафту, наявність ПНО інші особливості) здійснюється за рахунок відповідної насиченості елементів базового інформаційного модулю відповідними складовими. Для спрощення формування системи базових інформаційних модулів пропонується наступна уніфікація: загальний (без домінування складових), природно спрямований, техногенно спрямований (з домінуванням відповідних напрямів). Відпо-

відно на систему базових інформаційних модулів замикається об'єктовий рівень охвату інформаційного простору, який складається з об'єктових систем раннього виявлення критичних ситуацій (СРВКС). При цьому виникає можливість забезпечити багаторазове резервування надходження ІКП моніторингу у передумовах НС з об'єктових систем за рахунок наявної організаційної структури стільникового зв'язку (рис. 2).

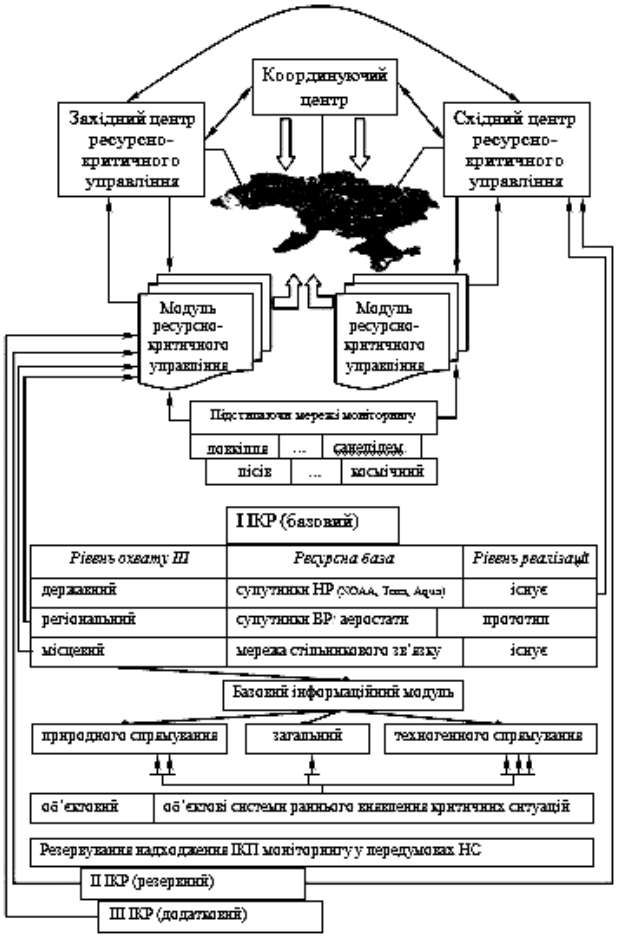
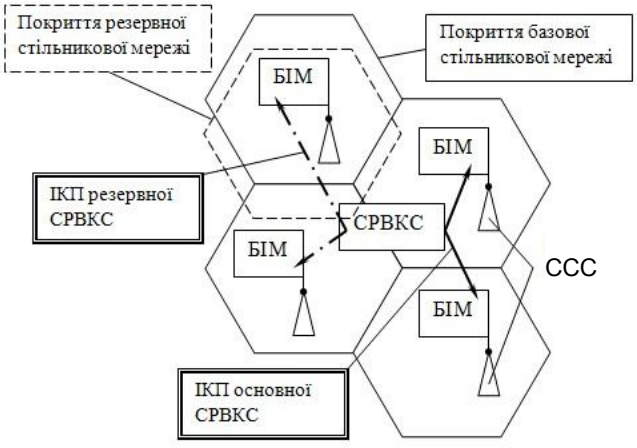


Рис. 1. Схема організації ешелонованого моніторингу у передумовах надзвичайних ситуацій



ССС – станції мережі оператора стільникового зв'язку

Рис. 2. Організаційна схема надходження ІКП об'єктового рівня охвату ІП з СРВКС до БІМ системи моніторингу у передумовах НС

За рахунок реалізації різних схем включення модулів БІМ є можливість організації додаткового резервування надходження ІКП як з основної СРВКС ПНО (принаймні створення одного резервного каналу), так і резервної СРВКС. Аналогічним чином можлива організація взаємодії БІМ-СРВКС на матеріальних ресурсах резервної стільникової мережі.

Важливим є виконання принципу децентралізації обробки ІКП моніторингу у передумовах НС. З метою його реалізації пропонується утворити два центри ресурсно-критичного управління східний (СЦРКУ) м. Харків на базі НУЦЗУ та західний (ЗЦРКУ) м. Львів на базі ЛДУБЖД відповідно та координуючий центр (КЦ) у м. Києві на базі ДСНС України.

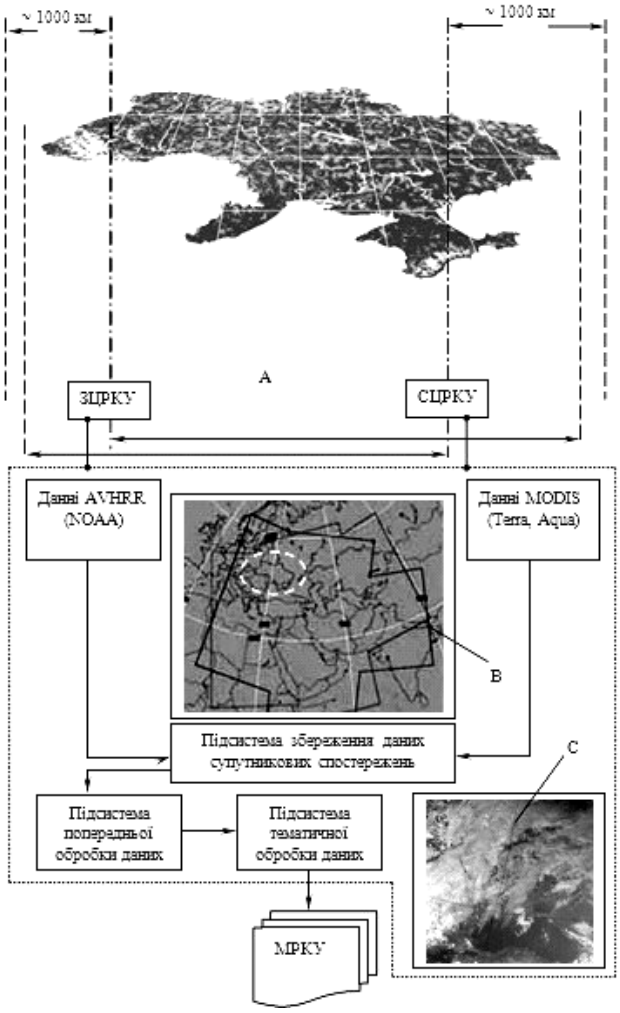


Рис. 3. Структурна схема супутникового моніторингу у передумовах надзвичайних ситуацій

Відповідно до організаційної схеми (рис. 1) безпосередньо на СЦРКУ та ЗЦРКУ замикаються ІКП державного рівня охвату ІП (рис. 3). Які організуються за рахунок станцій обробки супутникових даних низької та середньої роздільної здатності. Слід зазначити, що при цьому забезпечується подвійне перекриття території держави (рис. 3, А –

межі відповідальності ЦРКУ), а також покриття території держав які межують з Україною та відповідно є потенційним джерелом виникнення та розповсюдження трансграничних НС за участі території та об'єктів інфраструктури України. Так наприклад добова зона покриття супутниками серії NOAA (B) охвачує необхідний ІП державного рівня. До організаційної структури супутникового моніторингу у передумовах НМ входять підсистема збереження даних, підсистеми попередньої та тематичної обробки інформації. Результат функціонування останньої (у вигляді (С) – композиційне зображення з NOAA 18) надходять до мережі регіонально розміщених (наприклад на матеріальній базі ГУ(У)ДСНС) модулів ресурсно-критичного управління (МРКУ).

Характерною особливістю ЦРКУ є відсутність з боку останніх прямого управлінського впливу на об'єкти контролю системи моніторингу у передумовах НС. Натомість на ЦРКУ покладається функція інформаційної, методологічної, наукової, експертної та інноваційної підтримки функціонування системи моніторингу у передумовах НС та функція підготовки та перепідготовки менеджерського складу МРКУ та інших елементів системи моніторингу. Така система розподілу функцій вважається найбільш вдалою з урахуванням наявного наукового потенціалу потенційних ЦРКУ та їх можливостей щодо неупередженого (відсутність прямої участі у процесі прийняття рішень) аналізу та узагальнення як моніторингової, так і управлінської складової ІКП, яка надходитиме з МРКУ та КЦ, на які покладається безпосередньо функція прийняття управлінських рішень щодо стану безпеки об'єктів контролю, на базі ІКП системи моніторингу у передумовах НС.

МРКУ утворюються на базі існуючих ГУДСНС України в регіонах тим самим застосовується вже існуюча матеріальна та інформаційно-комунікативна база. Принциповою особливістю є включення до інформаційного простору ІКП підстилаючих систем моніторингу (рис. 1) безпосередньо на регіональному рівні в якості окремих незалежних потоків, як додаткових, але не базових джерел інформації, які доповнюють картину інформаційного простору у разі необхідності за запитом МРКУ.

Також на рівні МРКУ організується надходження ІКП з охватом інформаційного простору регіонального рівня. На сьогодні основним джерелом такої інформації вважається супутникова інформація високої роздільної здатності рис. 4.

Втім є досить багато вдалих спроб [9] використання, в якості альтернативного каналу отримання необхідної інформації з обмеженими інформаційно-комунікативними характеристиками, непілотуємих аеростатів середнього та малого розміру з різними технічними характеристиками [10].

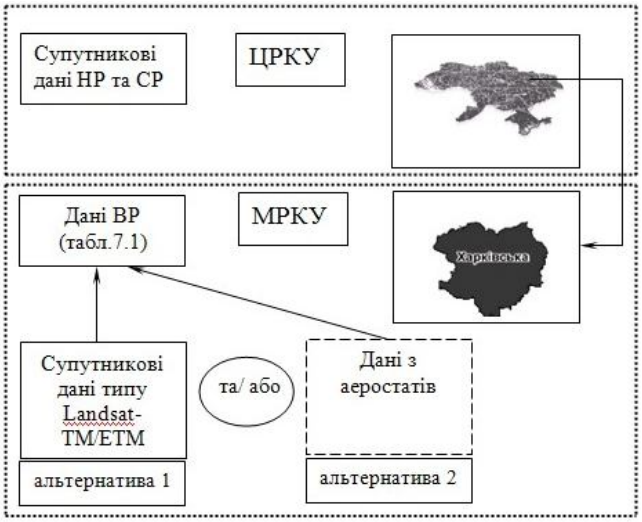


Рис. 4. Організація моніторингу у передумовах НС регіонального рівня охвату інформаційного простору

Проведений порівняльний аналіз (табл. 1) дозволяє констатувати недоцільність одноосібного використання однієї чи іншої альтернативи надходження ІКП регіонального рівня в силу наявності суттєвих обмежень. Останні досить ефективно невілюються у разі комбінованого застосування обох альтернативних підходів одночасно.

Таблиця 1

Порівняльний аналіз альтернативних шляхів отримання І КП моніторингу у передумовах НС регіонального рівня охвату ІП

Порівняльний параметр	**Альтернатива 1**	**Альтернатива 2**
Мобільність отримання ІКП	Низька	Висока
Деталізація ІКП	Нерегулюєма	Регулюєма за рахунок зміни висоти зйомки
Можливий охват території регіону для проведення моніторингу	Неповний. Насиченість досягається за рахунок архівних даних	Повний. Насиченість досягається за рахунок засобів моніторингу
Залежність від метеоданих регіону	Значна в частині отримання зображення	Значна в частині керування засобами моніторингу
Можливості резервування	За рахунок подібних даних комерційного характеру інших мереж	За рахунок засобів суміжних регіонів та зміни схеми обльоту
Рівень світової реалізації	Реалізовано в якості комерційних мереж	Існує в якості окремих прототипів з обмеженими характеристиками
Рівень реалізації в Україні	Вітчизняного аналогу не існує. Можливе комерційне використання закордонних мереж	Існує в якості окремих прототипів з обмеженими характеристиками

В природних (метеорологічних) умовах території України [11] застосування альтернативного підходу до отримання ІКП моніторингу у передумовах НС в якості системи аеростатів потребує деяких уточнень та інноваційних інженерних підходів.

Найбільш ефективним, з погляду особливостей загального розміщення території України, вважається застосування не технології обльоту відповідної території, а дискретне розміщення засобів спостереження (безпілотних аеростатів) над опорними вузлами (з урахуванням кластеризації території регіону за потенційною небезпекою [12]) з додатковим розміщенням на борту аеростату (Аn) блоку апаратури ретрансляції ІКП суміжних аеростатів (Аn-1, Аn+1 та інших) рис. 5.

Окремо слід звернути увагу на питання вибору базової та резервних мереж стільникового зв'язку у якості мережі покриття БІМ моніторингу у передумовах НС рис. 6. Основним критерієм вибору базової мережі (ОБ) є максимальний територіальний охват держави мережею можливих носіїв БІМ (станцій стільникового зв'язку). На сьогодні в якості такої мережі можна розглядати стільникові мережі операторів Kyivstar, life, Vodafone UA.

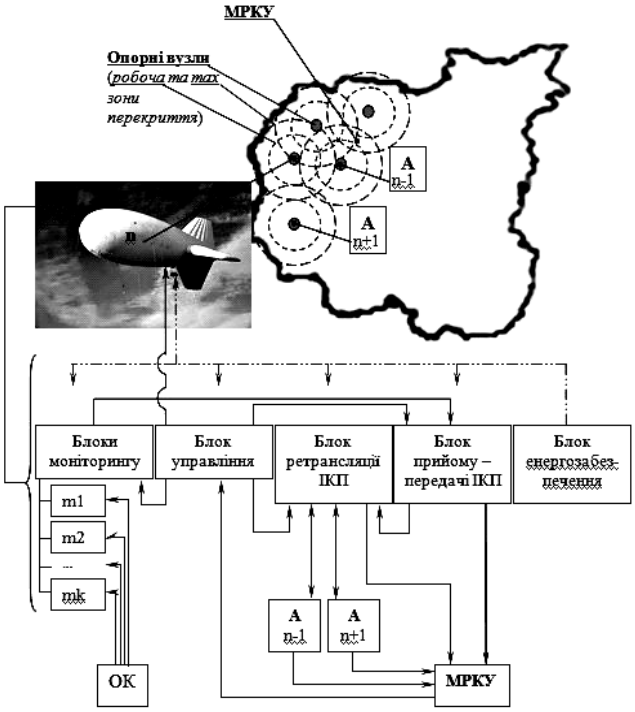


Рис. 5. Схема організації моніторингу у передумовах НС регіонального рівня охвату ІП на базі системи безпілотних аеростатів.

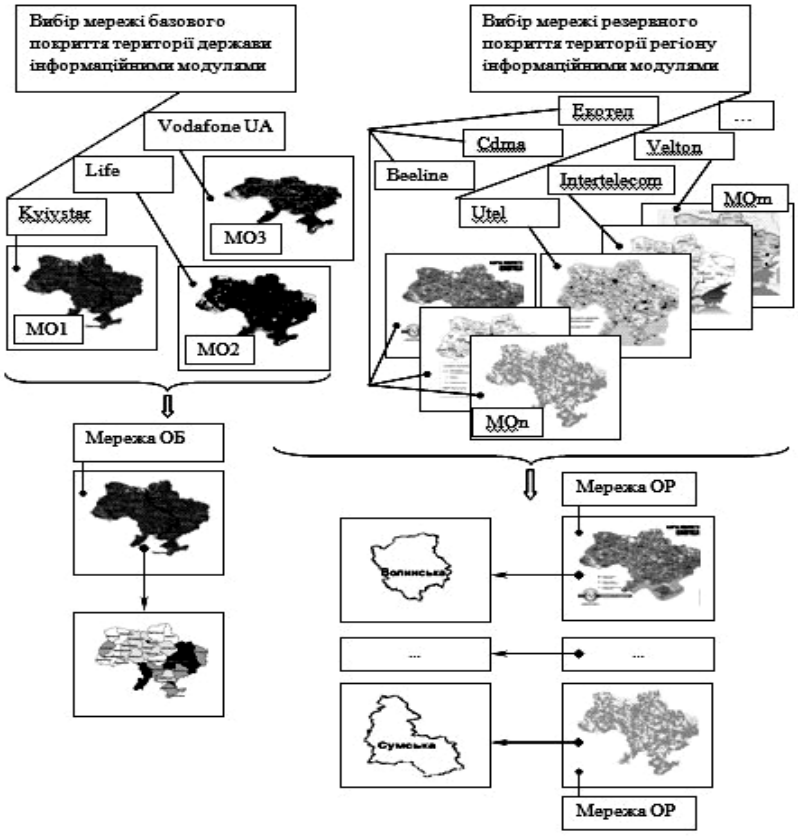


Рис. 6. Принцип організації базової та резервної мережі покриття БІМ

Фактично «стаціонарне» розміщення потребуватиме менше енергетичних витрат та дозволить досягти додаткового резервування передачі ІКП.

Розміщення блоків ретрансляції дозволяє завжди забезпечити необхідну кількість додаткових каналів надходження ІКП моніторингу у передумовах НС, як на рівні регіонального охвату інформаційного простору, так і на територіальному рівні у вигляді додаткової системи резервування та наявності у компоновці окремих БІМ блоків ретрансляції

та автономного живлення (БІМ – РАЖ). Прогнозуємо маємо недолік у вигляді наявності окремих осередків «білих плям» відсутності покриття у складних природних або антропогенних умовах. Компенсування останнього здійснюється, у разі природних обмежень за рахунок регіональної мережі охвату ІП, у разі антропогенних обмежень за рахунок додаткового залучення (або організації) об'єктових мереж.

Висновки

В роботі розроблена функціональна структура державної системи моніторингу у передумовах надзвичайних ситуацій природного та техногенного характеру, яка базується на сучасному погляді щодо реалізації останньої, як системи, управління інформаційно-комунікативними потоками стосовно стану безпеки об'єктів контролю, матеріально-інформаційно-розумного типу. Наведені окремі організаційні рішення щодо практичної реалізації запропонованої структури. Подальші дослідження будуть направлені на вдосконалення підготовки та функціонування системи менеджменту ресурсно-критичного управління функціональним полем моніторингу у передумовах надзвичайних ситуацій, як найбільш складного та мало дослідженого елементу останнього.

Список літератури

1. Шевченко Р.І. Оцінка ефективності функціонування системи моніторингу надзвичайних ситуацій природного та техногенного характеру в умовах впливу соціальних небезпек [Текст] / Р.І. Шевченко // Збірник наукових праць Харківського університету Повітряних Сил – Х.: ХУПС, 2015. – № 3 (44). – С. 105 – 111.

2. Шевченко Р.І. Інформаційно-функціональний аналіз системи моніторингу та прогнозування надзвичайних ситуацій [Текст] / Р.І. Шевченко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 8 (133). – С. 148 – 157.

3. Шевченко Р.І. Визначення теоретичних основ інформаційно-комунікативного підходу до формування та аналізу систем моніторингу надзвичайних ситуацій [Текст] / Р.І. Шевченко // Системи обробки інформації – Харків: ХУПС, 2016. – № 5 (142). – С. 202 – 206.

4. Шевченко Р.И. Концепция системы компенсирования внешнего влияния на функциональную устойчивость системы мониторинга чрезвычайных ситуаций природного и техногенного характера [Текст] / Р.И. Шевченко // «Актуальные проблемы пожарной безопасности, предупреждения и ликвидации чрезвычайных ситуаций», материалы VI Международной научно-практической конференции. – Кокшетау: КТИ КЧС МВД РК, 2015. – С. 245-247.

5. Шевченко Р.И. К вопросу формирования концепции системы мониторинга чрезвычайных ситуаций как системы материально-информационно-разумного типа [Текст] / Р.И. Шевченко // «Чрезвычайные ситуации: теория, практика, инновации», мат. межд. научно-практической конференции – Гомель: 2016. – С. 308-309.

6. Шевченко Р.І. Розробка методу інформаційно-комунікативної компенсації для системи моніторингу надзвичайних ситуацій природного та техногенного характеру [Текст] / Р.І. Шевченко // Системи обробки інформації – Х.: ХУПС, 2016. – № 2 (139). – С. 201 – 205.

7. Шевченко Р.І. Розвиток теоретичних основ комунікативно-компенсуючих фільтрів системи моніторингу надзвичайних ситуацій (інформаційна складова) [Текст] / Р.І. Шевченко// Системи обробки інформації – Харків: ХУПС, 2015. – № 9 (134). – С. 168 – 175.

8. Шевченко Р.І. Дослідження умов внутрішнього управління інформаційно-комунікативним потоком в рамках розбудови інформаційної логістики системи моніторингу надзвичайних ситуацій [Текст] / Р.І. Шевченко // Системи обробки інформації. – Харків: ХУПС, 2016. – Вип. 7 (144). – С. 189 – 195.

9. Фетисов В.С. Беспилотная авиация: терминология, классификация, современное состояние [Текст] / В.С. Фетисов, Л.М. Неугодникова, В.В. Адамовский и др. - Уфа: ФОТОН, 2014. – 217 с.

10. Вопросы создания и применения современных беспилотных систем на базе воздухоплавательной техники [Електронний ресурс] Режим доступу: http://uvs-info.com/phocadownload/02_2cba_UVS-Tech-2010_Presentations_PvB-130318/Vega-Corporation_Russia_1.pdf

11. Вальчук-Оркуша О.М. Метеорологія з основами кліматології : навч. посіб. [Текст] / О.М. Вальчук-Оркуша, О.І. Ситник. - Умань: «Візаві», 2015. – 224с.

12. Тютюник В.В. Кластерный анализ территории Украины по основным показателям повседневного функционирования и проявления техногенной опасности [Текст] / В.В. Тютюник, М.В. Бондарєв, Р.І. Шевченко та інші // Геоінформатика. – Київ: Інститут геологічних наук НАН України, 2014. – 4(52). – С. 63 – 72.

Надійшла до редколегії 25.01.2017

Рецензент: д-р техн. наук, проф. М.І. Адаменко, Харківський національний університет ім. В.Н. Каразіна, Харків.

ФОРМИРОВАНИЕ СТРУКТУРЫ И ОТДЕЛЬНЫХ ОРГАНИЗАЦИОННЫХ РЕШЕНИЙ ПО РАЗВИТИЮ СИСТЕМЫ ЭШЕЛОНИРОВАННОГО МОНИТОРИНГА В ПРЕДПОСЫЛКАХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Р.И. Шевченко

В работе, опираясь на теоретико-методологические основы информационно-коммуникативного подхода к развитию системы мониторинга в предпосылках чрезвычайных ситуаций, предложена современная структура последней и отдельные организационные решения по ее реализации как системы материально-информационно-разумного типа.

Ключевые слова: *мониторинг, информационно-коммуникативный подход, чрезвычайная ситуация, организационные решения.*

FORMATION OF INDIVIDUAL AND DECISIONS ORGANIZING BUILDING SYSTEMS LAYERED MONITORING PRECONDITION EMERGENCIES

R.I. Shevchenko

The paper, based on theoretical and methodological foundations of information-communicative approach to building monitoring system in the premises of emergencies, offered the latest modern structure and some organizational decisions for its implementation as a system of material and information-wise type.

Keywords: *monitoring, information-communicative approach, emergency, organizational decision.*

УДК 625.032

О.С. Задунай[1], С.І. Азаров[2]

[1] *Державний науково-дослідний інститут спеціального зв'язку та захисту інформації, Київ*
[2] *Інститут ядерних досліджень НАН України, Київ*

РОЗРОБКА МЕТОДОЛОГІЇ АНАЛІЗУ СИСТЕМНИХ РИЗИКІВ ПІД ЧАС ЕКСПЛУАТАЦІЇ ОБ'ЄКТІВ ПІДВИЩЕНОЇ ЕКОЛОГІЧНОЇ НЕБЕЗПЕКИ

Розглянуто сучасний стан розробки методології аналізу системних ризиків при експлуатації об'єктів підвищеної екологічної небезпеки.

Ключові слова: *об'єкти підвищеної екологічної небезпеки (ОПЕН), аварійна ситуація, екологічний ризик.*

Вступ

Враховуючи високу важливість проблеми підвищення безпеки в процесі експлуатації об'єктів підвищеної екологічної небезпеки (ОПЕН), на даний час велике значення набуває вирішення завдань пов'язаних з попередженням можливих аварійних ситуацій та мінімізацією технологічних і екологічних ризиків.

Існуючі на цей час методики оцінки та декларування промислової безпеки ОПЕН мають більше декларативний характер, а наявний досвід використання методології аналізу екологічних небезпек та їх оцінки, не завжди дозволяє враховувати його під час прийняття оптимальних рішень з попередження аварійних ситуацій через відсутність належного організаційного та інформаційного забезпечення з прогнозування і оперативного передчасного розпізнавання небезпечних ситуацій [1 – 3].

Технології моніторингу управління ризиками, що застосовуються під час експлуатації ОПЕН як статичних об'єктів мають значну методичну похибку, а прийняття рішень з попередження аварійних ситуацій не враховує випадковий нестаціонарний характер розвитку аварійних процесів. Крім того, вирішення проблеми попередження аварійних ситуацій ускладняється значними об'ємами вхідної діагностичної та технологічної інформації через відсутність системного підходу до рішення багатофакторних завдань безпеки, відсутності належних комп'ютеризованих інформаційно-керуючих систем моніторингу ризику, а також відповідного спеціального методичного та програмного забезпечення системи обробки даних, що ускладнює прийняття оптимальних керуючих рішень зі своєчасного прогнозування та запобігання виникнення аварійних ситуацій. Вітчизняні дослідження в галузі забезпечення безпеки ОПЕН розпочато відносно нещодавно - на початку 90-х років, та, в основному, були зосереджені в галузі теоретичних основ розробки нормативно-методичної документації з питань промислової безпеки з урахуванням ризику виникнення природних та техногенних катастроф [1]. Слід зазначити, що практична діяльність щодо реалізації концепції «абсолютної надійності» на основі абсолютних показників небезпеки ОПЕН в багатьох випадках виявилась неефективною при ранньому прогнозуванні та запобіганні надзвичайних ситуацій як у випадках виникнення великомасштабних катастроф так і при локальних аварійних ситуаціях.

Запропоновані останнім часом критерії оцінки «інтегрального» та «інтегрованого» ризиків, що відображують остаточні очікувані втрати (у вартісному відображенні), також є проблемними з точки зору раннього розпізнавання та попередження перед аварійних та аварійних ситуацій, а також відсутності експериментальних даних щодо нестаціонарності технологічних процесів. Крім того, негативним фактором у вирішенні проблеми екологічної безпеки на даний момент є не достатнє приділення уваги дослідників та розробників систем безпеки превентивному організаційному, технічному та інформаційному забезпеченню під час створення інженерного і технологічного протиаварійного захисту від аварійних ситуацій на ОПЕН.

Результати досліджень

Лише останнім часом в Україні розпочато розробку концепції припустимого ризику, яка заснована на застосуванні профілактичних заходів організаційного і технічного характеру та базується на розробці теоретичних положень адаптивного управління екологічною безпекою ОПЕН.

В цілому можна зробити висновок, що за результатами проведених досліджень виявлено що основними причинами низької ефективності управління екологічною безпекою та низької достовірності даних отриманих за результатами кількісного аналізу ризиків є: недостатня повнота статистичних даних щодо аналізу ризиків; висока методична похибка при екстраполяції вхідних даних, що призводить до низького ступеню оцінки небезпечних ситуацій; висока методична похибка, що обумовлена низькою якістю побудови «дерев подій та відмов» з використанням експертної оцінки небезпечних ситуацій; недостатній збір вхідної інформації; декларування безпеки ОПЕН як статистичних систем; не врахування чисельних факторів динамічної зміни інформаційних параметрів та навколишнього середовища в часовому відображенні; відсутність належного контролю за суб'єктивною експертною оцінкою ризиків, що в багатьох випадках обумовлює низьку достовірність інформації що не відповідає дійсності; неврахування не стаціонарності технологічних

процесів у часі; неврахування взаємозв'язку залежних і незалежних випадкових процесів при експлуатації обладнання та транспортуванні вибухопожеженебезпечних середовищ; неможливість оцінки впливу нестаціонарних режимів експлуатації на реальних ОПЕН експериментальним шляхом.

Методологічні заходи кількісної оцінки показників ризиків в процесі експлуатації ОПЕН знаходяться в стадії розробки і на даний момент не впроваджені в систему нормативно-правових та методичних основ екологічної безпеки. За останні роки відмічається велика кількість досліджень в зазначеному напрямку, в тому числі виконаних авторами на протязі 2010 – 2015 років. На підставі виконаного аналізу нами запропонована така функціональна схема методології аналізу ризику (рис. 1).

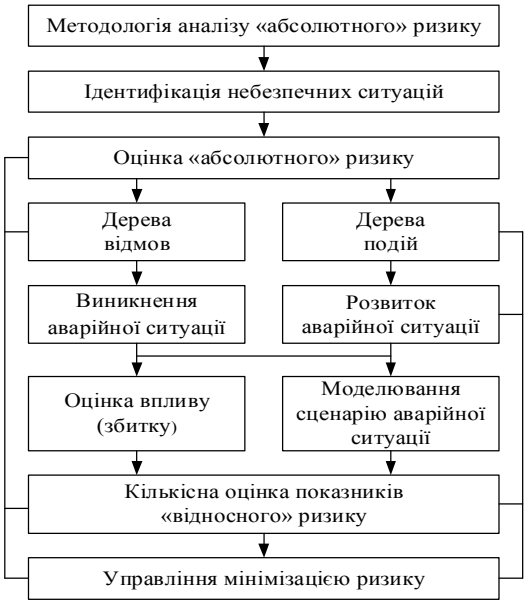


Рис. 1. Функціональна схема побудови системи аналізу ризику

В наведеній функціональній схемі методології аналізу ризику відмінною рисою (в порівнянні з вже відомими схемами) є наявність запропонованого авторами модуля визначення показника відносного ризику. Розглянемо основні положення та обґрунтування сучасних принципів побудови концептуальних засад методології аналізу ризиків.

Потенційний колективний ризик. При розмежуванні території по рівню потенційного ризику імовірність ураження людей внаслідок впливу фактору ураження можна визначити за формулою [2]:

$$P = 1/N_{л} \times \times \iint_{S} \int_{0}^{2\pi} \int_{0}^{L_{max}} P\left[\Phi(x,y)\right] \cdot \Psi(x,y) \cdot f(L)\phi(\beta)\, dL d\beta dx dy, \quad (1)$$

де $N_л$ – кількість людей на елементарному майданчику; $P[\Phi(x, y)]$ – вірогідність ураження людей в точці з координатами (x, y) під впливом вражаючого фактору Ф; $\Psi(x, y)$ – щільність людей в межах майданчику; $f(L)$ та $\varphi(\beta)$ – функції щільності розподілу вірогідності відповідно дрейфу хмари паливно повітряної суміші та повторюваність напрямку вітру за рік; S – площа території. Щільності вірогідності $f(L)$ і $\varphi(\beta)$ не залежать від x та y, також L не залежить функціонально від β, і навпаки. В цьому випадку формула (1) буде мати такий вигляд:

$$P = \frac{1}{N_{л}} \left[\iint_{S} \left[\Phi(x,y)\right] \cdot \Psi(x,y) \cdot dx dy \right] \times \times \left[\int_{0}^{2\pi} \phi(\beta) d\beta \right] \cdot \left[\int_{0}^{L_{max}} f(L) dL \right]. \quad (2)$$

Інтеграл від щільності розподілу вірогідності в межах всього діапазону змінювання випадкової величини дорівнює одиниці

$$\int_{0}^{2\pi} \varphi(\beta) d\beta = 1; \quad \int_{0}^{L_{max}} f(L) dL = 1, \quad (3)$$

отже, вираз (1) буде мати такий вигляд:

$$P = \frac{1}{N_{л}} \left[\iint_{S} P\left[\Phi(x,y)\right] \cdot \Psi(x,y) \cdot dx dy \right], \quad (4)$$

де $\iint_{S} P\left[\Phi(x,y)\right] \cdot \Psi(x,y) \cdot dx dy$ – очікувана кількість смертельних випадків або колективний ризик (смертей/рік) в межах території площею S, що розглядається. Відношення числа очікуваних летальних випадків в межах території що розглядається (колективного ризику) до загального числа людей що ризикують $N_л$ на цій території є середнім показником індивідуального ризику $R^{ср}_{ind}$.

Соціально-економічним ризиком $R_{c\text{-}e}$ можна вважати загальну кількість смертей за рік з розрахунку на одну тисячу людей, що обумовлена недостатнім рівнем розвитку економіки, рівнем харчування, рівнем життя. Величину $R_{c\text{-}e}$ можна представити як функцію, залежну головним чином від річного доходу людини:

$$R_{c\text{-}e} = A/\sqrt[3]{L}, \quad (5)$$

де A = 280; L – річний дохід людини.

Індивідуальний ризик визначається частотою загибелі людей від факторів ураження (або їх сукупності) визначеній у точці простору та розраховується так:

$$R_{in}(x,y) = \sum_{m \in M} \sum_{l \in L} P_{Qi}(x,y) F(A_m), \quad (6)$$

де $P_{Qi}(x,y)$ – вірогідність впливу на людину в точці з координатами (x, y) Q_l-го фактору ураження з інтенсивністю, що відповідає загибелі (ураженню) людини за умов реалізації A_m-ої події (аварії, небезпечного природного явища); $F(A_m)$ – частота виникнення A_m-ої події в рік; M – множина індексів, яка відповідає подіям, що розглядаються; L – множина індексів, яка відповідає переліку всіх факторів ураження.

Соціальний ризик визначається залежністю частоти виникнення подій, що викликають ураження певної кількості людей, яка розраховується таким чином:

$$R_c(N) = \sum_{m \in M} \sum_{l \in L} p(N/Q_l) P(Q_l/A_m) F(A_m), \quad (7)$$

де $P(N/Q_l)$ – вірогідність загибелі N людей від Q_l-го фактору ураження; $P(Q_l/A_m)$ – вірогідність виникнення Q_l-го фактору ураження при реалізації A_m-ої події; $F(A_m)$ – частота виникнення A_m-ої події. Середній за певний час ризик від події А дорівнює

$$R(A) = P(A) \cdot У(A), \quad (8)$$

де P(A) – повторюваність події А, що має зворотну часу розмірність; У(А) – можливий разовий збиток від події А, що має розмірність втрат.

Повторюваність в формулі (8) чисельно дорівнює частоті або статистичній вірогідності події А та відображається числом аварійних випадків за одиницю часу (відмов/місяць, аварій/рік та ін.). Ризик визначений за формулою (8), пропонується називати комбінованим, або приведеним (до одиниці часу) згідно з класифікатором ризику [3].

Подійний ризик є однією з характеристик небезпеки негативної події. На відміну від нього, вартісний ризик є показником уразливості об'єкту системи при впливі небезпеки певної інтенсивності. ***Вартісний ризик***, або розміри збитків, в кожному конкретному випадку залежать від інтенсивності негативної події та від уразливості об'єкту що знаходиться під впливом. ***Уразливість*** – це ступінь можливих втрат об'єкту, або його окремих елементів, під дією факторів ураження певної інтенсивності. Ступінь уразливості визначають, як правило, окремо для кожного об'єкту по емпіричним залежностям втрат в соціальній, економічній чи екологічній сферах від інтенсивності цих процесів, отриманих за результатами статистичної обробки фактичних даних, або за даними моделювання негативних подій. З урахуванням ступеня уразливості об'єкту формула (8) для комбінованого ризику приймає вигляд:

$$R(A) = P(A)C_{у}(A)У_{п}(A), \qquad (9)$$

де $C_{у}(A)$ – ступінь уразливості об'єкту при події А певної інтенсивності; $У_{п}(A)$ – умовні повні втрати від події А, що дорівнюють по кількості населення, кількості, або вартості всіх об'єктів у зоні ураження.

Соціальний ризик являє собою кількість загиблих (уражених і т.ін.) людей люд./рік. Цей показник можна розрахувати за допомогою наступної модифікованої відомої формули:

$$R_{с} = P(A)P(H)C^{C}_{у}(A)H, \qquad (10)$$

де P(H) – вірогідність знаходження групи людей (населення, працівників галузі, туристів та ін.) в зоні ураження; $C^{C}_{у}$ – ступінь соціальної уразливості цієї групи; H – чисельність групи відповідно (9). Як було зазначено раніше, індивідуальний ризик являє собою імовірнісну характеристику можливої загибелі поранення та(або) втрати здоров'я однієї людини з певної групи в певний проміжок часу з природних причин чи за результатами негативного впливу:

$$R_{і}(A) = P(A)P(H_{1})P(I)C^{C}_{у}(A)H, \qquad (11)$$

де $P(H_{1})$ – імовірність знаходження конкретного або типового індивідуума в зоні ураження, що відповідає фак.-тору зайнятості; P(I) – імовірність негативної події, що оцінюється для індивіда із певної групи. додатково вводиться поняття питомий економічний ризик від події А:

$$R_{у}(A) = R_{м}(A)/S, \qquad (12)$$

де $R_{М}(A)$ – економічний (матеріальний) ризик від події А; S – площа зони ураження при цій події.

Дана характеристика особливо цікава для реалізації об'ємного відображення результатів аналізу ризиків з метою виявлення просторових закономірностей зміни економічного ризику. Подібна питома та індивідуальна характеристики можуть бути використані і при аналізі ризику ОПЕН нафтогазового комплексу. Ризик від негативної події по-різному проявляється в соціальній, економічній та екологічній областях.

Повний соціально-еколого-економічний ризик від події А дорівнює сумі ризиків від цієї події в зазначених областях [4]:

$$R_{п}(A) = R_{с}(A) + R_{м}(A) + R_{е}(A). \qquad (13)$$

Повний ризик визначається за результатами детальних досліджень для окремих об'єктів у випадку виявлення всіх отриманих для різних факторів показників ризику в єдиних вартісних покажчиках.

Висновки

На підставі проведеного аналізу в цілому слід зазначити, що система оцінки системних ризиків, також як і оцінка впливів (збитку), представляє складну ієрархічну систему з нестаціонарними технологічними процесами, що відбуваються на різних стадіях реалізації проектних рішень в різних часових інтервалах. Отже дана методологія дозволяє врахувати зміну в часі умов виникнення і розвитку аварійних ситуацій, а також керувати мінімізацією ризику, тобто управляти прийнятною величиною ризику за кількісним критерієм раннього розпізнавання перед аварійної ситуації.

Список літератури

1. Лисанов, М.В. Методическое обеспечение декларирования промышленной безопасности [Текст] / М.В. Лисанов, А.С. Печеркин, В.И. Сидоров // Безопасность труда в промышленности. – 2000. – № 7. – С. 12–16.

2. Методология риска в надзорной деятельности. Проблемы и перспективы [Текст] / М.В. Лисанов и др.// Риск: наука, обучение, рынок труда: мат. межд. НПК, М. 13–17 окт. 1996 г. – М.: ВНИИПО, 1996. – С. 336–339.

3. Суворова, В.В. О выборе допустимого индивидуального риска [Текст] / В.В. Суворова, В.Ф. Мартынюк, С.А. Грудина // Безопасность жизнедеятельности. – 2005. – № 6. – С. 36–39.

4. Управление риском. Риск. Устойчивое развитие. Синергетика [Текст] / Под ред. Г.Г. Малинецкого. – М.: Наука, 2000. – 431 с.

Надійшла до редколегії 22.12.2016

Рецензент: д-р техн. наук, проф. О.А. Машков, Державна екологічна академія післядипломної освіти та управління, Київ.

РАЗРАБОТКА МЕТОДОЛОГИИ АНАЛИЗА СИСТЕМНЫХ РИСКОВ ПРИ ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ПОВЫШЕННОЙ ОПАСНОСТИ

А.С. Задунай, С.И. Азаров

Рассмотрено современное состояние разработки методологии анализа системных рисков при эксплуатации объектов повышенной опасности.

Ключевые слова: *объекты повышенной экологической опасности, аварийная ситуация, экологический риск.*

DEVELOPMENT OF METHODOLOGY FOR ANALYSIS OF SYSTEMIC RISKS IN THE OPERATION OF HIGH-RISK

O.S. Zadunaj, S.I. Azarov

The current state of development of systemic risk analysis methodology in the operation of high-risk.

Keywords: *objects of high environmental hazard, emergency, environmental risk.*

UDC 621.391

R.M. Zhyvotovskyi[1], Y.V. Tsimura[2], V.I. Nishchenko[2]

[1] *Central scientifically-explore institute of arming and military equipment, Kiev*
[2] *Military institute of telecommunications and informatization, Kiev*

METHOD OF FORMING RATIONAL VALUES PARAMETERS OF THE SIGNAL IN CONDITIONS OF DISTRIBUTION OF MULTIPATH RADIO WAVES

In the work offered method of forming rational values parameters of the signal in conditions of distribution of multipath radio waves. Specified method based on adaptive management parameters of the signal when dynamic changes of signal and noise conditions.

Keywords: *unmanned aviation complex, signal-code construction, speed of information transfer, bit error probability, radio-electronic suppression.*

Introduction. Experience of recent local conflicts, military training and fighting in eastern Ukraine unmanned aircraft systems increasingly using for solving tasks, communications and causing fire strikes on enemy positions [1]. As base technology of information transmission for unmanned aircraft systems using method of orthogonal frequency division multiplexing with OFDM (Orthogonal Frequency Division Multiplexing) [2, 7]. Main feature of OFDM signals invariance of phenomenon of multipath channel. However, these systems has drawbacks, the main ones are:

- high pic-factor;
- nonlinear distortion devices of radio communications;
- mistakes of synchronization;
- harmful effects of intentional interference.

Also characteristic of communication channels for unmanned aviation systems need permanent increasing range of management systems and data, increase data rates when working in unstable propagation. Conducted in uniforms [2, 7] analysis shows that using of OFDM technology does not fully satisfy all above requirements for control channels and communication with unmanned aircraft systems. One improving efficiency of radio communication systems is application of spatial processing signals in radio systems, including technology Multiple-Input Multiple-Output - MIMO [3,4]. In MIMO technology combined spatial-temporal methods of reception antennas using adaptive methods and space-time coding and space-time separation of signals.

Key feature is the ability to convert MIMO multipath propagation effects that significantly affects quality of wireless communication, advantage for user. Just MIMO makes it possible to improve operational performance without increasing required radio communication system bandwidth. Analysis different methods of improving efficiency wireless communication systems [2, 3, 4, 7] reveals number of contradictions. Growth channel bandwidth increases bandwidth of radio communication, but at the same time leads to increased noise power in channel. Increase transmitter power is ineffective and unacceptable in terms of ensuring the secrecy of radio communication.

Strategic direction in solving problem of improving effectiveness of information transfer is transition from system of rigid structure for adaptive systems [5, 6]. In adaptive algorithms systems for transmission and reception signals may vary depending on the agreed changes in external conditions. Algorithms should allow adaptation to work in conditions of minimal prior information to achieve optimum system parameters.

Searching alternatives of secure and speed control system and communications for unmanned aircraft systems showed that combined using OFDM and MIMO technologies for controlling and communication with unmanned aviation complexes are promising and appropriate.

Purpose is developing methods of forming rational parameters signal under conditions of multipath propagation. Methods of selecting rational parameters MIMO-OFDM-signal consists of following stages.

1. Data input. Introduced parameters and transmitter channel, value permissible value of probability of false signals and the minimum necessary information transfer rate.

2. Determination number of antennas in MIMO system. At that stage choosing depending on the channel number of transmitting and receiving antennas for unmanned aviation sector, taking into account required signal/noise ratio and required rate. So, if you set permissible speed MIMO-systems, fluctuations in average signals v_Σ, then threshold value $\lambda_{\text{threshold}}^{(Q^2)}$ for choosing necessary number of most powerful own channels, can search from equation:

$$P\left(\lambda_{\text{threshold}}^{(Q^2)}, Q_0^2\right) = 1 - v_\Sigma / v_{\max}.$$

So $\lambda_{\text{threshold}}^{(Q^2)}$ depends from average relation signal/noise Q_0^2, from this speed of data transfer $v_\Sigma = \left(\lambda_{\text{threshold}}^{(Q^2)} = \lambda_{\text{threshold}}^{(Q^2)} \left(Q_0^2, v_\Sigma \right) \right)$ and increase with increasing relation signal/noise Q_0^2.

3. Distribution of power between own channels.

With water filling method, carried out distribution of power between own channels. This procedure repeated at intervals of length group of characters that are divided flow signals.

4. Select number of subcarriers.

In OFDM group signal modem at interval transmission single character can be presented as [7]. At this stage, the number of selected subcarrier signal with OFDM, at which the predetermined signal / noise ratio. Evaluation of transmission characteristics of the communication channel. At this stage, using pilot-bearing condition estimated multipath channel and determines its transmission rate. In general, the assessment of the channel can be performed both direct and indirect methods. Also at this stage using method proposed in [6] assessed the state of multipath channel.

5. Convert channel with intersymbol distortion channel with set of Gaussian channels without memory. In real frequency-limited channels except additive noise occurs intersymbol interference (ISI), which is caused by memory channels. Reaction sequence channel input signals cause mutual overlay signal at output. As result of above conversion Gaussian channels with intersymbol interference in independent set of parallel Gaussian channels without memory input and output of each channel associated expression

$$Z_i = K_i X_i + B_i \ , \ i = \overline{0, L-1} .$$

6. Characterization previous distortion signals. Consider the approach to coding channels with ISI, based on a synthesis of signal-code designs that take into account the "deformation" space signals in the transmission channel for real [3]. To optimize parameters of OFDM signal group introduced prior to transmission signal distortion $X_i = \xi_i / |K_i|$ and correction on input $\xi_i = b_i Z_i$, where $b_i = e^{-j \arg K_i}$.

7. Determination of the average power of the output signal Gaussian channel without memory (GCWM). If the output channel has significant unevenness of amplitude-frequency characteristics in the band Nyquist is channels can be quite different. GCWM differences must be considered when building signals signal-code constructions (SCC).

Typically, in parallel with previous GCWM using different alphabets distortion signals with quadrature amplitude modulation (QAM), but at the same Euclidean minimum distance d, which is independent of number and GCWM. Need to consider possibility of constructing variant explained based on effective signal and signal-code constructions [7].

8. Organize subchannels in descending order of relation signal/noise ratio at receiver input. At this stage of evaluation of transmission characteristics of the channel assignment performed each subchannel sequence numbers in descending order of relation signal/noise (worse subchannels have larger numbers):

$$Q_1^2 \geq Q_2^2 \geq ... \geq Q_N^2 .$$

9. Iterative procedure disconnection subchannels doing by discarding inferior half of subchannels (subchannels screening poorer half, the redistribution of power on subchannel, adding better half in subchannels). Then the transmitter power is evenly distributed between other not unplugged (active) subchannels. Because through the redistribution of power by disabled subchannels signal / noise ratio in the active subchannels increases, it can be assumed that it is advisable not to turn off all subchannels for which $Q_i^2 \leq Q_{\text{per}}^2$, but only part of them.

10. Choosing rational signal-code constructions. At this stage of finite number of correcting codes and modulation types, determined by initial data, depending on the current signal / noise ratio for each subchannel determined by SCC, which allows to get maximum transmission rate while ensuring given probability of bit errors. Main stages of selecting optimal signal-code constructions are:

Based on parameters of radio and channel $\Psi = \{\psi_i\}$ and value of permissible value probability of bit error band of radio signals select the dimension N (design with one-dimensional, two-dimensional and multidimensional signals) and band structure signals. Detailed calculations of the probability of bit error for *M* positional signals with phase shift keying (PSK) and QAM are presented in [7]. Selects type correction code. In view of all SCC noise immunity codes can be divided into two major classes: on basis of block codes and based on continuous codes. In addition, a separate class consists SCC-based cascading of codes used both block and continuous codes.

Selects manipulation code. In agreeing codec binary code and noise-immune multiposition modem signals necessary to use manipulation code in which greater consideration in Hemet between code combinations to meet greater distance between Euclid signals that correspond to them. Control unit selection signal parameters should only choose from set of possible SCC optimal for channel status.

11. Calculation maximum rate in each subchannel. Maximum speed of each GCWM at fixed is defined as follows:

$$v\left(q_j, P_{q_j} / P_{\text{nonse}} \right) = v\left(q_j, d_E^2 \varphi^{(2^{q_j})} / P_{\text{nonse}} \right) .$$

12. Determination of maximum rate signal group. Total rate of GCWM given expression

$$v = v_0 \cdot \frac{1}{N} \cdot \sum_{j=1}^{Q} s_j \cdot \left(q_j, d_E^2 \varphi^{(2^{q_j})} / P_{\text{nonse}} \right),$$

where $s_j - m_j - m_{j-1}$, $m_0 = 0$ — number of GCWM with same alphabet QAM. Optimization options considered

by the speed with limited average signal power at the input channel comes down to choosing the optimal partitioning of parallel GCWM at the same rate, the optimal choice of alphabets and minimum FSK them. Accordingly, the maximum speed that can be achieved GCWM with previous distortions and arbitrary alphabets FSK in each of the parallel GCWM provided that the minimum distance in all alphabets constant and equal to d, given expression in the constraints described above, the permissible average power input signal GCWM, but $s_j = m_j - m_{j-1}, m_0 = 0,\ 0 < m_1 < m_2 < ... < m_Q \le M_1$ – breakdown many GCWM on groups with v_j parallel channels, each of which uses the same alphabet FSK with average power $P_{q_J} = d_E^2 x(2^{q_j})$.

13. Transfer next character. As result of determined parameters of next OFDM-symbol, number of active subchannels N_A and their numbers, M and R for each subchannel, information about value of which is transferred as part of service information for counter station.

Conclusion

1. In article offered method of forming rational parameters signal in terms of multipath radio propagation. Novelty of developed method is to adapt parameters of hybrid MIMO-OFDM-systems to improve the efficiency.

2. Novelty of technique lies in fact that optimal parameters signal-code constructions are determined in the case of transmitting information over communication channel. Also carried adaptive formation matrix subchannel by adaptive to signal-interference environment selection structure antenna system of unmanned aircraft systems, turning off generators matrices, thereby narrowing or expanding frequency range of signal OFDM (respectively decreasing or increasing number of subchannel) need to increase energy and frequency effectiveness of radio conditions of active electronic countermeasures.

Optimal parameters MIMO-OFDM-signal for particular channel state determined from finite allowable number of options that can simplify practical implementation of adaptive equipment modem radio communication systems.

Based on evaluation of efficiency techniques choice of rational parameters signal for unmanned aircraft systems to maximize energy efficiency, which amounted to about 2-3 dB depending on the depth of fading multipath channel, it can be argued that based on borders Shannon frequency efficiency using the proposed method and relevant SCC should rise in value of about 2-4 dB.

Direction of future research is development of information technology data for multipath channels of unmanned aviation systems.

References

1. Chekunov E. Using UAV AF of USA in military conflicts / E. Chekunov // Foreign military review. – 2010. – № 7. – P. 53-58.

2. Shyshatskyi A.V. Analysis of ways of increasing the efficiency of radio communication systems with orthogonal frequency multiplexing / A.V. Shyshatskyi, V.V. Lutov, O.G. Zhuk // Arms and military equipment. – K.: CSIAM AF of Ukraine, 2015. № 4(8) 2015. – P. 22-26.

3. Slusar V. Systems MIMO: principles of construction and signal processing / V. Slusar // Electronics: Science, Technology, Business. – 2005. – № 8. – P. 52-58.

4. Kuvshinov O.V. Analysis of performance of MIMO radio technology / O.V. Kuvshinov, D.A. Minochkin // Collection of scientific papers the Military Institute of Kyiv National Taras Shevchenko University. – Out. № 3 – K.: MIKNU, 2006. – P. 51 – 56.

5. Shishatskiy A. V. Methods of forming signal-code constructions OFDM-signal under influence of intentional interference and selective fading / A. V. Shishatskiy // Information processing systems. — 2015. — № 7. — P. 71-76.

6. Zhyvotovskyi R.M. Development method of dynamic control of channel in complex electronic environment / R.M. Zhyvotovskyi, A.V. Shishatskiy, V.V. Lutov // Collection of scientific papers CSIAM AF of Ukrine. – K.: CSIAM AF of Ukraine, 2016. № 1(60). – P. 253 –264.

7. Shyshatskyi A. V. Mathematical model of signal distortion in radio communication systems with orthogonal frequency multiplexing when subjected to intentional interference / A.V. Shyshatskyi, V.V. Lutov, M.V. Boroznuk, I.U. Rubtsov // Information processing systems. — 2016. — №3. — P. 181-186.

Надійшла до редколегії 18.01.2017

Рецензент: д-р техн. наук, проф. І.О. Романенко, Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ.

МЕТОДИКА ФОРМУВАННЯ РАЦІОНАЛЬНИХ ЗНАЧЕНЬ ПАРАМЕТРІВ СИГНАЛУ В УМОВАХ БАГАТОПРОМЕНЕВОГО ПОШИРЕННЯ РАДІОХВИЛЬ

Р.М. Животовський, Ю.В. Цімура, В.І. Ніщенко

В роботі запропонована методика формування раціональних значень параметрів сигналу в умовах багатопроменевого поширення радіохвиль. Зазначена методика базується на адаптивному управлінні параметрами сигналу при динамічній зміні сигнально-завадової обстановки.

Ключові слова: *безпілотний авіаційний комплекс, сигнально-кодова конструкція, швидкість передачі інформації, ймовірність бітової помилки, радіоелектронне подавлення.*

МЕТОДИКА ФОРМИРОВАНИЯ РАЦИОНАЛЬНЫХ ЗНАЧЕНИЙ ПАРАМЕТРОВ СИГНАЛА В УСЛОВИЯХ МНОГОЛУЧЕВОГО РАСПРОСТРАНЕНИЯ РАДИОВОЛН

Р.Н. Животовский, Ю.В. Цимура, В.И. Нищенко

В работе предложена методика формирования рациональных значений параметров сигнала в условиях многолучевого распространения радиоволн. Указанная методика основана на адаптивном управлении параметрами сигнала при динамическом изменении сигнально-помеховой обстановки.

Ключевые слова: *беспилотный авиационный комплекс, сигнально-кодовая конструкция, скорость передачи информации, вероятность битовых ошибок, радиоэлектронноее подавление.*

УДК 621.391

О.Г. Жук

Військовий інститут телекомунікацій та інформатизації, Київ

КОНЦЕПЦІЯ ОРГАНІЗАЦІЇ ВЗАЄМОДІЇ ЕЛЕМЕНТІВ ВІЙСЬКОВИХ СИСТЕМ РАДІОЗВ'ЯЗКУ

В роботі запропонована нова наукова концепція, за допомогою якої здійснюється організація взаємодії і узгодження моделей елементів військових систем радіозв'язку.

Ключові слова: *система радіозв'язку, графова модель, системне рішення, радіоелектронне подавлення, навмисні завади.*

Вступ

Сучасні військові системи радіозв'язку (ВСРЗ) являють собою складні системи розподіленою багатозв'язною структурою, в яких використовується весь комплекс існуючих технологій передачі інформації та різні комбінації каналів зв'язку, а також комунікаційне і технологічне обладнання [1 – 4]. Крім того, ВСРЗ повинні функціонувати в умовах складної радіоелектронної обстановки при впливі селективних завмирань, комплексу природних та навмисних завад [5 – 7].

На сьогоднішній день немає налагодженої, універсальної, єдиної методології, за допомогою якої, можна провести весь комплекс заходів по моделюванню, створенню і адаптації таких систем. Відсутність методології призводить до виникнення найрізноманітніших підходів до їх реалізації, які базуються на інтуїції й досвіді розроблювачів, при цьому використовується безліч технологій побудови, стандартів, різних методик і моделей, що призводить до зростання вартості системи. Аналіз відомих методів та методик [8–11] показав, що в них недостатньо розкриті питання взаємодії окремих елементів ВСРЗ при синтезі системи в цілому.

Тому ***метою статті*** є розробка наукової концепції організації взаємодії елементів військової системи радіозв'язку.

Виклад основного матеріалу дослідження

Створення і адаптація ВСРЗ пов'язані з оптимізацією й прийняттям рішень, як на рівні окремих часткових завдань, так і для всієї системи в цілому. Основну увагу тут варто зосередити на виборі альтернативних системних рішень, механізмів їх реалізації та визначенні найбільш ефективного або базового варіанта системи. Отже, потрібні методи, які дозволяли б уже на самих ранніх етапах створення і адаптації ВСРЗ досить правильно вибрати їх параметри та структуру, а також оцінювати різні характеристики якості, з тим, що б одержати системне рішення, яке не потребує серйозних змін у майбутньому.

Проблеми створення і адаптації ВСРЗ багато в чому схожі, тому адаптацію існуючих систем доцільно проводити на основі багатоваріантного синтезу системних рішень з врахуванням уже наявної системи та умов, що змінюються, відповідно до принципів модульності та стандартизації [9, 12, 13].

Процес багатоваріантного синтезу концептуального системного рішення подано на рис. 1.

Реалізація моделюючого комплексу запропонована на основі багаторівневого подання ВСРЗ – ієрархічної системи декількох взаємодіючих рівнів, які відповідають певному класу практичних завдань створення і адаптації з урахуванням критеріїв оцінки якості. В базі еталонних моделей представлені моделі і параметри ВСРЗ по кожному рівні ієрархії, а також необхідна довідкова інформація. Крім того, база містить мережні рішення та наявні наробітки в даній області.

Найбільш важливим є модуль організації взаємодії моделей елементів ВСРЗ. Його функціональне призначення – організація роботи модуля аналізу параметрів і моделей, розрахункового модуля, оцінка точності та калібрування моделей. В ньому реалізуються процеси організації взаємодії моделей мережних елементів. Проводиться аналіз характеристик моделей, аналіз і узгодження одиниць виміру вхідних і вихідних параметрів моделей елементів системи в процесі рішення кожного конкретного завдання при розробці варіантів ВСРЗ. Аналіз всієї системи на основі ієрархічного комплексу здійснюється за допомогою графової моделі.

Функціональне призначення модуля аналізу параметрів і моделей – визначення необхідних параметрів системи при рішенні часткових завдань створення і адаптації та побудова залежності критеріїв оцінки якості для кожного рівня системної ієрархії.

Розрахунковий модуль призначений для одержання на основі теоретико-розрахункових методів значень системних параметрів і характеристик, які можуть бути вихідними даними для наступних розрахунків ВСРЗ в цілому і по кожному системному елементі окремо.

Рис. 1. Процес багатоваріантного синтезу концептуального системного рішення варіанту побудови ВСРЗ

Організація взаємодії моделей елементів мереж при різноманітному синтезі системних рішень включає такі етапи:

визначення параметрів і характеристик розроблювальної системи;

аналіз взаємозв'язку параметрів і моделей елементів системи на основі розробленої структури ієрархічного моделюючого комплексу;

калібрування моделей, узгодження вхідних і вихідних параметрів моделей системи та її елементів, тобто вибір відповідних завдань створення й адаптації (визначення класів і підкласів завдань), виявлення приналежності кожного параметра системи до конкретних моделей;

побудова і аналіз графової моделі військової системи радіозв'язку.

ВСРЗ представляється у вигляді глобальної керованої мережі радіозв'язку, що складається з множини локальних підмереж радіозв'язку (рис. 2). Кожна з підмереж характеризується графом

$$G_q(\mathbf{V}^q, \mathbf{E}^q) \quad (q = \overline{1,Q}),$$

де $\mathbf{V}^q = \left\{V_i^q\right\}$ – множина вузлів, а $\mathbf{E}^q = \left\{E_{ij}^q\right\}$ – множина напрямів зв'язку або окремих радіоліній (радіоканалів) між вузлами V_i і V_j. При цьому вузли, можуть виконувати функції відправників, одержувачів або ретрансляторів повідомлень. Надалі, будемо розглядати вузли та канали, якими вони зв'язані в межах підмережі радіозв'язку q-го рівня ВСРЗ.

Початковими умовами для рішення задачі побудови адаптивної ВСРЗ є [3, 9]:

параметри вузла V_i: режим роботи засобу радіозв'язку, потужність сигналу, ймовірність помилкового приймання сигналів, розмірність ансамблю сигналів, швидкість коригувального коду, величина кодової відстані, швидкість передачі інформації; кількість активних піднесучих (у режимі ортогонального частотного мультиплексування), робоча частота, швидкість та алгоритм перестроювання частоти в режимі псевдовипадкового перестроювання робочої частоти;

параметри радіоканалу: оцінка частотної характеристики багатопроменевого каналу, відношення сигнал/(завада + шум); ширина смуги пропускання каналу, протокол множинного доступу до радіоканалу, ширина смуги навмисної завади; амплітуда навмисної завади; вид навмисної завади.

Найважливішими характеристиками, що визначають граф глобальної мережі $G(\mathbf{V}, \mathbf{E})$, є:

матриця зв'язності розмірністю $N \times N$

$$\mathbf{S}(t) = \left\|s_{ij}(t)\right\|, \qquad (1)$$

елементи якої визначаються як

$$s_{ij}(t) = \begin{cases} 1, & \text{якщо } E_{ij} \in \mathbf{E}, \\ 0, & \text{якщо } E_{ij} \notin \mathbf{E}; \end{cases}$$

матриця-стовпець координат місць розташування окремих вузлів зв'язку (ОВЗ) в просторі розміру $N \times 1$:

$$\mathbf{K}(t) = \left\|k_i(t)\right\|, \qquad (2)$$

де елементи $k_i(t)$ – координати ОВЗ $R_i (i = \overline{1,N})$;

матриця взаємного віддалення ОВЗ розміру $N \times N$:

$$\mathbf{R}(t) = \left\|r_{ji}(t)\right\|, \qquad (3)$$

в якій елементи $r_{ij}(t)$ – відстані між ОВЗ V_i і ОВЗ V_j $(i, j = \overline{1,N};\ i \neq j)$.

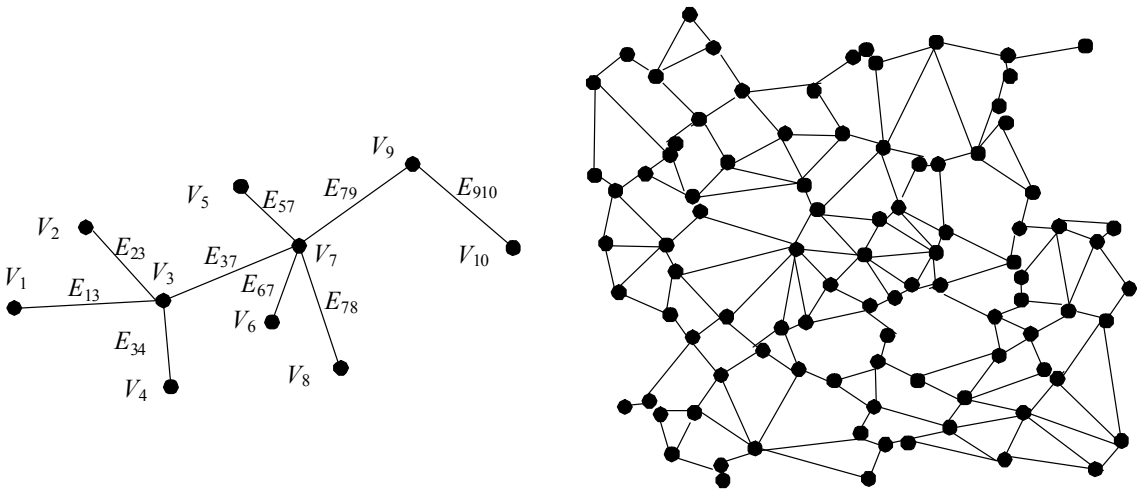


Рис. 2. Приклади структурних моделей ВСРЗ

Залежність елементів матриць (1) – (3) в часі означає той факт, що структура і топологія глобальної мережі радіозв'язку можуть змінюватися в процесі нормального функціонування (наприклад, під впливом протиборчої системи).

Позначимо через $\mathbf{R}_{ij} = \bigcup R_{ij}(m)$ множину можливих маршрутів передачі потоків повідомлень від ОВЗ V_i до ОВЗ V_j $(i, j = \overline{1,N};\ i \neq j)$ з числом складених ділянок $\tau = 1, 2$ (розглядаються тільки прямі канали радіозв'язку і обхідні шляхи з використанням лише однієї ретрансляції повідомлень). Тоді зв'язність повнозв'язної комутованої глобальної мережі радіозв'язку $M_{ij} = \left|\mathbf{R}_{ij}\right| = N - 1$.

Проведемо ієрархічну декомпозицію ВСРЗ. У загальній розподіленій структурі даної глобальної комутованої мережі радіозв'язку виділимо за ознакою оперативного призначення або регіональною ознакою Q локальних підмереж радіозв'язку $(Q > 1)$, кожна з яких характеризується підграфом

$$G_q(\mathbf{V}^q, \mathbf{E}^q) \quad (q = \overline{1,Q}),$$

де $\mathbf{V}^q = \left\{V_i^q\right\}$ – множина ОВЗ, а $\mathbf{E}^q = \left\{E_{ij}^q\right\}$ – множина напрямів зв'язку або окремих радіоліній між ОВЗ V_i і ОВЗ V_j, в q-й підмережі $(i, j = \overline{1, N_q};\ \sum_{q=1}^{Q} N_q = N;\ i \neq j)$. При цьому для $\forall q,\ p = \overline{1,Q};\ q \neq p$ вірно $\mathbf{V}^q \cap \mathbf{V}^p = \varnothing,\ \mathbf{V} = \bigcup_{q=1}^{Q} \mathbf{V}^q$.

Якщо передача потоків повідомлень будь-яким з маршрутів, задіяних за даним напрямом q-ї підмережі, виявляється неможливою (наприклад, внаслідок різкої зміни умов розповсюдження радіохвиль на трасі або дії завад), для передачі інформації адресатові виділяються радіолінії, задіяні для роботи в іншій, зокрема, p-ої підмережі. Кількість можливих маршрутів передачі в кожній q-й підмережі $M_q \leq N_q - 1$, а загальна їх кількість між двома ОВЗ в глобальній мережі $M \leq N - 1$. Всі можливі обхідні маршрути передачі повідомлень між двома будь-якими ОВЗ будь-якої підмережі радіозв'язку з використанням ОВЗ інших підмереж утворюють безліч ребер $E' = E \Big/ \bigcup_{q=1}^{Q} E^q$.

Величину Q при декомпозиції структури ВСРЗ можна трактувати як число рівнів ієрархії ОВЗ або кількість можливих зон обслуговування повідомлень (підмереж радіозв'язку з безліччю прямих і складених каналів між ОВЗ цих підмереж) в глобальній мережі радіозв'язку. В принципі на етапі планування ВСРЗ завжди можна добитися того, щоб кількість зон обслуговування була рівною числу рівнів ієрархії ОВЗ за їх оперативною приналежністю.

Ієрархічною структурою (або структурою з жорсткою ієрархією) мережі радіозв'язку називатимемо послідовність часткових графів (підграфів) $G_q(q = \overline{1,Q})$, впорядковану за допомогою відношення строгого домінування

$$G = G_1 \succ G_2 \succ \cdots \succ G_q \succ \cdots \succ G_Q, \qquad (4)$$

де $G_Q = G_Q(\mathbf{V}^q, \mathbf{E}^q)$.

Внаслідок можливого виходу з ладу і відновлення деякої множини елементів глобальної мережі радіозв'язку спочатку встановлені ієрархічні взаємозв'язки між ОВЗ можуть порушуватися випадковим чином. Тому в загальному випадку структура мережі радіозв'язку носитиме імовірнісний характер.

Випадковість знаходження будь-якого часткового графа підмережі G_q на p-му рівні $q, p = \overline{1,Q};\ q \neq p$ призводить до появи ансамблю **A** ієрархічних структур глобальної мережі радіозв'язку, що характеризуються графом G (**V**, **E**). Кожній структурі a_q в ансамблі **A** можна поставити у відповідність ймовірність її реалізації, а отже, визначити на ансамблі **A** функцію розподілу ймовірностей $P(a_q)$, де $a_q \in \mathbf{A}, q = \overline{1,Q}$.

Таким чином, імовірнісною ієрархічною структурою глобальної мережі радіозв'язку називатимемо ансамбль **A** ієрархічних структур із заданою на ньому функцією розподілу ймовірностей $P(a_q)$:

$$P = \left\{ \mathbf{A}, P(e_q) / a_q \in \mathbf{A};\ q = \overline{1,Q} \right\}. \qquad (5)$$

Таке представлення ВСРЗ дозволяє зручно формалізувати структуру ВСРЗ і значно спростити кількісну оцінку структурної стійкості системи.

У процесі організації взаємодії моделей елементів при створенні та адаптації ВСРЗ залежно від конкретних завдань і з метою економії часових і обчислювальних ресурсів здійснюється декомпозиція структури ієрархічної багаторівневої графової моделі системи з урахуванням числа зв'язків і аналізуються окремі підграфи. Далі встановлюються необхідні математичні залежності між підграфами й, після цього, аналізується система в цілому.

За допомогою багаторівневої графової моделі ВСРЗ створення й адаптацію системи можна розпочинати з будь-якого завдання (моделі), якій відповідає вершина графа (одна або декілька).

Висновки

У статті запропонована нова наукова концепція для організації взаємодії моделей елементів військових систем радіозв'язку у складі ієрархічного комплексу, що дозволяє: здійснювати організацію взаємодії розрізнених моделей і їх узгодження по параметрам і характеристикам ВСРЗ, за часом розрахунків, точністю й одиницями виміру; оперувати із уже існуючими моделями, а також включати до складу комплексу нові моделі, забезпечуючи можливість поповнення, удосконалювання й відновлення моделей; інтегрувати моделі комплексу залежно від конкретної ситуації створення й адаптації; моделювати мережі і їх елементи; проводити різноманітні розрахунки й багаторівневе моделювання; ефективно оцінювати мережні параметри та характеристики.

Напрямком подальших досліджень є розробка концепції адаптивного управління топологією радіомереж спеціального призначення.

Список літератури

1. Шишацький А.В. Розвиток інтегрованих систем зв'язку та передачі даних для потреб Збройних Сил / А.В. Шишацький О.М. Башкиров, О.М. Костина // Науково-технічний журнал "Озброєння та військова техніка". – К.: ЦНДІ ОВТ ЗС України, 2015. № 1(5) 2015. – С.35 –40.

2. Аналіз шляхів вдосконалення засобів радіозв'язку мережі радіодоступу військової телекомунікаційної системи / Т.Г. Гурський, С.О. Кравчук [та ін.] // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2007. – Вип. 1. – С. 30–42.

3. Гостев В.И. Динамическое управление радиоресурсом в системах связи / В.И. Гостев, В.Е. Федяев, Д.А. Худолий. – К: Радіоаматор, 1998. – 412 с.

4. Системы связи и управления. Средства телекоммуникаций [Електронний ресурс] // Mode of access: http://www.svyazexpo.rasu.ru/index.php?rubr=2.

5. Агафонов А.А. и др. Современная радиоэлектронная борьба. Вопросы методологии / под ред. В. Г. Радзиевского. – М.: Радиотехника, 2006. – 424 с.

6. Куприянов А.И. Теоретические основы радиоэлектронной борьбы: Учеб, пособие / А.И. Куприянов, А.В. Сахаров. – М.: Вузовская книга, 2007. – 356 с.

7. Кондратьев А. Перспективный комплекс РРТР и РЭВ сухопутных войск США „Профет" / А. Кондратьев // Зарубежное военное обозрение. – 2008. – № 7. – С. 37–41.

8. Кувшинов О.В. Адаптивне управління засобами завадозахисту військових систем радіозв'язку / О.В. Кувшинов // Збірник наук. праць ВІКНУ. – 2009. – Вип. 17. – С. 125–130.

9. Стеклов В. К. Оптимізація та моделювання пристроїв і систем зв'язку / В.К. Стеклов, Л.Н. Беркман, Є.В. Кільчицький. – К.: Техніка, 2004. – 576 с.

10. Міночкін А.І. Проблема створення системи управління мобільною компонентою мереж зв'язку військового призначення / А.І. Міночкін // Збірник наукових праць № 5. – К.: ВІКНУ. – 2006. – С. 86–97.

11. Alberts D. Network Centric Warfare: Developing and Leveraging Information Superiority / D. Alberts, J. Garstka, F. Stein // CCRP Publication Series. – Washington, 2000. – P. 2–3.

12. Голяницкий И.А. Математические модели и методы в радиосвязи / И.А. Голяницкий; под ред. Ю.А. Громакова. – М: Эко-Трендз, 2005. – 440 с.

13. Голдсмит А. Беспроводные коммуникации / А. Голдсмит. – М.: Техносфера, 2011 – 904 с.

Надійшла до редколегії 25.01.2017

Рецензент: д-р техн. наук, проф. І.О. Романенко, Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ.

КОНЦЕПЦИЯ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ЭЛЕМЕНТОВ ВОЕННЫХ СИСТЕМ РАДИОСВЯЗИ

А.Г. Жук

В работе предложена новая научная концепция, с помощью которой осуществляется организация взаимодействия и согласование моделей элементов военных систем радиосвязи.

Ключевые слова: *система радиосвязи, графовая модель, системное решение, радиоэлектронное подавление, преднамеренные помехи.*

THE CONCEPT OF THE ORGANIZATION OF INTERACTION ELEMENTS OF MILITARY RADIO COMMUNICATION SYSTEMS

A.G. Zhuk

In article offered a new scientific concept, which is organization of interaction and coordination models of the elements of military radio communication systems.

Keywords: *telecommunication system, the graph model, the system solution, electronic jamming and intentional interference.*

УДК 621.391

О.Ю. Іохов, В.Є. Козлов, В.Г. Малюк, К.М. Ткаченко, М.Д. Ткаченко

Національна академія Національної гвардії України. Харків

РАДІОМАСКУВАННЯ ВІЙСЬКОВИХ ПІДРОЗДІЛІВ ЗА УМОВ ЗАСТОСУВАННЯ ШТАТНИХ ТА ІМПРОВІЗОВАНИХ ЗАСОБІВ

В статті розглянуто спосіб комплексного застосування заходів активного радіомаскування з використанням спеціальних засобів радіоелектронного придушення (РЕП), що може бути використаний для побудови локальних систем радіозв'язку, призначених для обміну конфіденціальною інформацією в діапазоні ультракоротких хвиль в умовах штучних радіозавад і спроб несанкціонованого доступу до інформації, що передається.

Ключові слова: *система радіозв'язку, активне радіомаскування, розвідзахищеність, ультракороткі хвилі.*

Аналіз публікацій та постановка проблеми

Ведення радіоелектронної розвідки є невід'ємною частиною процесу отримання розвід даних. Аналіз досвіду проведення антитерористичної операції в Донецькій та Луганській областях України виявив неспроможність існуючої системи радіозв'язку НГУ забезпечити захист від дії засобів радіорозвідки противника (ЗРРПр). Це обумовлено використанням у військових підрозділах таких радіо засобів як Vertex VX-1210, MOTOTRBO DM 4601, MOTOTRBO DP 4801, MTR3000, що не пристосовані до захисту від ЗРРПр. Таким чином, використання зазначених радіозасобів вимагає ретельного вибору технічних засобів та/ або проведення організаційних заходів з радіомаскування (РМ).

Висунемо наукову гіпотезу про можливість забезпечення розвідзахищеного радіообміну підрозділи НГУ в обмеженому просторі шляхом застосування штатних та імпровізованих засобів пасивного та активного маскування.

Проведений у роботі [1] аналіз показав, що виконання окремих заходів пасивного РМ не забезпечує досягнення необхідного рівня захищеності за умови стабільної роботи радіомережі.

Орієнтовні розрахунки дають можливість стверджувати про необхідність комплексного застосування заходів маскування з використання спеціальних засобів радіоелектронного придушення (РЕП) [2, 3], що здатні створювати на вході приймача радіорозвідки перешкоди з необхідним рівнем потужності.

У роботах [4, 5] надані практичні рекомендацій щодо підвищення безпеки радіомереж тактичної ланки управління НГУ, однак вони не враховують необхідність постановки завад декількома джерелами для декількох засобів зв'язку підрозділів НГУ та розташування засобів радіоелектронної розвідки (РЕР) на висотах або на повітряних носіях.

Викладене вище зумовлює **актуальність та мету статті** – розглянути спосіб радіомаскування військових підрозділів за умов застосування штатних та імпровізованих засобів активного маскування.

Виклад основного матеріалу

Термін активне радіомаскування, як він розуміється в даний час, означає протидію радіо- і радіотехнічній розвідці шляхом створення спеціальних полів перешкод, що ускладнюють несанкціонований прийом сигналу засобами радіотехнічної розвідки і виділення повідомлень засобами радіорозвідки. Потребує уточнення істотно важливе обмеження:: перешкоди не повинні заважати роботі систем, що маскуються, тобто не повинні знижувати показники якості і ефективності радіозв'язку нижче деякого прийнятного рівня.

В [6] розглянуто спосіб захисту інформаційного обміну в локальній системі радіозв'язку, заснований на зменшені відношення сигнал/ шум для приймачів, що здійснюють спробу несанкціонованого доступу до інформації, яка передається, за рахунок того, що під час роботи системи радіозв'язку неперервно випромінюють за периметр системи і вгору шумові сигнали, які мають потужність більшу потужності робочих сигналів в системі радіозв'язку, що перекривають усю смугу частот, використовуваних в системі. Цей спосіб складний для побудови, потребує великих матеріальних та енергетичних витрат, а його фізичні (у смузі частот, використовуваних в системі) та візуальні (специфічний вигляд та розміри антен захисту і каналів зв'язку) якості є демаскуючими ознаками, що унеможливлюють скритне застосування.

Спосіб захисту інформації, розглянутий в роботі [7], передбачає використання окремо або в різних сполученнях будови системи зв'язку, при якій канали зв'язку мають мінімальний витік енергії за рахунок зменшення відношення сигнал/ шум для приймачів, що здійснюють спробу несанкціо-

нованого доступу до інформації, яка передається, шляхом зниження потужності робочих сигналів і неперервного випромінювання за периметр системи і вгору шумових сигналів, і канали передавання інформації з конфігурацією, що управляється. Недоліком цього способу є складність побудови системи зв'язку, зумовлена необхідністю використання абонентських радіостанцій зі спеціальними засобами формування, передавання, приймання та фільтрації шумових сигналів, і неможливість скритного застосування, обумовлена візуальними (специфічний вигляд та розміри антен каналів зв'язку) демаскуючими ознаками.

Спосіб захисту інформаційного обміну в локальній системі радіозв'язку [8], на відміну від попереднього, передбачає застосування сумісно скритних антенних пристроїв захисту і каналів передавання інформації з конфігурацією, що управляється.

Цей спосіб не забезпечує захист від спроб несанкціонованого доступу до інформації, яка передається, розвідувальних приймачів, розміщених на повітряних носіях, що переміщаються вище верхнього рівня основної пелюстки діаграми направленості (ДН) в площині кута місця антенних пристроїв захист, тобто розміщених у будь-якій точці простору.

Для реалізації сформульованої наукової гіпотези доцільним є сумісне застосування скритних антенних пристроїв захисту і каналів передавання інформації з конфігурацією, що управляється; при цьому, антенні пристрої захисту мають забезпечувати орієнтування діаграми направленості в визначених азимутальному напрямку β та куті місця ε.

На рис. 1 наведено в азимутальній площині варіант побудови локальної системи радіозв'язку (ЛСР), а на рис. 2 – фрагмент ЛСР в площині кута місця.

У кампусі – обмеженій території з постійним складом і місцем розміщення (студентське або військове містечко, майдан тощо) – розташовують один або декілька абонентів (А) 1 зв'язку, один або декілька пунктів управління (ПУ) 2, що удвох створюють канал передавання інформації (КПІ), та один або декілька пристроїв захисту (ПЗ) 3 відносно одного або декількох розвідувальних приймачів (РП), розміщених на площині 4 або на повітряних носіях 5 (безпілотні літальні апарати, квадрокоптери, повітряні змії або кулі) таким чином, щоб забезпечити надійний захист від спроб несанкціонованого доступу до інформації, яка передається, і електромагнітну сумісність засобів (ЕМС) ЛСР та мереж бездротового зв'язку легальних користувачів.

Конфігурація ЛСР змінюється зі зміною обстановки (переміщенні РП) шляхом взаємного переміщення відносно РП і один до одного ПЗ та КПІ (абонентів і, при необхідності, ПУ) таким чином, щоб директриси ДН ПЗ були спрямовані на розміщений у просторі або рухомий РП при умові забезпечення ЕМС.

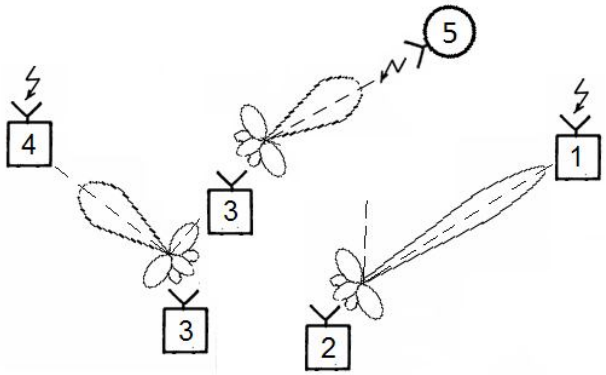


Рис. 1. Варіант побудови
локальної системи радіозв'язку

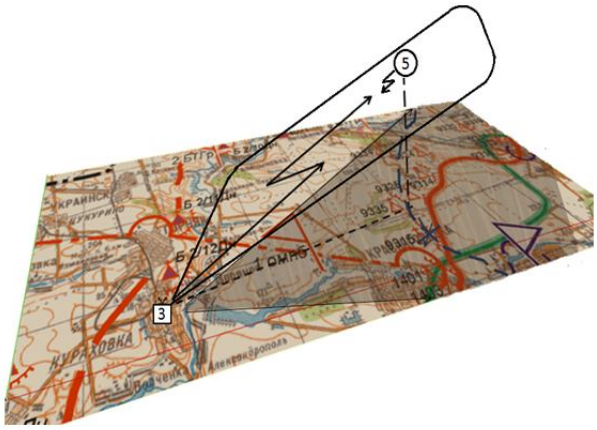


Рис. 2. Фрагмент ЛСР в площині кута місця

Адаптація до змін умов функціонування ЛСР потребує вирішення низки завдань, зокрема, визначення точок розміщення РП, оптимізації розташування ПЗ, розрахунку їх мінімальної потужності, розрахунку покриття, інтерференцій.

Перелічені завдання вирішує програмний виріб (ПВ) HTZ warfare, який може використовуватися на обчислювальному засобі (ноутбук, планшет тощо) ПУ. Результати розрахунків відображаються в 3D-форматі, що дозволяє уявити радіоелектронну обстановку у будь-якій точці об'єкта аналізу та визначити азимут β та кут місця ε окремого розвідувального приймача або зони його баражування, як показано на рис. 2.

В якості антен абонентів зв'язку 1 та пристроїв захисту 3 можуть застосовуватися антенні пристрої [9] або їм подібні, що забезпечують скритність застосування. Для пунктів управління 2 доцільне використання антенних пристроїв з більш вузькою діаграмою направленості [5].

Захист від засобів РР, розміщених у просторі можна забезпечити антенний пристрій [12], зовнішній вигляд якого наведено на рис. 3, що склада-

ється із куткового дзеркала (рефлектора) 1, утвореного двома пласкими металевими пластинами, і вібратора або системи колінеарних вібраторів 2, містить шарнірно приєднану усередині вершини дзеркала лінійку 3, розташовану у площині бісектриси кута дзеркала, з повзунком 4, який з обох боків з'єднаний шарнірно з пластинами дзеркала, та оптичного візиру 5, розташованого зверху рефлектора у площині бісектриси його кута.

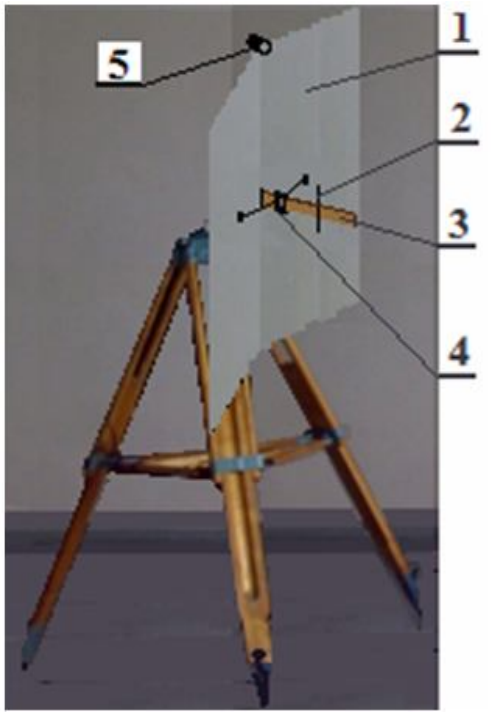


Рис. 3. Антенний пристрій

На рис. 4 наведено зовнішній вигляд повзунка 4 з нанесеною шкалою 6 кута нахилу рефлектора у площині кута місця, стрілкою-виском 7 і фіксатором 8.

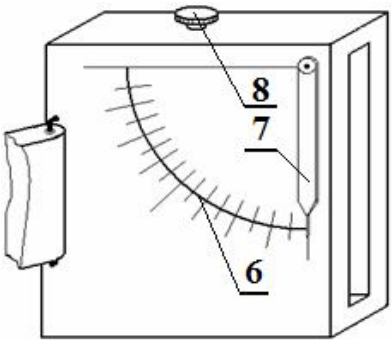


Рис. 4. Зовнішній вигляд повзунка 4

Переміщенням повзунка 4 встановлюють потрібний кут φ розкриву дзеркала, який фіксують фіксатором 8.

Кут місця ε можна також встановити за шкалою 6 і стрілкою-виском 7 без використання візиру (у випадку відсутності візуального контакту з ціллю).

Рис. 5 – частина лінійки 3 із градуюванням кутової шкали у значеннях кута розкриву дзеркала для довжини плеча шарнірного з'єднання повзунка 77 мм.

Наведення ДН антенного пристрою в потрібних азимутальному напрямку β та куті місця ε здійснюють за допомогою візиру 5, оптична вісь якого співпадає з бісектрисою кута дзеркала і перпендикулярна до нього; положення дзеркала фіксують, при цьому стрілка-висок 7 показує на шкалі 6 значення кута місця ε у напрямку максимуму ДН.

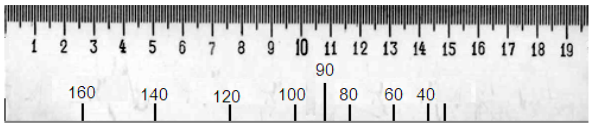


Рис. 5. Частина лінійки 3

При зміні кута розкриву дзеркала з φ_1 на φ_2 лінійка залишається у площині бісектриси кута завдяки рівноплечому шарнірному з'єднанню повзунка з пластинами дзеркала (рис. 6).

Зміна кута розкриву φ та відстані вібратора (системи вібраторів) від вершини дзеркала дозволяє змінювати ширину ДН та кількість її пелюстків в азимутальній площині з метою визначення азимуту цілі однопелюстковим методом максимуму або двохпелюстковим методом мінімуму.

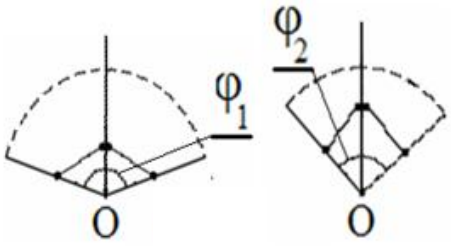


Рис. 6. Кута розкриву дзеркала

Розглянуте технічне рішення забезпечує точне наведення діаграми направленості у напрямку цілі (об'єкта спостереження) і може бути використана для пеленгування та/або придушення джерела радіовипромінювання (завад), розміщеного на повітряному носії.

Це гарантує адаптованість до будь-якої обстановки, що склалася в системі, і захист локальної системи радіозв'язку.

Антенний пристрій можна встановлювати на поворотному пристрої (наприклад, тринозі) на ґрунті, авто-та бронетехніці тощо.

На рис. 3 наведено зовнішній вигляд розміщеного на тринозі антенного пристрою у складі куткового дзеркала 1, вібратора (системи вібраторів) 2, лінійки 3 із повзунком 4 та оптичного візиру 5.

Аналіз характеристик перешкод показав [2, 3], що за характером впливу найбільш ефективними є імітуючі або прицільні активні перешкоди, які

ускладнюють виявлення і розпізнавання корисного сигналу та дозволяють вносити неправдиву інформацію.

На озброєнні підрозділів НГУ відсутні будь-які засоби постановки навмисних завад. У застосовуваних радіостанціях MOTOTRBO використовується два режими роботи: цифровий та аналоговий. Виходячи з цього, в якості навмисної завади можна використовувати сигнал радіостанції в аналоговому режимі для подавлення цифрового корисного сигналу та навпаки.

Проведений натурний експеримент з побудови розглянутого способу активного радіомаскування підтвердив його працездатність.

Висновки

Розглянутий спосіб радіомаскування з використанням імпровізованих антенних пристроїв та штатних засобів радіозв'язку може забезпечити розвідзахищений радіообмін підрозділів НГУ в обмеженому просторі, що дає змогу вважати доведеною висунуту в постановчій частині статті наукову гіпотезу.

Список літератури

1. Журавський Ю.В. Аналіз впливу заходів радіомаскування на розвідзахищеність радіоелектронних засобів / Ю. В. Журавський, Р. М. Жовноватюк, Г. Д. Носова, А. А. Завада // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. - 2015. - Вип. 10. - С. 43-50.

2. Куприянов А.И. Теоретические основы радиоэлектронной борьбы [Текст]/ А. И. Куприянов, А. В. Сахаров. – М.: Вузовская книга, 2007.- 356 с.

3. Активная радиомаскировка. Режим доступу: http://studopedia.media4biz.ru /2_46668_aktivnaya-radiomaskirovka.html.

4. Розроблення рекомендацій щодо підвищення безпеки радіомереж тактичної ланки управління ВВ МВС України: науково-дослідна робота [Текст]/ О.Ю. Іохов, І.В. Кузьминич, О.М. Горбов, О.О. Казіміров, О.М. Орлов, С.А. Горєлишев та інші – № держреєстрації 0112U000529. – Х.: Академія внутрішніх військ, 2012. – 175 с.

5. Іохов О.Ю. Основні аспекти радіоелектронного захисту системи радіозв'язку тактичної ланки управління внутрішніх військ МВС України під час виконання завдань за призначенням в умовах міста[Текст] / О.Ю. Іохов, В.В. Антонець, О.М. Горбов, І.В. Кузьминич, В.В. Овчаренко // Честь і закон. – Х. : Акад. ВВ МВС України, 2012. - № 4. – С. 40-47.

6. Пат. РФ №2114513, МПК (2006. 01) H04K 3/00. Способ защиты информационного обмена в локальной системе радиосвязи/ Опубл. 27.06.1998 [Электронный ресурс]. – Режим доступа: http://www.freepatent.ru.

7. Левин В.Н. Концептуальная основа информационной безопасности компьютерных сетей, технология электронных коммуникаций [Текст]/ В.Н. Левин, Д.М. Платонов, Ю.А. Тимофеев// Информационная безопасность компьютерных сетей. – Т. 45. – М.: Экотрендз, 1993. – С. 5-43.

8. Пат. України №104505 на корисну модель, МПК (2015.01) H04B 7/00. Спосіб захисту інформаційного обміну в локальній системі радіозв'язку/ Опубл. 10.02.2016, Бюл. №3.

9. Пат. України №95314 на корисну модель, МПК (2015.01) H04B 7/00. Антенний пристрій/ Опубл. 25.12.2014, Бюл. №24.

10. Кочержевский Г.И. Антенно-фидерные устройства [Текст]/ Г.И. Кочержевский. – М.: Связь, 1972. – 472 с.

11. Пат. РФ №2288528, МПК (2006. 01) H01 Q19/13. Уголковая антенна с повышенным коэффициентом направленного действия/ Опубл. 27.11.2006/ [Електронний ресурс]. – Режим доступу: http://www.freepatent.ru.

12. Пат. України на корисну модель №105732, МПК (2016. 01) H01Q 19/00, 9/00. Антенний пристрій/ Опубл. 11.04.2016, бюл. №7.

Надано до редколегії 24.12.2016

Рецензент: д-р техн. наук, проф. О.О. Морозов, Національна академія Національної гвардії України. Харків.

РАДИОМАСКИРОВКА ВОЕННЫХ ПОДРАЗДЕЛЕНИЙ В УСЛОВИЯХ ПРИМЕНЕНИЯ ШТАТНЫХ И ИМПРОВИЗИРОВАНЫХ СРЕДСТВ

А.Ю. Иохов, В.Є. Козлов, В.Г. Малюк, К.Н. Ткаченко, Н.Д., Ткаченко

В статье рассмотрены способ комплексного применения мер активной радиомаскировки с использованием специальных средств радиоэлектронного подавления, который может быть использован для построения локальных систем радиосвязи, предназначенных для обмена конфиденциальной информацией в диапазоне ультракоротких волн в условиях искусственных радиопомех и попыток несанкционированного доступа к передаваемой информации.

Ключевые слова: *система радиосвязи, активная радиомаскировка, разведзащищенность, ультракороткие волны.*

DECEPTION MILITARY UNITS THE CONDITIONS OF APPLICATION OF STANDARD AND IMPROVISED MEANS

A.Yu. Iohov, V.Ye. Kozlov, V.H. Maluk, K.N. Tkachenko, N.D. Tkachenko

The article describes the method of complex application of the active radio camouflage measures using special jamming devices. The method can be used to build a local radio communication systems for the exchange of confidential information in the VHF range in terms of artificial interference and unauthorized access to the transmitted information.

Keywords: *radio communication system, active deception, intelligence as protected, VHF.*

УДК 621.391

А.В. Шишацький

Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ

МЕТОДИКА ВИБОРУ РОБОЧИХ ЧАСТОТ В СКЛАДНІЙ ЕЛЕКТРОМАГНІТНІЙ ОБСТАНОВЦІ

У статті наведена методика вибору робочих частот, для роботи засобів зв'язку в складній електромагнітній обстановці, що обумовлена взаємними завадами та впливом навмисних завад. Зазначену методику доцільно використовувати при дефіциті радіочастотного ресурсу та активному радіоелектронного подавленні.

Ключові слова: *радіозавади, комбінаційні завади, радіоелектронне подавлення, навмисні завади.*

Вступ

У роботах [1, 2] проведено розробку методик вибору робочих та резервних частот для передавачів, що працюють в умовах активного радіоелектронного подавлення з застосуванням різноманітних типів навмисних завад та різній стратегії комплексів радіоелектронного подавлення. Проте, передавачі можуть утворювати ненавмисні завади приймачам що розміщені поблизу.

Ненавмисні завади від передавачів як правило проникають до індикатору приймача через комбінаційні канали прийому, що формуються в першому змішувачі приймача [3, 4]. Для боротьби з такими завадами використовують взаємне екранування передавачів та приймачів, що поєднане з надійною частотною фільтрацією сигналів у високочастотних (ВЧ) трактах або вирішується задача оптимізації вибору робочих частот приймача та передавача. Також хотілося б відмітити те, що оптимізація вибору робочих частот забезпечує найбільш високу ефективність в боротьбі з ненавмисними завадами при найменших матеріальних витратах.

Виникає актуальне наукове завдання, яке полягає у необхідності врахуванні взаємного впливу передавачів один на одного.

Тому ***метою статті*** є розробка методики вибору робочих частот для засобів зв'язку, що працюють в складній електромагнітній обстановці та дефіциті радіочастотного ресурсу, з метою забезпечення електромагнітної сумісності та підвищення ефективності використанні наявного радіочастотного ресурсу.

Виклад основного матеріалу дослідження

Для обгрунтування вибору робочих частот засобів зв'язку, при яких не створюються недопустимі завади прийому радіосигналів, нижче розглянуто взаємодію на першому змішувачі приймача першого гетеродина та гармонік п'яти зовнішніх завад, що надходять від сусідніх передавачів, які працюють на частотах $f_{п1} \div f_{п5}$ (рис. 1).

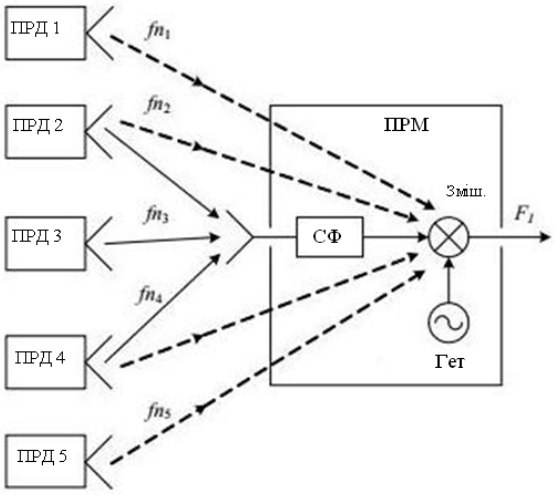


Рис. 1. Схема проникнення завад від передавачів в приймач (Зміш. – перший змішувач, Гет – перший гетеродин, СФ – смуговий фільтр, F1 – перша проміжна частота)

Завади, що проникають до індикатору приймача через комбінаційні канали прийому, які утворилися в результаті взаємодії в першому змішувачі гармонік корисного сигналу f_c з гармоніками зовнішніх завадових сигналів $f_з$, не розглядаються, оскільки рівень таких завад в індикаторі завад значно менше рівня корисного сигналу, що приймається через основний канал прийому. Якщо накласти використовуємі на практиці обмеження, $f_c > F_1 < f_{п1}$, $f_{п2} > F_1 < f_{п3}$, $f_{п4} > F_1 < f_{п5}$, а також позначити як "n" та "p" номера взаємодіючих у змішувачі гармонік першого гетеродина та гармонік сигналів передавача відповідно, то з самих загальних міркувань [3-5] умови для утворення комбінаційних каналів прийому можна записати у вигляді системи рівнянь, що наведені нижче.

При прийомі однієї завади:

1. $p_1 f_{п1} - nf_г = \pm F_l$
2. $p_2 f_{п2} - nf_г = \pm F_l$
3. $p_3 f_{п3} - nf_г = \pm F_l$
4. $p_4 f_{п4} - nf_г = \pm F_l$
5. $p_5 f_{п5} - nf_г = \pm F_l$

При прийомі двох завад:

6. $p_1 f_{п1} - p_2 f_{п2} = \pm F_l$

6a. $|p_1 f_{п1} \pm p_2 f_{п2}| - nf_г = \pm F_l$

7. $p_1 f_{п1} - p_3 f_{п3} = \pm F_l$

7a. $|p_1 f_{п1} \pm p_3 f_{п3}| - nf_г = \pm F_l$

8. $p_1 f_{п1} - p_4 f_{п4} = \pm F_l$

8a. $|p_1 f_{п1} \pm p_4 f_{п4}| - nf_г = \pm F_l$

9. $p_1 f_{п1} - p_1 f_{п5} = \pm F_l$

9a. $|p_1 f_{п1} \pm p_5 f_{п5}| - nf_г = \pm F_l$

10. $p_2 f_{п2} - p_3 f_{п3} = \pm F_l$

10a. $|p_2 f_{п2} \pm p_3 f_{п3}| - nf_г = \pm F_l$

11. $p_2 f_{п2} - p_4 f_{п4} = \pm F_l$

11a. $|p_2 f_{п2} \pm p_4 f_{п4}| - nf_г = \pm F_l$

12. $p_2 f_{п2} - p_5 f_{п5} = \pm F_l$

12a. $|p_2 f_{п2} \pm p_5 f_{п5}| - nf_г = \pm F_l$

13. $p_3 f_{п3} - p_4 f_{п4} = \pm F_l$

13a. $|p_2 f_{п2} \pm p_4 f_{п4}| - nf_г = \pm F_l$

14. $p_3 f_{п3} - p_5 f_{п5} = \pm F_l$

14a. $|p_3 f_{п3} \pm p_5 f_{п5}| - nf_г = \pm F_l$

15. $p_4 f_{п4} - p_5 f_{п5} = \pm F_l$

15a. $|p_4 f_{п4} \pm p_5 f_{п5}| - nf_г = \pm F_l$

При прийомі трьох завад:

16. $p_1 f_{п1} - p_2 f_{п2} \pm p_3 f_{п3} = \pm F_l$

16a. $|p_1 f_{п1} \pm p_2 f_{п2} \pm p_3 f_{п3}| - nf_г = \pm F_l$

17. $p_1 f_{п1} + p_2 f_{п2} - p_3 f_{п3} = \pm F_l$

17a. $|p_1 f_{п1} + p_2 f_{п2} \pm p_3 f_{п3}| - nf_г = \pm F_l$

18. $p_1 f_{п1} - p_2 f_{п2} \pm p_4 f_{п4} = \pm F_l$

18a. $|p_1 f_{п1} - p_2 f_{п2} \pm p_4 f_{п4}| - nf_г = \pm F_l$

19. $p_1 f_{п1} + p_2 f_{п2} - p_4 f_{п4} = \pm F_l$

19a. $|p_1 f_{п1} + p_2 f_{п2} \pm p_4 f_{п4}| - nf_г = \pm F_l$

20. $p_1 f_{п1} - p_2 f_{п2} \pm p_5 f_{п5} = \pm F_l$

20a. $|p_1 f_{п1} - p_2 f_{п2} \pm p_5 f_{п5}| - nf_г = \pm F_l$

21. $p_1 f_{п1} + p_2 f_{п2} - p_5 f_{п5} = \pm F_l$

21a. $|p_1 f_{п1} + p_2 f_{п2} \pm p_5 f_{п5}| - nf_г = \pm F_l$

22. $p_1 f_{п1} - p_3 f_{п3} \pm p_4 f_{п4} = \pm F_l$

22a. $|p_1 f_{п1} - p_3 f_{п3} \pm p_4 f_{п4}| - nf_г = \pm F_l$

23. $p_1 f_{п1} + p_3 f_{п3} - p_4 f_{п4} = \pm F_l$

23a. $|p_1 f_{п1} + p_3 f_{п3} \pm p_4 f_{п4}| - nf_г = \pm F_l$

24. $p_1 f_{п1} - p_3 f_{п3} \pm p_5 f_{п5} = \pm F_l$

24a. $|p_1 f_{п1} - p_3 f_{п3} \pm p_5 f_{п5}| - nf_г = \pm F_l$

25. $p_1 f_{п1} + p_3 f_{п3} - p_5 f_{п5} = \pm F_l$

25a. $|p_1 f_{п1} + p_3 f_{п3} \pm p_5 f_{п5}| - nf_г = \pm F_l$

26. $p_1 f_{п1} - p_4 f_{п4} \pm p_5 f_{п5} = \pm F_l$

26a. $|p_1 f_{п1} - p_4 f_{п4} \pm p_5 f_{п5}| - nf_г = \pm F_l$

27. $p_1 f_{п1} + p_4 f_{п4} - p_5 f_{п5} = \pm F_l$

27a. $|p_1 f_{п1} + p_4 f_{п4} \pm p_5 f_{п5}| - nf_г = \pm F_l$

28. $p_2 f_{п2} - p_3 f_{п3} \pm p_4 f_{п4} = \pm F_l$

28a. $|p_2 f_{п2} - p_3 f_{п3} \pm p_4 f_{п4}| - nf_г = \pm F_l$

29. $p_2 f_{п2} + p_3 f_{п3} - p_4 f_{п4} = \pm F_l$

29a. $|p_2 f_{п2} + p_3 f_{п3} \pm p_4 f_{п4}| - nf_г = \pm F_l$

30. $p_2 f_{п2} - p_3 f_{п3} \pm p_5 f_{п5} = \pm F_l$

30a. $|p_2 f_{п2} - p_3 f_{п3} \pm p_5 f_{п5}| - nf_г = \pm F_l$

31. $p_2 f_{п2} + p_3 f_{п3} - p_5 f_{п5} = \pm F_l$

31a. $|p_2 f_{п2} + p_3 f_{п3} \pm p_5 f_{п5}| - nf_г = \pm F_l$

32. $p_2 f_{п2} - p_4 f_{п4} \pm p_5 f_{п5} = \pm F_l$

32a. $|p_2 f_{п2} - p_4 f_{п4} \pm p_5 f_{п5}| - nf_г = \pm F_l$

33. $p_2 f_{п2} + p_4 f_{п4} - p_5 f_{п5} = \pm F_l$

33a. $|p_2 f_{п2} + p_4 f_{п4} \pm p_5 f_{п5}| - nf_г = \pm F_l$

34. $p_3 f_{п3} - p_4 f_{п4} \pm p_5 f_{п5} = \pm F_l$

34a. $|p_3 f_{п3} - p_4 f_{п4} \pm p_5 f_{п5}| - nf_г = \pm F_l$

35. $p_3 f_{п3} + p_4 f_{п4} - p_5 f_{п5} = \pm F_l$

35a. $|p_3 f_{п3} + p_4 f_{п4} \pm p_5 f_{п5}| - nf_г = \pm F_l$

При прийомі чотирьох завад:

36. $p_1 f_{п1} + p_2 f_{п2} + p_3 f_{п3} + p_4 f_{п4} = \pm F_l$

36a. $\pm|p_1 f_{п1} + p_2 f_{п2} + p_3 f_{п3} + p_4 f_{п4}| - nf_г = \pm F_l$

37. $p_1 f_{п1} - p_2 f_{п2} + p_3 f_{п3} + p_4 f_{п4} = \pm F_l$

37a. $|p_1 f_{п1} - p_2 f_{п2} + p_3 f_{п3} + p_4 f_{п4}| - nf_г = \pm F_l$

38. $p_1 f_{п1} + p_2 f_{п2} - p_3 f_{п3} + p_4 f_{п4} = \pm F_l$

38a. $|p_1 f_{п1} + p_2 f_{п2} - p_3 f_{п3} + p_4 f_{п4}| - nf_г = \pm F_l$

39. $p_1 f_{п1} + p_2 f_{п2} + p_3 f_{п3} - p_4 f_{п4} = \pm F_l$

39a. $|p_1 f_{п1} + p_2 f_{п2} + p_3 f_{п3} \pm p_4 f_{п4}| - nf_г = \pm F_l$

40. $p_1 f_{п1} + p_2 f_{п2} - p_3 f_{п3} - p_4 f_{п4} = \pm F_l$

40a. $|p_1 f_{п1} + p_2 f_{п2} - p_3 f_{п3} - p_4 f_{п4}| - nf_г = \pm F_l$

41. $p_1 f_{п1} - p_2 f_{п2} + p_3 f_{п3} - p_4 f_{п4} = \pm F_l$

41a. $|p_1 f_{п1} - p_2 f_{п2} + p_3 f_{п3} - p_4 f_{п4}| - nf_г = \pm F_l$

42. $p_1 f_{п1} - p_2 f_{п2} - p_3 f_{п3} + p_4 f_{п4} = \pm F_l$

42a. $|p_1 f_{п1} - p_2 f_{п2} - p_3 f_{п3} + p_4 f_{п4}| - nf_г = \pm F_l$

43. $p_1 f_{п1} - p_2 f_{п2} - p_3 f_{п3} + p_5 f_{п5} = \pm F_l$

43a $|p_1 f_{п1} - p_2 f_{п2} - p_3 f_{п3} + p_5 f_{п5}| - nf_г = \pm F_l$

44a. $p_1 f_{п1} - p_2 f_{п2} + p_3 f_{п3} + p_5 f_{п5} = \pm F_l$

45. $|p_1 f_{п1} - p_2 f_{п2} + p_3 f_{п3} + p_5 f_{п5}| - nf_г = \pm F_l$

45a. $p_1 f_{п1} + p_2 f_{п2} - p_3 f_{п3} + p_5 f_{п5} = \pm F_l$

46. $|p_1 f_{п1} + p_2 f_{п2} - p_3 f_{п3} + p_5 f_{п5}| - nf_г = \pm F_l$

46a. $p_1 f_{п1} + p_2 f_{п2} + p_3 f_{п3} - p_5 f_{п5} = \pm F_l$

47. $|p_1 f_{п1} + p_2 f_{п2} + p_3 f_{п3} \pm p_5 f_{п5}| - nf_г = \pm F_l$

47a. $p_1 f_{п1} + p_2 f_{п2} - p_3 f_{п3} - p_5 f_{п5} = \pm F_l$

48. $p_1 f_{п1} - p_2 f_{п2} + p_3 f_{п3} - p_5 f_{п5} = \pm F_l$

48a. $|p_1 f_{п1} - p_2 f_{п2} + p_3 f_{п3} - p_5 f_{п5}| - nf_г = \pm F_l$

49. $p_1 f_{п1} - p_2 f_{п2} - p_3 f_{п3} - p_5 f_{п5} = \pm F_l$

49a. $|p_1 f_{п1} - p_2 f_{п2} - p_3 f_{п3} - p_5 f_{п5}| - nf_г = \pm F_l$

50. $p_1 f_{п1} - p_2 f_{п2} - p_4 f_{п4} - p_5 f_{п5} = \pm F_l$

50a. $\left|p_1f_{п1}-p_2f_{п2}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

51. $p_1f_{п1}-p_2f_{п2}+p_4f_{п4}+p_5f_{п5}=\pm F_l$

51a. $\left|p_1f_{п1}-p_2f_{п2}+p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

52. $p_1f_{п1}+p_2f_{п2}-p_4f_{п4}+p_5f_{п5}=\pm F_l$

52a. $\left|p_1f_{п1}+p_2f_{п2}-p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

53. $p_1f_{п1}+p_2f_{п2}+p_4f_{п4}-p_5f_{п5}=\pm F_l$

53a. $\left|p_1f_{п1}+p_2f_{п2}+p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

54. $p_1f_{п1}+p_2f_{п2}-p_4f_{п4}-p_5f_{п5}=\pm F_l$

54a. $\left|p_1f_{п1}+p_2f_{п2}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

55. $p_1f_{п1}-p_2f_{п2}+p_4f_{п4}-p_5f_{п5}=\pm F_l$

55a. $\left|p_1f_{п1}-p_2f_{п2}+p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

56. $p_1f_{п1}-p_2f_{п2}-p_4f_{п4}+p_5f_{п5}=\pm F_l$

56a. $\left|p_1f_{п1}-p_2f_{п2}-p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

57. $p_1f_{п1}-p_3f_{п3}-p_4f_{п4}-p_5f_{п5}=\pm F_l$

57a. $\left|p_1f_{п1}-p_3f_{п3}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

58. $p_1f_{п1}-p_3f_{п3}+p_4f_{п4}+p_5f_{п5}=\pm F_l$

58a. $\left|p_1f_{п1}-p_3f_{п3}+p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

59. $p_1f_{п1}+p_3f_{п3}-p_4f_{п4}+p_5f_{п5}=\pm F_l$

59a. $\left|p_1f_{п1}+p_3f_{п3}-p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

60. $p_1f_{п1}+p_3f_{п3}+p_4f_{п4}-p_5f_{п5}=\pm F_l$

60a. $\left|p_1f_{п1}+p_3f_{п3}+p_4f_{п4}\pm p_5f_{п5}\right|-nf_г=\pm F_l$

61. $p_1f_{п1}+p_3f_{п3}-p_4f_{п4}-p_5f_{п5}=\pm F_l$

61a. $\left|p_1f_{п1}+p_3f_{п3}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

62. $p_1f_{п1}-p_3f_{п3}+p_4f_{п4}-p_5f_{п5}=\pm F_l$

62a. $\left|p_1f_{п1}-p_3f_{п3}+p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

63. $p_1f_{п1}-p_3f_{п3}-p_4f_{п4}+p_5f_{п5}=\pm F_l$

63a. $\left|p_1f_{п1}-p_3f_{п3}-p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

64. $p_2f_{п2}-p_3f_{п3}-p_4f_{п4}-p_5f_{п5}=\pm F_l$

64a. $\left|p_2f_{п2}-p_3f_{п3}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

65. $p_2f_{п2}-p_3f_{п3}+p_4f_{п4}+p_5f_{п5}=\pm F_l$

65a. $\left|p_2f_{п2}-p_3f_{п3}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

66. $p_2f_{п2}+p_3f_{п3}-p_4f_{п4}+p_5f_{п5}=\pm F_l$

66a. $\left|p_2f_{п2}+p_3f_{п3}-p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

67. $p_2f_{п2}+p_3f_{п3}+p_4f_{п4}-p_5f_{п5}=\pm F_l$

67a. $\left|p_2f_{п2}+p_3f_{п3}+p_4f_{п4}\pm p_5f_{п5}\right|-nf_г=\pm F_l$

68. $p_2f_{п2}+p_3f_{п3}-p_4f_{п4}-p_5f_{п5}=\pm F_l$

68a. $\left|p_2f_{п2}+p_3f_{п3}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

69. $p_2f_{п2}-p_3f_{п3}+p_4f_{п4}-p_5f_{п5}=\pm F_l$

69a. $\left|p_2f_{п2}-p_3f_{п3}+p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

70. $p_2f_{п2}-p_3f_{п3}-p_4f_{п4}+p_5f_{п5}=\pm F_l$

70a. $\left|p_2f_{п2}-p_3f_{п3}-p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

При прийманні п'яти завад:

71. $p_1f_{п1}+p_2f_{п2}+p_3f_{п3}+p_4f_{п4}-p_5f_{п5}=\pm F_l$

71a. $\left|p_1f_{п1}+p_2f_{п2}+p_3f_{п3}+p_4f_{п4}\pm p_5f_{п5}\right|-nf_г=\pm F_l$

72. $p_1f_{п1}+p_2f_{п2}+p_3f_{п3}-p_4f_{п4}-p_5f_{п5}=\pm F_l$

72a. $\left|p_1f_{п1}+p_2f_{п2}+p_3f_{п3}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

73. $p_1f_{п1}+p_2f_{п2}-p_3f_{п3}+p_4f_{п4}-p_5f_{п5}=\pm F_l$

73a. $\left|p_1f_{п1}+p_2f_{п2}-p_3f_{п3}+p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

74. $p_1f_{п1}-p_2f_{п2}+p_3f_{п3}+p_4f_{п4}-p_5f_{п5}=\pm F_l$

74a. $\left|p_1f_{п1}-p_2f_{п2}+p_3f_{п3}+p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

75. $p_1f_{п1}-p_2f_{п2}-p_3f_{п3}-p_4f_{п4}+p_5f_{п5}=\pm F_l$

75a. $\left|p_1f_{п1}-p_2f_{п2}-p_3f_{п3}-p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

76. $p_1f_{п1}+p_2f_{п2}-p_3f_{п3}-p_4f_{п4}-p_5f_{п5}=\pm F_l$

76a. $\left|p_1f_{п1}+p_2f_{п2}-p_3f_{п3}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

77. $p_1f_{п1}-p_2f_{п2}-p_3f_{п3}+p_4f_{п4}-p_5f_{п5}=\pm F_l$

77a. $\left|p_1f_{п1}-p_2f_{п2}-p_3f_{п3}+p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

78. $p_1f_{п1}+p_2f_{п2}-p_3f_{п3}-p_4f_{п4}+p_5f_{п5}=\pm F_l$

78a. $\left|p_1f_{п1}+p_2f_{п2}-p_3f_{п3}-p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

79. $p_1f_{п1}-p_2f_{п2}-p_3f_{п3}-p_4f_{п4}-p_5f_{п5}=\pm F_l$

79a. $\left|p_1f_{п1}-p_2f_{п2}-p_3f_{п3}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

80. $p_1f_{п1}+p_2f_{п2}+p_3f_{п3}-p_4f_{п4}+p_5f_{п5}=\pm F_l$

80a. $\left|p_1f_{п1}+p_2f_{п2}+p_3f_{п3}-p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

81. $p_1f_{п1}-p_2f_{п2}+p_3f_{п3}-p_4f_{п4}-p_5f_{п5}=\pm F_l$

81a. $\left|p_1f_{п1}-p_2f_{п2}+p_3f_{п3}-p_4f_{п4}-p_5f_{п5}\right|-nf_г=\pm F_l$

82. $p_1f_{п1}-p_2f_{п2}-p_3f_{п3}+p_4f_{п4}+p_5f_{п5}=\pm F_l$

82a. $\left|p_1f_{п1}-p_2f_{п2}-p_3f_{п3}+p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

83. $p_1f_{п1}-p_2f_{п2}+p_3f_{п3}-p_4f_{п4}+p_5f_{п5}=\pm F_l$

83a. $\left|p_1f_{п1}-p_2f_{п2}+p_3f_{п3}-p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

84. $p_1f_{п1}-p_2f_{п2}+p_3f_{п3}+p_4f_{п4}+p_5f_{п5}=\pm F_l$

84a. $\left|p_1f_{п1}-p_2f_{п2}+p_3f_{п3}+p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

85. $p_1f_{п1}+p_2f_{п2}-p_3f_{п3}+p_4f_{п4}+p_5f_{п5}=\pm F_l$

85a. $\left|p_1f_{п1}+p_2f_{п2}-p_3f_{п3}+p_4f_{п4}+p_5f_{п5}\right|-nf_г=\pm F_l$

Аналіз цієї системи рівнянь дозволяє припустити наступну послідовність розрахунку уражених завадами частот на вході приймача та порядок вибору робочих частот передавача, при яких не створюються недопустимі завади для прийому сигналів:

1. З рівняння №1 визначається уражені частоти, на яких завади від передавача №1 можуть проникнути в приймач:

$$f^*_{п1}=1/p\times\left(nf_г\pm F_l\right), \qquad (1)$$

та призначається найбільш прийнятна частота передавачу №1, $f_{п1}\neq f^*_{п1}$.

2. З рівняння №2, 6 та 6а розраховуються уражені частоти, на яких завади від передавача №2 можуть проникнути в приймач:

$$\begin{gathered} f^*_{п2}=1/p_2\times\left(nf_г\pm F_l\right);\\ f^*_{п2}=1/p_2\times\left(p_1nf_{п1}\pm F_l\right); \qquad (2)\\ f^*_{п2}=1/p_2\times\left|p_1nf_{п1}\pm\left(nf_{п1}\pm F_l\right)\right|. \end{gathered}$$

У вільному від завад інтервалі частот визначається робоча частота передавача №2, $f_{п2}\neq f^*_{п2}$.

3. З рівнянь №3, 7, 7а, 10, 10а, 16, 16а, 17, 17а розраховуються уражені частоти, на які завади від передавача №3 можуть проникати в приймач.

$$\begin{gathered} f^*_{п3}=1/p_3\times\left(nf_г\pm F_l\right);\\ f^*_{п3}=1/p_3\times\left(p_1f_{п1}\pm F_l\right);\\ f^*_{п3}=1/p_3\times\left|p_1f_{п1}-nf_г\pm F_l\right|; \end{gathered}$$

$$f^*_{п3} = 1/p_3 \times (p_2 f_{п2} \pm F_1);$$
$$f^*_{п3} = 1/p_3 \times |p_2 f_{п2} - n f_г \pm F_1|; \quad (3)$$
$$f^*_{п3} = 1/p_3 \times |p_1 f_{п1} - p_2 f_{п2} \pm F_1|;$$
$$f^*_{п3} = 1/p_3 \times |p_1 f_{п1} - p_2 f_{п2} \pm (n f_г \pm F_1)|;$$
$$f^*_{п3} = 1/p_3 \times (p_1 f_{п1} + p_2 f_{п2} \pm F_1);$$
$$f^*_{п3} = 1/p_3 \times |p_1 f_{п1} + p_2 f_{п2} \pm (n f_г \pm F_1)|.$$

Робоча частота передавача №3 обирається у вільному від завад інтервалі $f_{п3} \neq f^*_{п3}$.

4. З рівнянь №4, 8, 8а, 11, 11а, 13, 13а, 18, 18а, 19, 19а, 22-23а, 28-29а, 36-42а розраховується уражені частоти $f^*_{п4}$, на яких в приймач може проникнути завада від передавача №4. Робоча частота обирається при $f_{п4} \neq f^*_{п4}$.

5. З рівнянь №5, 9, 9а, 12, 12а, 14-15а, 20-21а, 24-27а, 30-35а, 43-85а розраховуються уражені частоти $f^*_{п5}$ для передавача №5. Робоча частота обирається при $f_{п5} \neq f^*_{п5}$.

Якщо кількість одночасно працюючих передавачів, що здатні створювати заваду приймачу, більше п'яти, то система рівнянь, що наведена вище, повинна бути розширена. При наявності в системі зв'язку декількох приймачів, на які впливають завади від, розрахунки уражених частот $f^*_п$ необхідно виконувати для кожного приймача окремо та обирати робочі частоти передавачів, що не створюють завад ні одному з приймачів. Розрахунки були обмежені тільки аналізом найбільш уразливим до завад комбінаційних каналів прийому, що утворюються:

а) при впливі в змішувачі гармонік однієї завади та гармонік гетеродина:

$$p_1 + n \le 8,\ p_2 + n \le 8;\ p_3 + n \le 8;$$

б) при впливі в змішувачі гармонік двох завад:

$$p_1 + p_1 \le 7,\ p_1 + p_3 \le 7;\ p_2 + p_3 \le 7;$$

в) при впливі в змішувачі гармонік двох завад та гармонік гетеродина:

$$p_1 + p_2 + n \le 6,\ p_1 + p_3 + n \le 6;\ p_2 + p_3 + n \le 6;$$

г) при впливі у змішувачі гармонік трьох завад:

$$p_1 + p_2 + p_3 \le 5;$$

д) при впливі у змішувачі гармонік трьох завад та гармонік гетеродина:

$$p_1 + p_2 + p_3 + n \le 4.$$

Висновки

В статті розроблена методика, що дозволяє врахувати взаємний вплив передавачів один на одного та розрахувати вільні від завад інтервали частот прийому при великій кількості різноманітних засобів випромінювання, що створюють завади. Зазначена методика дозволяє підвищити електромагнітну сумісність засобів зв'язку та підвищити ефективність використання радіочастотного ресурсу.

Було проведено аналітичне моделювання з використанням розробленої у статті методики, що показало підвищення електромагнітної сумісності засобів зв'язку на 13-17%.

Напрямком подальших досліджень є розробка удосконаленої методики вибору робочих частот для зі зменшиною обчислювальною складністю.

Список літератури

1. Шишацький А.В. Алгоритм вибору робочих частот для засобів військового радіозв'язку в умовах впливу навмисних завад / А.В. Шишацький, В.В. Ольшанський, Р.М. Животовський // Системи озброєння і військова техніка. – 2016. – № 2. – С. 62-66.

2. Шишацький А.В. Методика вибору резервних робочих частот в системах радіозв'язку з псевдовипадковою перестройкою робочої частоти/ А.В. Шишацький, О.В.Кувшинов // 12-та наук. конф. "Новітні технології - для захисту повітряного простору ", тези доповідей, 13-14 квітня 2016 року. –Х.:ХУПС, – 2016. – С. 214.

3. Царьков Н.М. Электромагнитная совместимость РЭС и систем / Н.М. Царьков. – М. : Радио и связь, 1985.

4. Сивоконь И.П. Ограничение динамического диапазона радиоприёмника связи из-за влияния комбинационных каналов приёма / И.П. Сивоконь, А.И. Мушенко // Сб. научн. докл. IV Межд. симпозиума "ЭМС-2001" / Санкт-Петербургский электротехнический ун-т, 2001. – 428 с.

5. Сивоконь И.П. Ограничение динамического диапазона анализатора спектра из-за нелинейных процессов в смесителе / И.П. Сивоконь, С.А. Синельников // Измерительная техника. – 2008. – № 7. – С. 57-59.

Надійшла до редколегії 25.01.2017

Рецензент: д-р техн. наук, проф. І.О. Романенко, Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ.

МЕТОДИКА ВЫБОРА РАБОЧИХ ЧАСТОТ В СЛОЖНОЙ ЭЛЕКТРОМАГНИТНОЙ ОБСТАНОВКЕ

А.В. Шишацкий

В статье приведена методика выбора рабочих частот, для работы средств связи в сложной электромагнитной обстановке, обусловленная взаимными помехами и влиянием преднамеренных помех. Указанную методику целесообразно использовать при дефиците радиочастотного ресурса и активном радиоэлектронном подавлении.

Ключевые слова: *радиопомехи, комбинационные помехи, радиоэлектронное подавление, умышленные помехи.*

THE METHOD OF CHOOSING WORKING FREQUENCIES IN HARD ELECTROMAGNETIC ENVIRONMENT

A.V. Shishatskyi

In the article give method of choosing working frequencies for working communications in hard electromagnetic environment, due to the mutual interference and the influence of intentional interference. This method is useful when the shortage of radio frequency resource and active electronic suppression.

Keywords: *radio interference matching the interference, electronic jamming, intentional interference.*

АЛФАВІТНИЙ ПОКАЖЧИК

Наукове видання

СИСТЕМИ УПРАВЛІННЯ, НАВІГАЦІЇ ТА ЗВ'ЯЗКУ

Збірник наукових праць

Випуск 1 (41)

Відповідальна за випуск *К. С. Козелкова*
Технічний редактор *Т. В. Уварова*
Коректор *О. В. Морозова*
Комп`ютерна верстка *Н. Г. Кучук*
Оформлення обкладинки *І. В. Ільїна*

Свідоцтво про державну реєстрацію КВ № 19512-93/2ПР від 16.11.2012 р.

Формат 60×84/8. Ум.-друк. арк. 18,7. Тираж 150 прим. Зам. 315-17

Адреса редакції: Україна, 36011, м. Полтава, Першотравневий проспект, 24, тел. (066) 706-18-30
Полтавський національний технічний університет імені Юрія Кондратюка

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: **bookfabrik@mail.ua**