МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
Військовий інститут телекомунікацій та інформатизації
Державного університету телекомунікацій

VII-й НАУКОВО-ПРАКТИЧНИЙ СЕМІНАР

„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”

24 жовтня 2013 року

(Доповіді та тези доповідей)

Київ – 2013

ББК
Ц4 (4Укр)39
П-768

У збірнику матеріалів сьомого науково-практичного семінару опубліковано доповіді та тези доповідей вчених, науково-педагогічних працівників, ад'юнктів, здобувачів, курсантів і студентів Військового інституту телекомунікацій та інформатизації Державного університету телекомунікацій та інших вищих навчальних закладів, в яких розглядаються пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення.

ЗМІСТ

(Доповіді)

(Тези доповідей)

Contents

(Reports)

(Tethys)

к.т.н. Бовда Е.М. (ВІТІ ДУТ)

СИСТЕМА ОПЕРАТИВНОГО УПРАВЛІННЯ ЗБРОЙНИХ СИЛ США

У сучасних військових конфліктах особлива увага відводиться системам управління, основу яких складають автоматизовані системи управління в поєднанні з системами космічної розвідки, радіонавігації, а також з розгалуженою системою зв'язку. Такі системи управління військами і зброєю дозволяють досягти переваги над противником через випередження його у виробленні рішень і в прийнятих діях.

Система управління військами і зброєю в США розробляється відповідно до концепції „Системи управління, зв'язку, розвідки та комп'ютерного забезпечення для учасників бойових дій" (Command, Control, Communications, Computers and Intelligence For The Warrior). На основі вимог концепції армія США отримає до 2020 р. нову систему управління Збройними Силами, яка забезпечить здійснення зв'язку на всіх рівнях управління і взаємодії, автоматичне оновлення баз даних всіх користувачів; відкриє можливість отримання необхідних даних з будь-якої точки земної кулі (у будь-який час); забезпечить автоматизацію процесу прийняття рішення командирами усіх рівнів.

В даний час продовжується виведення з експлуатації застарілої автоматизованої системи управління (АСУ) глобальної системи оперативного управління ЗС США (див. рис. 1) (World Wide Military Command Control System) та введення до ладу нової АСУ ЗС США GCCS (Global Command and Control System), яка дозволить автоматизувати процеси попередження про напад, контролювати приведення ЗС у бойову готовність, планувати і керувати бойовими діями, надавати командуванню оперативно-тактичну інформацію, а також організовувати тилове забезпечення.

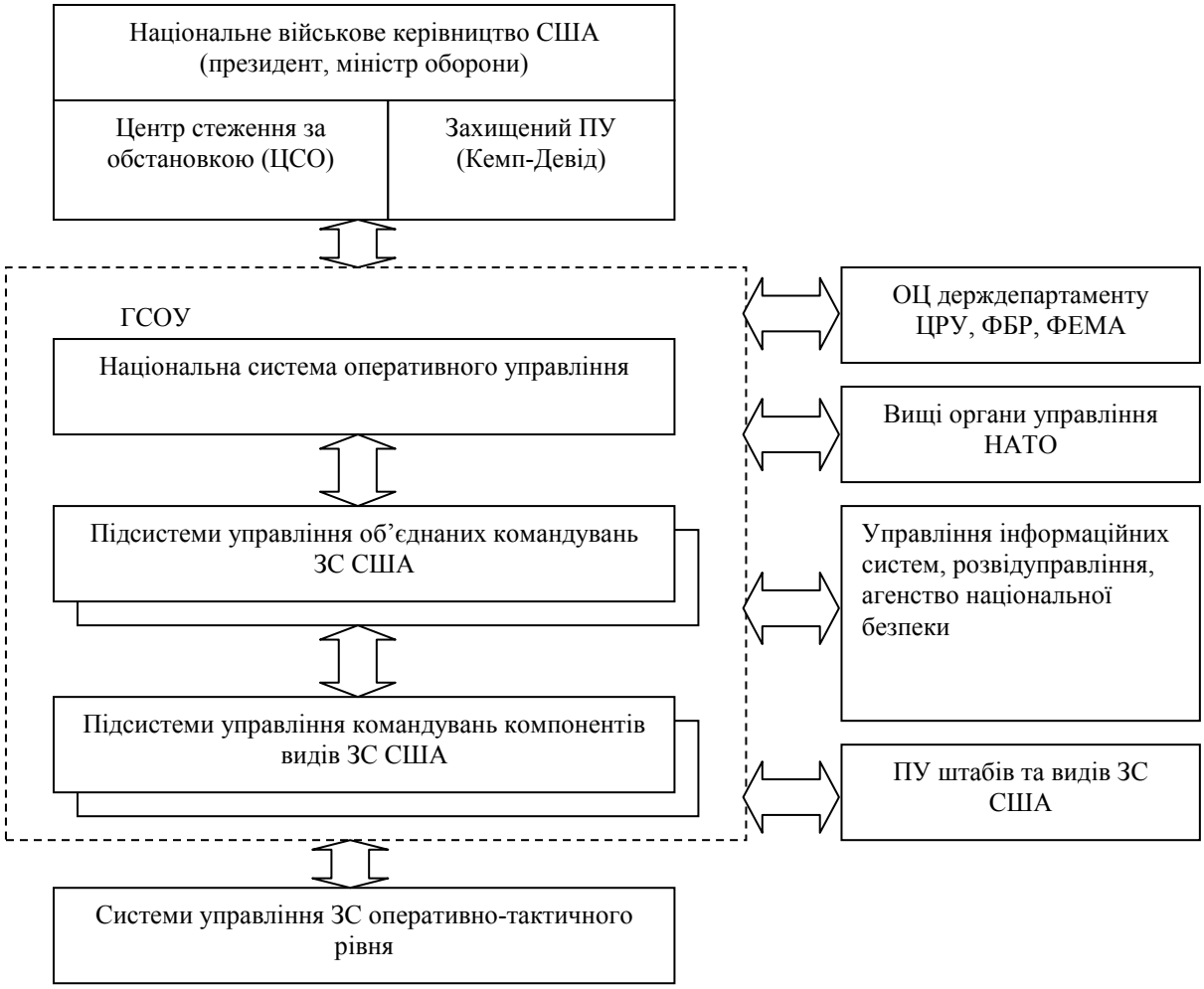


Рис. 1. Структура ГСОУ ЗС США

Сучасна ГСОУ буде однією зі складових концепції технологічного прориву США у військовій області, що отримала назву „революція у військовій області" (Revolution in Military Affairs). Створювана в ході реалізації цієї концепції так звана „система систем" включає в себе три складові частини: об'єднану систему спостереження і розвідки, автоматизовану систему бойового управління (АСБУ) силами та обміну інформацією С4І2 (Command, Control, Computers, Communications and Information / Intelligence); систему, що забезпечує застосування високоточної зброї.

Перша система забезпечує командування первинною інформацією, що надходить від джерел, що діють на всьому просторі поля бою. Вона узагальнює ці дані для того, щоб представити командуванню всіх рівнів єдину інформаційну картину про стан сил (як своїх, так і противника) і про навколишнє середовище (в тому числі метеоумови, стан поверхні ґрунту та гідрологічні умови моря, а також умови розповсюдження електромагнітних хвиль різних діапазонів у даному районі).

Друга система призначена для збору, обробки, об'єднання та аналізу первинних даних, а також для їх зберігання і передачі по запитам споживачів. На відміну від первинної ця інформація отримана в результаті класифікації цілей, розподілу за ними зброї та розробки даних наведення. Таким чином, ця система насичує тривимірний інформаційний простір поля бою даними планування бойових дій, управління та стрільби з метою досягнення панування над супротивником.

Третя система являє собою засоби, що забезпечують застосування зброї і поразки об'єктів високоточними боєприпасами, що дозволяє досягати цього панування. За допомогою високоточної зброї наноситься ряд точних ударів, дія яких доповнює застосування звичайних засобів ураження.

Таким чином, кінцева мета створюваної „системи систем" управління – це збір, обробка, аналіз і розподіл інформації, що забезпечує наведення та застосування зброї з таким ступенем надійності і швидкістю, які не дозволять противнику прийняти адекватні відповідні заходи. Завдяки її застосуванню максимально знижується ступінь участі людини за рахунок повної автоматизації всіх перерахованих вище процесів.

Нова концепція, за якою здійснюється модернізація ГСОУ – має за мету: вдосконалення структури командно-управлінської діяльності; вдосконалення пунктів управління; розвиток автоматизованих систем управління та зв'язку у всіх ланках в інтересах автоматизації всіх процесів управління, підвищення ефективності розвідувальних систем і структур, які забезпечують прийняття рішень усіма інстанціями у масштабі часу близькому до реального; подальший розвиток і всеосяжний охоплення комп'ютерної мережі і, нарешті, – FTW – створення „єдиного інформаційного простору поля бою". При цьому наголос робиться на вдосконалення системи в передових зонах.

Розглянемо більш детально ці положення концепції вдосконалення та модернізації ГСОУ. У вищих органах адміністративного (центральний апарат міністерства оборони та апарати міністрів видів ЗС) і оперативного (комітет начальників штабів) управління в основному відбудуться організаційно-штатні зміни як наслідок перерозподілу і уточнення вирішуваних завдань у зв'язку з переорієнтацією США на регіональні та локальні війни (конфлікти).

Для органів управління збройними силами США в регіонах (верховний головнокомандувач, командувач військами видів збройних сил) будуть характерні зміни , що є наслідком тенденції, що намітилася дозволяти вирішувати регіональні конфлікти застосуванням багатонаціональних сил. Залежно від організації багатонаціональних сил військове керівництво США змушене буде орієнтуватися на два варіанти органів управління – коаліційні або суто національні.

Отримають подальший розвиток і пункти управління. Це стосується насамперед пунктів управління військами (силами) при веденні регіональних і локальних війн. Більш за все в найбільш важливих районах світу американці змушені будуть розгорнути мережу

стаціонарних захищених пунктів управління насамперед в інтересах оперативно-стратегічної ланки управління. Однак основний акцент буде зроблений на подальший розвиток рухомих пунктів управління, передусім повітряних та аеромобільних. При цьому для повітряних командних пунктів буде характерна багатофункціональність.

У розвитку систем і засобів зв'язку буде реалізована ідея комплексування і сумісності систем і засобів збройних сил США у всіх ланках управління із засобами і системами можливих союзників США в регіональних і локальних війнах (передусім країн – учасниць НАТО, Японії, Південної Кореї). При цьому буде істотно підвищуватися роль і значимість супутникових систем зв'язку в стратегічному та оперативно-тактичному ланках управління. В цілому основна ідея в розвитку систем зв'язку полягає в тому, щоб вони дозволяли керувати коаліційними силами і реалізувати всі можливості, які з'являються у зв'язку з розвитком систем розвідки і автоматизації процесів управління військами (силами).

Для систем розвідки стратегічного, оперативного та тактичного ланок, що включають в себе космічні, повітряні, наземні і корабельні засоби, буде характерно комплексування в рамках єдиного оперативно-технічного задуму в єдину інтегровану систему, здатну здобувати і представляти дані про війська (силах) протиборчої сторони на всю глибину їх оперативної побудови і цілеспрямовано використовувати здобуті дані стосовно кожного ланці управління (від комітету начальників штабів до командирів частин і підрозділів). При цьому інформація буде представлятися практично в реальному масштабі часу відповідно з динамікою розвитку обстановки і точністю, достатньою для застосування вогневих засобів ураження. У найближчі 5 – 10 років можлива реалізація циклу оновлення даних по важливим цілям на глибину оперативної побудови військ протиборчої сторони з періодичністю 5 – 10 хвилин. Особливі вимоги пред'являються до скорочення часу від моменту добування даних до їх подання в інтересах оцінки обстановки та прийняття рішення. У перспективі ставиться завдання скоротити цей час до 15 секунд. Це в першу чергу має серйозне значення для частин і підрозділів вогневого ураження і радіоелектронного придушення.

Ключовою ідеєю, що сприяє найбільш повної реалізації зусиль з удосконалення всіх структурних компонентів системи управління, є автоматизація процесів управління в стратегічному, оперативному і тактичному ланках управління.

У стратегічному ланці буде реалізовуватися програма заміни існуючої системи оперативного управління ЗС США (ГСОУ) на нову (ГККС), в якій будуть більш широко використовуватися інформаційні системи як цільового, так і загального характеру. У цілому основний акцент робиться на сполучення автоматизованої системи стратегічної ланки з системами управління оперативного і тактичного ланок, а також на розширення можливостей з планування бойового застосування ЗС США в різних видах війн і регіонах світу.

Новим напрямком у концепції розвитку ГСОУ є напрямок формування „єдиного інформаційного простору поля бою" (*FTW*) для всіх учасників системи, де головною ланкою на полі бою є солдат. Передбачається, що у нього повинен бути планшет – табло, на якому передбачається відображати реальну обстановку (бойове завдання, противник і вогневі точки в секторі його дії, сусіди, можливі удари своїх вогневих засобів) і т.д.

Вирішення цього завдання має забезпечити за задумом фахівців доступність кожного абонента системи до потрібної йому інформації в реальному масштабі часу. Реалізація всіх вищевикладених концептуальних положень дозволить, як вважає командування ЗС США, інтегрувати всі компоненти ГСОУ і забезпечити „безшовний" обмін даними, як по вертикалі, так і по горизонталі між видовими компонентами з метою випередження можливого противника в циклі управління. Загалом вважається , що реалізація всіх ідей концепції C4I FTW дозволить найбільш повно задовольнити постійно зростаючі вимоги, пропоновані до ГСОУ і підвищити ефективність бойового застосування військ (сил) в операціях та веденні військових дій на різних театрах війни, в тому числі і операціях багатонаціональних формувань під керівництвом командування США.

Система бойового управління Збройними Силами США і їх союзників широко використовувалася у військових діях проти Іраку, Югославії, Афганістану, які володіли незрівнянно більш низьким військово-технічним потенціалом порівняно з США. При цьому головною особливістю проведених американцями операцій була демонстрація досягнутих успіхів в управлінні ЗС і зброєю стосовно до контактним і безконтактним війнам.

До настання бойових дій США в зоні конфлікту створювали потужну угруповання космічних засобів різного призначення. З космосу велася безперервна розвідка супутниками оптичної, радіолокаційної розвідки, здійснювалися управління, навігація, зв'язок, метеозабезпечення. Космічні угруповання в сполученні з АСУ різного рівня утворювали єдину систему бойового управління, оптимізовану до конкретних завдань військової операції. У кінцевому рахунку така система управління забезпечувала безперервність і швидкість процесів управління від стратегічної ланки аж до окремого солдата.

Значним досягненням США у вищезазначених конфліктах є використання розвідувально-ударних бойових систем високоточної далекобійного зброї, до складу якого входили крилаті ракети повітряного і морського базування.

У процесі бойових дій було виявлено ряд недоліків, особливо в АСУ на тактичному рівні. Наприклад, виявилося, що багато радіостанції не сумісні один з одним. Виявилася труднощі управління мобільного операцією на марші, що вимагає більш компактних, мобільних і добре захищених машин і.т.д. Насправді список виявлених недоліків має набагато більший обсяг, але робота над помилками дозволить ліквідувати ці недоробки.

Створення системи управління ЗС США зумовило створення відповідної штатної структури, яка заповнюється фахівцями – випускниками військово-навчальних закладів. Нова структура автоматизованого управління зажадала наявності спеціально навчених кадрів, які значно підвищили свою кваліфікацію, беручи участь у військових конфліктах.

В якості результатів бойового використання систем управління військами і зброєю заслуговують уваги підсумки безконтактної війни (1999 р.) США проти Югославії. Для виведення з ладу 900 цивільних і військових об'єктів було використано приблизно 1500 високоточних ракет, за допомогою яких була зруйнована нафтопереробна промисловість і знищено 40 % нафтосховищ, виведені з ладу 70 % автомобільних і залізних доріг з руйнуванням 80 мостів; знищено не менше 50 % оборонних підприємств та ін. Іншими словами, економіка Югославії була повністю зруйнована. Для вирішення завдання інтеграції систем управління видів збройних сил в основу побудови глобальної системи управління GCCS (Global Command and Control System)) був покладений принцип створення єдиної операційної середовища інформаційної інфраструктури міністерства оборони DIICOE (Defense Information Infrastructure Common Operating Environment). Він передбачає три рівні узагальнення: ядро системи, набір функцій, загальних для всіх ЕОМ; єдина обчислювальна мережа. Ядром системи є єдина операційна система ЕОМ, структура даних та програмних додатків, формат друкованих документів і вид інформації, що відображається. Це дозволяє виконати завдання, призначених для звичайних персональних комп'ютерів, на ЕОМ, встановлених на борту бойових кораблів і літаків.

Наступний рівень – загальний набір функцій для всіх ЕОМ з обміну користувачів інформацією в мережі і зберігання її в базах даних.

На третьому рівні відбудеться підключення користувачів до мережі передачі інформації міністерства оборони DISN (Defense Information System Network), за якою можуть передаватися оцифровані голосові, відео-і аналогові дані. У результаті цього GCCS і DISN стануть єдиною системою ГСОУ.

Програмами GCCS-A,-AF і-М передбачається розгортання автоматичних систем управління командувань СВ, ВПС і ВМС на континентальній частині США та в передових зонах, повністю сумісних з єдиною АСУ GCCS. Відповідно до програм „Ентерпрайз", „Горизонт" та „Коперник" планується створення в масштабі командувань компонентів видів збройних сил інтегрованих мереж телекомунікаційних систем за типом DISN, повністю з

нею сумісних. Наприклад, завершення програми „Ентерпрайз” дозволить вирішувати такі завдання: виявляти, розпізнавати і супроводжувати кілька тисяч повітряних і наземних цілей; автоматично наводити керовану зброю на сотні цілей; забезпечувати командирів усіх рівнів електронними картами поточної обстановки; керувати підлеглими підрозділами та здійснювати автоматизовану підготовку варіантів можливих дій військ в межах ТВД.

Таким чином, ГСОУ безпосередньо пов’язує вище військове керівництво зі стратегічними ядерними силами США, що забезпечує централізоване управління ними. ГСОУ безпосередньо функціонально сполучається з системами управління основних командувань (формувань) оперативно-тактичної ланки, що дозволяє забезпечувати як централізоване, так і децентралізоване управління ними в ході підготовки і ведення операцій. У ГСОУ входить близько 130 органів і пунктів управління, 60 мереж АСУ і близько 10 систем тактичного попередження. Вона забезпечує глобальне охоплення управління всіма компонентами ЗС США.

На командних центрах (пунктах) управління від КНШ і до КП кінцевих виконавчих ланок управління СНР здійснюється постійне цілодобове чергування. У всіх ланках стратегічного рівня є захищені в протиатомному відношенні ПУ, а також запасні та резервні мобільні ПУ – ВКП і НМКП, які підтримуються в постійній готовності до вильоту і виходу на маршрути. Безперервне функціонування ГСОУ забезпечується національною системою зв'язку США. Її основою є об’єднана система зв’язку (ОСЗ) МО. До її складу входять близько 100 автоматичних комутаційних центрів (АКЦ) зв’язку, більше 10 тис. магістральних (комутованих) і прямих ліній зв’язку, близько 100 великих вузлів зв’язку (ВЗ), десятки станцій тропосферного та більше 100 пунктів космічного зв’язку. ОСЗ МО обслуговує близько 2 тис. штабів і ПУ. Велика частина систем зв’язку автоматизована і закрита ЗАЗ. Міжконтинентальні кабелі, прокладені по дну океану, з’єднують вищу ланку ГСОУ з КП ЦК ЗС США в передових зонах в Європі, Атлантиці і Тихого океану, а також з окремими базами США.

Таким чином, реалізація цих можливостей ГСОУ дозволить забезпечувати як централізоване, так і децентралізоване управління об’єднаними угрупованнями збройних сил в умовах їх негайного заподіяння у разі різкої зміни військово-політичної обстановки в будь-якому регіоні світу, з мінімально допустимим за часом періодом підготовки до ведення бойових дій, в тому числі і на необладнаних ТВД. Водночас це дозволить командуванню об’єднаних оперативних формувань США здійснювати адаптивний підхід до планування операцій, швидко реагувати на зміни обстановки в зоні бойових дій, випереджати супротивника у прийнятті рішень і в кінцевому підсумку забезпечити стратегічну і тактичну перевагу. Для Збройних Сил України розглянуті підходи вже втілені в проекти перспективних АСУ.

ЛІТЕРАТУРА

1. Роль и место глобальной системы оперативного управления в стратегическом руководстве США. Полковник В. Азов. „Зарубежное военное обозрение” № 5, 2003 с 2 – 7.

2. Глобальная система оперативного управления вооруженными силами США и концепция ее развития. В.С. Ткачев, академик АВН, А.А. Лелехов, академик АВН.

3. Автоматизированные системы управления сухопутными войсками США. Полковник В. Масной; полковник Ю. Судаков, канд. технических наук. „Зарубежное военное обозрение” 2003 № 9,10.

4. Разработка АСУ и информационных технологий в ВМС США. Капитан 1 ранга И.Быков.

5. Подходят ли стандарты НАТО для Вооружённых сил России? Newsland.com.

6. Как управлять войсками и оружием? Михаил Растопшин.

7. „Сетецентрическая война” и ВМС США Полковник В. Баулин; подполковник А. Кондратьев.

Горецький О.В. (ГУЗІС ГШ ЗСУ)

СИСТЕМА ЗВ'ЯЗКУ ЗБРОЙНИХ СИЛ УКРАЇНИ, ОСНОВНІ НАПРЯМИ ЇЇ РОЗВИТКУ ТА ОЧІКУВАНІ РЕЗУЛЬТАТИ РЕФОРМУВАННЯ ВІЙСЬК ЗВ'ЯЗКУ

В умовах швидкоплинності сучасних війн і збройних конфліктів якісне інформаційне забезпечення бойових дій військ (сил) стає визначальною умовою досягнення стратегічної, оперативної та тактичної переваги над супротивником.

Це приводить до пошуку нових способів ведення бойових дій, а також організації підтримки військ на полі бою з урахуванням останніх досягнень у галузі інформаційних технологій і телекомунікацій.

Саме тому в комплексі заходів щодо забезпечення обороноздатності держави поряд з підтриманням високої бойової готовності військ (сил) пріоритетним напрямом є розвиток і вдосконалення системи військового управління та її технічної основи – системи зв'язку Збройних сил України, як найважливішого елемента державної та військової інфраструктури, яка визначає ефективність застосування військ та зброї.

Отже, під час реформування системи зв'язку Збройних сил України необхідно враховувати:

перспективну структуру Збройних сил України до 2017 року;

перспективну систему управління Збройними силами України;

перспективну структуру пунктів управління Збройних сил України, а також вимоги, які ставляться до системи зв'язку Єдиною автоматизованою системою управління Збройними силами України.

Існуюча структура військ зв'язку на цей час забезпечує функціонування чотирирівневої системи управління:

на **стратегічному рівні** – пунктів управління Генерального штабу Збройних сил України, утримуючи при цьому частини зв'язку безпосереднього підпорядкування;

на **оперативно-стратегічному рівні** – штаби видів Збройних сил України, що мають у своєму підпорядкуванні стаціонарні інформаційно-телекомунікаційні вузли штабів, пунктів управління, польові вузли зв'язку, які входять до штатів полків зв'язку, пункти управління системою зв'язку та інформаційних систем, центри контролю безпеки інформації в інформаційно-телекомунікаційних системах (ІТС), бази зберігання засобів зв'язку, а також військові частини та підрозділи фельд'єгерсько-поштового зв'язку;

на **оперативному рівні** до складу військових частин та підрозділів зв'язку армійських корпусів та повітряних командувань включено пункти управління системою зв'язку, стаціонарні інформаційно-телекомунікаційні вузли штабів та пунктів управління, окремі лінійно-вузлові полки зв'язку (окремі полки зв'язку), ремонтні майстерні засобів зв'язку та частини і підрозділи фельд'єгерсько-поштового зв'язку;

на **тактичному рівні** до складу бригад включено польові вузли зв'язку. На окремих штатах утримуються підпорядковані бригадам стаціонарні інформаційно-телекомунікаційні вузли.

З метою підвищення ефективності та оперативності управління військами (силами) на цей час у Збройних силах України проводяться організаційні заходи, спрямовані на створення **трирівневої системи управління Збройних сил**, яка має включати:

Генеральний штаб Збройних сил України як головний військовий орган з планування оборони держави, управління застосуванням Збройних сил, координації та контролю за виконанням завдань у сфері оборони органами виконавчої влади, органами місцевого самоврядування, утвореними відповідно до законів України військовими формуваннями, а також правоохоронними органами;

оперативні командування „Північ”, „Південь” та Командування Військово-Морських сил з підпорядкованими військами, які дислоковані в межах, визначених військово-адміністративним поділом території України;

управління бригад (полків), інших військових частин і військових навчальних закладів, установ та організацій.

В існуючій структурі Збройних сил України війська зв’язку нараховують понад 80 військових частин, що становить 8% від загальної чисельності Збройних сил України. Для прикладу, у збройних силах Франції цей показник сягає понад 11%.

Тому Головним управлінням зв’язку та інформаційних систем ГШ ЗС України розроблено та начальником Генерального штабу – Головнокомандувачем Збройних сил України затверджено Замисел реформування і розвитку системи та військ зв’язку Збройних сил України, Замисел переоснащення системи зв’язку Збройних сил України цифровими засобами на період 2013 – 2017 років та шляхи його реалізації, що неодмінно враховує основні положення Державної комплексної програми реформування та розвитку Збройних сил України до 2017 року.

Вказані Замисли узято за основу при розробці Програми розвитку військ зв’язку Збройних сил України на 2014 – 2018 роки, над якою зараз працює Головне управління зв’язку та інформаційних систем ГШ ЗС України.

Вказані документи враховують перспективну структуру ЗС України до 2017 року, систему управління та структуру пунктів управління ЗС України.

З метою реалізації концептуальних положень вищезазначених документів та забезпечення переходу на трирівневу систему управління спільними директивами Міністерства оборони України та Генерального штабу Збройних сил України визначено проведення організаційних заходів щодо оптимізації структури та чисельності військ зв’язку.

Щодо системи технічного забезпечення зв’язку і автоматизації. Пропонується бази ремонту та зберігання засобів зв’язку Генерального штабу та видів ЗС України перепідпорядкувати оперативним командуванням за територіальним принципом.

Щодо оптимізації системи підготовки військових фахівців зв’язку. Постановою Кабінету Міністрів України створено Державний університет телекомунікацій, якому пере підпорядковано, в тому числі, і Військовий інститут телекомунікацій та інформатизації Національного технічного університету України “Київський політехнічний інститут”.

Протягом 2013 – 2016 років буде поступово здійснюватися скорочення чисельності Військового інституту телекомунікацій та інформатизації Державного університету телекомунікацій за рахунок впровадження системи підготовки „студент-курсант”.

У 2014 році планується розформувати Військовий коледж сержантського складу при Військовому інституті телекомунікацій та інформатизації Державного університету телекомунікацій (далі – ВІТІ ДУТ) та Об’єднаний навчально-тренувальний центр військ зв’язку ЗС України, сформувати у складі ВІТІ ДУТ навчальний центр з дислокацією у м. Києві загальною чисельністю понад 50 посад постійного складу та понад 150 курсантів змінного складу за рахунок військ.

Це дасть можливість на високому професійному рівні здійснювати початкову фахову підготовку військовослужбовців військової служби за контрактом для підрозділів і військових частин зв’язку та базову підготовку сержантського складу.

У ході реформування військ зв’язку Збройних сил України також планується оптимізація військових частин і підрозділів фельд’єгерсько-поштового зв’язку.

Перспективний склад військ зв’язку Збройних сил України повинен відповідати перспективній системі управління згідно з Державною комплексною програмою реформування та розвитку Збройних сил України до 2017 року, затвердженому Замислу реформування військ зв’язку та переоснащення системи зв’язку Збройних сил України цифровими засобами в період 2013 – 2017 років та Програмі розвитку військ зв’язку Збройних сил України на 2014–2018 роки.

Критеріями оптимізації під час розроблення перспективного складу військ зв'язку Збройних Сил були забезпечення належного та якісного функціонування системи зв'язку та мінімально необхідна кількість військових частин зв'язку, особового складу, техніки, спроможних забезпечити стійке управління визначеним комплектом військ відповідно до потреб Збройних сил України.

Щодо перспектив розвитку стаціонарної та польової компонент системи зв'язку Збройних сил України. На цей час вона технічно базується переважно на застарілих системах радянського виробництва 70 – 80-х років минулого століття. Це переважно аналогові засоби, в яких реалізовані технічні рішення, які вже не підтримуються виробниками засобів зв'язку. У свою чергу, утримання застарілих аналогових систем призводить до надмірних (зайвих) витрат коштів.

У той же час протягом 2006 – 2012 років у Збройних силах виконувалися заходи щодо переоснащення системи зв'язку цифровими засобами. Співвідношення стаціонарних цифрових систем і аналогових становить приблизно 25% і 75%. За вказаний період апробовані типові технічні рішення щодо забезпечення сучасними послугами зв'язку (захищений обмін голосом, даними, відео), які відповідають вимогам щодо відкритості, комплексності та модульності їх побудови.

Гірший стан переоснащення польової компоненти, її показник не перевищує 3% від потреби. Польова компонента переоснащується новітніми комплексними апаратними зв'язку, модернізованими станціями тропосферного зв'язку Р-417МУ та Р-423МУ, цифровими УКХ засобами радіозв'язку. Крім того, за програмою міжнародної технічної допомоги від США отримано засоби радіозв'язку тактичної ланки „Харріс", які призначені для досягнення взаємосумісності засобів зв'язку в ході міжнародних навчань і миротворчих операцій.

На жаль, динаміка розвитку системи зв'язку ЗС України залежить від рівня фінансування, наявності цифрових систем спеціального призначення, які прийнято на озброєння, або подвійного використання, а також від структури системи управління, погляди на яку доволі часто змінюються.

Аналізуючи досвід попередніх років, розвиток системи зв'язку Збройних сил України планується здійснювати на основі створення єдиного інформаційно-телекомунікаційного середовища, із впровадженням сучасних інформаційно-телекомунікаційних технологій, протоколів обміну інформацією (IP, VPN MPLS, E1), комплексів і систем зв'язку спеціального призначення, що забезпечить обмін усією інформацією (голос, дані, відео) між органами й пунктами управління (всіх ланок) з відповідною пропускною спроможністю, достовірністю та надійністю.

Реформування системи зв'язку Збройних сил України планується здійснити шляхом виконання таких основних заходів:

1. Визначення оптимального складу військ зв'язку, які забезпечать розгортання та функціонування системи зв'язку з метою якісного управління військами (силами).

2. Забезпечення надання послуг зв'язку органам державного і військового управління Міністерства оборони та Збройних сил України.

3. Переоснащення стаціонарної та польової компонент системи зв'язку новітніми цифровими засобами (комплексами).

4. Виведення з експлуатації, списання та утилізація морально застарілої техніки зв'язку.

Шляхи розвитку стаціонарної компоненти системи зв'язку та автоматизації ЗС України:

застосування технології MPLS для потреб ЗС України;

переоснащення телекомунікаційної мережі на цифрові засоби;

розроблення та впровадження АСУ системою зв'язку;

створення стаціонарної автоматизованої системи радіозв'язку;

створення інтегрованої системи супутникового зв'язку ЗС України;

впровадження засекречувальної апаратури вітчизняного виробництва.

В основі переоснащення стаціонарної компоненти системи зв'язку Збройних сил України цифровими засобами на період до 2017 року є підключення та використання телекомунікаційної мережі спеціального призначення Державної служби спеціального зв'язку та захисту інформації України, побудованої в рамках приватизації Укртелекому.

З метою зазначеного переоснащення планується виконати такі заходи:

розгортання відомчої мережі Збройних Сил України з використанням IP-технологій, впровадження сучасних телекомунікаційних та інформаційних систем, апаратно-програмних комплексів;

розгортання стаціонарної компоненти захищеної системи обміну інформацією Збройних сил України;

розгортання системи захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах Збройних сил України;

створення системи супутникового зв'язку ЗС України на базі національного супутника;

створення цифрової мережі радіозв'язку, у тому числі транкінгової;

удосконалення технічної складової системи оповіщення ЗС України;

поступове скорочення послуг аналогового зв'язку, відмова від використання застарілих систем зв'язку та виведення їх з експлуатації.

Таким чином, у результаті переоснащення стаціонарна компонента системи зв'язку Збройних сил України буде мати цільну структуру в усіх ланках управління, яка забезпечить якісний відкритий та закритий цифровий зв'язок.

Якщо, як основа буде використовуватися телекомунікаційна мережа спеціального призначення Державної служби спеціального зв'язку та захисту інформації України, то проблема щодо взаємосумісності систем зв'язку буде практично вирішена.

Шляхи розвитку польової компоненти системи зв'язку та автоматизації ЗС України:

впровадження єдиного типу засекречувальної апаратури по всіх родах зв'язку;

забезпечення сумісності зі стаціонарною телекомунікаційною мережею;

використання самоналагоджувальних мереж та впровадження IP-технологій в ПОМЗ ЗС України в оперативній і тактичній ланках управління;

оптимізація структури та складу рухомих ІТВ ПУ ЗС України за рахунок упровадження комплексних апаратних зв'язку;

модернізація засобів радіо-, радіорелейного та тропосферного зв'язку на лініях прямого зв'язку;

використання комплексних апаратних зв'язку доступу ІТВ та самоналагоджувальних мереж як ліній прив'язки.

В основу переоснащення польової компоненти системи зв'язку покладено:

поетапне переоснащення цифровими засобами польових інформаційно-телекомунікаційних вузлів рухомих пунктів управління стратегічної, оперативної та тактичної ланок;

переоснащення новітніми цифровими радіорелейними та тропосферними засобами зв'язку лінійних підрозділів зв'язку стратегічної та оперативної ланок управління;

забезпечення сумісності польової та стаціонарної компонент системи зв'язку Збройних сил України шляхом використання ідентичних за можливостями телекомунікаційних та інформаційних систем і апаратно-програмних комплексів;

забезпечення можливості управління військами Збройних сил України без використання стаціонарної компоненти системи зв'язку Збройних сил України на двох інформаційних напрямках;

створення технічних умов для спроможності польової компоненти системи зв'язку забезпечити обмін розвідувальною інформацією в оперативній та тактичній ланках управління, в т.ч. з безпілотними літальними апаратами.

Переоснащення польової компоненти системи зв'язку передбачається здійснювати шляхом закупівлі польових засобів зв'язку, прийнятих на озброєння, та переобладнання силами ремонтних баз (майстерень) зв'язку апаратних (станцій) виробництва колишнього СРСР цифровими засобами зв'язку, які також прийнято на озброєння (постачання), або засобами подвійного використання.

На сьогоднішній день переоснащення польової компоненти системи зв'язку здійснюється шляхом розробки та модернізації техніки зв'язку в рамках виконання відповідних ДКР державними й комерційними підприємствами, перелік яких визначено рішенням Уряду України.

Такий підхід потребує значних бюджетних (фінансових) витрат.

Іншим підходом до розробки (модернізації) техніки зв'язку виробництва колишнього СРСР є залучення до цього процесу науково-дослідних установ Збройних сил України, зокрема Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації Державного університету телекомунікацій.

Відповідно до чинного законодавства України Науковий центр зв'язку та інформатизації ВІТІ ДУТ, за рахунок утримання, має можливість виконувати дослідно-конструкторські роботи з модернізації техніки зв'язку, а виробництво дослідних зразків планується здійснити силами Центральної бази ремонту та зберігання засобів зв'язку.

Таким чином, на кінець 2017 року польова компонента буде мати:

систему переоснащених польових ІТВ;

30% від потреби переоснащення польових ІТВ усіх ланок управління радіостанціями середньої потужності КХ діапазону;

укомплектованість лінійної частини та підрозділів зв'язку цифровими засобами для побудови польової цифрової опорної мережі (з яких: 40% від потреби укомплектування об'єднаного польового вузла зв'язку ГШ ЗС України переобладнаними цифровими радіорелейними станціями та 5% від потреби укомплектування бригад (полків) зв'язку оперативних командувань новітніми засобами тропосферного зв'язку).

Оснащення польових ІТВ пунктів управління надасть можливість забезпечити оперативний склад усіх ланок управління якісними послугами зв'язку аналогічно тим, які надаються на стаціонарних пунктах управління (відкриті та закриті голос, дані, відео). Це дасть змогу побудувати цифрову польову опорну мережу зв'язку в стратегічній ланці управління на двох інформаційних напрямках, яка буде резервуватися стаціонарною компонентою.

Отже, за умови виконання заходів переоснащення системи зв'язку Збройних сил України очікуються такі результати:

1. У стаціонарній компоненті системи зв'язку ЗС України буде переоснащено на цифрові засоби 100% ІТВ від загальної кількості, та при цьому буде забезпечено:

скорочення до 85% аналогових каналів зв'язку на пунктах управління ЗС України та до 70% у частинах і підрозділах Повітряних сил;

відмову від використання системи відкритого телеграфного зв'язку за рахунок впровадження засобів передачі даних;

створення системи супутникового зв'язку з використанням новітніх засобів (у разі запуску національного супутника зв'язку) для резервування наземної компоненти системи зв'язку та збільшення рівня її гнучкості й мобільності;

функціонування захищеної системи обміну інформацією Збройних сил України в усіх ланках управління;

виведення з експлуатації засекречувальної апаратури телеграфного зв'язку виробництва колишнього СРСР;

поступове виведення з експлуатації комутаторів засекреченого зв'язку, крім ІТВ.

2. У польовій компоненті системи зв'язку ЗС України буде переоснащено на цифрові засоби 70% – стратегічної, 20% – оперативної та 10% – тактичної ланок управління, та при цьому буде забезпечено:

мінімально необхідну укомплектованість лінійних частин, що дасть можливість будувати переважно цифрову польову опорну мережу;

можливість надання послуг цифрового зв'язку в усіх ланках управління;

100% резервування стаціонарної мережі зв'язку на двох інформаційних напрямках.

Підбиваючи підсумки, можна зазначити, що на кінець 2017 року планується:

переоснастити 100% стаціонарної та до 10% мобільної компоненти системи зв'язку Збройних сил і продовжити їх удосконалення в інтересах створення Єдиної автоматизованої системи управління Збройних сил України;

забезпечити можливість управління військами Збройних сил України на двох інформаційних напрямках з наданням сучасних цифрових послуг зв'язку за допомогою стаціонарної та частково польової опорної мереж зв'язку Збройних сил України;

завершити на 100% створення стаціонарної та довести до 70% створення польової складової частини захищеної системи обміну інформацією Збройних сил України;

забезпечити сумісність стаціонарної та польової компонент системи зв'язку, створити технічні умови для спроможності польової компоненти системи зв'язку забезпечувати обмін розвідувальною інформацією в оперативній та тактичній ланках управління, у тому числі з використанням безпілотних літальних апаратів;

завершити створення інтегрованої системи супутникового зв'язку Збройних сил як підсистеми Національної системи супутникового зв'язку України та цифрової системи радіозв'язку Збройних сил;

зменшити витрати на утримання стаціонарної компоненти системи зв'язку Збройних сил України.

ЛІТЕРАТУРА

1. Замисел реформування і розвитку системи та військ зв'язку Збройних сил України.

2. Замисел переоснащення системи зв'язку Збройних сил України цифровими засобами на період 2013–2017 років та шляхи його реалізації.

3. Державна комплексна Програма реформування та розвитку Збройних сил України на період до 2017 року.

Мазниченко Ю.А. (НЦЗІ ВІТІ ДУТ)
Бондаренко О.Є. (НЦЗІ ВІТІ ДУТ)
Чередниченко О.Ю. (НЦЗІ ВІТІ ДУТ)
Черкасова Ю.О. (НЦЗІ ВІТІ ДУТ)

СТВОРЕННЯ СИСТЕМИ СУПУТНИКОВОГО ЗВ'ЯЗКУ ЗБРОЙНИХ СИЛ УКРАЇНИ НА ОСНОВІ НАЦІОНАЛЬНОГО СУПУТНИКА ЗВ'ЯЗКУ ТА МОВЛЕННЯ

У сучасних умовах та в перспективі практично неможливо забезпечити неперервне та стійке управління збройними силами та силовими структурами без використання супутникового зв'язку.

В багатьох випадках супутниковий зв'язок є єдиним способом, який дозволяє забезпечити управління військами (силами), особливо в початковий період їх розгортання на непідготовленому оперативному напрямку. З впевненістю можна сказати, що супутникові канали з резервних стали основними при організації зв'язку з миротворчими контингентами. Особливу значимість супутниковий зв'язок набуває в умовах локальних конфліктів, коли відсутня можливість розгортання повнофункіональної польової системи зв'язку або умови оточуючого середовища не дозволяють цього зробити, що неодноразово підтверджено досвідом багатьох армій світу.

На теперішній час однією з важливих складових системи зв'язку збройних сил технічно розвинутих країн світу є система супутникового зв'язку, що обумовлено наступними особливостями супутникового зв'язку, які відрізняють її від інших родів зв'язку:

оперативність розгортання та згортання відповідних мереж зв'язку;

висока якість каналів зв'язку;

слабка залежність від рельєфу місцевості та погодних умов;

скритність зв'язку за рахунок використання вузько направлених антен та широкосмугових сигналів.

До 1996 року у Збройних Силах України функціонувала система супутникового зв'язку з використанням комплексу станцій супутникового зв'язку Р-440 „Кристал", що використовував для ретрансляції космічні апарати (КА) зв'язку типу „Грань" системи Єдиної Системи Супутникового Зв'язку-1 (ЄССЗ-1), яка належала Росії.

Згідно „Соглашения об использовании систем спутниковой связи военного назначения и их дальнейшем совершенствовании" підписаному прем'єр-міністрами держав СНД, Україна мала право безкоштовно користуватися ресурсом пропускної спроможності ретрансляторів КА, виведених на орбіту до 13.11.92 року (у межах раніше виділених радіо даних), поки не закінчиться їх гарантійний строк роботи.

Тобто, після 1996 року Збройні Сили України не мають ресурсу ретранслятора для забезпечення роботи своїх супутникових мереж, так як гарантійний термін самого „свіжого" з угрупування КА закінчився 12.12.94 року.

Згідно „Соглашения об использовании систем спутниковой связи военного назначения и их дальнейшем совершенствовании" було передбачено укладання двосторонніх угод між Міністерством оборони (МО) Російської Федерації та Міністерствами оборони зацікавлених держав бувшого СРСР про дольове фінансування виробництва, запуску і управління КА ЄССЗ-1 у межах ресурсу, що замовляється. Але нажаль відповідна угода між МО РФ і МО України не була укладена.

Таким чином відсутність ресурсу пропускної спроможності КА не дозволяє забезпечити супутниковий зв'язок з використанням станцій супутникового зв'язку комплексу „Кристал", які до теперішнього часу перебувають на озброєнні Збройних Сил України.

На сьогодні у Збройних Силах України для забезпечення супутникового зв'язку використовуються:

станції супутникового зв’язку;

термінали супутникового зв’язку;

телефонні термінали супутникового зв’язку системи.

Основними завданнями цих станцій є забезпечення голосового зв’язку, передачі даних та забезпечення відео конференційного зв’язку.

Забезпечення супутникового зв’язку в інтересах Збройних Сил України здійснюється шляхом оренди ресурсу іноземних провайдерів супутникового зв’язку через операторів, що діють на території України.

Тому, на сьогоднішній день, створення військової системи супутникового зв’язку залишається актуальною проблемою.

Слід зауважити, що лідерами у використанні супутникового зв’язку для забезпечення управління військами (силами) безперечно залишаються Росія та США, які мають у своєму розпорядженні спеціалізовані військові системи супутникового зв’язку.

Значна кількість країн використовує для забезпечення потреб збройних сил ресурс комерційних супутників зв’язку, що значно здешевлює вартість утримання системи супутникового зв’язку.

Правовою основою створення військової системи супутникового зв’язку є постанова Кабінету Міністрів України від 3 травня 2007 року №696 „Про заходи щодо створення національної супутникової системи зв’язку” та „Замисел реформування і розвитку системи та військ зв’язку Збройних Сил України”.

Узагальненою характеристикою створюваної військової системи супутникового зв’язку є наступні положення:

– система супутникового зв’язку Збройних Сил України створюється як складова частина Національної супутникової системи зв’язку на основі Національного супутника зв’язку та мовлення;

– зона обслуговування супутникового зв’язку Збройних Сил України включає території: України; країн східної та центральної Європи; центральної та західної Африки; Індії; акваторії Чорного та східної частини Середземного морів. Глобальна зона покриття забезпечується орендованим супутниковим ресурсом;

– передбачається застосування станцій супутникового зв’язку стандарту VSAT.

Запуск національного супутника зв’язку та мовлення заплановано на початок 2014 року. Основні характеристики супутника приведені в таблиці 1.

Таблиця 1

Основні характеристики супутника ретранслятора

Характеристики	Значення / Вимога
Орбіта виведення	Геостаціонарна
Орбітальна позиція	48° сх.д.
Тривалість Космічної Операції	15 років
Корисне Навантаження	до 30 активних каналів зі смугою пропускання 33 МГц
Діапазон частот	Ku - діапазон
Маса Супутника (з адаптером)	1845 кг
Маса Корисного Навантаження	350 кг

Зона покриття національного супутника зв’язку та мовлення складається з трьох променів євро-українського, індійського, західно-африканського. Вигляд зон покриття променів, які плануються показано на рисунку 1.

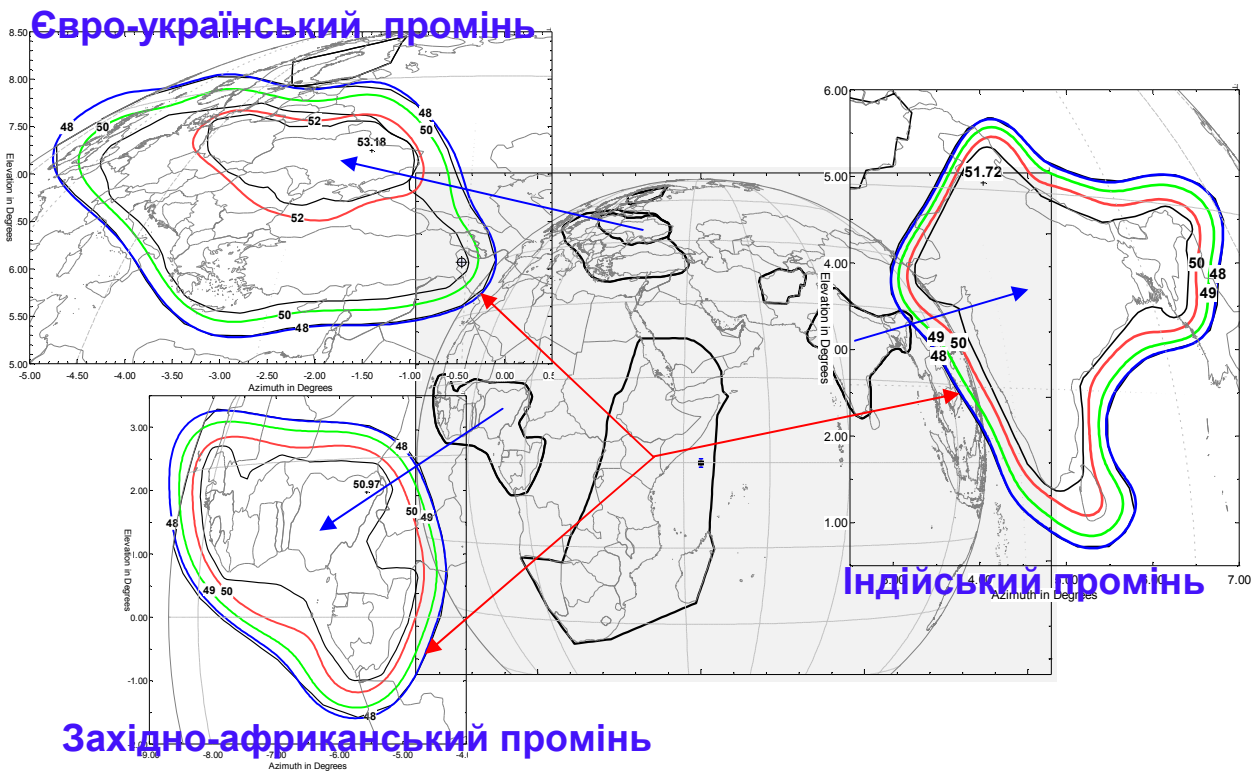


Рис. 1 – Зони покриття променів національного супутника зв'язку та мовлення, які плануються

З метою економії частотно-орбітального ресурсу штучного супутника зв'язку та мінімізації витрат на побудову системи супутникового зв'язку доцільно створювати систему у якій робота земних станцій супутникового зв'язку (стаціонарних та мобільних) буде забезпечена через центральну земну станцію, яка буде виконувати функцію маршрутизатора та комутатора супутникових каналів зв'язку. Зважаючи на зазначене склад системи супутникового зв'язку Збройних Сил України буде складатись з:

– центральної станції супутникового зв'язку основної та резервної, доцільно також передбачити можливість в подальшому створення мобільного варіанту центральної станції;

– стаціонарних станцій супутникового зв'язку для використання їх на стаціонарних ІТВ пунктів управління;

– мобільних станції супутникового зв'язку:

станцій супутникового зв'язку перевізних та контейнерного типу, які будуть встановлені на об'єктах на колісних та гусеничних шасі, кораблях;

переносних станцій супутникового зв'язку.

Систему супутникового зв'язку Збройних Сил України доцільно будувати з топологією „зірка" та у подальшому передбачити можливість використання топології „кожен з кожним" для підвищення її живучості.

Отже можна зазначити, що на сьогоднішній день, створення системи супутникового зв'язку Збройних Сил України залишається актуальним завданням. Вирішення цього завдання дасть можливість резервування та нарощування транспортної мережі стаціонарного і мобільного компонентів.

к.т.н. Могилевич Д.І. (ВІТІ ДУТ)

ПОКАЗНИКИ ЯКОСТІ ТА НАДІЙНОСТІ ФУНКЦІОНУВАННЯ МЕРЕЖ ЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Введення. Система зв'язку є однією з основних частин виробничої та соціальної інфраструктури України, від стану якої залежить можливість військово-політичного керівництва України реагувати на зміну оперативно-стратегічних і військово-політичних умов у світі. Тому, питанням вдосконалення та підвищенню ефективності функціонування системи зв'язку і її технічної основи – мережі зв'язку, приділяється постійна та не послаблена увага. Це відноситься як до мереж зв'язку загального користування, так і до мереж зв'язку різних відомств. Поряд з загальними закономірностями побудови та функціонуванням мереж зв'язку будь-якого типу, відомчі мережі зв'язку можуть істотно відрізнятися від мереж зв'язку загального користування. Це пов'язано із специфічними вимогами, які висуваються з боку користувачів до відомчих мереж і необхідністю забезпечення функціонування таких мереж в умовах, що істотно відрізняються від тих, у яких перебувають мережі зв'язку загального користування. Таким чином, відомчі мережі виділяють в окремий клас – мереж зв'язку спеціального призначення (МЗСП). На даний час іде процес вдосконалення МЗСП, що вимагає наукового обґрунтування різноманітних задач, які вирішуються на всіх етапах реформування системи управління (наприклад, системи управління Збройних Сил України). Дослідження МЗСП вимагають вибору та обґрунтування показників якості та надійності функціонування.

Основна частина. Найбільш повною характеристикою мереж зв'язку спеціального призначення, як і будь-яких складних технічних систем є якість функціонування. Як відомо, якість – сукупність властивостей, які обумовлюють її здатність задовольняти певні потреби у відповідності зі своїм призначенням протягом встановленого часу. Цю сукупність властивостей можна умовно розбити на наступні групи:

1. Характеристики, які визначають можливості системи виконувати визначені функції відповідно призначенню за умови, що апаратура, механізми та обладнання повністю працездатні.

2. Характеристики, які визначають здатність системи зберігати свої можливості в заданих межах у процесі функціонування за певних умов експлуатації, а також часові, матеріальні та трудові витрати на підтримку системи у працездатному стані.

Перша група характеристик визначає цільове призначення МЗСП і вимоги до достовірної та своєчасної передачі інформації при забезпеченні вимог безпеки. Для МЗСП своєчасність передачі інформації є однією з найважливіших властивостей за умови виконання заданих вимог до вірогідності і безвідмовності.

Кількісною мірою, яка характеризує властивість своєчасності інформаційного обміну є показник ймовірності своєчасної доставки повідомлень (пакетів), що визначає ймовірність того, що сумарний час очікування в черзі, обслуговування пакетів та інших затримок, обумовлених збоями, відмовами обладнання, перешкодами та т.п., не перевищить заданий (допустимий) час доставки. Заданий час є системним параметром і призначається з урахуванням оперативної і тактичної обстановки та вимог, що висуваються до часу старіння переданої інформації. Цей час визначає допустимий час затримки в доставці повідомлень (пакетів) користувачу.

При цьому ймовірність своєчасної доставки повідомлень – комплексний показник, що залежить від сукупності факторів, які впливають на час передачі. До числа таких факторів варто віднести: виникнення відмов і збоїв обладнання, час його відновлення, швидкодії та інше. Даний показник якості функціонування МЗСП – ймовірність своєчасної доставки повідомлень, використовується як цільова функція при розв'язанні різних задач, зокрема:

при оптимізації побудови МЗСП показник ймовірності своєчасної доставки при заданих обмеженнях (фінансових, часових та ін.) має максимальне значення у деякій

граничній області;

при порівнянні різних варіантів побудови МЗСП і виборі кращого за показником ймовірності своєчасної доставки пакетів мережі з розглянутих альтернатив;

при оцінці придатності МЗСП для виконання задач за призначенням у заданих умовах функціонування – критерій придатності.

У ряді випадків як узагальнений показник якості функціонування МЗСП розглядають також продуктивність – кількість вчасно переданих повідомлень.

До другої групи характеристик належать експлуатаційно-технічні характеристики мережі зв'язку. До їх числа відносять показники надійності обладнання, параметри контролю працездатності, обслуговування та ремонту, вид та кількість використаної надмірності і т.д.

З визначення та складу експлуатаційно-технічних характеристик можна зробити висновок: по-перше, всі характеристики тісно пов'язані між собою, доповнюють одна одну, відображають різні сторони технічного розв'язку мережі зв'язку; по-друге, центральне місце серед них займає надійність. Дійсно, досвід експлуатації МЗСП показує, що чим нижче надійність обладнання, тим більш високі вимоги висуваються до об'єму і якості резервування, системи технічного обслуговування, ремонту і контролю, складу та кваліфікації обслуговуючого персоналу і т.д. Тому, забезпечення високих експлуатаційно-технічних характеристик обладнання мережі зв'язку є засобом забезпечення її високої надійності функціонування, а, отже, високої ефективності інформаційного обміну.

Вартість створення та експлуатації МЗСП також є узагальнюючою характеристикою, однак, будучи специфічною економічною категорією, вона звичайно відіграє роль загального обмежувального фактору.

У загальному випадку надійність – комплексна властивість, що включає в себе ряд окремих властивостей (безвідмовність, ремонтопридатність, довговічність, збережуваність) і залежить від різноманітних факторів. Надійність функціонування МЗСП виражає ступінь реалізації їхніх можливостей за здійсненням та інформаційним обміном в реальних умовах експлуатації. Вона залежить не тільки від показників надійності обладнання, але визначається також характером навантаження на мережу зв'язку та цілим рядом організаційно-технічних заходів і факторів, які впливають на загальний процес функціонування МЗСП: видом використовуваної надмірності та кратністю резервування, режимами технічного обслуговування, якістю контролю, структурою та організацією системи ремонту і т.п. Урахування всіх цих факторів при розрахунках показників надійності дозволяє не тільки повною мірою враховувати реальні можливості МЗСП, але й більш обґрунтовано вибирати шляхи і методи забезпечення їхнього нормального функціонування в процесі тривалої експлуатації.

Висновок. Комплексне урахування показників функціональних та експлуатаційно-технічні характеристики дає можливість кількісно оцінювати реальну надійність та якість функціонування мереж зв'язку спеціального призначення і науково обґрунтовувати доцільність (ефективність) різних технічних та організаційних рішень при вдосконаленні існуючих та побудові перспективних мереж зв'язку.

ЛІТЕРАТУРА

1. Надежность и эффективность в технике: Справочник: в 10т. / Т. 1: Методология. Организация. Терминология // Под ред. А.И. Рембезы. – М.: Машиностроение, 1986. – 224 с.

2. Надійність техніки. Терміни та визначення: ДСТУ 2860-94. – [Чинний від 1996-01-01]. – К.: Держстандарт України, 1995. – 90 с. (Національний стандарт України).

3. Могилевич Д.І. Надійність систем епізодичного використання в умовах обмеженої інформації про вихідні дані / Могилевич Д.І., Креденцер Б.П., Міночкін А.І. // Збірник наукових праць – К.: ВІТІ НТУУ «КПІ», 2010. – №2. – С. 37 – 41.

4.Оцінка надійності резервованих систем при обмеженій вихідній інформації: монографія / [Креденцер Б.П., Вишнівський В.В., Могилевич Д.І. та ін.]; – К.: Фенікс, 2013. – 336 с.

к.т.н. Павлов І.М. (ВІТІ ДУТ)

ПЕРСПЕКТИВИ РОЗВИТКУ ПОЛЬОВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ВУЗЛІВ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ З ВИКОРИСТАННЯМ НОВИХ ТЕХНОЛОГІЙ

Вступ. У наступний час у світі виконується повномасштабна модернізація систем управління і зв'язку військового призначення, яка передбачає наряду з внесенням змін у організаційно-штатну структуру інформаційно-телекомунікаційних вузлів (ІТВ) різного призначення також самих принципів організації зв'язку на полі бою (під час проведення бойових дій підрозділами та частинами).

У зв'язку з цим приділяються значні зусилля по реалізації програм впровадження мережевих інформаційних технологій у практику бойового застосування військ. Мета цих змін – створення формувань нового модульного типу, оснащених системами і засобами інформаційного забезпечення модульної конструкції, нових принципів маршрутизації інформаційних потоків, що дозволяє відмовитися від жорсткої централізації управління, оптимізувати структуру систем зв'язку з врахуванням процесів виконання раптових задач, які виникають на полі бою, виключити „людський фактор", та істотно підвищити бойову могутність і ефективність застосування сил і засобів управління під час ведення бойових дій.

Спектр напрямків робіт, у цій області, достатньо широкий, починаючи з індивідуальної екіпіровки військовослужбовців засобами інформаційних технологій (маршрутизатори, навігатори, комунікатори, інтерактивні дисплеї, хаби, радіостанції з виходом на тактичний інтернет і т.п.), які спроможні вести бойові дії у єдиному інформаційному просторі – цю екіпіровку можна представити як носимий варіант інформаційно-телекомунікаційного вузла і закінчуючи створенням апаратно-програмних комплексів на транспортній базі (наземна, морська, повітряна), які повинні працювати сумісно у єдиному часі з носимими комплектами. Все це визначає необхідність аналізу шляхів розвитку польових інформаційно-телекомунікаційних вузлів, *що є метою цієї роботи*.

Основна частина. Ключове місце, під час рішення задач у тактичній ланці управління, займають технології безпроводового доступу до розподілених інформаційних ресурсів, оскільки переваги використання засобів радіозв'язку під час роботи у мережі зрозумілі: мобільність, простота і оперативність доступу до даних і т.п. Безпроводові персональні, локальні і регіональні мережі вже стали реальністю; після появи відповідних стандартів світових виробників почали створюватися засоби для комерційних і військових користувачів.

Основним засобом зв'язку для формування тактичного рівня є мережеві радіостанції. Так у американській системі класу „C2SR" – „Force XXI Battle Command Brigade and Below" (FBCB2) – ця назва в доволі вільному перекладі можу бути визначена як „Система управління бригадою і підлеглими підрозділами у бою (битві) двадцять першого століття"(Northrop Grumman Corporation), зв'язок між апаратно-програмними комплексами на транспортній базі підтримується двома комунікаційними системами: інформаційною мережею „ТІ" (тактичний інтернет), з використанням систем радіозв'язку EPLRS та SINGARS, і системою рухомого супутникового зв'язку „Інмарсат" (станції PSC-5 Spitfire діапазону 225-400 МГц). При цьому, для забезпечення супутникового зв'язку під час переміщення, пункти управління розвідувальних підрозділів і машини командного пункту бригади оснащуються спеціальними стабілізованими супутниковими антенами.

Зв'язок КП бригади з вищестоячими органами управління і КП сусідніх бригад виконується або через малий польовий районий вузол зв'язку системи зв'язку загального користування Enhanced MSE („Удосконалена MSE"), яка має структуру „сітки" побудовану на комутаторах асинхронного режиму доставки, або через військову систему зв'язку вищестоящого командування. Планування, конфігурація і реконфігурація мережі в ланці

„бригада-батальйон” виконується під управлінням програмного забезпечення системи „ISYSCON” (ПЗ управління інтегрованими системами, версія 4).

Дані в мережах зв’язку, які об’єднують АРМ системи FBCB2, передаються під управлінням протоколів IP, адаптованих у відповідності з вимогами і умовами функціонування мереж радіозв’язку в тактичній ланці управління. В межах КП бригади і батальйону (при їх розміщенні на місці) усі засоби зв’язку і засоби системи FBCB2 з’єднані між собою в ЛОМ (локальну обчислювальну мережу) за допомогою проводових засобів.

Машини КП бригади з’єднуються між собою і з районним вузлом зв’язку системи Enhanced MSE волоконно-оптичною лінією зв’язку (ВОЛЗ) з перепускною спроможністю 100 Мбит/с. Районна обчислювальна мережа, яка охоплює КП бригади і батальйонів, будується на основі радіостанцій NTDR і терміналів зв’язку JNN. Крім того, радіостанції NTDR забезпечують резервні канали зв’язку для ланки управління „бригада і вище”

Однак, особливе значення у бойових умовах, які характеризуються швидкою зміною обстановки і динамічністю ситуації, передбачає можливість формування радіомережі, усі функції адміністрування, якої, виконують самі вузли (як на транспортній базі так і носимі) без участі людини. Мережі цього типу отримали назву мобільних, адаптивних, що відображають нестандартну архітектуру, які відрізняється від класичної схеми.

В цілому під мобільною адаптивною мережею розуміють сукупність мобільних вузлів, мережева інфраструктура, яка динамічно змінюється і яка має наступні особливості:

відсутність зовнішніх механізмів настроювання, тобто мережа є самоконфігуруємою;

мережевий вузол виконує функції як маршрутизатора, так і кінцевого пристрою;

відносно малий час життя мережі у одному і тому-ж стані.

Одним з класичних прикладів системи зв’язку з цими особливостями є розробляєма спеціалізована мобільна мережа MANET, яка характеризується:

багатошляховими маршрутами, при цьому маршрутизація повинна самостійно знаходити шлях від джерела до приймача;

підтримкою маршруту (наприклад, якщо проміжний вузол відбув і шлях зруйнувався);

визначенням механізмів обміну інформацією про маршрутизацію тощо.

Для чого реалізуються наступні протоколи маршрутизації, які представлені на рис. 1.

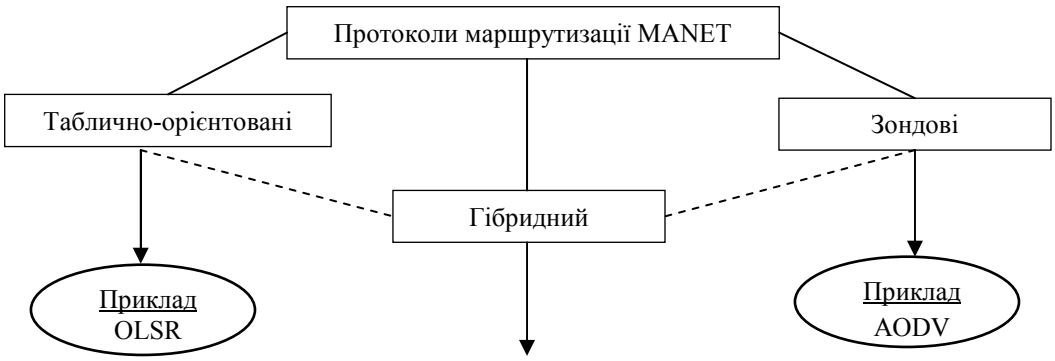


Рис. 1. Приклади протоколів маршрутизації мобільної мережі MANET

При цьому зондові протоколи повинні знаходити маршрут у тому випадку, коли необхідно передати пакет і для нього нема відомого шляху а також змінюють шлях, якщо пройшла маршруту. Превентивні протоколи знаходять маршрут завчасно для усіх пар джерело-приймач і періодично оновлюють інформацію про маршрутизацію підтримки шляхів. Гібридні протоколи повинні мати усі ці переваги. У наступний час проводиться робота по впровадженню 4-х основних протоколів маршрутизації:

спеціалізований протокол вектора відстані по запиту (AODV);

протокол динамічної маршрутизації джерела (DSR);

протокол оптимізованої маршрутизації стану з’єднань (OLSR);

протокол топологічного оповіщення, який базується на зворотному проходженні даних (TBRPF).

Мобільна адаптивна мережа зв'язку тактичної ланки управління на базі польових мобільних інформаційно-телекомунікаційних вузлів (носимих і на транспортній базі) має наступні переваги по відношенню з мережами фіксованих архітектур (які впроваджуються на більш високих ланках управління – оперативній та стратегічній) – висока живучість, гнучкість топології і автоматична адаптація до змін мережевої конфігурації на базі програмованих цифрових радіостанцій, носимих станцій супутникового зв'язку, пристроїв передачі даних та програмування бойових дій.

На рис. 2 представлена перспективна схема розгортання інформаційно-телекомунікаційних вузлів єдиної системи зв'язку тактичної ланки управління.

Рис. 2. Перспективна схема розгортання інформаційно-телекомунікаційних вузлів єдиної системи зв'язку тактичної ланки управління

Висновки. Створення нових інформаційно-телекомунікаційних вузлів тактичної ланки управління приведе до змін в системі управління. Повна автоматична децентралізація управління з використанням елементів штучного інтелекту приведе до зміни класичних пунктів управління (КП, ЗКП, ТПУ) на *віртуальні пункти управління*, коли той або інший командир буде мати автономну, мобільну і різноваріантну топологію системи управління, яка буде змінюватися в залежності від обстановки, задач, місць і способів розташування органів управління з головною метою: досягнення переваги над противником за рахунок впровадження нових інформаційних технологій і поглядів на управління підлеглими під час ведення бойових дій.

ЛІТЕРАТУРА

1. http://www.ietf.org/html.charters/manet-charter.html.
2. http://protean.itd.nrl.navy.mil/manet/manet_home.html.
3. http://commi.narod.ru/2012/1201.htm.
4. Жуков В.Б. Система управления Вооружёнными Силами США / В.Б. Жуков, А.Р. Оберстов. Зарубежное военное обозрение. – № 12. – 2011. – С. 12 – 19.
5. http://www.flickr.com/2010.1345.htm.

Поліщук Л.І. (НЦСВ АСВ)
к.т.н. Богуцький С.М. (НЦСВ АСВ)

АНАЛІЗ ДОСВІДУ ЩОДО ПЕРЕДУМОВ ТА ОСНОВНИХ НАПРЯМКІВ РОЗВИТКУ ТА РЕФОРМУВАННЯ СИСТЕМ УПРАВЛІННЯ СУХОПУТНИХ ВІЙСЬК ЗБРОЙНИХ СИЛ ПРОВІДНИХ КРАЇН СВІТУ

В останні роки в технічно розвинених державах світу особлива увага приділяється активному розвитку теорії і практики ведення мережецентричних дій, які кардинально змінюють погляди на підготовку і застосування Збройних сил (ЗС) в сучасних війнах і конфліктах, а саме: НАТО – реалізує концепцію „комплексні мережеві можливості»; Франція – „інформаційно-центрична віна”; Великобританія – „мережеві можливості”; Швеція – „мережева оборона”; Ізраїль – „цифрова армія”; Нідерланди – „мережецентричні операції”; Китай – „система бойового управління, зв’язку, обчислювальної техніки, розвідки і вогневого ураження” [9].

Глобально воєнно-політичні і економічні обставини в кінці ХХ – початку ХХІ століття формуються під впливом складних процесів геоекономічної та геополітичної побудови системи міжнародних відносин, пов’язаних, у першу чергу, з загостренням боротьби за контроль над природними ресурсами, особливо енергетичними, а також з невизначеністю її подальшого розвитку.

Разом з тим, передумовами переходу до нових форм і способів ведення бойових дій у останні роки стали:

1. Зростання значення стратегічного неядерного стримування супротивника шляхом масового оснащення військ новітніми засобами збройної боротьби для ведення неядерних, неконтактних (дистанційних) бойових дій.
2. Підвищення ролі динамічності та маневреності дій військ (сил) на розрізнених напрямках з широким застосуванням сил швидкого реагування, аеромобільних військ і військ спеціального призначення.
3. Розширення простору та масштабів збройної боротьби, перенесення бойових дій із землі і поверхні морів у повітря, під воду та у космос. Одночасне вогневе та електронне ураження військ, об’єктів тилу, економіки, комунікацій на всій території супротивника.
4. Зростання ролі і значимості протиборства в інформаційній сфері (розвідці, керуванні військами і зброєю) та використання для цього новітніх інформаційних технологій.
5. Боротьба з міжнародним тероризмом, створення експедиційних сил для проведення миротворчих і антитерористичних операцій [4].

Все це створило передумови докорінного перегляду системи поглядів на характер майбутніх операцій і ведення бойових дій, які набувають технологічного характеру у всіх сферах воєнних дій.

Суттєвою ознакою збройних конфліктів стала відмова від проведення масштабних стратегічних операцій, що пов’язано з високим динамізмом та швидкоплинністю воєнних дій.

Характерною рисою сучасних і майбутніх конфліктів є підвищення ролі політичних, економічних, інформаційних заходів під час підготовки і в ході воєнного конфлікту, створення коаліційних і багатонаціональних сил, розширення масштабу операцій і перетворення морського, повітряного, космічного та сухопутного простору в єдиний глобальний театр воєнних дій. При цьому зростають загальна динаміка та швидкість воєнних дій, які будуть швидко поширюватись на всю територію держави.

Це змусило військово-політичне керівництво провідних держав переглянути погляди на роль і значення силового компоненту в досягненні стратегічних цілей держав на

міжнародній арені, в тому числі і на теорію та практику військового будівництва. Була визнана необхідність удосконалення процесів управління і застосування ЗС.

НАТО перебуває на стадії подальшої військової трансформації. Зважаючи на стрімке скорочення оборонних бюджетів європейських країн, обговорюється ініціатива керівництва НАТО щодо „інтелектуальної побудови НАТО". Дослідження сучасних воєнних конфліктів вказують на збільшення можливостей озброєння та одночасне скорочення чисельності ЗС.

Якісно новим кроком у розвитку теорії воєнного мистецтва стала концепція „об'єднаної операції", яка викладена у новій редакції статуту ЗС США. „Об'єднана операція" – це сукупність зведених у єдиний план за метою, місцем та часом, адаптованих до змін в обстановці синхронізованих боїв, ударів, маневру та спеціальних дій об'єднань, з'єднань, частин та підрозділів декількох видів Збройних Сил для вирішення завдань щодо знищення противника. Об'єднаність дій військ досягається створенням єдиного інформаційного простору.

Перехід до глобальних інтегрованих АСУ військами і зброєю, застосування новітніх систем озброєння дозволяють досягти мети за короткий час. Нові, так звані, мережецентричні, або безконтактні війни можуть вести лише надзвичайно розвинені у військовому аспекті країни, насамперед США.

Військове керівництво США в якості одного з основних напрямків своєї діяльності з підвищення бойових можливостей об'єднаних ЗС та підготовки їх до проведення спільних операцій в XXI столітті, в кінці 90-х років минулого століття визначило реалізацію концепції ведення військових дій в єдиному інформаційному просторі або з використанням об'єднаних інформаційно-керованих мереж (NCW – Network Centric Warfare).

У відповідності до цієї концепції передбачається за допомогою забезпечення військ передовими інформаційними технологіями об'єднати розосереджені в широкому бойовому просторі різнорідні сили і засоби (особовий склад, органи і пункти управління, органи бойового забезпечення, зброю і військову техніку наземного, повітряного і морського базування) в об'єднання з високою мережевою архітектурою – глобальні і локальні інформаційні мережі.

За оцінками експертів з Пентагону ці об'єднання, порівняно з традиційними, мають безумовну перевагу і забезпечують:

створення в реальному масштабі часу єдиної картини оперативно-тактичної обстановки;

значне скорочення часу доведення інформації від системи розвідки до засобів вогневого ураження;

значне випередження противника в прийнятті і виконанні рішень, плануванні бойових дій;

прискорену концентрацію розосереджених в бойовому просторі різних засобів ураження для нанесення ударів.

В результаті реалізації цих можливостей, бойова ефективність об'єднань з мережевою архітектурою порівняно з існуючою, виростає багаторазово [1].

В даний час в ЗС США проводяться заходи по розвитку системи управління бойовими діями. Напрямки діяльності в цій області викладені у прийнятій в США концепції «Системи управління, зв'язку, розвідки і комп'ютерного забезпечення для учасників бойових дій» (Command Communications Computers and Intellegence for the Warrior).

До цих напрямків відносяться:

забезпечення оперативно-технічних можливостей для організації взаємодії і спільного бойового використання сил і засобів в рамках єдиної структури управління (головний напрямок);

широке застосування автоматизованих систем управління (АСУ), які максимально виключають ступінь участі людини в зборі, обробці, аналізі і розподілі інформації, і

забезпечують підвищення ефективності оперативного управління військами за критеріями: поінформованість, коректність рішень, які приймаються, виграш в часі;

забезпечення підвищеної стійкості управління в будь-яких умовах обстановки за рахунок живучості, надійності, завадостійкості та інформаційної захищеності засобів;

максимально можливе застосування останніх досягнень науки і техніки в області телекомунікацій, а також готових комерційних стандартів і апаратно-програмних засобів з метою скорочення термінів проектування і введення в дію нових систем.

В реалізації цієї концепції створюється „система систем", яка включає в себе три складові частини:

об'єднану систему спостереження та розвідки;

автоматизовану систему бойового управління силами та обміну інформацією;

систему, яка забезпечує застосування високоточної зброї (ВТЗ).

Кінцевим результатом реалізації програми за вказаними напрямками є створення єдиної інформаційно-керованої структури, здатної забезпечити централізоване управління в реальному масштабі часу діями всіх видів ЗС США, як в широкомасштабних війнах, так і в регіональних конфліктах, вільний доступ користувачів до ресурсів системи, а також оптимізацію процесів обробки і обміну даних в усіх ланках управління військами. Завдячуючи запровадженню цієї структури, наведення і застосування зброї буде здійснюватись з високим ступенем надійності і оперативності, що не дозволить противнику прийняти адекватні відповідні міри [2].

Таким чином закономірно, що з врахуванням вищенаведеного вносяться відповідні зміни не тільки в структуру управління ЗС США, але і в зміст самих процесів та функцій системи управління. Тому, з врахуванням змін характеру війн і воєнних конфліктів, в США продовжується масштабне, цілеспрямоване реформування ЗС, направлене, в тому числі, на здійснення структурних і функціональних змін в системі їх управління. Основним змістом цього процесу є трансформація взаємозв'язків різнорідних сил і засобів, які перейшли від індустріальної епохи, в об'єднані ЗС інформаційного часу – більш гнучкі і мобільні, здатні, використовуючи сучасні системи зв'язку і автоматизовані інформаційно-управлінські системи, вдосконалені засоби розвідки і високоточну зброю, в мінімальні терміни і при мінімальних втратах забезпечити ефективне досягнення воєнно-політичних чи інших цілей держави (коаліції держав) в ході протиборства з будь-яким противником.

В новій редакції „Єдина перспектива – 2020" відмічено, що „інформаційна революція", яка продовжується, створює не тільки кількісні, але і якісні зміни в інформаційній сфері, яка до 2020 року приведе до значних змін в проведенні воєнних операцій. Рішення конгресу США про чисельне скорочення ЗС підвищило вимоги до інформаційних технологій. Тому в „Єдиній перспективі-2020" були уточнені концепції розвитку архітектури систем управління і зв'язку видів ЗС (Сухопутні війська (СВ) – „Ентерпрайз", Військово-Морські Сили (ВМС) – „Коперник", Повітряні Сили (ПС) – „Горизонт"). (див. Рис. 1)

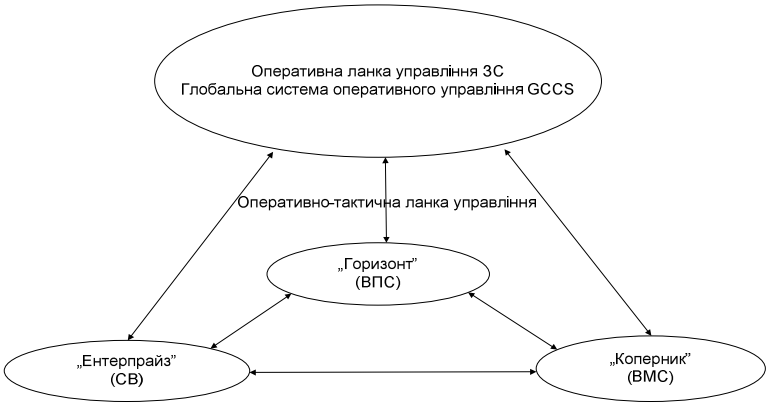


Рис. 1. Архітектура систем управління і зв'язку видів ЗС

В оперативно-стратегічній ланці управління ЗС США введена в дію глобальна АСУ ЗС США GCCS (Global Command Control Sustem), в якій реалізується новий стратегічний принцип – ураження будь-якої цілі – в будь-якому районі – в будь-який час. Вона являється системою, яка надає засоби для оперативного управління і адміністративного забезпечення ЗС США. Її обладнання забезпечує зв'язком вище воєнно-політичне керівництво, об'єднаний штабу КНШ з штабами видів ЗС, управління центрального підпорядкування МО, об'єднані командування, командувачів об'єднаними оперативними формуваннями і формування забезпечення. (див. Рис. 2).

Рис. 2. Глобальна АСУ ЗС США GCCS (Global Command Control Sustem)

На ряду з широко розвиненою мережею захищених стаціонарних ПУ, як на території США так і за її межами, обладнаних багатозарезервованими системами зв'язку і АСУ, найбільш важливими елементами в системі управління СВ є центри управління бойовими діями (ЦУБД), командні пункти (КП), штабні машини управління. Здійснюється модульний принцип побудови апаратури ЦУБД.

Для підвищення можливостей по управлінню дивізією, поступають нові машини управління, із яких швидко формується мобільний КП і ЦУБД дивізії. Вони мають весь необхідний комплект апаратури, яка забезпечує безперервний доступ в розподілену базу даних дивізії і до єдиної картини оперативної (тактичної) обстановки.

Створена машина бойового управління BCV (Battle Command Vehicle) для командирів бригад і батальйонів. Її бортові системи можуть отримувати оперативну і розвідувальну інформацію з ЦУБД дивізії, зв'язуватись з передовими підрозділами і, при необхідності, обмінюватись інформацією з вищестоящими і сусідніми штабами. Є дві версії – на базі БМП „БРЕДЛІ" (для командирів бригад і командирів піхотних підрозділів) і на базі танка М1А1 „Абрамс" (для командирів бронетанкових підрозділів) [2].

Систему зв'язку і автоматизації системи управління ЗС США складають: розгалужена мережа оптоволоконного зв'язку, системи супутникового зв'язку, а також сучасні багатоканальні лінії радіорелейного, тропосферного і радіо зв'язку.

Командування ЗС США розраховує отримати в своє розпорядження в 2010 – 2020 роках нову систему управління усіма видами ЗС, яка передбачає повну перевагу над противником, що досягається не за рахунок сил і засобів, а за рахунок створення необхідних умов для більш ефективного їх застосування. Пентагон приступив до розгортання глобальної

інформаційної мережі і практичного відпрацювання технологій нового типу війн – мережецентричної (мережевої) війни.

Таким чином, удосконалення систем управління СВ ЗС різних держав за результатами реформування проводиться:

органів управління – реорганізація проводиться за рахунок зменшення кількості штабів і командувань удосконалення їх організаційно-штатної структури, адміністративних і функціональних повноважень, взаємної сумісності органів управління різних ланок, зменшення органів логістики, відповідності стандартам НАТО;

пунктів управління – удосконалення як стаціонарних, так і мобільних ПУ в напрямках стандартизації їх обладнання як робочих місць, так і засобів пересування, забезпечення достатньої захищеності, живучості, мобільності, нормальних умов для роботи обслуговуючого персоналу;

зв'язок і АСУ – реорганізація проводиться як з удосконалення існуючих систем зв'язку (сумісна робота військових і державних систем та уніфікація засобів зв'язку у цьому напрямку з широким використанням комерційних технологій), так і створення нових супутникових, радіорелейних, тропосферних, волоконно-оптичних і радіосистем для різних ланок військового управління з можливістю загального користування їх послугами;

АСУ повинні відповідати розвитку і вимогам інших підсистем управління і забезпечувати: оперативно-технічні можливості для організації взаємодії і спільного бойового використання сил і засобів в рамках єдиної структури управління; максимальне виключення участі людини в зборі, обробці, аналізі і розподілі інформації; підвищення стійкості управління військами за рахунок живучості, надійності, завадостійкості та інформаційної захищеності засобів; постійне поповнення бази даних як за війська противника, так і за свої, а також забезпечення доступу до цієї бази даних користувачів всіх ланок управління.

ЛІТЕРАТУРА

1. Масной В., Судоков Ю. Автоматизированные системы управления Сухопутными войсками США. Зарубежное военное обозрение. – 2003. – №9. – с. 25 – 32, №10 – с. 28 – 36.

2. Кучеренко Ю.Ф., Гузько О.М. Основні шляхи розвитку систем управління військами та зброєю на сучасному етапі. Системи озброєння і військова техніка. – 2008 – №4(16). – с. 73 – 76.

3. Левков А. Сетевая война XXI века. Военная мысль. – 2005. – №4. – с.7 – 51.

4. Косс В.А. Інформаційна модель системи управління Збройними силами як сучасний різновид стратегічного озброєння. Збірник доповідей наукового семінару ЦНДІ ЗСУ – К.: ЦНДІ ЗСУ, 2004. – с. 3 – 15.

5. Романюк В.А. Напрямки розвитку тактичних систем зв'язку. Науково-технічна конференція ВІТІ. – К.: ВІТІ НТУУ „КПІ" – 200. – с.23 – 33.

6. Чайка Ю.Д. Архітектура систем військового зв'язку армій країн НАТО. Матеріали II науково-практичного семінару „Проблеми розвитку інформаційних мереж військового призначення", К.: НАОУ. – 200. – с. 71 – 90.

7. Біла книга 2012.

8. Концепція реформування і розвитку Збройних Сил України на період до 2017 року.

9. Ковба М.Ф. Мережецентричні дії – як форма застосування військ (сил) у техносфер ній війні. Труди університету. – 2012. – №7. – с.44.

к.т.н. Раєвський В.М. (УІТ МОУ)
Соколов К.О. (УІТ МОУ)

РОЗВИТОК НОРМАТИВНО-ПРАВОВОЇ БАЗИ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Питання інформаційної безпеки (в широкому розумінні) використовується усіма без винятку сферами діяльності людства – політиці, економіці, суспільному житті, інформаційно-телекомунікаційних системах і навіть екології (в розвинених країнах все частіше можна зустріти поняття інформаційна екологія)

Довідково: інформаційна екологія - наука, що вивчає закономірності впливу інформації на формування та функціонування людини, людського суспільства та людства в цілому, на здоров'я, як стан психічного, фізичного та соціального благополуччя, що розробляє заходи по оздоровленню оточуючого інформаційного середовища

Для прикладу можна привести слова професора Преображкенського з Булгаківського "Собачого серця" – (рос.) "Запомните батенька, никогда не читайте газет перед обедом, от этого ухудшается пищеварение".

Не є винятком і військова справа. За відомою класифікацією сучасні війни віднесені до війн 7-го покоління (звичайна "холодна зброя" – перше покоління, використання пороху – друге покоління, застосування нарізної зброї – третє покоління, використання танків – четверте покоління, застосування ядерної зброї – п'яте покоління, шосте покоління – застосування високоточної зброї та сьоме покоління – інформаційні війні) [1] (рис. 1).

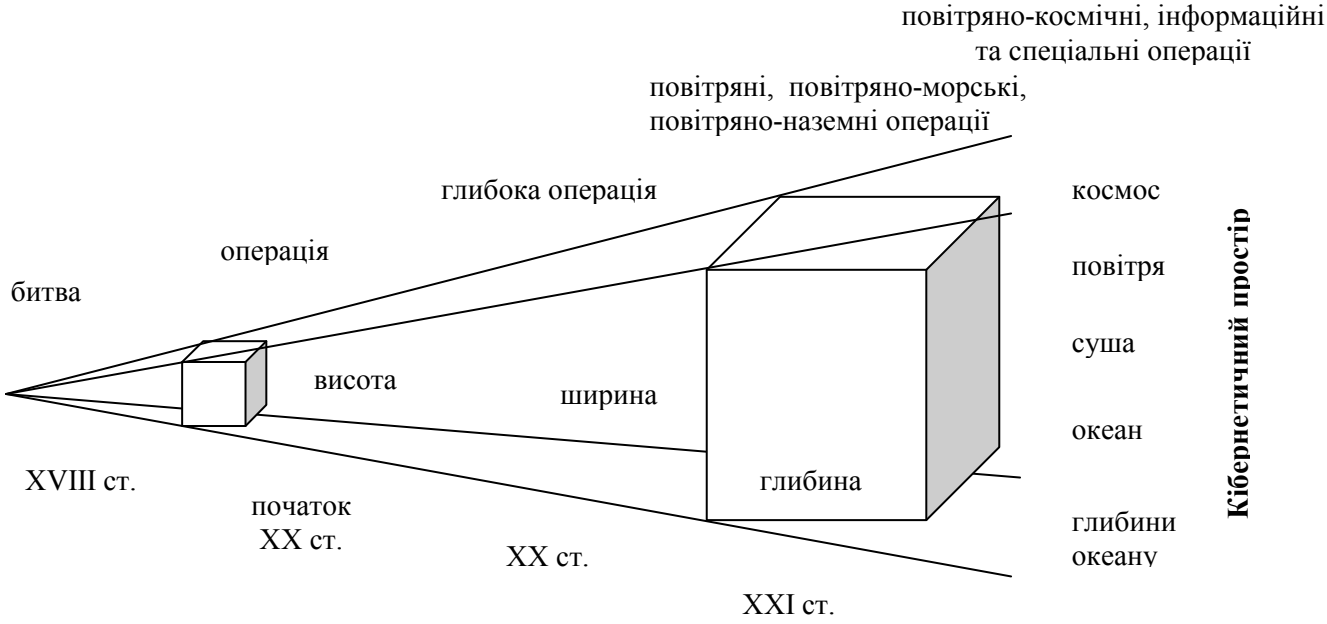


Рис. 1. Еволюція основних просторово-часових показників і форм збройної боротьби

Сучасні міжнародні організації та передові країни світу достатньо давно приділяють велику увагу питанням інформаційної безпеки та започаткували створення відповідних систем інформаційної безпеки. Як в цілому для країни так і сектору безпеки, розглянемо приклади деяких з них, особливо які відносяться до сектору безпеки і оборони.

Довідково: під час саміту НАТО у листопаді 2010 року в Лісабоні була прийнята Стратегічна Концепція оборони та безпеки НАТО в якій зазначено, що ...кібератаки стають все більш частішими, більш організованими та більш збитковими для державних установ, підприємств, економіки та об'єктів критичної інфраструктури. Вони можуть досягти критичного рівня, який загрожує національному та Євроатлантичному процвітанню, безпеці і стабільності".

У США зазначена система формується спільними зусиллями декількох державних органів управління: Міністерства оборони, Агентства національної безпеки та Міністерства внутрішньої безпеки (рис. 2).

а **б** **в**

Рис. 2. Емблеми об'єднаного кіберкомандування міністерства оборони США (а), національного центру кібербезпеки (б) та інтеграційного центру кібербезпеки Агентства національної безпеки (в)

Найбільш показовою є складова міністерства оборони: кібернетичне командування армії США, кіберкомандування ВПС, кіберкомандуваня ВМС, що об'єднані загальним керівництвом Ситратегічного командування МО США [2]. Слід зазначити, що загальна чисельність кіберкомандування США складає близько 190 тис. особового складу.

Довідково: згідно Закону України "Про чисельність ЗС України в 2012 році" загальна чисельність особового складу ЗС України складає 184 000осіб.

Російська федерація останім часом також, активно здійснює заходи зі створення подібних структур та декларує їх створення вже наприкінці 2013 року [3].

В Україні зазначене питання також обговорювалось на державному рівні під час засідання Ради національної безпеки і оборони в березні 2008 року, але більшість заходів, що були сплановані на той час, не виконані.

Пропонується розглянути існуючий стан нормативного забезпечення інформаційної безпеки в Україні, можливо, визначити напрями подальшого розвитку.

Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки визначає **інформаційну безпеку** як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. В цьому ж законі визначені шляхи вирішення проблеми інформаційної безпеки [4].

Загалом кількість нормативно-правових документів, що визначають правові основи зазначеного та суміжних питань, наприклад інформатизації, сягає близько 80, основними з яких є :

Закон України "Про основи національної безпеки України" визначено **основні загрози національним інтересам і національній безпеці України в інформаційній сфері.** В цьому ж законі визначені **основні напрями державної політики з питань національної безпеки України в інформаційній сфері** [4].

Реальні та потенційні загрози інформаційній безпеці України за сферами національної безпеки наведені в ***Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 8 липня 2009 року № 514/2009*** [4].

Ключові завдань політики національної безпеки щодо забезпечення інформаційної безпеки визначені ***Стратегією національної безпеки України "Україна у світі, що***

змінюється", затверджена Указом Президента України від 8 червня 2012 року № 389/2012 [4].

У ***Воєнній доктрині України, затвердженій Указом Президента України від 15 червня 2004 року № 648 (в редакції Указу Президента України від 8 червня 2012 року № 390/2012,)*** визначені основні шляхи **запобігання виникненню воєнних конфліктів** віднесені [4].

Законом України "Про оборону України" та відповідними положеннями про Міністерство оборони України та про Генеральний штаб Збройних Сил України (затвердженими ***Указом Президента України від 6 квітня 2011 року № 406/2011***) визначені функції Міністерства оборони України, зокрема щодо інформаційних загроз [4].

Таким чином, в Україні створена достатня нормативно-правова база щодо визначення інформаційної безпеки та напрямів її забезпечення. Разом з тим, у Міністерстві оборони України та Збройних Силах України зазначеному питанню не надано системного підходу, навіть за наявності окремих складових, що можуть бути віднесеними до системи інформаційної безпеки.

Для виправлення зазначеної ситуації рішенням Міністра оборони України було створено Управління інформаційних технологій Міністерства оборони України як відокремлений підрозділ Міністерства оборони України, який призначений для реалізації єдиної стратегії Міністерства оборони у сфері інформатизації відповідно до державної політики у цій сфері; організації та координації заходів щодо впровадження сучасних інформаційних технологій у діяльність Міністерства оборони України; координації організаційних заходів щодо формування єдиного інформаційного простору та заходів з питань інформаційної безпеки у Міністерстві оборони.

Для нормативного забезпечення організації заходів з питань інформаційної безпеки підготовлено ряд документів:

1. **Перспективна Система забезпечення інформаційної безпеки Міністерства оборони України та Збройних Сил України** (далі – Система), метою функціонування якої є створення умов для реалізації національних інтересів держави у воєнній сфері, розвитку й функціонування Збройних Сил України, а також захисту інформаційних систем і збереження інформаційних можливостей об'єктів інформаційної діяльності структурних підрозділів та усієї інформаційної інфраструктури Міністерства оборони України, Збройних Сил України, Генерального штабу Збройних Сил України та інших органів військового управління в умовах впливу зовнішніх та внутрішніх інформаційних загроз.

2. **Концепція забезпечення інформаційної безпеки Міністерства оборони України та Збройних Сил України** (далі – Концепція), яка відображає офіційно прийняту в Міністерстві оборони України та Збройних Силах України систему поглядів на мету, завдання, принципи та способи забезпечення інформаційної безпеки та є основою для формування та реалізації інформаційної політики Міністерства оборони України стосовно забезпечення інформаційної безпеки, розробки і проведення відповідних заходів.

Напрямами подальших досліджень є наукове супроводження створення зазначеної Системи та виконання заходів Концепції.

ЛІТЕРАТУРА

1. Сліпченко В. Войны нового поколения. Дистанционные и бесконтактные. – ОЛМА-ПРЕСС Образование, 2004. – 400 с.

2. Бобров А. Информационная война: от листовки до Твиттера // Зарубежное военное обозрение – 2013. – 1. – С. 20 – 27.

3. Россия готовит киберкомандование в армии. Електронний ресурс. http://www.securitylab.ru/news/442185.php.

4. Офіційний сайт Верховної Ради України. Електронний ресурс. http://www.rada.gov.ua.

д.т.н. Романюк В.А. (ВІТІ ДУТ)

НАПРЯМКИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ТАКТИЧНИХ МОБІЛЬНИХ РАДІОМЕРЕЖ

В останнє десятиріччя розвинуті країни світу особливу увагу приділяють створенню перспективних тактичних радіомереж. До них пред'являються наступні основні вимоги: автоматичний режим функціонування, значну пропускну здатність при різних типах трафіку, висока мобільність всіх її елементів, здатність швидкого розгортання (в масштабі реального часу) та відновлення роботи в умовах вогневого враження тощо. Тому в епоху мережецентричних війн при створенні перспективних тактичних мереж ключову роль будуть грати мобільні радіомережі (рис. 1) або MANET (Mobile Ad-Hoc Networks) [1, 2]. Переваги мобільних радіомереж очевидні: відсутність етапу планування (можливість самоорганізації та легкість нарощування), швидке розгортання, висока живучість, робота в русі всіх елементів мережі тощо (табл. 1).

Однак не дивлячись на багаточисельні наукові дослідження по створенню тактичних MANET та приклади реального функціонування [3 – 8] вимоги інформаційного обміну [8] в умовах сучасного бою (за пропускною здатністю, затримки передачі тощо) визначають більш жорсткі вимоги до параметрів їх функціонування.

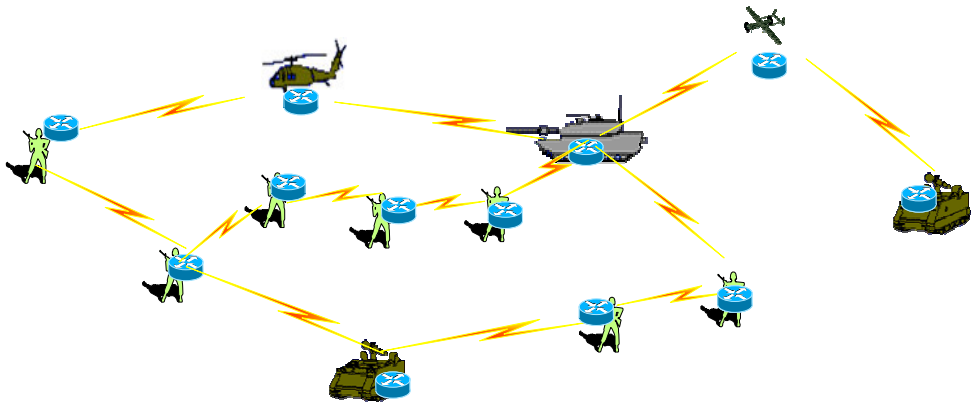


Рис.1. Представлення мережі MANET у вигляді мережі безпроводових маршрутизаторів

В багатьох країнах застосування технологій MANET у тактичних радіомережах пропонується вирішувати двома шляхами: модернізації існуючих вузькосмугових радіозасобів та/або створенням сучасних широкосмугових.

При першому [7], в існуючих мережах вузькосмугового тактичного радіозв'язку (таких засобів в арміях розвинутих країн десятки тисяч) пропонується реалізувати розроблені основні алгоритми (протоколи) функціонування MANET.

При цьому беруться за увагу наступні обмеження: кількість абонентів окремих тактичних мереж обмежена (наприклад, в низовій тактичній ланці значенням 16), мобільність абонентів відносно невисока, кількість переприйомів у маршрутах передачі – не більше трьох, превалює речовий трафік, інтенсивність трафіка даних незначна (кількість даних обмежується передачею наступної інформації: координати місця знаходження, напрямок переміщення, команди управління і підтвердження виконання тощо). Робиться висновок, що застосування технологій MANET значно покращить показники функціонування цих мереж.

Так, наприклад, в США за останні десять років втричі зросла кількість тактичних радіозасобів, їх загальна пропускна здатність збільшена на порядок (2001 рік в США – 365000 радіозасобів, 11 типів, 46 Мбіт/с; в 2011 році – 919000 радіозасобів, 20 типів, 9.6 Гбайт/с) [3, 4].

Таблиця 1

Переваги (недоліки)	**За рахунок чого може бути досягнуто (напрямки вдосконалення, усунення недоліків), наслідки**
(+) Можливість самоорганізації, швидке розгортання, нарощування, відновлення.	Застосування алгоритмів децентралізованого управління мережею (однак це приводить до необхідності збору значного обсягу службової інформації про стан мережі кожним вузлом мережі). Функції системи управління реалізуються кожнім вузлом мережі, що потребує створення відповідного математичного, алгоритмічного та програмного забезпечення.
(+) Висока живучість.	Відсутність фіксованої архітектури, можливість зв'язку в русі всіх елементів мережі, децентралізований спосіб управління мережею, здатність до самоорганізації. Кожний вузол – маршрутизатор, алгоритми управління у вузлах (на всіх рівнях еталонної моделі взаємодії відкритих систем) повинні буди адаптовані до умов функціонування мережі.
(+) Висока продуктивність мережі.	За рівнями еталонної моделі взаємодії відкритих систем. 1. На фізичному рівні: підвищення швидкості передачі радіоканалом (Мб/с) за рахунок зсуву діапазону частот (сотні Мгц, од. ГГц), можливо використання оптичного діапазону; динамічний розподіл спектра (когнітивне радіо); завдання розподіленого призначення частот; використання спрямованих антен; застосування технології MIMO (Multiple Input Multiple Output); застосування надширокосмугових імпульсних сигналів (IR-UWB) [2] тощо. 2. На канальному рівні – застосування ефективних протоколів канального рівня (наприклад, для забезпечення якості обслуговування QoS в радіоканалі). 3. На мережевому рівні – застосування ефективних протоколів мережевого рівня (наприклад, для забезпечення якості обслуговування QoS в маршрутах передачі, багато шляхової маршрутизації тощо) [2]. Необхідно введення додаткового підрівня управління топологією мережі. 4. На транспортному рівні – застосування ефективних протоколів транспортного рівня. 5. На прикладному рівні – координація та інтеграція рівнів еталонної моделі, застосування інтелектуальних методів управління мережею [2]. 6. Введення додаткових мережевих рівнів в архітектуру мобільної компоненти (мобільних базових станцій, безпілотних літальних апаратів, супутників) для підвищення продуктивності мережі, площі покриття).
(+) Передача різних видів трафіку.	Застосування нових протоколів канального та мережевого рівнів (протоколів підтримки заданої якості обслуговування).
(+) Маршрутизація.	Застосування ефективних методів маршрутизації [2].
(+) Висока безпека.	Застосування систем захисту, створення розподілених трастових центрів, систем виявлення вторгнень, використання HIP (Host Identify Protocol) тощо.
(–) Значний службовий трафік.	Зменшення службового трафіку може бути досягнуто за рахунок застосування відповідних алгоритмів (протоколів) на всіх рівнях еталонної моделі (координація роботи рівнів, інтелектуалізація системи управління мережею [2] тощо).
(–) Незначна відстань безпосереднього зв'язку.	Зв'язок в умовах прямої видимості – дальність зв'язку залежить від місцевості, частоти, потужності, типу антени тощо. Недолік усувається за рахунок маршрутизації (побудовою маршрутів з певною кількістю переприйомів) та введення в архітектуру мобільних базових станцій, безпілотних літальних апаратів маршрутизаторів.
(+) Висока Завадо захищеність.	Використання широкосмугових сигналів (метод частотних стрибків – FHSS, метод прямої послідовності – DSSS), в перспективі застосування гібридних схем розподілу ресурсів (FDMA/TDMA/CDMA).

При іншому шляху [5] створюються широкосмугові, багатодіапазонні, високошвидкісні, програмуємі, багатоканальні (декілька прийомопередавачів), когнітивні радіозасоби. Так в [7] визначено основні вимоги до них:

– висока пропускна здатність радіоканалу (> 200 Кб/с);

– багатодіапазонність (від 900 МГц до 6 Ггц) і багатофункціональність (можливість різних способів поділу радіоресурсу FDMA/TDMA/CDMA);

– здатність програмування всіх видів і режимів роботи;

– автоматизація процесів ведення зв'язку (режим „включив та працюй" – Plug-and-Play) та можливість самоорганізації мережі;

– інтелектуальність, децентралізованість й оптимізація функцій управління мережевими ресурсами (маршрутизація, навантаження, топологія, радіоресурс, безпека і т.д.);

– робота з різними видами трафіка (мова, дані, відео);

– наявність системи позиціювання, спрямованих антен, робота в русі;

– модульність виконання, відкрита архітектура, низьке енергоспоживання.

В той же час існують значні *труднощі створення мобільних радіомереж* – необхідність рішення великої кількості наукових проблем децентралізованого управління мережею (маршрутизація, розподіл радіоресурсів, управління потужністю, управління топологією, безпека передачі інформації, забезпечення заданої якості передачі інформації тощо) при обмеженнях ресурсів радіотерміналів (за ємністю пам'яті, продуктивністю процесора, енергоємністю батареї). Пропозиції щодо частини їх рішення можуть бути знайдені як в багатьох роботах зарубіжних авторів так і в монографії [2].

Аналіз останніх публікацій дозволив визначити орієнтовний виграш (в умовних одиницях) у продуктивності бездротових мереж (табл. 2) при застосуванні різних технологій або способів рішення.

Таблиця 2

Проблема	**Технології (способи рішення)**	**Виграш**
На канальному рівні		
Збільшення пропускної здатності радіоканалів	Зсув діапазону частот (сотні Мгц, одиниці ГГц), використання оптичного діапазону. Оптимізація використання радіоспектра. Спрямовані антени.	10 2…20 2…30
На мережевому рівні.		
Маршрутизація	Нові гібридні протоколи маршрутизації.	2…5
Додаткові елементи архітектури	Мобільні базові станції, безпілотні літальні апарати.	2…4
Управління ресурсами мережі	Інтелектуалізація процесу управління мережами.	3…5

Подальше використання мобільних радіомереж у військовій та цивільній сферах передбачає функціонування MANET великої розмірності мережі (мережі з 10000 або більше мобільних вузлів, діаметр і, отже, довжина маршруту може становити 50–100 ретрансляцій), з продуктивністю порівнянної з провідними мережами: пропускна спроможність 1 Гбіт в секунду, затримка при передачі від відправника до одержувача менше 10 мс, і надійність доставки на рівні провідних мереж.

Такі вимоги притаманні до майбутніх військових мереж MANET: мереж сенсорів, бойових роботів, безпілотних літальних апаратів, військовослужбовців тощо [5]. Мета – створення нових мереж MANET великої розмірності з дуже малими затримками і дуже

високою пропускною здатністю. Реалізація даної ідеї вимагає вирішення ряду складних наукових задач.

Для отримання визначених показників в роботах [5 – 12] пропонуються принципово нові підходи відносно функціонування перспективних мереж.

1. *Ретрансляція пакетів „на льоту”* [9].

Існуючий механізм передачі пакета прийняв–обробив–передав повторюються на кожному вузлі при кожній ретрансляції. Кожен пакет на всіх вузлах у маршруті проходить наступні процедури обробки (рис. 2): постановка в чергу, обробка на трьох рівнях OSI, додавання заголовків тощо, повторно постановка в чергу на мережевому і канальних рівнях, вставка нових даних у заголовки, організація доступу до каналу, з обов’язковим звітуванням (можлива і повторна передача). Це призводить до великих затримок при передачі даних по маршрут від адресата до одержувача.

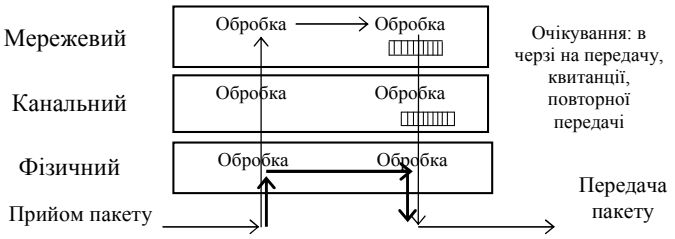


Рис. 2. Запропонована схема обробки

Ідея – зменшити час, що витрачається на обробку пакетів за рахунок ретрансляції пакетів „на льоту”. Для цього на фізичному рівні обробляється тільки заголовок пакета без втручання канального або мережевого рівнів (за умови наявності вже побудованого маршруту). Побудова маршруту схожа з маршрутизацією за мітками технології MPLS. Наприклад, будується та позначається міткою маршрут одним з методів зондової маршрутизації. І потім кожен пакет ретранслюється тільки за позначеним маршрутом. На фізичному рівні аналізується адреса, мітка маршруту (стоять перші в заголовку). Якщо не мені, то пакет ретранслюються за маршрутом. Рішення полягає в поєднанні функцій прийому і передачі так, що перші частини пакета передаються в той час як інші частини приймаються. Переваги очевидні, але цей підхід вимагає заздалегідь резервування ресурсу каналів у маршрутах передачі.

2. *Управління топології мережі або її зоною* [10] за рахунок введення додаткового підрівня мережевого рівня OSI.

Топологія мережі визначає потенційну можливість мережі з передачі потоків даних. За рахунок управління потужністю передачі та / або діаграми спрямованості антени (за її наявності) можна отримати різні топології з різною потенціальною пропускною здатністю і довжинами маршрутів передачі. Даний підрівень повинен відпрацьовувати перед підрівнем маршрутизації.

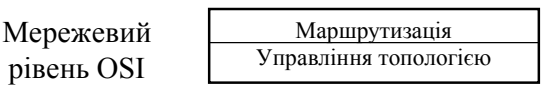


Рис. 3. Розбиття мережевого рівня OSI на підрівні

Пропонується ввести додатковий підрівень мережевого рівня моделі OSI для управління топологією мережі за рахунок зміни потужності передачі та (або) діаграми спрямованості антени. Збільшення (зменшення) потужності передачі збільшує (зменшує) кількість „сусідніх” вузлів та зменшує (додає) кількість ретрансляцій за маршрутами передачі, однак розширює (зменшує) зону взаємних завад (проблема „прихованого термінала”), тим самим зменшує (підвищує) пропускну здатність радіоканалів зони та

потребує більших (менших) витрат енергії батареї вузлів. Існує певний оптимум параметрів мережі при управлінні її топологією. Методи досягнення наведені в [10].

3. *Розбиття маршруту передачі на сегменті при реалізації транспортного рівня* OSI [9].

Даний підхід дозволяє зменшити кількість перерваних сесій транспортного рівня за рахунок зменшення кількості перебудов маршрутів передачі внаслідок змін топології мережі.

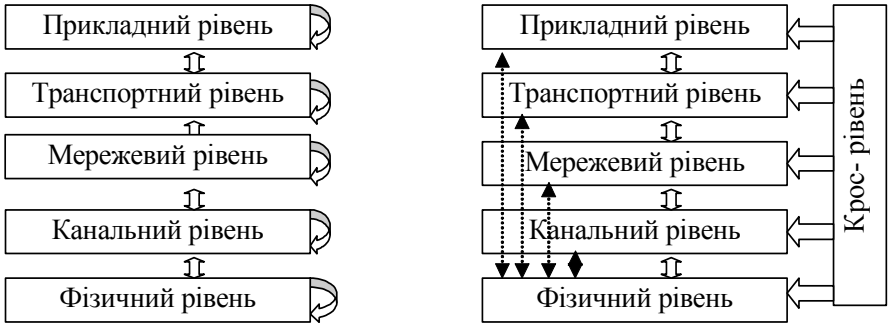
4. *Паралельна багаторазова ретрансляція пакетів з метою підвищення надійності передачі* [9].

На мережевому рівні паралельна передача пакетів може бути здійснена за рахунок багатошляхової маршрутизації, яка передбачає побудову декількох незалежних маршрутів передачі та балансування навантаження між ними [12]. Однак це приводить до значного службового трафіка. Тому ефективним є паралельна передача на фізичному рівні (*cooperative diversity*) – це майже одночасна передача однієї інформації декілька вузлами, яка когерентно складається в приймальну. Ще один спосіб реалізації – використання антенної решітки, де вузли виступають в якості елементів. Використання паралельної передачі на фізичному рівні значно покращує SNR в приймальну.

5. *Координація и інтелектуалізація рівнів OSI* (рис. 3) [11].

Існуючі підходи до проектування телекомунікаційних мереж зв'язку припускають незалежність функцій управління за рівнями OSI (рис. 4). Так стікання протоколів кожного рівня працює незалежно (рис. 4а).

Однак даний підхід не враховує особливості MANET і не дозволяє забезпечити оптимізацію показників ефективності на кожному рівні OSI (або в цілому) при різних умовах функціонування мережі та вимогах конкретного типу трафіка (наприклад, відео або мови) [9].



а) *б*)

Рис. 4. Архітектура OSI (а) та координаційна (cross-level) архітектура (б)

При цьому необхідно відмитими, що досягання глобальної оптимізації при оперативному управлінні для всієї мережі неможливо внаслідок неможливості побудови відповідної моделі її функціонування, а також (що саме важливе) неможливістю зібрати в реальному часі інформацію про її стан. Тому доцільно говорити про користувальницьку оптимізацію (задоволення користувальницьких вимог) між парами відправник-адресат при мінімізації витрат мережевих ресурсів (наприклад, мінімізація службового трафіка) [9].

6. *Узгодження цілей управління з розподілу ресурсу мережі або її зони* [11].

Збільшення розмірності мережі призводить до значного зростання службового трафіку (обсяг службового трафіку зростає як мінімум квадратично розмірності мережі). Тому можливим рішенням зменшення службового трафіку є створення розумної (інтелектуальної) мережі. У MANET кожен вузол децентралізовано реалізує функції управління.

Для прийняття рішень з передачі вхідної інформації кожен вузол повинен зібрати інформацію про мережу (або її зону) і прийняти рішення по передачі всіма рівнями OSI і функцій управління: побудувати (обрати) маршрут або маршрути з безлічі наявних, визначити або вибрати алгоритм доступу до каналу, вибрати оптимальними параметри

передачі на фізичному рівні: швидкість передачі, вид модуляції, довжину пакета). При цьому йому необхідно враховувати тип трафіку, завантаження, мобільність свою, зони і всієї мережі.

В умовах децентралізованого управління кожен вузол буде реалізовувати дві групи цілей: користувальницьку оптимізацію і мережеву (зонову). Користувальницька оптимізація полягає в побудові (підтримці) маршруту передачі заданої якості між відправником і адресатом відповідно до типу трафіку при прагненні мінімізувати службовий трафік (витрату ресурсів) мережі, тобто досягти мережевої оптимізації. Для цієї мети пропонується кожному вузлу координувати і погоджувати свої цілі управління з вузлами, які він задіє при прийнятті даного рішення. Для цього пропонується використовувати технологію інтелектуальних агентів.

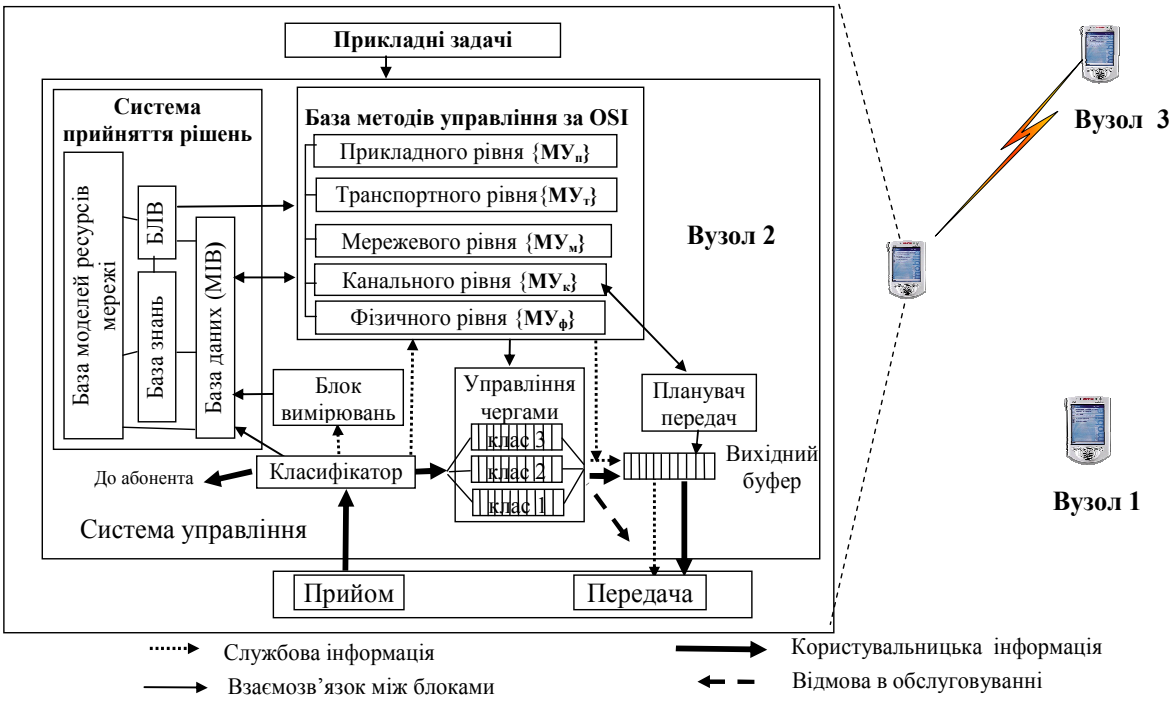


Рис. 5. Архітектура інтелектуальної системи управління вузла мережі

Прикладний рівень (міжрівнева інтеграція). Пропонується нова парадигма побудови системи управління – ввести базу методів управління та інтелектуальну надбудову над нею (систему прийняття рішень з управління), що координує функціонування множини методів управління за рівнями OSI з метою оптимізації показників функціонування мережі (рис. 5). База методів управління $\{МУ\}=\{МУ_ф, МУ_к, МУ_м, МУ_т, МУ_п\}$ містить множину методів управління для кожного рівня OSI.

Система прийняття рішень складається з бази знань (містить знання про об'єкт управління, знання про цілі функціонування та управління, знання про способи досягнення цілей), бази дані управління, блока логічного висновку (БЛВ) і моделей ресурсів мережі [11, 13].

Відмінність запропонованого підходу від існуючих – координація та інтеграція між рівнями OSI не тільки за різними параметрами, а за цілями управління, які визначають певний метод управління на кожному рівні моделі OSI.

Завдання ухвалення рішення по управлінню мережею (вибір конкретних методів управління за кожним рівнем OSI) зведена до завдання ієрархічного цільового динамічного оцінювання альтернатив при нечітких вихідних даних.

Висновки

1. Система зв'язку тактичної ланки розвивається в напрямку застосування відкритої архітектури, створення багатоканальних, багатосмугових, програмуємих, високошвидкісних, інтелектуальних радіозасобів, впровадження новітніх телекомунікаційних технологій MANET.

2. Застосування MANET дозволить створити транспортну основу мережецентричних способів ведення бойових дій та призведе до появи принципово нових форм (способів) ведення бойових дій.

3. Зростання розмірності мережі, багатоманіття складу вузлів та їх параметрів, наявність нових сервісів вимагають нових апаратних, архітектурних і наукових рішень для підвищення ефективності даного класу мереж. Запропоновані основні підходи щодо підвищення ефективності функціонування мереж класу MANET.

ЛІТЕРАТУРА

1. Романюк В.А. Еволюція тактичних радіомереж: Тези доповідей та виступів учасників VI науково-практичного семінару [„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"] / Романюк В.А. – К.: ВІТІ НТУУ „КПІ", 2011. – С. 45 – 52.

2. Самоорганизующиеся радиосети со сверхширокополосными сигналами / [С.Г. Бунин, А.П. Войтер, М.Е. Ильченко, В.А. Романюк]. – К.: НПП „Издательство „Наукова думка" НАН Украины". – 444 с.: ил.

3. Tactical Radios// Compendium by Armada. – 2013.

4. Radio // Compendium by Armada. – October 2013.

5. Redi J., Ramanathan R. The DARPA WNaN Network Architecture // In IEEE Proceeding MILCOM, 2011.

6. Li L., Lamont L. Support real-time interactive session applications over a tactical mobile ad-hoc networks // In IEEE Proceeding MILCOM, 2005.

7. Wang H., Crilly B., Zhao W., Autry C., Swank S. Implementation Mobile Ad-hoc Networks over legacy tactical radio links// In IEEE Proceeding MILCOM, 2007.

8. Suman B., Sharma S., Kumar M. Investigation commucation architecture for tactical radio networks design // IJREAS Volume 2, Issue 2, 2012.

9. Ramanathan R. A Radically New Architecture for Next Generation Mobile Ad Hoc Networks // In IEEE Proceeding MOBICOM, 2005.

10. Романюк В.А. Управление топологией мобильной радиосети / Миночкин А.И., Романюк В.А. // Зв'язок. – 2003. – № 2. – С. 28 – 33.

11. Романюк В.А. Архітектура системи оперативного управління тактичними радіомережами /Романюк В.А.// Збірник наукових праць № 3. – К.: ВІТІ НТУУ "КПІ". – 2009. – С. 70 – 76.

12. Романюк В.А. Многопутевая маршрутизация в мобильных радиосетях / Миночкин А.И., Романюк В.А. // Зв'язок. – 2004. – № 6.

13. Романюк В.А. Цільові функції оперативного управління тактичними радіомережами / Романюк В.А. // Збірник наукових праць ВІТІ НТУУ "КПІ". – 2012. – № 1. – С. 109 – 117.

к.т.н. Самойлов І.В. (ВІТІ ДУТ)
к.т.н. Кокотов О.В. (ВІТІ ДУТ)

ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНИХ ВІЙН. КОНЦЕПЦІЯ БОЙДА

Сьогодні багато говориться про „інформаційну війну". Однак лише деякі можуть точно сказати, що це таке, коли ж все-таки з'явилося саме словосполучення „інформаційна війна" і коли вперше стали розглядати можливість використання інформації як зброї. У зв'язку із цим виникає питання: що таке інформаційна війна (ІВ) і що є теоретичною основою інформаційного протиборства. Щоб відповісти на це питання необхідно розглянути теорії ведення бойових дій, які панували в армії США в останні десятиліття.

Досвід ведення армією США війн в Індокитаї та радянською армією в Афганістані показав військовим аналітикам справедливість висловлень великого китайського полководця Сунь-Цзи, які наведені у його праці „Мистецтво війни":

„Одержати сто перемог у ста боях – це не вершина переваги. Підкорити армію ворога не борючись – от справжня вершина переваги. Той, хто досяг вершин у військовій справі, підкоряє чужі армії, не вступаючи в битву, захоплює чужі міста, не осаджуючи їх, і руйнує чужі держави без тривалого бою".

„Війна любить перемогу й не любить тривалості. Я чув про успіх швидких військових походів, і не чув про успіх затяжних. Жодна держава не отримала вигоди з тривалої війни".

Виходячи із цього, американськими військовими експертами був запропонований ряд концепцій ведення бойових дій. Найбільш відома з них це концепція або теорія Бойда [1, 2].

У своїх теоретичних побудовах Бойд підрозділяв війну на три елементи:

– моральну війну (moral warfare): руйнування волі противника до досягнення перемоги шляхом його відділення від союзників (або потенційних союзників) і внутрішнього роздроблення, підриваючи загальну віру й загальні погляди;

– ментальну війну (mental warfare): деформація і перекручування сприйняття противником реальності на основі дезінформації і створення неправильної уяви про ситуацію;

– фізичну війну (physical warfare): руйнування фізичних ресурсів противника (озброєння, живої сили, інфраструктури).

Відповідно до ідей Бойда та його послідовників будь-яка діяльність у військовій сфері з певним ступенем наближення може бути представлена у вигляді кібернетичної моделі OODA (Observe – спостерігай, Orient – орієнтуйся, Decide – вирішуй, Act – дій). Зазначена модель припускає багаторазове повторення петлі дій, складеної із чотирьох послідовних взаємодіючих процесів: спостереження, орієнтація, рішення, дія. Фактично має місце розвиток ситуації по спіралі і на кожному етапі цієї спіралі здійснюється взаємодія із зовнішнім середовищем і вплив на противника. Цю модель відносять до розряду кібернетичних, тому що в ній реалізується принцип „зворотнього зв'язку", відповідно до якого частина виходу з системи знову подається на її вхід, щоб уточнити, а якщо буде потрібно, і скорегувати розвиток системи на наступних етапах. У ряді офіційних доктринальних документів МО США, зокрема в спільній публікації Joint Publication 3 – 13.1 [3], петля OODA розглядається в якості єдиної типової моделі циклу прийняття рішень для систем командування і керування (C2 systems), як своїх військ, так і військ противника.

Відмітна риса циклу OODA від інших циклічних моделей полягає в тому, що в будь-якій ситуації завжди передбачається наявність противника, з якими ведеться збройна боротьба. Противник також діє та приймає рішення в рамках своєї аналогічної петлі.

На основі аналізу робіт Бойда і його послідовників виділені наступні постулати теорії OODA [4, 5]:

1. Військова діяльність (бойові дії) протиборчих сторін здійснюється в однакових кібернетичних циклах OODA.

2. Зміст основних елементів циклу OODA наступний:

спостереження – збір інформації від внутрішніх і зовнішніх джерел;

орієнтація – формування множини можливих планів (варіантів) і оцінка кожного з них за сукупністю критеріїв;

рішення – вибір найкращого плану дій для практичної реалізації;

дія – практична реалізація вибраного плану дій.

3. Цикл OODA є моделлю військової діяльності окремих осіб і організацій для війн і конфліктів будь-якого рівня (тактичного, оперативного й стратегічного).

4. Напрямки досягнення перемоги (одержання конкурентних переваг):

скорочення часу виконання циклу OODA;

поліпшення якості прийнятих у циклі рішень.

5. Збільшення швидкості всіх чотирьох елементів циклу OODA – головний шлях досягнення перемоги.

Із чотирьох етапів OODA-циклу три безпосередньо пов’язані з обробкою інформації й з комп’ютерними технологіями. Четвертий етап (дія) носить у цілому „кінематичний” характер і пов’язаний з переміщенням у просторі, захистом і поразкою противника на основі вогневої моці.

Щоб зберегти часові рамки OODA-циклу дій своїх сил і забезпечити більш високий, чим у противника, темп бою, необхідно прискорити всі чотири етапи циклу, які реалізуються військами (силами). Протягом двадцятого століття всі зусилля військових, учених і інженерів були спрямовані на вдосконалювання озброєння і технологій у частині кінематичної частини петлі OODA. Результатом цих зусиль було збільшення мобільності, точності і вогневої моці озброєння. Однак на сучасному етапі наступила технологічна межа кінематичної частини OODA-циклу – могутніші види зброї наносять не прийнятний супутній збиток, а більш швидкісні і більше захищені платформи озброєння та засоби доставки вражаючого фактора до цілі припускають непомірні на сучасному етапі матеріальні витрати. У зв’язку з цим з'явилася необхідність в удосконалюванні інших етапів OODA-циклу.

Так, як перші три кроки OODA-циклу пов’язані безпосередньо із процесами збору інформації, її розподілу, осмислення, аналізу і прийняття рішень на основі отриманої інформації, то чим швидше здійснюються збір, розподіл, аналіз, сприйняття інформації, тим швидше приймається рішення. Саме швидкість і правильність прийняття рішень найбільш важливі в сучасних реальних бойових діях. Це послужило поштовхом до розробки концепції мережно-центричної військової діяльності (network-centric warfare) або як дещо неточно його переводять мережно-центричної війни.

Відповідно до принципів мережно-центричної військової діяльності (МЦВД) комп’ютерні системи зв’язують елементи бойової техніки в мережу. Це забезпечує збільшення темпу дій OODA-циклу за рахунок скорочення тривалості етапів спостереження та орієнтації. Ефективність створеної на основі встановлення зв’язків „системи систем” (system of systems) визначається також фазами прийняття рішень і дій.

У найбільш загальному випадку створення мережних структур спрямовано на скорочення часу циклу бою й підвищення темпу бойових (військових) дій на всіх рівнях військової організації. Таким чином, організація мережі є механізмом прискорення етапів спостереження та орієнтації, а також підвищення ефективності для етапу прийняття рішень.

У військово-практичному змісті, МЦВД дозволяє перейти від війни на виснаження до більше швидкоплинної і більш ефективної форми, для якої характерні дві основних характеристики: швидкість управління й принцип самосинхронізації.

Швидкість управління, у поданні американських експертів, має на увазі три аспекти: 1. Війська досягають інформаційної переваги, під якою розуміється не просто надходження інформації в більшій кількості, а більш високий ступінь її усвідомлення і більш глибоке розуміння ситуації на поле бою. У технологічному плані все це припускає впровадження нових систем управління, зв’язку, спостереження, розвідки, контролю, комп’ютерного

моделювання. 2. Війська завдяки своїм інформаційним перевагам запроваджують у життя принцип масування результатів, а не масування сил. 3. В результаті таких дій противник втрачає можливості спрямовувати свої дії і впадає в стан шоку.

Застосування системи самосинхронізації дозволяє досягти переваги над противником у швидкості й раптовості дій. Зникають тактичні та оперативні паузи, якими противник міг би скористатися, всі процеси управління та самих бойових дій стають більш динамічними, активними і результативними. Воєнні дії здобувають не форму послідовних боїв і операцій з відповідними проміжками (паузами) між ними, а форму безперервних високошвидкісних дій (операцій, акцій) з рішучими цілями. Завдяки створенню єдиного інформаційно-комунікаційного простору досягається інформаційна перевага (домінування) на поле бою, що дозволяє в багато разів підвищити ефективність та оперативність реалізації бойового потенціал угруповань військ (сил) у ході воєнних дій. Завдяки інформаційній перевазі з'являється можливість упереджувати противника на всіх етапах підготовки та ведення бойових дій. Противна сторона втрачає можливості почати хоч які-небудь кроки у відповідь і, в остаточному підсумку, як вважають західні фахівці, впадає в стан повного шоку.

Інформаційна перевага визначається, як здатність збирати, обробляти і розподіляти безперервний потік інформації про ситуацію, перешкоджаючи супротивникові робити те ж саме. Відповідно до концепції Бойда вона відповідає здатності призначити і підтримувати такий темп проведення операції, що перевершує будь-який можливий темп противника, дозволяючи домінувати протягом усього часу проведення операції, залишаючись непередбаченим, і діяти, випереджаючи противника в його відповідних акціях. Інформаційна перевага завойовується в процесі інформаційного протиборства (ІП).

В основу концепції ІП закладена взаємна залежність (вразливість) своєї країни і її потенційних противників від інформації та інформаційних систем. У зв'язку з цим під час реалізації концепції ІП розглядаються два аспекти діяльності: вплив на інформаційну інфраструктуру противника та захист свого власного інформаційного середовища. Відповідно всі інформаційні операції підрозділяються на наступальні інформаційні операції (НІО) та оборонні (ОІО).

З точки зору теорії Бойда ІП дозволяє вирішити два завдання:

– знизити швидкість реалізації циклу OODA і зменшити якість прийнятих рішень противника за рахунок проведення НІО;

– не дати противнику знизити швидкість реалізації власного циклу OODA і зменшити якість прийняття власних рішень за рахунок проведення ОІО.

Вирішення першого завдання є бажаним під час ведення ІП, в той час як виконання другого завдання є обов'язковим. Це пов'язано з тим, що невдале проведення ОІО призведе до „паралічу" систему управління і не можливості адекватно ситуації впливати на противника. Тому інформаційна безпека є важливою складовою ІП.

Таким чином, ІП складається з дій, що вживаються з метою досягнення інформаційної переваги в забезпеченні національної військової стратегії шляхом впливу на інформацію та інформаційні системи противника з одночасним зміцненням і захистом власної інформації, а також власних інформаційних систем і інфраструктури.

ЛІТЕРАТУРА

1. Boyd J.R. The Essence of Winning and Losing. Unpublished lecture notes. 1996.

2. Richards C.W. A Swift, Elusive Sword. What if Sun Tzu and Join Boyd did a national defense review? Center for Defense Information, February 2003.

3. Joint Publication 3-13.1 (Joint Doctrine for Command and Control Warfare (C2W)).

4. Guitouni A., Wheaton K. and Wood D., An Essay to Characterize Models of the Military Decision – Making Processes, 11th ICCRTS, 26-28 Sep 06, Cambridge UK.

5. Dettmen H.W., Strategic Navigation: The Constraint Management Model. Proceedings of the APICS International Conference, Las Vegas, Nevada (USA), October 6-9, 2003.

к.т.н. Сова О.Я. (ВІТІ ДУТ)
к.т.н. Жук П.В. (ВІТІ ДУТ)
к.т.н. Міночкін Д.А. (ІТС НТУУ „КПІ”)

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ АГЕНТІВ ДЛЯ ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ ВУЗЛАМИ РАДІОМЕРЕЖ КЛАСУ MANET

Ефективне управління бойовими підрозділами в ході сучасних високоманеврених бойових дій вимагає повної поінформованості командирів та інших посадових осіб щодо ситуації, яка склалася на полі бою в той чи інший момент часу. Збір та отримання такої інформації, особливо в тактичній ланці управління, можливий лише шляхом використання сучасних мереж радіозв’язку, які надають користувачам доступ до необхідної інформації та сервісів за принципом „в будь-якому місці, в будь-який час”.

Прикладом таких мереж є радіомережі класу *Ad-Hoc* та *Mobile Ad-Hoc Networks* (так-звані мобільні радіомережі, МР) [1], які передбачають відсутність базових станцій та фіксованих маршрутів передачі інформації, а також надають можливість мобільним абонентам (вузлам) самоорганізовуватися в радіомережу без завчасно розгорнутої мережевої інфраструктури.

Однак, здатність МР до самоорганізації вимагає наявності системи управління (СУ) у складі кожного мобільного вузла, здатної приймати рішення в умовах невизначеності, викликаних непередбачуваною природою середовища в якому функціонують МР, а також різними вимогами до передачі того чи іншого типу трафіка (дані, мова, відео).

Прийняттю рішень СУ щодо управління вузловими та мережевими ресурсами передує етап оцінки різнорідних параметрів функціонування вузла та мережі. Основними з них є: швидкість та напрям переміщення вузла, ємність вузлової батареї, потужність передавача, ширина смуги пропускання інформаційного напрямку та час затримки передачі пакетів на ньому, тощо. Зважаючи на те, що природа поведінки вузлів МР непередбачувана і отримати чіткі значення зазначених параметрів в режимі реального часу неможливо, для прийняття управлінського рішення доцільно отримати хоча б наближені значення цих величин („мале”, „середнє”, „велике”, тощо). З метою оперування зазначеними величинами, в [1] запропоновано використання технологій обробки даних та отримання знань, що дозволить інтелектуалізувати процес управління вузлами МР.

Зважаючи на особливості функціонування вузлових СУ, які, з одного боку передбачають відносну автономність при вирішенні завдань з управління вузловими ресурсами, а з іншого боку – повинні враховувати стан вузлів-сусідів при прийнятті управлінських рішень, в [2] запропоновано використовувати технологію інтелектуальних агентів для побудови структурних елементів СУ вузлами радіомереж класу MANET.

Перш ніж розглядати можливість використання інтелектуальних агентів для побудови СУ вузлами МР необхідно дати визначення того, що собою являє інтелектуальна СУ, а також сам процес інтелектуалізації управління.

У загальному випадку *інтелектуальною системою управління* (ІСУ) називають кібернетичну систему, призначену для вирішення задач, точний алгоритмізований метод вирішення яких апріорі є невідомим [3]. При цьому під вирішенням задач розуміється будь-яка діяльність, пов’язана зі збором інформації про стан об’єкта управління та середовища, в якому він функціонує, розробкою планів і виконанням дій, необхідних для досягнення визначеної мети [4]. Головна відмінність ІСУ від інших кібернетичних систем, полягає в наявності характерних їм ознак:

– наявність у ІСУ власних внутрішніх моделей об’єкту (об’єктів) управління та навколишнього середовища, що забезпечує здатність системи самостійно оцінювати вхідну інформацію;

– здатність ІСУ поповнювати наявні знання, засвоювати їх та навчатися на основі отриманої вхідної інформації про стан об'єктів управління та навколишнього середовища;

– здатність ІСУ виділяти нові якісні характеристики об'єктів управління та навколишнього середовища;

– здатність до дедуктивного виведення та генерації нового рішення, що у явному і готовому вигляді не міститься в самій системі;

– здатність до прийняття рішень в умовах невизначеності (нечіткої, неточної, недостатньої вхідної інформації);

– еволюційність і адаптивність ІСУ – набуття знань системою здійснюється за допомогою навчання, заснованого на адаптації (пристосуванні) її структури і параметрів у процесі еволюційного розвитку до умов зовнішнього середовища, що змінюються.

Тривалий час вважалося, що ІСУ ефективні лише для вирішення так званих неформалізованих і погано формалізованих завдань, пов'язаних з необхідністю включення в алгоритм їхнього вирішення даних про навчання на реальному експериментальному матеріалі (наприклад, завдання розпізнавання образів). Однак останнім часом ІСУ все ширше використовуються при вирішенні завдань у системах зв'язку й телекомунікацій: управління комутацією, маршрутизація, управління трафіком, розподіл каналів у рухомих системах радіозв'язку й т.д. [5, 6].

Разом з тим, доцільно чітко описати процес інтелектуалізації управління, з огляду на зазначені вище особливості функціонування СУ вузлом МР. З урахуванням ознак, характерних ІСУ, *інтелектуалізація* системи управління вузлом МР – це процес використання технологій обробки знань для формування правил доцільної поведінки вузла МР в залежності від умов які склалися в радіомережі.

Узагальнюючи наведені вище визначення, функціями ІСУ вузлом МР є:

– збір і обробка даних про ситуацію, що склалася в МР за допомогою спеціалізованих алгоритмів обробки знань, а також програмних і апаратних засобів для їхнього перетворення (поповнення бази знань вузла або всієї МР);

– планування ефективної і доцільної поведінки мобільного вузла, що вимагає створення відповідних методів формування цілей і вирішення задач управління вузловими та мережевими ресурсами;

– розпізнавання змін обстановки в МР і формування відповідних реакцій на них з боку мобільних радіовузлів на основі правил, що містяться в базі знань ІСУ, які були отримані шляхом навчання.

В [7] представлено узагальнену модель інтелектуальної системи управління вузлом МР, яка повинна бути реалізована всіма елементами МР, зокрема – центром управління мережею, базовими станціями і мобільними користувачами (вузлами) [5, 8]. Запропонована модель ІСУ вузлом МР має досить складну структуру і включає до свого складу низку функціонально-підлеглих підсистем, реалізація яких можлива з використанням так званих програм-агентів, наділених інтелектом щодо обробки службової інформації, необхідної для прийняття рішень з управління вузлом МР.

З одного боку, агент – це програма, яка знаходиться в середовищі, від якого отримуються дані про події, що відбуваються, інтерпретує їх і виконує команди, що впливають на це середовище. З іншого боку, поняття агента стало одним з розширень поняття програми. Воно з'явилося у зв'язку з використанням програм не тільки для вирішення численних завдань, пов'язаних зі збором, обробкою та структуризацією інформації, але і в системах реального часу (*real-time systems*) для швидкого прийняття рішень різними системами управління. Агент може містити програмні і апаратні компоненти.

На рис. 1 зображена класифікація агентів за різними ознаками. Розглянемо наведену класифікацію детальніше.

Головна відмінність агентів, що працюють у *режимі реального часу*, полягає в тому, що вони функціонують (запускаються, призупиняються, поновлюються, завершуються, запускаються знову) у відповідності із зовнішніми фізичними збудниками (змінами у навколишньому чи програмному середовищі). Програма-агент, що працює в реальному часі, взаємодіє з оточенням (отримує і передає інформацію) за допомогою інтерфейсів, тобто вона впливає на навколишнє середовище і відчуває, в свою чергу, вплив навколишнього середовища. Звідси випливає інша відмінність програм-агентів реального часу, яка полягає у потенційній можливості оцінювати результати свого функціонування (зворотній зв'язок) і міняти свої дії в майбутньому з урахуванням досвіду, отриманого в минулому. Саме ці відмінності від звичайної програми призвели до виникнення поняття інтелектуального агента (ІА). У традиційних системах програми можуть правильно функціонувати тільки в умовах повністю передбачуваного оточення, а не в умовах невизначеності. Для того щоб виконати за допомогою програми деякі обчислення користувач повинен задати всю вхідну інформацію (аргументи). Якщо програма бере вихідні дані з бази даних, то повинна бути повна впевненість у тому, що ці дані є в базі. *Реактивні* ж агенти не мають ніякого уявлення про стан зовнішнього середовища, ні механізму вирішення завдань, ні достатньої кількості власних ресурсів.

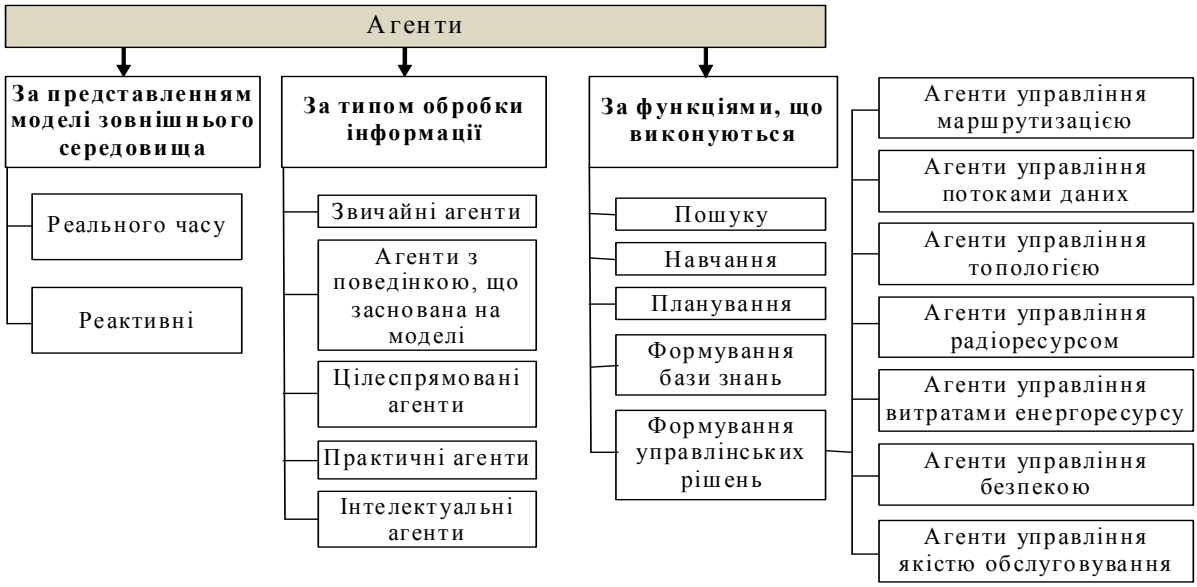


Рис. 1. Класифікація агентів

Агенти *пошуку* займаються пошуком інформації та поповнюють нею наявну базу даних, з якої потім агенти *формування бази знань* формують знання та правила, що застосовуються при вирішенні поставлених завдань. Агент *планування* відповідає за організацію діяльності ІСУ при вирішенні різних задач. Він повинен балансувати діяльність ІСУ між метою її функціонування в умовах, що змінюються, і безпосереднім виконанням поставлених на вузол МР завдань з урахуванням доступних вузлових та мережевих ресурсів.

Агенти *навчання* здійснюють процес інтелектуалізації системи управління, тобто забезпечують здатність самостійно приймати рішення.

Агенти *формування управлінських рішень* відповідають за реалізацію множини методів управління вузловими та мережевими ресурсами, які функціонують на різних рівнях моделі OSI.

Звичайні агенти діють тільки на основі поточних знань (рис. 2). Їх агентська функція заснована на схемі умова-дія (*IF* (умова) *THEN* (дія)). Така функція може бути успішною, тільки якщо навколишнє середовище повністю піддається спостереженню. Деякі агенти також можуть мати інформацію про власний поточний стан, що дозволяє їм не звертати уваги на умови, передумови яких вже виконані.

Агенти з поведінкою, що засновані на моделі, можуть оперувати з середовищем, яке лише частково піддається спостереженню. Усередині агента зберігається уявлення про ту частину, що знаходиться поза межами огляду. Щоб мати таке уявлення, агенту необхідно знати, як виглядає навколишній світ, як він влаштований.

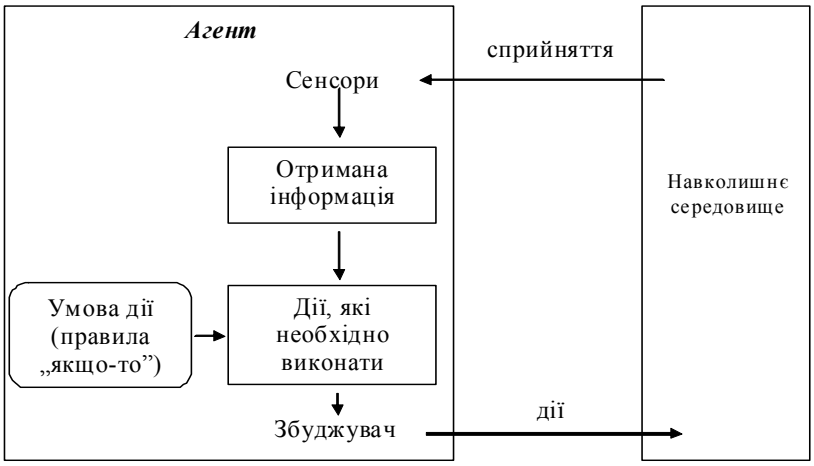


Рис. 2. Структурна схема звичайного агента

Цілеспрямовані агенти схожі з попереднім типом, проте вони, крім іншого, зберігають інформацію про ті ситуації, які для них прийнятні. Це дає агенту можливість вибрати серед багатьох шляхів той, що приведе до потрібної мети.

Цілеспрямовані агенти розрізняють тільки стан, коли мета досягнута, і коли не досягнута. *Практичні агенти*, крім цього, здатні розрізняти, наскільки бажаний для них поточний стан. Така оцінка може бути отримана за допомогою „функції корисності", яка проектує безліч станів на безліч заходів корисності станів.

ІА мають здатність до навчання і пристосування до змін навколишнього середовища. На відміну від звичайного агента (рис. 2), який передбачає реакцію на зовнішній вплив, шляхом перебору правил, наявних в базі знань, яка самостійно не поповнюється, ІА в своєму складі має блоки, які дозволяють їм виробляти нові знання в процесі функціонування (рис. 3).

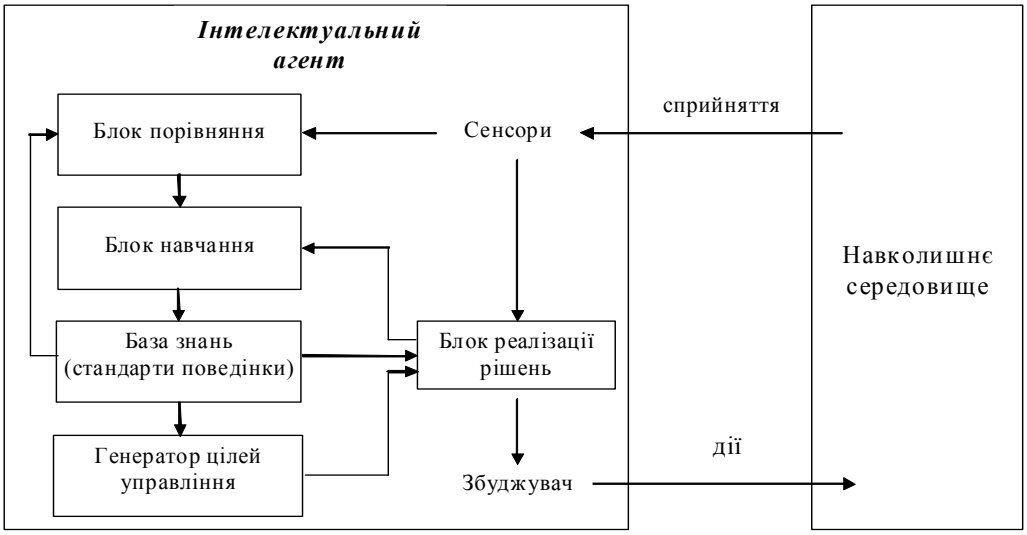


Рис. 3. Структурна схема інтелектуального агента

Сенсори агента відповідають за отримання повідомлень від середовища та інших агентів і деяким чином перетворюють їх у внутрішнє представлення агента (які, в разі

автономності агента, нічим не відрізняються від середовища за способом взаємодії). У *блоці порівняння* агента здійснюється порівняння наявної інформації, що міститься в базі знань, з інформацією, яка надходить від зовнішнього середовища та інших агентів.

Блок навчання агента відповідає за поповнення новими знаннями існуючої *бази знань*, яка служить для зберігання всіх без винятку знань, отриманих в процесі функціонування агента. Сюди входять база моделей агентів, база знань про розв'язувані задачі і база знань власного „досвіду". На етапі ініціалізації в базі знань знаходиться деяка інформація про стан зовнішнього середовища та інших агентів. Дані поміщаються в базу по мірі взаємодії з іншими агентами чи навколишнім середовищем. База знань, опрацьовуючи ситуацію, яка склалася, зберігає знання про способи вирішення завдань і методи вибору цих способів.

В блоці *генератор цілей управління* обробляються всі отримані дані та показники і формується ціль, яку потрібно досягти для вирішення поставленої задачі. У блоці *реалізації рішень*, на основі правил поведінки, визначених базою знань, а також поставленої мети здійснюється формування та реалізація управляючого впливу. *Збуджувачі* агента служать засобом відправлення управляючих повідомлень до середовища та інших агентів.

Таким чином, на відміну від звичайних агентів, ІА володіють деякими знаннями про навколишній світ, які дозволяють їм самим вирішувати завдання без втручання користувача. Крім того, ІА може взаємодіяти з іншими агентами з метою спільного вирішення певних завдань. Сьогодні прийнято розрізняти два визначення інтелектуального агента – „слабке" і „сильне" [9].

Під ІА в слабкому сенсі розуміється програмно або апаратно реалізована система, яка володіє такими властивостями:

автономність – здатність інтелектуального агента функціонувати без втручання людини і при цьому здійснювати самоконтроль над своїми діями і внутрішнім станом;

суспільна поведінка (*social ability*) – здатність функціонувати у взаємодії з іншими агентами, обмінюючись з ними повідомленнями за допомогою деякої загальнозрозумілої мови комунікацій;

реактивність (*reactivity*) – здатність сприймати стан середовища і своєчасно відповідати (реагувати) на ті зміни, які в ній відбуваються;

мобільність (*mobility*) – здатність агента мігрувати мережею в пошуках необхідної інформації для вирішення своїх завдань, при кооперативному вирішенні завдань спільно або за допомогою інших агентів і т.д.;

проактивність (*proactivity*) – здатність агента брати на себе ініціативу, тобто здатність генерувати цілі і діяти раціонально для їх досягнення, а не тільки реагувати на зовнішні події.

Сильне визначення агента формується за допомогою доповнень до вище перелічених властивостей. Зокрема, головним з них є наявність у агента хоча б деякої підмножини так званих „ментальних властивостей", або інтенсіональних понять, до яких відносяться наступні:

знання (*knowledge*) – це постійна частина знань агента про себе, середовище і інших агентів, тобто та частина, яка не змінюється в процесі його функціонування;

переконання (*beliefs*) – знання агента про середовище, зокрема, про інших агентів; це ті знання, які можуть змінюватися в часі і ставати невірними, проте агент може не мати про це інформації і продовжувати залишатися в переконанні, що на них можна засновувати свої висновки;

бажання (*desires*) – це стани, ситуації, досягнення яких з різних причин є для агента бажаним, проте вони можуть бути суперечливими і тому агент не очікує, що всі вони будуть досягнуті;

наміри (*intentions*) – це те, що агент або зобов'язаний зробити в силу своїх зобов'язань по відношенню до інших агентам (йому „це" доручено і він узяв цю задачу на себе), або те,

що випливає з його бажань (тобто несуперечливе підмножина бажань, вибране з тих чи інших причин, і яке є сумісним з прийнятими на себе зобов'язаннями);

цілі (*goals*) – конкретика множини кінцевих і проміжних станів, досягнення яких агент прийняв в якості поточної стратегії поведінки;

зобов'язання по відношенню до інших агентів (*commitments*) – завдання, які агент бере на себе на прохання (дорученням) інших агентів у рамках кооперативних цілей або цілей окремих агентів в рамках співпраці.

Відповідно до представленої в [7] концепції, а також проведеної вище класифікації агентів інтелектуальну систему управління вузлом МР можна представити у вигляді моделі, що складається з ІА різного призначення (рис. 4). Координація роботи ІА здійснюється метаагентом, який відповідає за функціонування вузлової ІСУ, метою якого є забезпечення заданої якості обслуговування різних типів трафіка, що передаються в радіомережі.

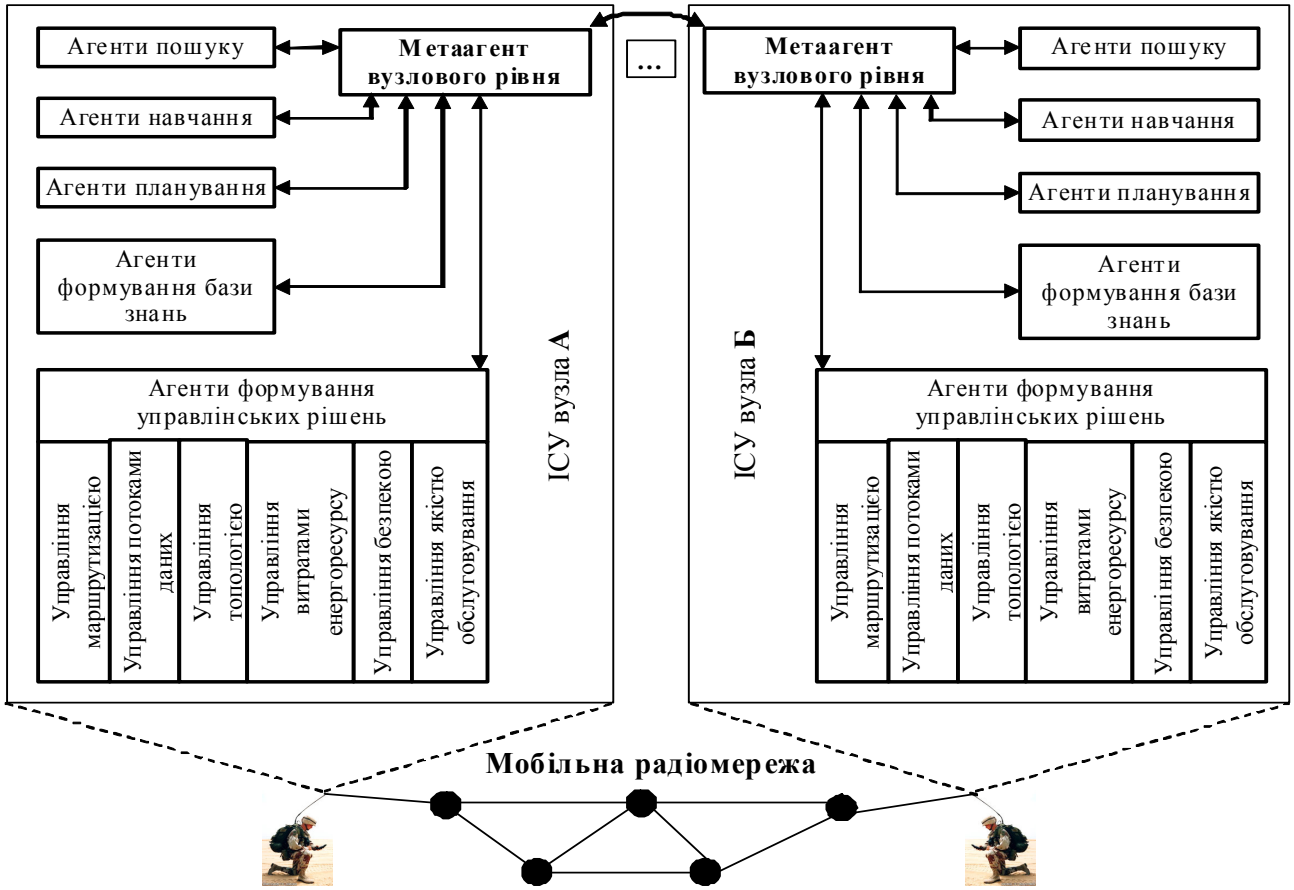


Рис. 4. Модель системи управління вузла МР з використанням ІА

З урахуванням поточного стану вузла зв'язку та вимог до якості передачі певного типу інформації, а також поточного стану та динаміки зміни середовища, ІА повинні здійснювати формування управляючих рішень та забезпечувати адаптацію системи управління до зміни зовнішнього середовища або зміни параметрів вузлової системи управління шляхом:

– підтримки необхідних режимів функціонування мобільних вузлів (радіомережі чи її зони);

– створення правил поведінки та моделей реакцій на основі даних, отриманих з зовнішнього середовища;

– перерозподілу функцій мобільного вузла, у разі виходу його з ладу, на інший мобільний вузол чи групу вузлів;

– визначення (зміна, у разі необхідності) пріоритетів функціонування ІА в залежності від доступних йому внутрішніх ресурсів, що дозволить уникнути ситуації, за якої прийняття управляючих рішень буде покладене на ІА з недостатніми внутрішніми ресурсами;

– активізації інших ІА у разі зміни параметрів зовнішнього середовища чи після надходження команд з ІСУ;

– збору даних про стан навколишнього середовища, а також вузлові та мережеві ресурси і передача цих даних (за необхідності) іншим ІА;

– забезпечення самонавчання ІСУ на основі зібраної інформації про стан навколишнього середовища та стан самої системи управління;

– виконання функцій тимчасового координатора МР, при втраті зв'язку з вузлом, який координує роботу МР, в залежності від визначеної в процесі функціонування пріоритетності;

– відстеження подій і сигналізації про їх виникнення при надходженні управляючої команди від ІСУ;

– отримання даних про правила поведінки та моделі реакцій від ІА вузлового рівня.

Таким чином, головною особливістю інтелектуальних агентів, запропонованих для реалізації функцій різних підсистем інтелектуальної системи управління вузлом МР, є здатність до навчання і пристосування до змін навколишнього середовища. Проведена класифікація програм-агентів, а також розглянуті структура та властивості інтелектуальних агентів дозволили зробити висновки про те, що для побудови ІСУ вузлом радіомережі класу MANET доцільно використовувати інтелектуальні агенти різного призначення, які відрізнятимуться за потужністю та покладеними на них функціями.

ЛІТЕРАТУРА

1. Романюк В.А. Мобільні радіомережі (MANET) – основа побудови тактичних мереж зв'язку / В.А. Романюк // IV Науково-практичний семінар ВІТІ „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення". – К.: ВІТІ НТУУ „КПІ". – 2007. – С. 5 – 18.

2. Аналіз можливостей використання інтелектуальних агентів для побудови системи управління вузлами радіомереж класу MANET / [Симоненко О.А., Уманець Я.Л., Романюк В.А., Сова О.Я.] // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2013. – № 1. – С. 76 – 84.

3. Гаврилова Т.А. Базы знаний интеллектуальных систем / Гаврилова Т.А., Хорошевский В.Ф. – СПб: Питер, 2000. – 384 с.

4. Макаров И.М. Искусственный интеллект и интеллектуальные системы управления / И.М. Макаров, В.М. Лохин, С.В. Манько, М.П. Романов; [отв. ред. И.М. Макарова]; Отделение информ. технологий и вычислит. систем РАН. – М.: Наука, 2006. – 333 с.

5. Міночкін А.І. Концепція управління мобільною компонентою мереж зв'язку військового призначення / Міночкін А.І., Романюк В.А. // Збірник наукових праць ВІТІ НТУУ "КПІ". – 2005. – № 3. – С. 51 – 60.

6. Романюк В.А. Інтелектуальні мобільні радіомережі: збірник матеріалів V науково-технічної конференції [„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"] / – К.: ВІТІ НТУУ „КПІ", 2010. – С. 28 – 36.

7. Романюк В.А. Концепция иерархического построения интеллектуальных систем управления тактическими радиосетями класса MANET: сборник тезисов докладов и выступлений участников XXII Международной Крымской конференции ["СВЧ-техника и телекоммуникационные технологии"], (КрыМиКо). / Романюк В.А., Сова О.Я., Жук П.В., Романюк А.В. – Севастополь, 2012. – С. 265.

8. Романюк В.А. Принципи побудови системи управління автоматизованою мережею радіозв'язку / Романюк В.А. // Збірник наукових праць КВІУЗ. – 2000. – № 5. – С. 60 – 64.

9. D. Karthik. Suituation based intelligence routing in wireless sensor network / D. karthik, S. Nagarajan // International Conference on Computational Intelligence and Computing Research. – 2011.

д.т.н. Субач І. Ю. (ВІТІ ДУТ)

МЕТОДИКА СИНТЕЗУ ОПТИМАЛЬНОЇ СТРУКТУРИ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ОБСЛУГОВУЮЧОГО ПЕРСОНАЛУ ІНФОРМАЦІЙНОЇ МЕРЕЖІ ОРГАНУ ВІЙСЬКОВОГО УПРАВЛІННЯ

Технічною основою системи зв'язку та автоматизації управління військами є інформаційні мережі, що являють собою сукупність інформаційно-телекомунікаційних вузлів, локальних обчислювальних мереж, окремих робочих станцій та засобів зв'язку. Сукупність зазначених елементів має досить складну топологію проте, аналіз показує, що масовий характер несправностей обумовлює необхідність обробки обслуговуючим персоналом інформаційної мережі (ІМ) значного об'єму даних в умовах дефіциту часу. Враховуючи, що процес прийняття рішення є складним психологічним процесом, виникають передумови для перевищення перепускної спроможності обслуговуючого персоналу і зниження якості рішень, які він приймає в ході управління ІМ.

Основними недоліками існуючого інформаційно-аналітичного забезпечення обслуговуючого персоналу інформаційної мережі є:

складність структури інформаційної мережі;

високий внутрішній і зовнішній динамізм;

неповнота та недостовірність вихідних даних про стан системи;

складність та обмеженість можливостей математичного опису стану системи; висока ротація кадрів та низький рівень професіоналізму фахівців.

Аналіз досвіду управління функціонуванням ІМ військового призначення показує, що однією з головних задач є задача аналізу стану ІМ, яка у теперішній час є практично не автоматизованою. Обслуговуючий персонал системи приймає рішення тільки на основі особистого досвіду та інтуїції. Оскільки в даний час має місце велика ротація кадрів Збройних Сил (ЗС), то рівень професіоналізму таких фахівців є не дуже високим. У зв'язку з цим час, який витрачається обслуговуючим персоналом на аналіз стану та локалізацію несправностей, не відповідає нормативному часу, що у свою чергу, впливає на оперативність вирішення задач управління у цілому.

Наявність наведеної невідповідності обумовлює актуальність досліджень, які полягають у підвищенні обґрунтованості та оперативності рішень обслуговуючого персоналу ІМ військового призначення на основі розробки та впровадження систем підтримки прийняття його рішень (СППР). Аналіз останніх досліджень і публікацій у галузі управління ІМ показує, що засоби інтелектуалізації процесів прийняття рішень обслуговуючого персоналу ІМ є найбільш важливими та практично необхідними в сфері інфокомунікацій. Створення подібних систем є основним напрямом розвитку проблемно-орієнтованих програмних засобів, що забезпечують ефективне застосування засобів обчислювальної техніки в даній сфері людської діяльності, що пов'язана з прийняттям рішень.

СППР обслуговуючого персоналу ІМ являє собою складну систему, що характеризується комплексною взаємодією територіально та функціонально розподілених елементів тому, від її організації, а також від якості джерел отримання знань та потужності бази знань залежить ефективність усієї інтелектуальної системи у цілому.

Під час вибору оптимального варіанту структури системи є можливими два варіанти відображення елементів множини взаємозв'язаних функцій (задач, інформації) СППР відповідно до принципів її побудови на елементи множини можливих зв'язаних елементів системи (вузлів, рівнів системи та інше): перший, коли кожна задача виконується лише одним з декількох можливих вузлів системи та другий, коли задача виконується декількома вузлами системи. Аналіз функцій, задач та технологій мережного управління щодо усунення несправностей обслуговуючим персоналом ІМ свідчить про те, що більш придатним є другий випадок, тобто відбувається декомпозиція вихідної задачі на підзадачі, паралельне їх

рішення локальними СППР з наступним агрегуванням результатів рішення підзадач у загальне рішення вихідної задачі.

У якості показника ефективності доцільно обрати відношення ефективності до вартості та звести задачу до оцінки можливості досягнення максимуму ефективності при заданій вартості. Багатокритеріальна задача синтезу оптимальної структури розподіленої СППР обслуговуючого персоналу ІМ є основою для синтезу оптимальної структури СППР обслуговуючого персоналу ІМ, але слід зауважити, що вона є нелінійною задачею математичного програмування. Тому, для її рішення слід застосовувати агрегативно-декомпозиційний підхід, який складається з двох взаємозв'язаних етапів: послідовної декомпозиції цілей, функцій та задач, що виконуються системою та агрегуванні (об'єднанні) на відповідному рівні деталізації елементів побудови системи у цілому.

Таким чином, процес проектування оптимальної структури СППР обслуговуючого персоналу ІМ включає послідовне рішення задач синтезу основних елементів та частин системи.

На першому етапі визначається організаційна структура системи, виходячи з цілей та стратегій функціонування ІМ, в результаті чого, визначається число рівнів ієрархії та вузлів системи.

На другому етапі оптимізується розподіл функцій (задач) за рівнями та вузлами системи. Далі, вибирається комплекс програмних та технічних засобів для реалізації СППР. При цьому враховуються витрати на обладнання вузлів обраними засобами та їх експлуатацію.

Розподіл функцій (задач) між елементами СППР є задачею проектування складних технічних систем. Для мінімізації часових витрат, які є зв'язаними з обміном інформацією між рівнями та вузлами системи, необхідно сконцентрувати на кожному рівні (вузлі) СППР функції (задачі), які мають максимальний взаємозв'язок у процесі функціонування системи. Найбільш поширеними методами рішення таких задач є методи, які базуються на розрізанні графів. Постановка задачі може змінюватися у відповідності до властивостей графів, котрі визначаються структурою та функціями системи.

Для вирішення даної задачі застосовуються точні методи (повного або упорядкованого перебору, наприклад, метод „гілок та границь"), а також наближені, евристичні методи. Застосування того чи іншого методу залежить від числа вершин графу та насиченості його матриці суміжності. Після попереднього розподілу функцій між елементами СППР виконується етап вибору технічних та програмних засобів. Оскільки вибір технічних засобів здійснюється за часом раніше, ніж закінчення етапу розробки функціональних підсистем, то на цьому етапі є об'єктивно присутньою невизначеність вимог, що висуваються до наведених засобів. Ця невизначеність вимагає застосування адекватних методів прийняття рішень, які ґрунтуються на експертних оцінках та опрацюванні їх результатів методами теорії нечітких множин.

Дана задача відноситься до класу задач нечіткої багатокритеріальної оптимізації та може бути вирішеною за допомогою лексикографічного методу, який є не складним у реалізації та вимагає мінімальної експертної інформації про ступінь переваги показників.

Загальна постановка задачі вибору програмних засобів може бути описаною та вирішеною за аналогічною схемою. Крім того, у процесі проектування СППР на основі технологій обробки знань необхідно найбільш повно враховувати характерні особливості предметної області та забезпечити адекватне подання знань про об'єкти прийняття рішень у базі знань СППР. Адекватність подання знань до задач, що вирішуються СППР, забезпечується обґрунтованим вибором моделі подання знань та відповідних методів логічного виводу на знаннях.

Класичними моделями, що використовуються для подання знань в СППР, є семантичні сітки, фрейми, логічні та продукційні моделі. Значного розвитку в останній час набули нейронні мережі, квантові моделі, а також гібридні моделі подання знань.

Застосування моделей подання знань при створенні СППР на сучасному етапі найчастіше базується на логіко-лінгвістичному підході. Основою логіко-лінгвістичного підходу є теорія нечітких множин, яка дозволяє формалізувати нечітке вербальне описання об'єктів прийняття рішень і застосувати відповідні математичні методи для обробки нечітких даних. Метою застосування математичного та логічного апарату теорії нечітких множин є пошук та оцінка переважних альтернатив з використанням процедур експертного опитування з урахуванням нечіткості висловлювань експертів та невизначеності вихідних даних. Даний підхід широко застосовується для модифікації описаних моделей подання знань. З метою порівняння властивостей описаних моделей подання знань доцільно визначити основні функції підсистеми подання знань в СППР:організація зберігання знань в системі; введення нових знань та поєднання їх з існуючими; вивід нових знань; знаходження знань; вилучення непотрібних знань; перевірка несуперечливості бази знань; здійснення інтерфейсу між користувачем і базою знань.

Для ефективного виконання наведених функцій моделі подання знань повинні задовольняти наступним основним вимогам: прогнозована ефективність; здатність пояснення рішення; здатність до навчання; продуктивність; масштабованість; можливість експорту та імпорту знань; наочність.

Вимоги до ефективності визначають здатність системи оцінити ефективність генерованого рішення. У разі незадовільної оцінки рішення система повинна спробувати вказати обслуговуючому персоналу ІМ джерела суперечливості або неповноти для уточнення вихідних даних. Здатність пояснення генерованого рішення є очевидною вимогою до організаційно-технічних систем управління.

На основі аналізу властивостей моделей подання знань, їхніх переваг та недоліків, а також вимог, яким вони мають відповідати, можна зробити висновок, що кожна з розглянутих моделей знань лише частково відповідає заданим вимогам.

Задача вибору адекватної моделі подання знань в СППР за своїм характером є багатокритеріальною та слабо формалізованою, тому традиційно вирішується на основі досвіду та кваліфікації розробників, їх суб'єктивних поглядів та переваг. Недоліки такого підходу є відомими.

Перспективним напрямком для її рішення є застосування методів парних порівнянь, наприклад, методу аналізу ієрархій.

Рішення задачі на основі використання методу аналізу ієрархій полягає у виконанні чотирьох етапів:

формалізація задачі у вигляді ієрархічної структури з декількома рівнями (ціль, показники, альтернативи);

виконання експертами попарних порівнянь елементів кожного рівня та оформлення результатів у вигляді сукупності матриць парних порівнянь;

на основі отриманих матриць парних порівнянь обчислення коефіцієнтів важливості для елементів кожного рівня (при цьому перевіряється погодженість суджень експертів за допомогою індексу погодженості);

розрахунок підсумкової ваги кожної з альтернатив та визначення або ранжування найкращої альтернативи.

Запропонована у доповіді методика дозволяє вирішити задачу синтезу оптимальної структури СППР обслуговуючого персоналу ІМ, яка є нелінійною задачею математичного програмування, на основі агрегативно-декомпозиційного підходу, який полягає у послідовному ітераційному розв'язуванні взаємозв'язаних задач синтезу її основних елементів та частин. Вона може бути застосованою на етапі проектування СППР обслуговуючого персоналу ІМ органу військового управління.

Подальшими напрямками досліджень можна вважати пошук шляхів удосконалення методології оптимальної організації функціонування системи та її реалізації й еволюціонування.

к.т.н. Чевардін В. Є. (ВІТІ ДУТ)
Живило Є. О. (ВІТІ ДУТ)
Куцаєв В. В. (ВІТІ ДУТ)

РЕЗУЛЬТАТИ АНАЛІЗУ СТАТИСТИЧНОЇ БЕЗПЕКИ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ПОБУДОВАНИХ НА ОСНОВІ ІЗОМОРФНИХ ТРАНСФОРМАЦІЙ ЕЛІПТИЧНИХ КРИВИХ

Вступ.

Суттєве збільшення активності кібернетичних інцидентів в сучасних комп'ютерних мережах (впливів небезпечного програмного забезпечення, кібернетичних атак) збільшують загрози інформаційної безпеки в інформаційно-телекомунікаційних системах критичного застосування. В таких умовах забезпечення інформаційної безпеки не можливо без збільшення числа механізмів захисту інформації (механізмів шифрування, цифрового підпису, гешування даних), які використовуються як окремо так і у складі підсистем забезпечення кібербезпеки (систем аналізу вразливостей, виявлення атак, протидії та інших). Враховуючі, що зростання числа програмних реалізацій механізмів криптографічного захисту приведе до збільшення числа криптографічних ключів та псевдовипадкових послідовностей (ПВП), розробка нових, вдосконалення існуючих методів генерації псевдовипадкових послідовностей є **актуальним** науково-технічним завданням.

За останні десятиріччя зусилля багатьох вчених в галузі дослідження генераторів ПВП були спрямовані на пошук нових шляхів побудови генераторів ПВП з теоретично доведеними властивостями та порівняно невеликою обчислювальною складністю. Більшість отриманих результатів в цієї галузі можна розділити на два класи. По-перше, це генератори, які мають структуру характерну для блочних шифрів, стійкість яких еквівалентна алгоритму блочного шифрування або гешування даних [6]. Цей клас дозволяє отримати порівняно невелику обчислювальну складність, але не має можливості теоретичного обґрунтування властивостей ПВП. По-друге, це генератори, які базуються на теоретико-складних задачах математики (дискретний логарифм в простому полі, дискретний логарифм в групі точок еліптичної кривої, факторизація цілих чисел та інші) [1 – 5]. Цей клас має можливість теоретичного обґрунтування властивостей ПВП, але має велику обчислювальну складність. Для вирішення виявленого протиріччя було обрано напрямок на побудову нового підходу до побудови генераторів ПВП на основі перетворень в групі точок еліптичної кривої з використанням ізоморфних трансформацій [3 – 5]. Прототипом для розробки генераторів нового класу були обрані генератори на основі перетворень в групі точок еліптичної кривої – Dual_EC_DRBG [6]. В якості головного показника для оцінки ефективності генераторів була обрана статистична безпека генераторів ПВП, яка формується на основі проходження генераторами методики NIST STS 211 [7].

1. Модель генератора Dual_EC_DRBG. Нехай $E_{a,b}(F_p): y^2 = (x^3 + ax + b) \bmod p$ – еліптична крива визначена над скінченним полем F_p, E_p – циклічна підгрупа точок еліптичної кривої достатньо великого простого порядку *n*. Послідовність внутрішніх станів генератору: $t_1, ..., t_n$ створюється за правилом: $t_i = X_\psi[t_{i-1} * P] \bmod n$, де $t_1 = X_\psi[t_0 * P]$, $t_0 = seed$, P – базова точка кривої, алгоритми генерації яких наведені у [6]. Функціонування генератору Dual_EC_DRBG описується виразом (1).

$$b_i = extr\left[t_i * Q\right] = extr\left[(X_\psi[t_{i-1} * P] \bmod n) * Q\right], \qquad (1)$$

де X_ψ – *X*-координата точки кривої, яка подана у вигляді цілого числа; t_i – ціле число;

P, Q – базові точки кривої; *n* – порядок циклічної групи точок кривої; *extr* – операція виділення бітів з *X*-координати точки кривої.

2. Модель генератора Isomorphic_EC_DRBG. Нехай P – базова точка кривої $E_{a,b}(F_p)$, порядок якої $n = ordP$, ω – генератор циклічної групи G_n. В якості секретного параметру використовується значення *entropy*, на основі якого обчислюються значення: *seed*. Чергова точка (внутрішній стан генератору) розраховується шляхом обчислення: $P_i = t_i * P$. Параметр ізоморфної трансформації обчислюється як: $u_i = f^k{}_i(u)$. Математична модель запропонованого генератору наведена виразом (2).

$$b_j = extr[r_i] = extr\left[\phi_{f_i^k(u)}\left(X_\psi[t_i * P]\right)\right]. \quad (2)$$

Для отримання секретного значення *seed* для генерації ПВП використовувалось перетворення (3).

$$seed = HDF(entropy, nonce, personal\_string, add\_inp), \quad (3)$$

де *entropy* – бітове значення ентропійного джерела; *nonce* – неповторна мітка; *personal_string* – бітовий рядок (визначається додатком); *add_inp* – додаткове значення. Для генерації нового значення ізоморфної трансформації u_i запропоновано використовувати наступні функції.

mark 1. $u_0 = \omega^k \bmod p$, $u_i = u_{i-1}{}^2 \bmod p$, $k = HDF(seed) \bmod p$, де $(k, p-1) = 1$.

mark 2. $u_0 = \omega^{2k} \bmod p$, $k = HDF(seed) \bmod p$, де $(k, p-1) = 1$, $r = HDF(seed\,1) \bmod p$, $r = r_1 \| r_2 \| r_3 \| ... r_{10}$, $u_i = u^{r_i} \bmod p$.

mark 3. $u_0 = \omega^{2k} \bmod p$, $k = HDF(seed) \bmod p$, де $(k, p-1) = 1$, $r_{if\ i=0 \bmod 10} = HDF(seed++) \bmod p$, $u_i = u^{r_{i \bmod 10}} \bmod p$.

3. Оцінка статистичної безпеки генераторів ПВП на основі еліптичних кривих та їх ізоморфних трансформацій. В якості значення *entropy* використовувались 80 бітів, які були отримані генератором Dual_EC_DRBG (P-521), для якого *seed* був створений лінійним конгруентним генератором Marsaglia&Zaman random bit generator з бібліотеки MIRACLE. Для проведення дослідження було згенеровано значення *entropy* 128 біт, на основі якого генерувались відповідні значення *seed* для кожного генератору. На основі кожного з реалізованих алгоритмів генерації ПВП було отримано 10^9 бітів ПВП, які були розділені на 10 частин. Результати тестування за методикою NIST STS 2.1.1 наведені у таблиці, де знаком „–" позначені експерименти, в яких були отримані неякісні ПВП.

Таблиця

Результати тестування генераторів ПВП

№ послід.	Isomorphic_EC_DRBG												Dual_EC_DRBG	
	mark1				mark2				mark3					
	K–163	K–233	P–192	P–224	K–163	K–233	P–192	P–224	K–163	K–233	P–192	P–224	P–256	P–384
1	+	+	–	–	+	–	+	–	+	–	–	–	–	+
2	+	+	–	+	+	–	+	–	+	–	+	+	–	–
3	+	–	+	–	–	–	–	+	+	–	+	–	+	–
4	–	+	–	+	–	–	–	–	+	–	+	–	+	–
5	+	–	–	–	+	+	+	+	+	+	+	+	–	–
6	–	+	+	+	–	–	–	–	+	–	–	+	–	+
7	–	–	–	–	+	–	+	+	+	–	–	+	+	–
8	–	+	–	–	+	+	+	–	–	+	+	+	+	–
9	–	+	+	–	+	–	+	+	+	+	+	–	+	–
10	+	+	+	–	+	+	+	+	–	+	–	–	–	–
+/∑	5/10	7/10	4/10	3/10	7/10	3/10	7/10	5/10	8/10	4/10	6/10	5/10	6/10	2/10

Висновки

Результати дослідження статистичної безпеки дозволили визначити безпечність генераторів Isomorphic_EC_DRBG. Генератори: Isomorphic_EC_DRBG_mark1(K-233), Isomorphic_EC_DRBG_mark2(K-163),Isomorphic_EC_DRBG_mark2(P-192), Isomorphic_EC_DRBG_mark3(K-163), Isomorphic_EC_DRBG_mark1(K-233) в середньому створюють якісну кожну другу ПВП. Генератор Isomorphic_EC_DRBG_mark3(K-163) показав найкращі результати тестування статистичної безпеки 8 з 10. Стандартизовані генератори Dual_EC_ DRBG(P-256) та Dual_EC_ DRBG(P-384) не пройшли тестування у 4 з 10 та у 8 з 10 випадків відповідно, що викриває їх дефект великого числа m-бітних серій з одиниць в ПВП.

Таким чином, проведений аналіз статистичної безпеки відомих генераторів ПВП дозволив відкрити можливість використання для побудови алгоритмів генерації крім рекомендованих еліптичних кривих: P-192, P-224, P-512 криві: K-163, K-233, K-283, K-571, B-163, B-233, B-283, B-571, U-163, U-239, U-307.

ЛІТЕРАТУРА

1. Impagliazzo R. One-way functions are essential for complexity based cryptography / R. Impagliazzo, M. Luby // Proc. 30th Annu. Symp. On Found. of Comput. Sci. 1989. P. 230 – 235.
2. Impagliazzo R. Pseudo-random generation from one-way functions / R. Impagliazzo , L. Levin, M. Luby // Proc. 21st Annu. ACM Symp. on Theory of Computing. 1989. P. 12 – 24.
3. Burton S. One-Way Permutations on Elliptic Curves / Burton S. Kaliski, Jr. // Journal of Cryptology (1991) International Association for Cryptologic Research. 1991. – P.187 – 199.
4. Бессалов А. Метод генерации псевдослучайных последовательностей на основе изоморфных трансформаций эллиптической кривой / Бессалов А. В., Чевардин В. Е. // Прикладная радиоэлектроника: научно-технический журнал – 2012. – Том 11. № 2. – С. 234 – 237.
5. Чевардин В. Е. Генераторы псевдослучайных последовательностей на основе теоретикосложностных задач математики / В. Е. Чевардин // Збірник наукових праць ВІТІ НТУУ „КПІ”, Випуск № 1, Київ, ВІТІ НТУУ „КПІ”. – 2012 р. – С.125 – 134.
6. NIST Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators / Elaine Barker, John Kelsey // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. – January 2012.
7. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / National Institute of Standards and Technology. – 2010. http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf.

Ахтирський І.П. (ВІТІ ДУТ)
к.т.н. Сілко О.В. (ВІТІ ДУТ)

ЗАСТОСУВАННЯ ДИСТАНЦІЙНО-КЕРУЄМОГО ЛІТАЛЬНОГО АПАРАТУ „*ARDRONE*" У НАВЧАЛЬНОМУ ПРОЦЕСІ

Розширення діапазону зору людини з метою візуалізації та розпізнавання недоступної для його очей інформації є одним з найважливіших і важких завдань. Проблема спостереження в небезпечних для людини умовах (радіаційне зараження) або під час проведення бойових дій вже давно набула особливої актуальності, наукові дослідження в цій області постійно стимулюються потребами військової діяльності. Пристрої, що використовуються технологією роспізнавання образів, знаходять широке застосування на озброєнні армій розвинених країн, ними користуються майже всі державні цивільні та силові структури. На жаль, дуже мало вітчизняних видань технічної і спеціальної літератури, що мають військову спрямованість і досліджують один із перспективних напрямків робототехніки – а саме проблеми розпізнавання образів та спостереження за об'єктами. Але навчальна програма дисциплін ВІТІ ДУТ дозволяє курсантам під час проведення практичних занять проводити дослідження в цьому напрямку використовуючи квадрокоптер, який має велику кількість сенсорів і приладів,а також відкритий API, що робить його зручною платформою для наукових та освітніх цілей військової галузі.

Квадро-гелікоптер „*ArDrone*" з бортовою ЕОМ та операційною системою Linux застосовується членами військово-наукового гуртка під час проведення експериментів, які пов'язані з дослідженням питань застосування безпілотних літаючих апаратів у військовій справі. Актуальність досліджень полягає в тому, що використовуючи сенсори і прилади квадро-гелікоптера „*ArDrone*", а також відкритого API перед курсантами відкриваються можливості з виконання низки завдань таких як: розпізнавання військових об'єктів та нанесення їх на топографічну мапу, створення схем важкодоступних приміщень, пошук візуальних несправностей військового обладнання та техніки.

Особливу увагу приділяється розробці програмного забезпечення для квадро-гелікоптера з функціями безпілотного літаючого робота, який за допомогою двох камер спроможний вести відео спостереження. Реалізація функції відео спостереження передбачає застосовування теорії розпізнавання образів, методів класифікації та ідентифікації предметів, явищ, процесів, сигналів, ситуацій, об'єктів, які характеризуються кінцевим набором деяких властивостей і ознак. Для створення програмного додатку який буде розпізнавати об'єкти на відео з квадро-гелікоптера пропонується використати засоби технології комп'ютерного зору, а саме бібліотеку алгоритмів комп'ютерного зору та обробки зображень з відкритим кодом *OpenCV*, яка реалізована на мові *C* / *C* +. Для реалізації функції розпізнавання військових об'єктів та нанесення їх на топографічну мапу застосовується алгоритм надійного тривалого супроводу заздалегідь відомих об'єктів, який підтримує розриви між кадрами відео потоку, швидкий рух камери, повне зникнення, а потім появу об'єкта. Підхід, який використаний в даному алгоритмі називається Супровід-Моделювання-Виявлення (*Tracking-Modeling-Detection*), він поєднує адаптивний супровід об'єкта з навчанням детектора об'єкта в процесі розпізнавання. Після того як об'єкт був захоплений за допомогою алгоритму захоплення, траєкторія об'єкта починає спостерігатися двома процесами (розширювання і урізання події). Вони будують детектор об'єкта на льоту. Алгоритм дозволяє оптимально виділити об'єкт з відео потоку, з подальшою ідентифікацією в реальному часі.

Одже, дослідження технології розпізнавання образів на базі квадро-гелікоптера „ArDrone" відкриває широкі можливості з розробки програмного забезпечення розвідки та оцінки обстановки, а також виконання інших військових завдань потенційно небезпечних для людини при веденні та підготовки бойових дій.

Бабінець Т.М. (ВІТІ ДУТ)
к.т.н. Макарчук О.М. (ВІТІ ДУТ)

ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ В ВИЩОМУ НАВЧАЛЬНОМУ ЗАКЛАДІ

В сучасних умовах формування нового освітнього простору спостерігається тенденція укрупнення ВНЗ, яке приводить до створення своєрідних корпоративних об'єднань, структурні підрозділи якого розкидані територіально. У цих умовах розвитку корпоративної форми ВНЗ виникає проблема організації ефективної системи документообігу як всередині самої центральної установи між її структурними підрозділами, так і територіально відокремлених структурних підрозділів. Правильно організована технологія роботи з документами у подібних корпоративних об'єднаннях ВНЗ дозволить скоротити невиправдану бюрократію („паперову тяганину") зекономити часові і трудові ресурси, а також збільшити швидкість обміну документною інформацією між усіма структурними підрозділами ВНЗ. Спираючись на низку загальнодержавних нормативних актів і методик, які регламентують найбільш загальні правила організації роботи з документами та вимоги до їхнього оформлення, було проведено аналіз основних видів і потоків документів в ВНЗ.

В результаті аналізу в системі документообігу в військовому ВНЗ виділено п'ять основних документопотоків: 1) службова кореспонденція; 2) документи щодо організації навчального процесу; 3) документи з контролю виконання; 4) нормативні документи установи; 5) підготовка і погодження проектів документів. В основу побудови моделі „корпоративної" системи документообігу ВНЗ запропоновано модульний принцип. Корпоративна система складається із базової системи діловодства центральної установи, яка встановлена у всіх її структурних підрозділах. Кожна із базових систем має реалізувати в об'єднанні установ єдину інформаційну логіку і на цій основі налагодити ефективний обмін даними з будь – якою іншою базовою системою діловодства. Важливо, щоб при цьому структура побудови „корпоративної" системи документообігу ВНЗ відповідала її організаційній структурі.

Для реалізації цієї моделі системи документообігу центральна установа має забезпечити технічну платформу – корпоративну комп'ютерну мережу. Обмін даними між базовими автоматизованими системами в межах однієї локальної комп'ютерної мережі ВНЗ забезпечується шляхом стандартного механізму обміну. Для автоматизованого опрацювання документів, їх розсилання виконавцям, контролю за їх виконанням для кожного типу документів розробляється маршрут. Кожна точка маршруту визначає дії, які делеговані кожному з виконавців в цій точці, умови переходу в наступну точку маршруту. Автоматично формуються повідомлення виконавцям про необхідність виконання певних дій на кожній точці маршруту. Після опрацювання останньої точки маршруту документ направляється в централізований архів. Відслідковування маршруту дає інформацію про стан документа для прийняття оперативних рішень. У системі документообігу ВНЗ банк документів можна формувати на основі систем „*Neo Cad – Intranet*". Технологія доступу до банку документів для всіх користувачів може бути забезпечена за уже апробованою на практиці технологією *Internet/Intranet*. Однією з важливих умов функціонування системи є створення банків документів у ЦУ та кожній уставі і їхніх структурних підрозділах. Така система банків документів ЦУ та її структурних підрозділів забезпечує систему інформаційної підтримки прийняття рішень на центральному рівні та рівні підрозділів за участю кожного його працівника. Поряд із застосуванням документів у банк документів можуть бути включені відповідні розділи інформації Міністерства освіти і науки України, а також можуть бути створені різноманітні довідкові інформації.

Таким чином, впровадження системи електронного документообігу в вищому навчальному закладі дозволить: покращити виконавчу дисципліну, контроль над постановкою і виконанням завдань, прискорити пошук документів, мінімізувати втрату документів, захистити інформацію.

Барба І.Б. (ОНАЗ ім. О.С.Попова)

МОДУЛЯЦІЯ – ДЕМОДУЛЯЦІЯ ШИРОКОСМУГОВИХ СИСТЕМ ПЕРЕДАЧІ З ОРТОГОНАЛЬНО ГАРМОНІЙНИМИ СИГНАЛАМИ

Широке поширення серед сучасних засобів зв'язку отримали системи передачі (СП), які використовують широкосмугові сигнали [1]. Традиційно до широкосмугових відносять сигнали на базі функцій Уолша і відповідно до широкосмугових СП, використовують ці сигнали, наприклад, СП стандарту CDMA [2]. Поняття широкосмуговості вживають по відношенню до сигналів, які застосовуються в технологіях передачі, що використовують безліч ортогональних гармонійних сигналів(ОГС), одночасно і незалежно модульованих переданими інформаційними сигналами: OFDM – модуляція (Orthogonal Frequency Division Multiplexing) [3, 4].

Актуальною проблемою розвитку телекомунікацій є підвищення ефективності СП інформації. При цьому однією з важливих наукових завдань є розробка ефективних алгоритмів демодуляції сигналів узагальненого класу ОГС запропонованого в [1].

Відомо, що ефективні алгоритми демодуляції сигналів СП ОГС будуються на основі швидкого перетворення Фур'є (ШПФ) [4]. Для запропонованого узагальненого класу ОГС застосування алгоритмів ШПФ розглядалося в [4], однак без суворого обґрунтування.

Метою роботи є суворе обґрунтування застосування ШПФ для підвищення обчислювальної ефективності демодуляції сигналів СП з ОГС.

На рис. 1 наведена структурна схема l -го каналу традиційної СП ОГС. Передані на p - му тактовому інтервалі інформаційні символи a_{lp} і b_{lp} $l = 0, 1, 2, \ldots, \ldots, L-1$, $p = \pm 0, \pm 1, \pm 2, \ldots \pm \infty$ модулюють незалежно квадратурні несущі $\cos l\omega_0(t-pT)$ та $\sin l\omega_0(t-pT)$. На приймальній стороні здійснюється кореляційна обробка на інтервалі τ_0 прийнятого сигналу. На рис. 2 наведена структурна схема l – го каналу СП ОГС із запропонованими сигналами. Вона відрізняється від схеми рис. 1 наявністю перемножувача на $s(t) = \sqrt{u(t-pT)}$ на передачі і прийомі. У силу лінійності моделі каналу можна перемножувачі об'єднати, і на прийомі груповий сигнал помножити на $s(t) = u(t-pT)$ (рис. 3).

Структурна схема демодулятора сигналів узагальненого класу ОГС наведена в [5]. Відліки цифрового групового сигналу перемножуються з відліками періодичного цифрового сигналу u(t), межі якого (початок сигналу) синхронізовані з межами тактових інтервалів прийнятих посилок. Результуючий сигнал у суматорі підсумовується з сигналом, затриманим на τ_0. З потоку відліків виділяється N відліків, потім здійснюється пряме ДПФ виділеної групи відліків. Результатом ДПФ є N відліків дискретного спектру відрізка прийнятого сигналу. Виділення L відліків спектру , відповідних несущим групового сигналу завершує демодуляцію сигналів узагальненого класу ОГС.

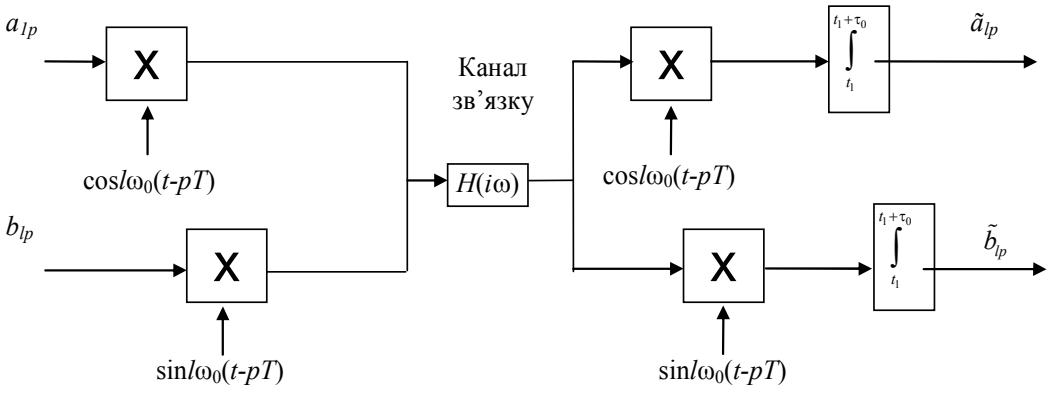


Рис. 1 – Структурна схема l – го каналу традиційної СП ОГС

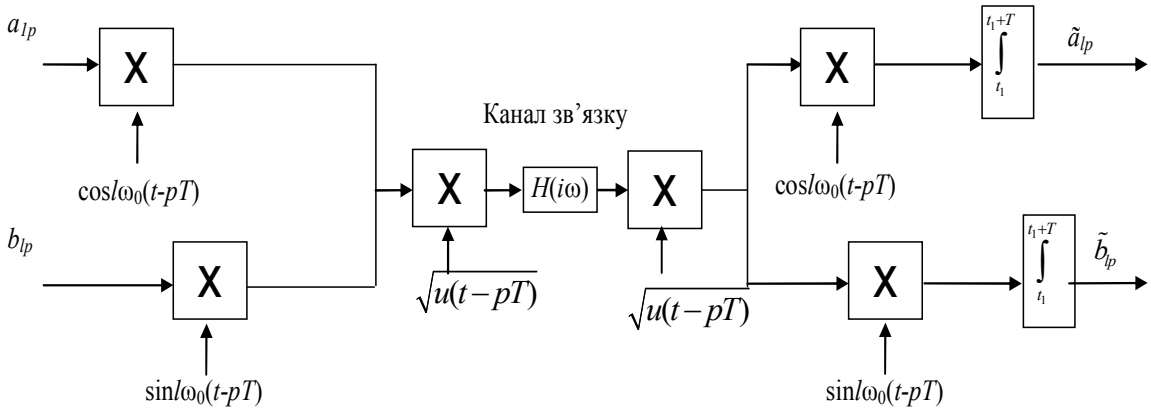


Рис. 2 – Структурна схема *l* – го каналу СП ОГС з сигналами – переносчиками узагальненого класу

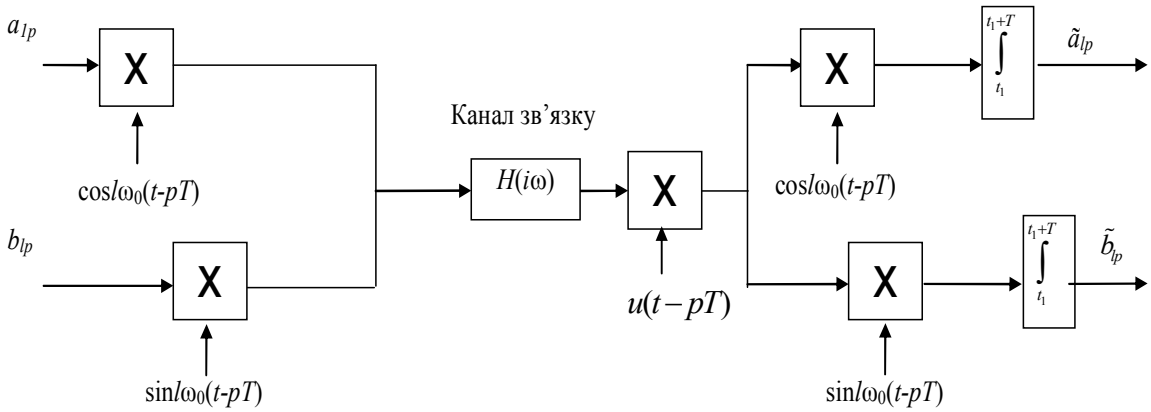


Рис. 3 – Структурна схема *l* – го каналу СП ОГС з одним додатковим перемножувачем

У роботі обґрунтовується застосування алгоритмів ШПФ для демодуляції сигналів узагальненого класу ОГС, що дозволяє досягти високої обчислювальної ефективності алгоритмів демодуляції СП ОГС. Виграш визначається співвідношенням числа операцій виконання звичайного перетворення Фур'є по відношенню до швидкого перетворення Фур'є.

ЛІТЕРАТУРА:

1. Ипатов В.П. Широкополосные системы и кодовое разделение сигналов / В.П. Ипатов. – М.: Техносфера, 2007. − 488 с.

2. Берлин А. Н. Цифровые сотовые системы связи / А.Н.Берлин. – М.: Эко-Трендз, 2007. – 296 с.

3. В. А. Балашов. Системы передачи ортогональными гармоническими сигналами / В. А. Балашов, П.П. Воробиенко, Л.М.Ляховецкий // – М.:Эко – Трендз, 2012. – 228с.: ил.

4. Балашов В.А. Ортогональные гармонические сигналы для широкополосных систем передачи / В.А. Балашов, Л.М. Ляховецкий, И.Б. Барба // Загальногалузевий науково – виробничий журнал Зв'язок. – Київ. – 2012. – № 3. – с. 17 – 20.

5. Барба І.Б. Повышение вычислительной эффективности демодуляции сигналов систем передачи с ОГС / І.Б. Барба // Наукові праці ОНАЗ ім. О.С. Попова. – 2013. – 1. – С.134 – 139.

Бєляков В.Ф. (НЦСВ АСВ)
к.т.н. Богуцький С.М. (НЦСВ АСВ)

ДООСНАЩЕННЯ КОМБІНОВАНИХ АРТИЛЕРІЙСЬКИХ ГАРМАТ (КАГ) НАВІГАЦІЙНИМ КОМПЛЕКСОМ (НК) ДЛЯ ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ЇХ БОЙОВОГО ЗАСТОСУВАННЯ

Здатність КАГ раптово і у короткий час наносити удари по цілях, а також наявність сучасних досить потужних та різноманітних за призначенням мін та снарядів в поєднанні з невеликою вартістю, забезпечили їх популярність і перспективність. На сьогоднішній день комбіновані артилерійські гармати є на озброєнні багатьох армій провідних у військовому відношенні країн світу. Розробники КАГ постійно прагнули і прагнуть до покращення їхніх тактико-технічних характеристик, розглядаючи основні напрямки щодо підвищення ефективності використання – збільшення дальності стрільби, потужності і точності влучення в цілі, покращення показників точності стрільби і забезпечення автоматизації підготовки і ведення вогню.

Використання радіолокаторів виявлення наземних цілей, прицілів і спостережних приладів нічного бачення, гірокомпасів, звукометричних і метеорологічних станцій, засобів топографічної прив'язки дозволило суттєво збільшити точність стрільби. Мобільність артилерійських підрозділів суттєво підвищилась за рахунок створення самохідних комбінованих артилерійських гармат.

Основною метою модернізації комбінованих артилерійських гармат є забезпечення необхідного бойового потенціалу артилерійських вогневих засобів повітрянодесантних військ та засобів вогневої підтримки загальновійськових підрозділів Сухопутних військ на прогнозований період за допомогою розширення бойових можливостей наявних комбінованих артилерійських гармат відповідно до сучасних вимог. Модернізована комбінована артилерійська гармата переважно не поступається закордонним аналогам, разом з тим встановлення засобів навігації значно підвищить її оперативність, маневреність, точність, вогневе ураження і, як наслідок, збільшить ефективність бойового застосування.

Запропоновано використання координатного способу визначення дирекційного кута цілі і кута лафета комбінованих артилерійських гармат типу „Нона – С", „Нона – СВК" та „Вена". Проаналізовані його характеристики точності. Запропоновано структуру навігаційного комплексу для КАГ типу „Нона – С", „Нона – СВК" та „Вена". Дооснащення КАГ типу „Нона – С", „Нона – СВК" та „Вена" навігаційним комплексом, що запропоновано, дасть змогу вести вогонь з непідготовлених в топогеодезичному аспекті позицій з маршу і бути готовим змінити вогневу позицію у продовж декількох десятків секунд після закінчення стрільби, що допоможе значно підвищити оперативність їх бойового застосування.

Висновки

1. Дооснащення КАГ типу „Нона – С", „Нона – СВК" та „Вена" порівняно недорогим навігаційним комплексом, який забезпечує визначення координат позицій КАГ дозволить обчислювати та визначати дирекційний кут цілі у режимі реального часу.
2. Запропонований навігаційний комплекс повинен забезпечити визначення дирекційного кута КАГ, що дасть змогу обчислювати та визначати кут довороту платформи.
3. Дооснащення КАГ вказаним навігаційним комплексом дасть йому змогу вести вогонь з непідготовлених в топогеодезичному аспекті позицій з маршу і в найкоротший час змінювати вогневу позицію, що значно підвищить оперативність його бойового застосування.
4. На базі запропонованого комплексу надалі можливе розроблення автоматизованої системи управління вогнем КАГ типу „Нона – С", „Нона – СВК" та „Вена" та інших аналогічних систем.

к.т.н. Богданов В.В. (ВІТІ ДУТ)
Бабич І.В. (Київський ОВК)
Мальцева І.Р. (ВІТІ ДУТ)
Паламарчук С.А. (ВІТІ ДУТ)

ДОЦІЛЬНІСТЬ ВПРОВАДЖЕННЯ СИСТЕМИ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Результатом провадження інформаційної діяльності підрозділами є інформаційні ресурси, які створюються, зберігаються, передаються, використовуються за призначенням в структурі інформаційно-телекомунікаційних систем військового призначення (ІТС ВП). Поряд з розвитком ІТС (автоматизованих систем класу 2, 3) в усіх сферах життєдіяльності, в тому числі й ЗС України розвиваються й засоби перехоплення інформації в таких системах під час її передачі. Тому, вкрай важливе забезпечення захищеності інформаційних ресурсів ІТС від загроз конфіденційності, цілісності та доступності без зниження продуктивності системи в цілому. Враховуючи розподіленість зазначених систем, сучасну статистику щодо реалізації кіберзлочинів, порушень доступу до ресурсів та системи в цілому, актуальною відповідно до НД ТЗІ 2.5-004-99 є вимога забезпечення послуги безпеки „***Конфіденційність при обміні***” (т.з послуга безпеки КВ). Для виконання даної послуги поряд з криптографічними методами (засобами) перетворення інформації широкого застосування набувають стеганографічні методи (засоби) перетворення інформації. Їх різноманіття (складність) в повній мірі залежить від розвитку інформаційних технологій, потребує детальних досліджень та інтеграції в процеси інформаційної взаємодії на рівні прикладних процесів ІТС ВП.

Таким чином, загалом, в структурі функціонуючої ІТС ВП пропонується впровадження системи стеганографічного захисту інформації як складової захищеної ІТС ВП. Структура системи повинна розроблятися з врахуванням загального призначення ІТС, функціонуючих інформаційних сервісів (функціональних підсистем), спеціалізованих додатків, що породжують інформаційні потоки різноманітних форматів (текст, звук, відео). Нажаль, на даний час відсутні дійсно стійкі системи стеганографічного захисту інформації, а існуючі, мають занадто підвищені демаскуючі ознаки. Що в цілому, враховуючи призначення систем стеганографічного захисту інформації, нівелює можливість їх застосування.

Відповідно, для впровадження системи стеганографічного захисту інформації в ІТС ВП, необхідно вирішити наступні завдання:

– розробка оптимальної структури системи стеганографічного захисту інформації;

– розробка надійних методів та алгоритмів стеганографічного перетворення інформації;

– визначення необхідних та достатніх показників функціонування системи для оцінки ефективності та можливості використання в структурі ІТС ВП;

– визначення форматів (протоколів), які доцільно використовувати в якості контейнера системи стеганографічного захисту з врахуванням інформаційних сервісів, що найчастіше використовуються.

– розробка адекватного програмного забезпечення даних методів (алгоритмів) з оптимальним використанням обчислювальних ресурсів ІТС ВП;

– розробка інтерфейсу взаємодії користувача з забезпеченням багатокористувацького режиму доступу;

– визначення варіативних опцій програмного забезпечення щодо налаштування системи.

Проведено ряд досліджень, серед яких визначено вимоги до стеганографічних методів перетворення інформації, проаналізовано недоліки існуючих алгоритмів стеганографічного перетворення інформації. Подальші дослідження в області стеганографії для ІТС ВП доцільні для визначення форматів контейнерів інформації системи стеганографічного захисту, що реалізовані в сервісах *IP*-телефонії та відеоконференцзв’язку.

к.т.н. Богданов В.В. (ВІТІ ДУТ)
Паламарчук Н.А. (ВІТІ ДУТ)
Паламарчук С.А. (ВІТІ ДУТ)

НОВІТНІ СТАНДАРТИ СЕРІЇ ISO/IEC 27000 ЗІ СТВОРЕННЯ, РОЗВИТКУ ТА ПІДТРИМКИ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

При проектуванні захищених інформаційно-телекомунікаційних систем важливо чітко визначити, яким вимогам вони повинні задовольняти, перелік основних показників якості, методику контролю і оцінки їх ефективності. На сьогодні ця задача може бути вирішена за допомогою спеціально розроблених для цього нормативних документів, які отримали назву стандартів інформаційної безпеки (СІБ). Відповідно до СІБ захищеною вважається система обробки та передачі інформації, що відповідає встановленим вимогам і гарантіям щодо забезпечення конфіденційності, цілісності, доступності і спостережності інформаційних активів (документів, носіїв, додатків, інформаційних систем, знань персоналу). Міжнародна стандартизація складових систем управління інформаційною безпекою (ІБ) формує три напрямки розвитку в даній сфері:

сімейство стандартів „Методи забезпечення безпеки" – ISO/IEC 27000-ISO/IEC 27037;

сімейство стандартів „Методи та засоби забезпечення безпеки" – ISO/IEC 15408 („Загальні критерії", 3 частини), ISO/IEC 13335 (5 частин), ISO/IEC 18045;

сімейство стандартів „Управління та аудиту інформаційних технологій" (CobIT, ITSM, ITIL, і т.ін.).

Особливе місце в цьому переліку посідають Міжнародні стандарти, що присвячені практичним питанням забезпечення ІБ в різних галузях захисту інформації, до яких відносяться міжнародні стандарти оцінки і управління інформаційною безпекою серії ISO/IEC 27000 „Інформаційні технології – Засоби забезпечення безпеки", що ґрунтуються на авторитетних британських стандартах BS 17799 (в подальшому ISO/IEC 17799). Відповідно до підходу, прийнятого в стандартах цієї серії, безперервний процес управління розбито на чотири фази менеджменту: оцінювання ризиків, що включає в себе ідентифікацію активів, аналіз і обчислення ризиків; оброблення ризику: вибір і реалізація заходів і засобів безпеки; контроль ризиків шляхом моніторингу, тестування, аналізу механізмів безпеки, а також аудиту системи; оптимізація ризиків шляхом модифікації та оновлення правил, заходів і засобів безпеки. Перелік чинних та перспективних стандартів серії ISO/IEC 27000 включає близько 20-ти найменувань – від стандарту 27001 (Системи управління інформаційною безпекою) до стандарту 27037 (Настанови з ідентифікації, виявлення, збору та збереження цифрових доказів). Найбільш значимі з них, впровадження яких вже здійснюється або очікується найближчим часом, приведені в табл.1.

*Таблиця*1

Перелік чинних та перспективних стандартів серії ISO/IEC 27000

Шифр стандарту	**Назва (призначення) стандарту**
ISO/IEC 27000: 2009	Управління ІБ. Короткий огляд і словник
ISO/IEC 27001: 2005	Системи управління ІБ. Вимоги
ISO/IEC 27002: 2005	Звід практики для управління ІБ (ISO/IEC 17799:2005)
ISO/IEC 27003: 2010	Керівництво по реалізації системи управління ІБ
ISO/IEC 27004: 2009	Вимірювання в управлінні ІБ
ISO/IEC 27005: 2008	Ризик-менеджмент ІБ
ISO/IEC 27006: 2007	Вимоги до органів аудиту і сертифікації систем управління ІБ
ISO/IEC 27007: 2011	Настанови щодо аудиту ІБ системи управління
ISO/IEC 27011: 2008	Настанови щодо управління ІБ для телекомунікацій
ISO/IEC 27031: 2011	Настанови щодо інформаційно-комунікаційних технологій. Готовність до безперервності бізнесу.

Названі стандарти отримали широке розповсюдження і послужили поштовхом для створення національних нормативних документів в галузі інформаційної безпеки в багатьох країнах світу. Так, в Російській Федерації Федеральним агентством по технічному регулюванню і метрології, починаючи з 2005 року, в прийнятих державних стандартах робляться відповідні посилання на стандарти серії ISO 27001-27006, а з 2006 р. вже діє стандарт ГОСТ Р ИСО/МЭК 27001 „Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".

В нашій державі з липня 2012 р. набув чинності державний стандарт ДСТУ ISO/IEC 27001:2010 „Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Система управління інформаційною безпекою. Вимоги". Також, в якості галузевих, з березня 2011 р. прийняті два стандарти Національного банку України: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 „Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги". (ISO/IEC 27001:2005, MOD); ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 „Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою". (ISO/IEC 27002:2005, MOD).

Слід зазначити, що застосування ДСТУ ISO/IEC 27001 для банківських структур є обов'язковим, для структур з іншими видами діяльності – на власний розсуд. Окрім цього, для реалізації вимог СУІБ в Україні гармонізації потребують міжнародні стандарти ISO/IEC 27005:2008 і ISO/IEC 27003:2010. ISO/IEC 27005:2008 надає структури для визначення підходу до управління ризиками в залежності від області дії СУІБ, області застосування управління ризиками ІБ або сектора промисловості та процес оцінки інформаційних ризиків (ІР) (2 етапи: *аналіз ІР* (ідентифікація і кількісна оцінка активів, загроз, існуючих засобів контролю, вразливостей і наслідків; *оцінювання ІР* (управління ризиком на основі ітераційного підходу щодо його оцінки до отримання прийнятного значення). ISO/IEC 27003:2010 описує процес специфікації та проектування СУІБ з моменту початку проектування до подання планів впровадження системи. Метою стандарту є надання практичної допомоги при реалізації СУІБ у межах організації відповідно до ISO/IEC 27001:2005. На основі міжнародного стандарту ISO/IEC 27003:2010 Департамент інформатизації Національного банку України розробив Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України (галузевих) з урахуванням особливостей банківської діяльності, стандартів та вимог Національного банку України з питань ІБ. Виходячи з загального призначення і практичної користі у встановленні контролю за інформаційною безпекою на основі стандартів ISO/IEC 27001, 27002 і 27003 авторами розроблений алгоритм впровадження СУІБ при створенні (модернізації) комплексної системи захисту інформації (КСЗІ) в автоматизованій системі (АС). Алгоритм включає 32 етапи – від усвідомлення цілей та вигод впровадження СУІБ до проведення аналізу СУІБ в АС з боку вищого керівництва і прийняття відповідного наказу про введення в дію СУІБ. Порівняльний аналіз вимог нормативних документів в галузі створення КСЗІ в АС і вимог стандартів ISO/IEC 27001, 27002 і 27003 свідчить про необхідність перегляду більше 10 вимог, прописаних в нормативних документах системи технічного захисту інформації (т.з. НД ТЗІ), пов'язаних з необхідністю ідентифікації активів, загроз, вразливостей, оцінкою та ранжуванням ризиків і проведенням аудиту.

Загалом, питання ефективної реалізації будь-якого стандарту невід'ємне від його інструментальних можливостей, що дозволяє автоматизувати роботу, забезпечити гнучкість і адаптивність застосування різноманітних „паперових" методик. Найкращими можливостями в цьому плані володіє стандарт ISO/IEC 27002: 2005 (ISO 17799).

Виходячи з зазначеного, доцільно доповнити діючі та перспективні стандарти такими програмними продуктами як довідник з питань інформаційної безпеки, гіпертекстовий довідник з питань захисту інформації, керівництво для співпрацівників служби безпеки, різноманітні демонстраційні версії і презентації, зручною навігацією.

к.т.н. Богуцький С.М. (НЦСВ АСВ)

ТЕНДЕНЦІЇ РОЗВИТКУ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ (РЕБ) ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ВІД ВИСОКОТОЧНОЇ ЗБРОЇ (ВТЗ)

Практично у всіх сучасних збройних конфліктах, де мало місце протистояння регулярних військових формувань, РЕБ відводилась виключно важлива роль. Із створенням нових удосконалених ударних та розвідувальних систем вона буде тільки зростати.

Одним з головних напрямків такого удосконалення є створення високоточної зброї та боєприпасів. Сучасні військові доктрини розвинених, у військовому відношенні, країн відводять високоточній зброї повітряного, наземного і морського базування роль головної ударної сили в конфліктах різного рівня. Постійне розширення типів ВТЗ, підвищення їх технічних характеристик, збільшення загальної кількості у військах створюють умови для інтенсивного використання цієї зброї для вибіркового і гарантованого ураження найбільш важливих об’єктів противника на всій його території. Наглядно використання ВТЗ та його висока ефективність продемонстрували конфлікти останніх років.

Захист об’єктів, озброєння та військової техніки від ВТЗ вимагає комплексних та узгоджених дій, РЕБ в цих діях займає і буде займати особливе місце в силу того, що інформаційно-технічною основою ВТЗ є використання електромагнітного спектру системами і засобами розвідки, радіонавігації, радіозв’язку, наведення і прицілювання.

Основними принципами розвитку і вдосконалення систем озброєння РЕБ на сучасному етапі є:

– відповідність складу і структури систем озброєння сучасним і перспективним задачам РЕБ і збройної боротьби в цілому;

– поетапне нарощування бойових можливостей по радіоелектронному подавленню (ураженню) найбільш важливих об’єктів в системах ВТЗ;

– випереджаючий розвиток автоматизованих систем управління комплексів і систем РЕБ;

– комплексний підхід до пониження помітності об’єктів і техніки в різних фізичних полях, секторах спостереження та діапазонах хвиль.

За результатами аналізу тенденції розвитку засобів і комплексів РЕБ слід відзначити, що систему захисту об’єктів і техніки від перспективних ВТЗ і зниження їх помітності необхідно будувати як багато ешелоновану, яка включає підсистеми РЕБ для індивідуального (об’єктового), групового та зонального захисту.

Підсистеми РЕБ для індивідуального (об’єктового) захисту призначені для впливу на радіо- та оптико-електронні засоби і системи прицілювання і управління боєприпасами. Техніка РЕБ цієї підсистеми повинна створюватись як уніфікована для міжвидового використання, що встановлюється безпосередньо на об’єкт захисту, при цьому, засоби РЕБ повинні розглядатися як складові частини зразків ОВТ. Підсистема РЕБ для групового захисту від ВТЗ частин і підрозділів призначена для прикриття їх на марші, в районах очікування, зосередження і на полі бою, в тому числі для захисту особового складу від ураження боєприпасами з радіопідривачами та з радіокерованими мінно-підривними пристроями. Засоби РЕБ групового захисту можуть бути штатними засобами, частин і підрозділів, які захищають, а також у складі частин (підрозділів) РЕБ видів та родів військ Збройних Сил України.

Підсистема РЕБ для зонального захисту від ВТЗ супротивника призначені для прикриття об’єктів і військової техніки, які розміщені на значній території, шляхом радіоелектронного подавлення (ураження) засобів розвідки космічного, повітряного, наземного і морського базування, радіонавігації, радіозв’язку і передачі даних, які задіяні в розвідувально-ударних контурах управління ВТЗ.

Аналіз використання засобів і систем РЕБ в сучасних конфліктах дозволяє передбачити зниження ефективності використання ВТЗ у 2 – 2,5 рази.

Бондаренко О.Є. (НЦЗІ ВІТІ ДУТ)
Черкасова Ю.О. (НЦЗІ ВІТІ ДУТ)
Чередниченко О.Ю. (НЦЗІ ВІТІ ДУТ)

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ PON У МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Існуючі польові системи зв'язку пунктів управління не спроможні у повній мірі задовольняти сучасним вимогам до інформаційного забезпечення в інтересах управління військами (силами). Вони мають досить низьку пропускну спроможність, що не дозволяє впроваджувати сучасні інформаційні технології для надання всього спектру інформаційних послуг для потреб військ і штабів усіх рівнів.

Перспективні польові системи зв'язку пунктів управління повинні забезпечувати необхідну пропускну спроможність для кожного виду інформації; мінімально допустимі затримки при передачі зображення та відео. Крім того, вони повинні відповідати сучасним вимогам із завадозахищеності та розвідзахищеності.

Для вирішення вказаних проблем пропонується технологія PON (Passive Optical Network – пасивна оптична мережа). PON – перспективна технологія широкосмугового мультисервісного множинного доступу по оптичному волокну з використанням хвильового розділення трактів приймання/передавання дозволяє реалізовувати одноволоконну деревоподібну топологію без використання активних мережевих елементів у вузлах розгалуження.

У загальному випадку мережа PON містить: приймально-передавальний модуль OLT (Optical line terminal) – активний пристрій, що забезпечує обмін інформацією між абонентськими терміналами; оптичний мережевий пристрій ONU (Optical network unit) – активний пристрій, що забезпечує обмін інформацією абонентських терміналів з приймально-передавальним модулем OLT; оптичне волокна – середовище поширення сигналів; оптичний розгалужувач (splitter) – пасивний оптичний багатополюсник, який здійснює розгалуження потоку оптичного випромінювання в одному напрямку та об'єднання декілька потоків у зворотному напрямку. Мережі PON, в основному, організовуються з використанням одного оптичного волокна, а при необхідності резервування – два волокна.

Порівняльні характеристики технологій PON надані у таблиці.

Характеристики	APON (ATM PON)	BPON (Broadband PON)	EPON/GEPON (Ethernet PON)	GPON (Gigabit PON)
Стандарт	ITU-T G.983	ITU-T G.983	IEEE 802.3ah	ITU-T G.984.x
Швидкість передачі прямий/зворотний потік, Мбіт/с	155/155 622/155	622/622	1244/1244	2488/2488
Кількість абонентських вузлів	32	32	16	64 (128)
Максимальний радіус мережі, км	20	20	20	20 (60)
Загасання лінії PON, дБ	н/д	н/д	26	22

Основні переваги технології PON: ефективне використання смуги пропускання та економія оптичного волокна; високі швидкості передачі прямого і зворотного інформаційних потоків; висока надійність мережі (у проміжних вузлах дерева знаходяться тільки пасивні оптичні розгалужувачі, що не вимагають обслуговування); масштабованість мережі (нарощування топології мережі без додаткових витрат на активне обладнання); можливість резервування каналів (ліній); високі завадозахищеність та розвідзахищеність мережі (використання оптичного волокна та мінімальної кількості активного обладнання).

Борисов О.В.(ВІТІ ДУТ)
Заіка Р.В. (ВІТІ ДУТ)
Ляхович В.Р. (ВІТІ ДУТ)

МЕТОД АДАПТИВНОГО ПЕРЕСТРОЮВАННЯ РАДІОТРАКТУ СИСТЕМ РАДІОЗВ'ЯЗКУ

У сучасних умовах бурхливий розвиток систем рухомого радіозв'язку призвів до необхідності пошуку системотехнічних рішень, спрямованих на підвищення ефективності як окремих радіозасобів, так і системи радіозв'язку в цілому. Стратегічним напрямком при рішенні завдання підвищення ефективності системи передачі інформації є перехід від систем із незмінною структурою до адаптивних систем, де алгоритми передачі й прийому сигналів можуть узгоджено змінюватися залежно від зміни зовнішніх умов.

В роботі запропоновано метод адаптивного перестроювання радіотракту систем радіозв'язку, сутність якого полягає в адаптивній зміні виду сигнально-кодової конструкції (структури кодека і модема) залежно від зміни завадової обстановки в каналі зв'язку з метою одержання максимального значення коефіцієнта використання потужності переданого сигналу (енергетичної ефективності).

Нехай задано параметри передавального пристрою і каналу зв'язку $\Psi = \{\psi_i\}$, $i = \overline{1, m}$, де $\psi_1 \ldots \psi_m$ – потужність корисного сигналу, тривалість імпульсу сигналу, смуга пропускання каналу зв'язку, вид маніпуляції, вид коректувального коду, спосіб обробки сигналу, вид завади, відношення сигнал/завада.

Необхідно максимізувати величину коефіцієнта використання потужності сигналу β_E СРЗ при забезпеченні заданого значення ймовірності помилкового приймання $P_{\text{пом}} \geq P_{\text{пом доп}}$.

Метод заснований на поданні системи радіозв'язку у вигляді керованої системи, що працює за принципом відхилення. Структурна адаптація СРЗ в умовах впливу завад відповідно до розробленого методу реалізується в наступній послідовності. У переважній більшості випадків виявляється можливим виділити декілька можливих сценарію розвитку завадової обстановки. Цим сценаріям у відповідність можуть бути поставлені N різних сигнально-кодових конструкцій (N структур модему і кодека), які доцільно вибирати виходячи з параметрів ефективності СРЗ при впливі різних видів завад.

Вихідними даними в режимі ведення зв'язку є поточні значення векторів: контрольованої величини x (x_1 – коефіцієнт використання потужності сигналу, x_2 – імовірність помилкового приймання $P_{\text{пом}}$); регулюючих впливів u (u_1 – вид модуляції; u_2 – довжина кодової комбінації, u_3 – коригувальна здатність коду, u_4 – швидкість коду); завад z (z_1 – вид завади, z_2 – частина смуги пропускання СРЗ, яку займає завада, z_3 – відношення сигнал/шум, z_4 – відношення сигнал/завада). Ведення зв'язку з використанням обраної в режимі сигнально-кодової конструкції здійснюється доти, поки імовірність помилкового приймання не зменшиться нижче заданого рівня ($P_{\text{пом}} < P_{\text{пом доп}}$).

У процесі функціонування адаптивної СРЗ здійснюється перевірка поточного значення імовірності помилкового приймання і визначаються вид і параметри завади, що діє в каналі зв'язку. У випадку, якщо в результаті зміни завадової обстановки поточне значення $P_{\text{пом}}$ стає менш ніж допустиме значення $P_{\text{пом доп}}$, приймається рішення про зміну параметрів кодека і модема. Також блок адаптації здійснює зміну відповідних параметрів СРЗ при зміні виду завади, що діє в каналі зв'язку.

Таким чином, у запропонованому методі, на відміну від розроблених раніше, адаптація до стану завадової обстановки здійснюється за рахунок зміни виду модуляції і типу коригувального коду, що дозволяє підвищити енергетичну ефективність системи радіозв'язку в умовах впливу найгірших завад при забезпеченні заданого рівня завадостійкості.

к.т.н. Борисов І.В. (ВІТІ ДУТ)
Чміль В.Ю. (ВІТІ ДУТ)
Калітник М.І. (ВІТІ ДУТ)

УДОСКОНАЛЕНА МЕТОДИКА РОЗРАХУНКУ ПАРАМЕТРІВ ЦИФРОВИХ РАДІОРЕЛЕЙНИХ ЛІНІЙ

Визначальною особливістю радіорелейних ліній (РРЛ) військового призначення у порівнянні з лініями загального призначення є необхідність постійної зміни дислокації радіорелейних станцій (РРС). Тому виникає необхідність у розробці методики розрахунку РРЛ, що дозволить скоротити час на прийняття рішення посадовими особами з планування зв'язку.

Розрахунок РРЛ – один з основних етапів її планування. Мета розрахунку полягає у визначенні придатності вибраного розміщення РРС на планованій трасі для забезпечення необхідної якості зв'язку по її каналах.

Методика розрахунку параметрів радіорелейних інтервалів цифрових радіорелейних ліній складається з наступних етапів:

1) за топографічною картою вибираються місця розгортання РРС на планованій трасі РРЛ;

2) побудова в масштабі довжин і висот креслення профілю місцевості на інтервалах РРЛ;

3) розрахунок медіанного ослаблення радіохвиль (без урахування завмирань) на кожному інтервалі РРЛ;

4) визначення величини медіанної потужності сигналу на вході приймача на кожному інтервалі;

5) розрахунок величини потужності сигналу, потрібної на вході приймача для забезпечення зв'язку на лінії із заданою якістю, тобто реальна чутливість приймача РРС;

6) визначення запасу високочастотного рівня сигналу на кожному інтервалі;

7) за величиною запасу визначається втрата надійності за рахунок завмирань на інтервалах за графіками, отриманими із статистичних даних, зібраних при експлуатації різних РРЛ у різних діапазонах частот (наводяться у довідниках);

8) формулювання висновку про придатність інтервалів РРЛ для забезпечення зв'язку в лінії із заданою якістю.

Проте вказана методика потребує значних часових затрат. У роботі розроблено вдосконалену методику розрахунку за рахунок автоматизації процесу побудови профілю місцевості з використанням розробленої розрахункової програми у форматі Excel.

В перспективі шляхом автоматизації визначення параметрів показників рельєфу з програми Google Earth з алгоритмом можна практично повністю автоматизувати процес розрахунку РРЛ. Єдиним етапом, який складно реалізувати без участі людини є нанесення місцевих перешкод на лінію рельєфу. Така методика дозволить значно скоротити час на розрахунок, досягнути більшої точності за рахунок усунення людського фактору (можливих помилок при проведенні побудови профілю місцевості), усуває потребу в кваліфікованих фахівцях для розрахунку.

ЛІТЕРАТУРА

1. Расчет радиорелейных линий связи: методические указания по курсовому проектированию для студентов специальностей 21030265 и 21020165 / А.С. Садомовский, В.А. Гульшин. – Ульяновск: УлГТУ, 2010. – 28 с.

2. Радиорелейнне и спутниковые системи передачи. Учебник для вузов / А.С. Немировский, О.С. Даншевич, Ю.И. Маршюнт и др. Под. ред. А.С. Немировского. – М.: Радио и связь, 2011. – 392 с.

Борознюк М.В. (ВІТІ ДУТ)

ВИБІР МЕТОДУ ФОРМУВАННЯ СИГНАЛІВ В СИСТЕМАХ З MIMO

Для сучасних систем радіозв'язку (СРЗ) особливо актуальним завданням є підвищення пропускної спроможності та якості обслуговування користувачів (зменшення вірогідності помилки передачі інформації). Це обумовлено рядом причин, основними з яких є обмежений частотний ресурс і підвищення вимог до об'єму та швидкості передачі інформації радіозасобами.

Помилки при передачі інформації можливо істотно зменшити за допомогою застосування технології MIMO (Multiple-input Multiple-output). У таких системах зменшення ймовірності помилки забезпечується за рахунок одночасного рознесення сигналів на передачі і на прийомі, а значне збільшення швидкості передачі даних досягається за рахунок використання методів адаптивної просторової обробки сигналів (просторового кодування), що забезпечують формування паралельних інформаційних потоків.

Тому ефективність використання MIMO в сучасних системах радіозв'язку, значною мірою, залежить від вибору методу формування сигналів при рознесеній передачі. У MIMO-системах можливе використання різних методів просторової обробки сигналів в передавальних антенах.

Проведена порівняльна оцінка ефективності різних методів формування сигналів в системах з рознесеною передачею. Ефективність рознесеної передачі (РП) значною мірою залежить від того, є чи відсутня на передавальній стороні інформація про стан каналу (про вектор вагових коефіцієнтів). За наявності такої інформації можлива реалізація адаптивної передачі, узгодженої з каналом.

Якщо передавачу невідомий стан каналу, то використання РП шляхом простого розділення потужності між передавальними антенами не змінює ймовірності бітової помилки. Тому на практиці використовуються різні методи формування сигналів в передавальних антенах, яким відповідають різні види РП. Розглянемо деякі з них для випадку рознесеної передачі з двох антен.

Для оцінки ефективності запропонованих видів РП було проведено імітаційне моделювання за допомогою програмного пакету SimuLink середовища MatLab для MIMO-системи. Ефективність різних методів неадаптивної рознесеної передачі порівнюватимемо за вірогідністю помилки передачі фреймів.

Передбачалося, що просторовий канал є релеєвським каналом з частотною дисперсією, обумовленою рухом користувача.

Аналіз результатів показав, що найбільш ефективним видом рознесеної передачі в MIMO-системах є просторово-часова рознесена передача. Така рознесена передача є найбільш ефективним видом неадаптивної РП, оскільки об'єднує просторове і часове рознесення. Модульовані імпульси розділяються на блоки по два послідовні імпульси в кожному, і поступають на просторово-часовий кодер, в якому фаза кожного з імпульсів змінюється (кодується) спеціальним чином, і потім вони випромінюється обома антенами.

Просторово-часова рознесена передача забезпечує найменшу середню потужність при заданій помилці передачі фрейму, припускає достатньо просту лінійну обробку сигналів на приймальному кінці лінії і не вимагає передачі даних про стан каналу на передавальний кінець лінії зв'язку.

Ефективність адаптивної РП співпадає з ефективністю неадаптивної просторово-часової РП.

Бохно Г.Т. (ВІТІ ДУТ)

МОНІТОРИНГ ПЕРЕСУВАННЯ ВІЙСЬКОВИХ ОБ'ЄКТІВ ЗА ДОПОМОГОЮ СИСТЕМИ ГЛОБАЛЬНОГО ПОЗИЦІОНУВАННЯ

З метою гнучкого і безперервного контролю та управління пересуванням вантажів необхідна точна інформація про їх місцезнаходження. Особливістю систем ГЛОНАСС – або GPS-моніторингу є не тільки визначення точного місцезнаходження об’єкта, але й можливість вести спостереження у режимі реального часу. Такі характеристики системи супутникового моніторингу дозволяють точно визначати маршрути пересування, час, швидкість та пройдену відстань. Використання системи GPS-моніторингу транспорту дозволяє оптимізувати роботу не тільки з контролю за рухом транспортних засобів, але й по розрахунку найбільш оптимальних маршрутів

Вирішення цієї задачі забезпечується широким застосуванням на транспортних рухомих об’єктах та вантажах засобів навігації. Для цього всі рухомі одиниці, що беруть участь в перевезенні, та об’єкти, що потребують перевезення, повинні бути оснащені системами навігації, які здатні безперервно, надійно та точно визначати їх територіальне місцезнаходження в різних метеоумовах та в будь-який час доби і пору року. Найбільш повно в досягненні зазначених цілей зарекомендували себе комплексні системи навігації до складу яких входять елементи автономних навігаційних систем та супутникових радіонавігаційних систем. Спільна обробка інформації, отриманої від різних незалежних систем навігації, дозволяє підвищити точність та достовірність визначення місцезнаходження вантажів та транспортних рухомих об’єктів [1].

Навігаційна інформація, отримана з комплексних навігаційних систем, знаходить широке застосування не тільки в цивільних транспортних мережах, а й у військових мережах тилового та технічного забезпечення (логістики). Навігаційне забезпечення є одним з важливих елементів бойового забезпечення військ та оперативного сервісного забезпечення цивільних користувачів, які керують рухомими об’єктами.

Метою даної роботи є розробка варіанту використання системи глобального позиціонування для забезпечення збереження вантажів, які циркулюють в військових транспортних мережах, із застосуванням глобальної системи визначення координат GPS (Global Positioning System) в якості складової частини комплексної системи навігації.

Проведено аналіз існуючих систем навігації наземних рухомих об’єктів та їх експлуатаційно-технічних характеристик, детально розглянуті принципи роботи систем супутникового позиціонування NAVSTAR та Galileo [2]. Проведено аналіз шляхів модернізації цих систем, що, в свою чергу, надасть значну користь при вирішенні завдань, де необхідно швидке та точне позиціонування рухомих об’єктів. Розглянуто ряд питань, які відносяться до наслідків модернізації глобальних систем визначення координат, що дозволять вдосконалити конструкцію приймачів сигналів та їх програмне забезпечення.

Таким чином, в результаті виконання роботи була запропонована оптимізація варіанту використання системи глобального позиціонування GPS для забезпечення моніторингу пересування військових вантажів або об’єктів, перевагою якої є зменшення економічних витрат на їх перевезення за рахунок вирішення „транспортної задачі” з урахуванням категорій важливості вантажів. Результати, отримані в ході виконання даної роботи, можуть бути використані при розробці комплексних систем навігації військового призначення.

ЛІТЕРАТУРА

1. Волчко П.І., Іванов В.І., Корольов В.М. та інші. „Вимоги до характеристик навігаційної інформації і систем навігації наземних рухомих об’єктів у сучасному штатному процесі”. Сучасні досягнення геодезичної науки та виробництва, № 5. С. 280 – 283, Ліга-Прес, Львів, 2000.

2. „La navigation par satellite, le point de vue des utilisateurs europeens”. Bara J. M., Navigation (France). 2000. № 191. С. 69 – 75.

Бунаков В.П (ЦНДІ ОВТ ЗСУ)
Завадський Д.С. (ЦНДІ ОВТ ЗСУ)
Слободенюк С.Й. (ЦНДІ ОВТ ЗСУ)

МЕТОДИКА РОЗРАХУНКУ АКТИВНОГО МІКРОПОЛОСКОВОГО ВІБРАТОРА

Жорсткі та неоднозначні вимоги до електродинамічних, масогабаритних, вартісних та конструктивних параметрів сучасних антен з одного боку та подальша мініатюризація радіоелектронної апаратури з іншого, призводить до необхідності розробки методик розрахунку активних мікрополоскових приймальних антен. В роботі запропонована методика розрахунку однієї з таких антен, а саме, активного мікрополоскового вібратора.

За умови визначеного розподілу комплексних амплітуд струмів електричних і магнітних полів на активному мікрополосковому вібраторі (МВ) послідовно вирішуються ряд задач, а саме:

– здійснюється розрахунок сили струму що наводиться на вході активного елементу (АЕ) МВ;

– здійснюється розрахунок (визначаються вимоги) до (АЕ);

– здійснюється вибір критерію оптимального узгодження МВ з активним елементом;

– здійснюється коректування вихідних параметрів МВ і вхідних параметрів АЕ.

Розрахунок електродинамічних характеристик мікрополоскового вібратора здійснюється за чисельно-аналітичним методом, коли в першому наближенні до істинного розподілу струмів електричного і магнітного полів на МВ спочатку визначається повний опір МВ як результат взаємодії електричного струму та електричного поля, що наведений цім струмом [1], потім, за отриманими значеннями активної та реактивної частину опору визначається струм на вхідних клемах АЕ [2]. В зв’язку з тим, що в приймальному каналі АЕ [3] працює в режимі близькому до лінійного, він представляється як перетворювач вхідного сигналу у відклик, який описується деяким оператором, що перетворює вектор вхідного сигналу у вектор вихідних параметрів. Знаючи матрицю провідностей АЕ (оператор), ЄДС що наводиться на вході АЕ (вектор вхідних параметрів), можливо розрахувати вектор вихідних параметрів (силу струму на виході АЕ), як добуток вектора вхідних параметрів та матриці провідностей.

Оцінити ефективність використання МВ з АЕ у порівнянні з пасивним МВ можливо за покращенням відношення сигнал/шум на виході приймального каналу МВ з АЕ по відношенню до її пасивного аналогу, або по відношенню квадратів чутливості за напруженістю поля антени з активним елементом та без нього, що і є критерієм оптимального узгодження в запропонованій методиці [4].

Запропонована методика дозволяє за заданими параметрами комплексних амплітуд струмів електричних і магнітних полів здійснити параметричний синтез мікрополозкового вібратора з активним елементом. Можливість керування фазовою, поляризаційною та характеристики направленості активного мікрополозкового вібратора дозволяє використати його в приймальному модулі активної фазованої антенної решітки, для зменшення її енергетичних та масогабаритних характеристик.

ЛІТЕРАТУРА.

1. Harrington R.F. Time-harmonic electromagnetic waves. – New York: McGfawHill, 1961, p.480.

2. Панченко Б.А. Микрополосковые антенны / Б.А. Панченко, Е.І Нефедов – М.: Радио и связь, 1986- 144с.

3. Бахрах Л.Д., Проблемы антенной техники/ Л.Д. Бахрах, Д.И.Воскресенский – М.: Радио и связь, 1989 – 368 с.

4. Цыбаев Б.Г. Антенны-усилители/ Б.Г. Цыбае, Б.С. Романов – М.: Сов.радио, 1980, –240 с.

к.т.н. Бурба О.І. (в/ч А1906)
Пасічник О.О (в/ч А1906)

МЕТОДИЧНІ АСПЕКТИ ПОБУДОВИ ІНФОРМАЦІЙНОГО ПРОСТОРУ ФУНКЦІОНУВАННЯ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НА ОСНОВІ СЕРВІС-ОРІЄНТОВАНОЇ АРХІТЕКТУРИ

Фундаментальною основою інформаційної індустрії останніх десятиліть та найближчого майбутнього є створення високоорганізованого інформаційного середовища, яке має забезпечити можливість формування і використання ефективного системно-аналітичного апарату. В свою чергу це дасть змогу на якісно новому рівні інформаційного обслуговування вести повсякденну оперативну роботу, здійснювати системний аналіз стану і перспектив діяльності інформаційно-аналітичних підрозділів та приймати відповідні науково обґрунтовані рішення щодо функціонування систем спеціального призначення.

При побудові інформаційного простору функціонування систем спеціального призначення превалює підхід, який полягає у системній інтеграції локальних, сегментів територіальних і глобальних мереж, систем та засобів телекомунікації для підвищення ефективності збору, обробки та розподілу інформації. Нерідко це призводить до механічного об'єднання розрізнених програмно-апаратних комплексів структурних підрозділів без врахування системоутворюючих принципів автоматизації та вимог до ефективності функціонування системи у цілому.

З урахуванням цього, актуальним завданням є дослідження, яке полягає у формалізації процесу побудови інформаційного простору та розробці відповідних механізмів, які розкривають застосування розглянутого в доповіді методичного підходу.

Згідно з принципами побудови сучасних розподілених інформаційних систем, вони повинні відповідати таким властивостями як гнучкість, розширюваність і масштабованість. Ці вимоги можуть бути ефективно реалізованими в рамках сервіс-орієнтованої архітектури (SOA – Service Oriented Architecture) [1]. Базовим компонентом SOA є сервіс, який визначається як деяке повторюване завдання зі стандартним інтерфейсом.

Використання сервіс-орієнтованої архітектури дає можливість системно інтегрувати у єдиному інформаційному просторі такі компоненти: інформаційні ресурси, організаційні структури та засоби інформаційної взаємодії. Організаційні структури та засоби інформаційної взаємодії утворюють інформаційну інфраструктуру (структуру розподіленої інформаційної системи).

На практиці для вирішення завдань синтезу структури складних інформаційних систем широко використовується агрегативно-декомпозиційний підхід [2], з урахуванням якого побудова інформаційного простору функціонування систем спеціального призначення на основі сервіс-орієнтованої архітектури полягає у вирішенні сукупності завдань:

визначенні оптимального варіанту інформаційної інфраструктури, яка забезпечує максимальну ефективність вирішення всієї сукупності інформаційних завдань;

визначенні на основі оптимального варіанту інформаційної інфраструктури сервісів реалізації єдиного інформаційного простору.

Таким чином, розглянуті в доповіді методичні аспекти дають можливість структурувати процес побудови інформаційного простору систем спеціального призначення послідовністю процедур, які в сукупності можна використовувати в якості методичного забезпечення цього процесу.

ЛІТЕРАТУРА

1. Thomas E. Service-Oriented Architecture (SOA): Concepts, Technology, and Design / E. Thomas Prentice Hall PTR, 2005. 792 p.

2. Цвиркун А. Д. Основы синтеза структуры сложных систем / А. Д. Цвиркун – М.: Наука, 1982. – 197 с.

Вакуленко О.В. (ВІТІ ДУТ)
Кононова І.В. (ВІТІ ДУТ)
Тищенко О.П. (ВІТІ ДУТ)

МЕТОДИКА ПРОЕКТУВАННЯ ВІДОМЧОЇ МЕРЕЖІ ДОСТУПУ НА ОСНОВІ FTTX ТЕХНОЛОГІЙ

В наш час проектування – це невід'ємна складова частина процесу побудови IT-інфраструктури, тому побудова відомчої мережі на основі використання FTTx (Fiber To The x) є досить актуальною.

Мета розробки методики проектування мережі доступу на основі технології FTTx полягає в забезпеченні ефективності прийняття управлінських рішень компаніями – провайдерами телекомунікаційних систем та мереж при розгортанні, модернізації та оптимізації сучасних мереж доступу.

Постановка задачі:

Задано:

– призначення та основні варіанти топології волоконно-оптичних мереж доступу;

– вимоги до характеристик мережі та її окремих складових;

– перелік існуючого мережевого обладнання;

– інші існуючі пристрої та програмне забезпечення (склад і характеристики).

Необхідно:

– розробити методику проектування сучасної мережі доступу на основі технології FTTx.

Обмеження:

– характеристики мережі доступу розраховуються на основі існуючого телекомунікаційного обладнання відомих фірм виробників та згідно вимог керівних документів і ДСТУ;

– час на розробку проекту та розрахунки техніко-економічних показників визначає замовник.

Основні етапи реалізації методики (рис.1)**:**

1). Збір вихідних даних;
2). Проводимо огляд місцевості та приміщень;
3). Вибираємо розмір та структуру мережі;
4). Вибираємо технологію FTTx;
5). Вибір рішення на базі пасивних оптичних мереж (PON);
6). Вибір рішення на базі активної оптичної мережі (AON Ethernet);
7). Організація електроживлення;
8). Вибір топології;
9). Вибір обладнання;
10).Вибір кабелю;
11). Вибір програмного забезпечення, адміністрування;
12). Визначення обсягу робіт;
13). Розрахунок витрат на впровадження;
14). Розрахунок технічної підтримки;
15). Прийняття рішення ефективності проекту;
16). Оформлення технічної документації проекту;
17). Прийняття рішення щодо узгодження документації проекту;
18). Організація охорони праці;
19). Монтаж кабельних трас;
20). Прокладка кабелю;
21). Монтаж комутаційних шаф;

22). Монтаж розеток робочої зони;

23). Підключення користувачів;

24). Оптимізація мережі(перевірка економічної та технічної ефективності мережі);

25). Тестування та сертифікація;

26). Прийняття рішення щодо прихованих витрат;

27). Здача в експлуатацію.

Таким чином в пропонованому алгоритмі враховані основні та необхідні етапи побудови сучасної мережі доступу на основі волоконно-оптичних систем передачі.

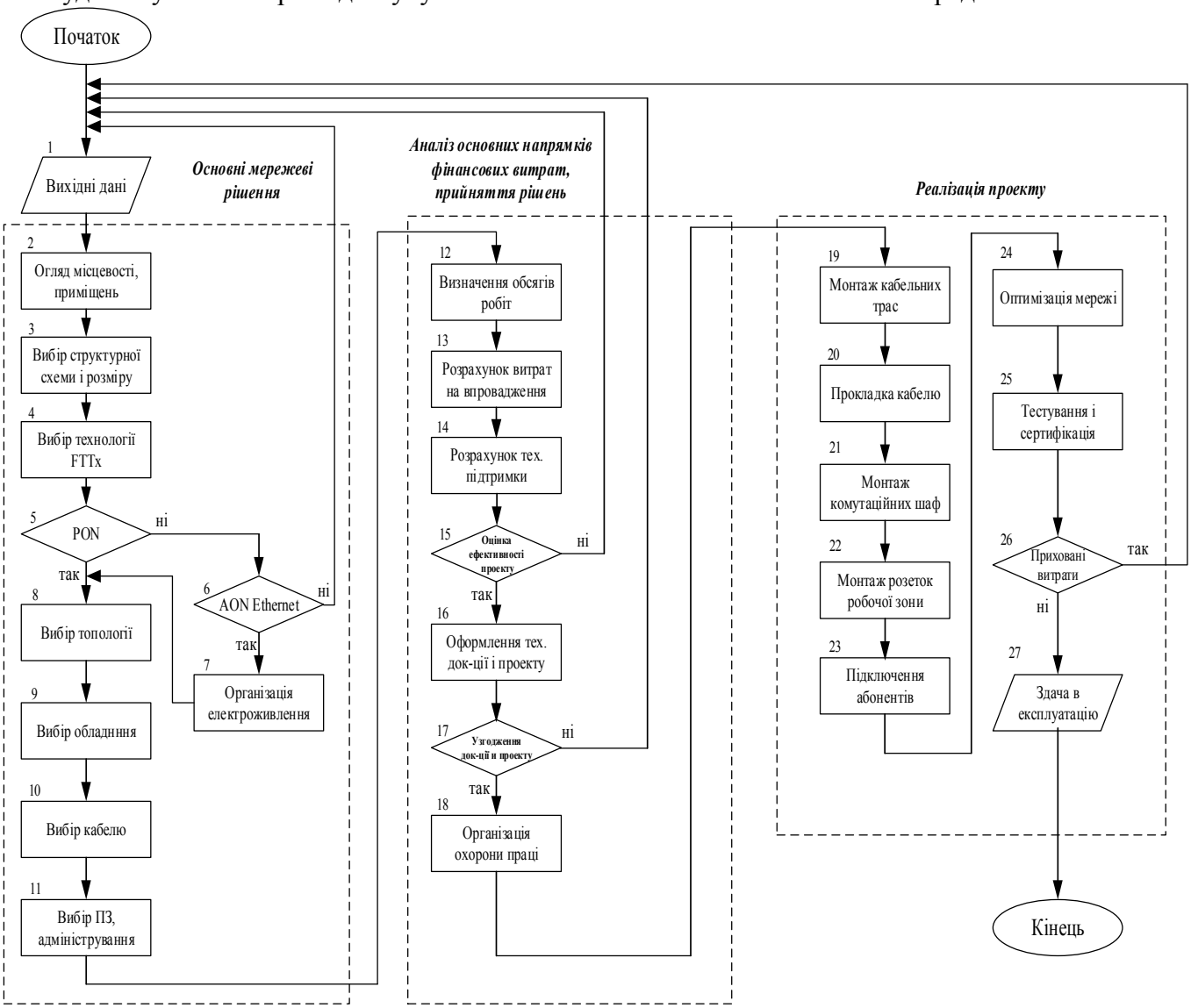


Рис.1. Схема алгоритму проектування сучасних мереж доступу на основі FTTx технологій

ЛІТЕРАТУРА:

1. Андрушко Л.М., Вознесенкий В.А., Каток В.Б. и др. Справочник по волоконно-оптическим линиям связи / Під ред. Свечникова С.М. и Андрушко Л.М. – К.: Техніка, 1988. – 239 с.

2. Бейли Д., Райт Э. Волоконная оптика: теория и практика. – М.: КУДИЦ-ОБРАЗ, 2006. – 320 с.

3. Берлин Б.З. и др. Волоконно-оптические системы связи на ГТС: Справочник – М.: Радиосвязь, 1994. – 160 с.

4. Портнов Э.Л. Оптические кабели связи и пассивные компоненты волоконно-оптических линий связи: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2007. – 464 с.

Вакуленко О.В. (ВІТІ ДУТ)
Явіся В.С. (ВІТІ ДУТ)

ПРОТОКОЛ PTP ДЛЯ СИНХРОНІЗАЦІЇ МЕРЕЖ NGN ВІДОМЧОГО ПРИЗНАЧЕННЯ

При реалізації концепції NGN, на мережах відомчого призначення, стає актуальним питання відновлення синхронізації на границях транспортного середовища з комутацією пакетів при передачі в ній групового сигналу з часовим мультиплексуванням у вигляді послуги емуляції каналів. Для вирішення задач синхронізації застосовують три основних способи [2]. Кожен із способів має свої переваги та недоліки.

Наступним щаблем розвитку способів синхронізації є окрема передача сигналів синхронізації мережі з комутацією пакетів за допомогою спеціально розроблених протоколів [5]. На даний момент такими є протоколи NTP [6] і PTP [7]. Протокол NTP (Network Time Protocol) широко використовується для синхронізації поточного часу на прикладному рівні. На відміну від нього, протокол „точного часу" PTP (Precision Time Protocol) діє на другому рівні моделі взаємодії відкритих систем (OSI). Протокол PTP описаний у стандарті IEEE 1588. Очікується, що надалі PTP може бути використаний як для високоточної синхронізації поточного часу, так і для тактової синхронізації встаткування.

Стандарт IEEE 1588 припускає, що протокол PTP надає стандартний метод синхронізації пристроїв у мережі з точністю вище 1 мкс (до 10 нс). Даний протокол забезпечує синхронізацію ведених пристроїв від ведучого, засвідчуючи, що події та часові мітки на всіх пристроях використовують ту саму часову базу. У протоколі передбачено два щаблі для синхронізації пристроїв: визначення ведучого пристрою (1) і корекція розбігу в часі, викликаного зсувом відліку часу у кожному пристрої та затримки передачі даних по мережі (2). При ініціалізації системи протокол PTP використовує алгоритм найкращого ведучого часу для визначення найточнішого джерела синхронізації в мережі. Такий пристрій стає ведучим, а всі інші пристрої в мережі – ведені й підбудовують свій синхрогенератор по ведучому пристрою.

Різниця в часі між ведучим і веденим пристроями є комбінацією зсуву відліку часу та затримки передачі синхронізуючого повідомлення. Тому корекція часового зрушення повинна виконуватися у два етапи: обчислення затримок передачі та зрушення, а потім їх корекція. При розгляді послідовності синхронізації часу двох пристроїв становиться очевидним, що ведучий пристрій починає корекцію зрушення часу, використовуючи повідомлення Sync і Follow-up. У повідомленні Follow-up вказується час відправлення повідомлення Sync (T_{M1}), обмірюване найбільше близько до середовища передачі для мінімізації помилки в часі опорного джерела. Після того, як ведений пристрій одержує перші повідомлення Sync і Follow-up, воно використовує свій синхрогенератор для оцінки часу прибуття повідомлення Sync (T_{S1}) та порівнює дану оцінку з тією, що прийшла від ведучого пристрою в повідомленні Follow-up. Різниця між цими двома мітками відбиває зрушення часу T_0 плюс затримку передачі повідомлення від ведучого пристрою до веденого ΔT_{MS}: $T_{S1} - T_{M1} = T_0 + \Delta T_{MS}$.

Для обчислення часу затримки передачі повідомлення й зрушення відліку часу ведений пристрій відправляє повідомлення Delay_request зі своїм часом T_{S2}. Ведучий пристрій відзначає прибуття даного повідомлення та відправляє у відповідь повідомлення Delay_response міткою T_{M2}. Різниця між двома мітками – це затримка передачі від веденого пристрою до ведучого ΔT_{SM} мінус зрушення у відліку веденого пристрою: $T_{M2}-T_{S2}=\Delta T_{SM}-T_0$.

При обчисленні затримки передачі повідомлення ухвалюється, що середня затримка передачі даних у каналі рівна середньому арифметичному затримок поширення в різні сторони каналу: $\Delta T = (\Delta T_{MS} + \Delta T_{SM})/2$. Знаючи час T_{S1}, T_{M1}, T_{M2} і T_{S2}, ведений пристрій обчислює усереднену затримку поширення в каналі передачі даних: $\Delta T = (T_{S1} - T_{M1}) + (T_{M2} - T_{S2})/2$.

Фінальна синхронізація часу виконується після відправлення ведучим пристроєм другого набору повідомлень Sync (T_{S3}) і Follow-up (T_{M3}). Ведений пристрій обчислює зрушення свого часу по формулі $T_0 = T_{S3} – T_{M3} – \Delta T$.

Після цього ведений пристрій підбудовує свій синхрогенератор відповідно до обчислених значень. Оскільки опорні джерела синхронізації в кожному пристрої нестабільні, а затримки в каналі можуть мінятися згодом, необхідно періодично повторювати корекцію часу веденого пристрою.

Більшість реалізацій PTP мають відхилення менше 1 мкс, однак реальна точність роботи залежить від додатка. Протокол PTP у пристроях реалізують трьома способами: програмним, програмно-апаратним та апаратним. Програмні реалізації PTP дозволяють передавати сигнали синхронізації з точністю порядку 100 мкс. Щоб досягти більш високої точності, необхідно використовувати апаратні засоби. Кожний компонент, який обробляє пакет PTP після його одержання з фізичного середовища передачі, збільшує помилку синхронізації. Програмна частина вносить найбільшу помилку, оскільки завантаження процесора й затримка, пов’язана з обробкою переривання, впливають на швидкість обробки запиту синхронізації. При програмно-апаратної реалізації найбільш чутливі функції протоколу, такі як запис часової мітки PTP-пакету, реалізуються на фізичному рівні Ethernet [8], наприклад, в окремій мікросхемі програмувальної логіки. Такі методи сьогодні найбільш оптимальні, тому що вимагають не занадто багато ресурсів і часу на розробку пристрою, дозволяючи добитися точності порядку 20 нс. У випадку ж повної апаратної реалізації [9] протоколу PTP досяжна точність порядку 10 нс.

Таким чином, протокол PTP є альтернативним способом синхронізації мереж, який може одержати поширення у відомчих мережах NGN. У порівнянні із засобами синхронізації, які використовуються в наш час, даний спосіб має ряд переваг: 1). Не потрібен доступ устаткування прямо до стику синхронізації PRC, що дозволить оптимізувати витрати на побудову мережі. При цьому протокол PTP може забезпечити передачу синхронізації із субмікросекундною точністю, досяжна стабільність краще, чим 1 ppm; 2). На відміну від адаптивного способу, для відновлення синхронізації необхідний високостабільний опорний генератор тільки в ведучому пристрої; 3). Для вирішення задач синхронізації можна використовувати асинхронний канал з порівняно невеликою пропускною здатністю, що значно зменшує вартість реалізації. Бажано, щоб цей канал був виділеним.

ЛІТЕРАТУРА

1. Брени С. Синхронизация цифровых сетей связи: Пер. с анг. – М.: Мир, 2003. – 456 с.

2. ITU-T G.8261/Y.1361 Timing and synchronization aspects in packet networks. – ITU_T, April 2008.

3. Rodrigues S. Technology options for sync delivery in Next Generation Networks. – 3rd International Telecom Sync Forum, 17 – 19 October 2005.

4. Телегин С.А. Применение TDMoIP мультиплексирования для передачи данных в транспортных сетях GSM. – Нелинейный мир, 2007, т.5, №5, с. 270 – 271.

5. Телегин С.А. Протокол PTP для синхронизации сетей NGN. Вопросы применения. – Первая миля, 2009. №5-6, с. 20 – 23.

6. IEEE Std. 1588–2008 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. – IEEE, July 2008.

7. IETF RFC1305 Network Time Protocol (Version 3). Specification, Implementation and Analysis. – IETF, March 1992.

8. Tan E. IEEE 1588 Precision Time Protocol Time Synchronization Performance. Application Note 1728. – National Semiconductor, October 2007.

9. Hamdi M. Neagoe T. A Hardware IEEE-1588 Implementation with Processor Frequency Control. – Arrow Electronics, August 2006.

10. Stein Y., Schwartz E. Circuit Extension over IP: The Evolutionary Approach to Transporting Voice and Legacy Data over IP Networks. – RAD Data Communications, 2008.

Вакуленко О.В. (ВІТІ ДУТ)
Османов Р.Н. (ВІТІ ДУТ)
Явіся В.С. (ВІТІ ДУТ)

СИНХРОНІЗАЦІЯ МЕРЕЖ NGN ВІДОМЧОГО ПРИЗНАЧЕННЯ

Розвиток телекомунікаційних технологій і мереж передачі даних поступово приводить до побудови на відомчих мережах конвергентних мереж наступного покоління (NGN – Next Generation Networks). Основна відмінність таких мереж від традиційних мереж із синхронною цифровою ієрархією (SDH) – у них для магістральної передачі даних поряд зі звичайними синхронними каналами використовуються такі асинхронні технології, як Ethernet (Gigabit Ethernet, 10 Gigabit Ethernet). Головною вимогою до мереж наступного покоління є одночасна передача голосу, відео та даних по єдиній мережі.

При переході від традиційних мереж передачі даних, заснованих на часовому мультиплексуванні, до мереж NGN особлива увага приділяється передачі сигналів синхронізації. Синхронізація встаткування необхідна в першу чергу для безпомилкової передачі даних реального часу – голосу та відеозображень.

Оскільки в мережах Ethernet використовується комутація пакетів, яка в силу статистичних властивостей поширення пакетів даних по асинхронних каналах передачі порушує спочатку синхронізований потік даних, тому передача синхронізації в мережах NGN відомчого призначення виділяється в окреме завдання.

Для передачі синхронних даних по мережах з комутацією пакетів, як правило, використовується емуляція каналів з часовим мультиплексуванням, що полягає в інкапсуляції синхронних даних в UDP-датаграми й наступнім їхньому відновленні на вузлі призначення. Для безпомилкового відновлення переданих даних на стику асинхронного та синхронного каналів устаткування також повинне одержувати синхросигнал. Вимоги до стабільності синхросигнала варіюються залежно від конкретного призначення мережі передачі даних. Так, в операторських мережах по наданню послуг телефонії й доступу в Інтернет вимоги до синхронізації є досить м'якими – 50 ppm (одиниць на мільйон), а в стільникових мережах для безшовного переходу мобільних абонентів від однієї базової станції до іншої необхідна стабільність 50 ppb (одиниць на мільярд).

У рекомендації ITU-T G.8261 [2] розглянуто три основні способи відновлення синхронізації на границях транспортного середовища з комутацією пакетів при передачі в ній групового сигналу з часовим мультиплексуванням у вигляді послуги емуляції каналів. Вони наступні:

синхронізація від єдиного опорного джерела. Для цього в кінцевому станційному устаткуванні повинні бути передбачені функції міжмережевої взаємодії. Усі абоненти транспортного середовища з комутацією пакетів можуть одержувати тактову частоту від мережі синхронізації за допомогою звичайного централізованого розподілу;

синхронізація від обладнання часового ущільнення з використанням єдиної опорної частоти. Абонентське встаткування працює на власній тактовій частоті і тому на границі мережі з комутацією пакетів її відновлюють різними відносними способами, наприклад, за допомогою алгоритму узгодження швидкостей SRTS.

адаптивна синхронізація. Використовується коли користувачі послуг (абоненти) не пред'являють високих вимог до синхронізації кінцевого обладнання або коли побудова мережі синхронізації (або використання стиків синхронізації) на відомчій мережі неможлива чи небажана.

При застосуванні перших двох способів синхронізації у вузлі міжмережевої взаємодії повинен бути доступ до стику з генератором первинної синхронізації (PRC). Для цього на мережі відомчого призначення необхідно або будувати окрему мережу синхронізації, або орендувати її в існуючих операторів транспортної мережі SDH. При цьому, також існує

безліч прикладів локальної синхронізації встаткування. Так, наприклад, у станційному приміщенні розміщують недороге джерело первинної синхронізації (PRS) на основі GPS і розподіляють від нього тактову частоту за допомогою безпроводових технологій або по звичайних виділених кабелях, у фізичному середовищі Ethernet, а також за допомогою інших оригінальних схем [3].

При застосуванні адаптивного способу не має потреби у власній мережі синхронізації. Як показують результати проведених досліджень [4], що адаптивний спосіб можна застосовувати, якщо абонент не пред'являє строгих вимог до стабільності своєї тактової частоти, а якщо ні, то необхідно додаткове апаратне згладжування відновленого синхросигналу. Альтернативою адаптивному методу є використання протоколу RTP при інкапсуляції даних з часовим мультиплексуванням у пакети асинхронних даних. Як показали експерименти, у цьому випадку при високій стабільності відновленого синхросигналу встаткування виявляється слабочутливим до зміни частоти джерела синхронізації, що є необхідним, наприклад, при переході на резервний синхросигнал.

Для якісної роботи відомчої мережі, побудованої за концепцією NGN, необхідно забезпечити реалізацію одного із способів синхронізації. Вибір способу залежить від основних вимог, які висуваються до відомчих мереж. Ці вимоги достатньо жорсткі та потребують певних системних рішень, які тягнуть за собою збільшення вартості побудови та експлуатації мережі. Тому для зменшення витрат доцільно застосувати реалізацію синхронізації мережі на основі наступних принципів:

ядро мережі синхронізувати за способом синхронізації від єдиного опорного джерела (будувати самостійно або орендувати у Укртелекома);

периферію мережі за способом адаптивної синхронізації (використовувати сучасні протоколи такі, як PTP).

ЛІТЕРАТУРА

1. Брени С. Синхронизация цифровых сетей связи: Пер. с анг. – М.: Мир, 2003. – 456 с.

2. ITU-T G.8261/Y.1361 Timing and synchronization aspects in packet networks. – ITU_T, April 2008.

3. Rodrigues S. Technology options for sync delivery in Next Generation Networks. – 3rd International Telecom Sync Forum, 17–19 October 2005.

4. Телегин С.А. Применение TDMoIP мультиплексирования для передачи данных в транспортных сетях GSM. – Нелинейный мир, 2007, т.5, №5, с. 270 – 271.

5. Телегин С.А. Протокол PTP для синхронизации сетей NGN. Вопросы применения. – Первая миля, 2009. №5 – 6, с. 20 – 23.

6. IEEE Std. 1588–2008 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. – IEEE, July 2008.

7. IETF RFC1305 Network Time Protocol (Version 3). Specification, Implementation and Analysis. – IETF, March 1992.

8. Tan E. IEEE 1588 Precision Time Protocol Time Synchronization Performance. Application Note 1728. – National Semiconductor, October 2007.

9. Hamdi M. Neagoe T. A Hardware IEEE-1588 Implementation with Processor Frequency Control. – Arrow Electronics, August 2006.

10. Stein Y., Schwartz E. Circuit Extension over IP: The Evolutionary Approach to Transporting Voice and Legacy Data over IP Networks. – RAD Data Communications, 2008.

Васильців А.А.(ВІТІ ДУТ)
к.т.н. Хусаінов П.В.(ВІТІ ДУТ)

ОЦІНКА КІЛЬКОСТІ ДЕФЕКТІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ МЕТРИК СКЛАДНОСТІ

Програмне забезпечення сучасних ІС є доволі складним продуктом, в створенні якого можуть приймати участь десятки і сотні спеціалістів. Велика кількість спеціалістів називають велику складність сучасного ПЗ ключовим фактором виникнення програмних дефектів. Зі зростом складності і кількості дефектів ПЗ збільшуються розміри втрат у випадку відмов і залежність безпосередніх користувачів ІС від її безвідказної роботи.

На сьогодні має місце проблема достовірності і точності характеристики ПП в плані наявності програмних дефектів. Тому розробка моделей і методик оцінки кількості дефектів ПП являється актуальною науково-технічною задачею, рішення якої дозволить отримати достовірну характеристику рівня безпеки початкового тексту цільових програм кібернетичного впливу, спланувати необхідні ресурси для усунення дефектів, підвищити ефективність процесу розробки і експлуатації ПП.

Апріорні моделі оцінки кількості дефектів використовуються на етапі розробки до початку тестування і експлуатації ПП. Для оцінки кількості дефектів апріорні моделі використовують показник кількості рядків програмного коду (Lines of Code – LOC). LOC-оцінка являється найбільш простою і поширеною метрикою розміру ПП(Метрика ПП визначається як міра, яка дозволяє отримати численне значення деякої властивості ПЗ. Певний вид програмної складності кількісно виражається значенням оцінки по конкретному виду метрики). Як відомо, наявні апріорні моделі оцінки кількості дефектів Гафнії і Акіямі були вже досліджені на предмет достовірності і точності оцінки кількості дефектів і, як показали дослідження вони несли доволі грубу похибку.

Зниження рівня дефектів в сучасному ПЗ пояснюється прогресом методів, засобів і технологій програмної інженерії, збільшенням степені повторного використання бездефектного коду, можливістю сучасних систем розробки генерувати бездефектний код. Тому ці моделі втратили свою актуальність, їх оцінка не є достовірною.

Фізичний розмір ПЗ у вигляді LOC-оцінки не містить інформації про його складність, тому були запропоновані нові моделі, які б змогли дати більш точні кількісні характеристики ПЗ. Велика кількість дослідників відмічає високу кореляцію між складністю програми, частими помилками і низькою надійністю. Для кількісної оцінки складності ПЗ розроблено десятки різних метрик складності. Наявні моделі складності ПО засновані на припущенні, що кількість дефектів може бути вирахувана з допомогою метрик складності, оскільки чим складніша програма тим вища вірогідність помилки програміста при її написанні.

Найбільш відомою і класичною являється система метрик Холстеда, на основі якої було розроблено метрики МакКейба, Джилба і Чепіна, метрику фірми TRW, яка використовує багатофакторну модель складності – вона враховує складність керівної логіки програми, складність взаємних зв’язків, складність обчислень, складність операцій введення/виведення, читабельність ПЗ, коефіцієнт кореляції кількості дефектів з поточним показником складності. Але і дана метрика не враховує повторного використання бездефектного коду та інших факторів різного плану.

В зрізі інформаційної безпеки і кібернетичного впливу на потенційно-небезпечні дефекти реакції програм пропоную включити в дані моделі складову аналізу програмного коду на предмет коректності організації поведінки на критичних ділянках та слідування рекомендаціям щодо використання функцій стандартних бібліотек задля збереження цілісності адресного простору потенційно-вразливого ПЗ. Це пропоную реалізувати за допомогою аналізу попередньо створеного абстрактного синтаксичного дерева коду, абстрактного сематичного, графу потоку виконання, графу потоку даних.

д.т.н. Вишнівський В.В. (ВІКНУ)
к.т.н. Кузавков В.В. (ВІТІ ДУТ)
Редзюк Є.В. (ВІТІ ДУТ)

ТЕРМОГРАФІЯ ЯК ЗАСІБ ПАСИВНОГО КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ РАДІОЕЛЕКТРОННИХ СХЕМ

Кожен етап життєвого циклу радіоелектронних схем (РЕС) потребує контролю технічного стану. Контроль бажано здійснювати без втручання в процес функціонування системи не руйнуючи вихідний матеріал та в реальному часі. Кожен метод неруйнівного контролю має свої особливості проведення. У статті викладені можливості застосування теплового методу неруйнівного контролю для визначення технічного стану радіоелектронних систем.

Неруйнівний контроль (НК) – це контроль, який не руйнує [1]. Під словом „контроль" мається на увазі вимір значень робочих параметрів і властивостей об'єкта та їх перевірка на відповідність допустимим величинам. „Неруйнівний" означає „не вимагає демонтажу або зупинки роботи об'єкта, не припускає безпосереднього втручання в досліджуване середовище".

Методи, за допомогою яких реалізується НК, називаються методами неруйнівного контролю (далі МНК).

Серед існуючих МНК (магнітний, електричний радіохвильовий оптичний радіаційний акустичний) тепловий МНК є найбільш інформативним та оперативнім методом проведення контролю та оцінки технічного стану РЕС. Інтерес до теплового МНК обумовлений його універсальністю, високою продуктивністю і безпекою обслуговування апаратури (на відміну від таких методів неруйнівного контролю, як, наприклад, рентгенівський або радіаційний).

Теплові МНК в якості пробної (несучої інформацію) енергії використовують теплову енергію, що поширюється на об'єкті контролю. Температура як кількісний показник внутрішньої енергії тіл є універсальною характеристикою об'єктів і процесів фізичного світу, в якому безперервно відбувається генерація, перетворення, передача, накопичення і використання енергії в її різних формах. Аналіз теплових процесів (температурних полів, втрат тепла тощо) дозволяє отримати різноманітну інформацію про стан об'єктів і протіканні фізичних процесів у різних областях діяльності.

Основний інформативний параметр теплових МНК – різниця температур між бездефектними і дефектними областями об'єкта. Температура може вимірюватися контактним і безконтактним методом. Залежно від характеру взаємодії контрольованого об'єкту і теплової енергії розрізняють активний і пасивний методи теплових МНК. Для діагностики РЕС найбільш актуальний пасивний метод МНК. При використанні пасивного методу (його називають методом власного випромінювання) реєструють теплові потоки працюючих об'єктів, ставлячи у відповідність місцям підвищеного нагріву несправності і дефекти.

За сформованою до теперішнього часу термінологією під термографами розуміють метод аналізу просторового і часового розподілу теплової енергії (температури) у фізичних об'єктах, що супроводжується, як правило, побудовою теплових зображень (**термограм**) [2].

Термографія як засіб пасивного ТК (цей напрямок ще називають тепловою діагностикою) визнана вже протягом тривалого часу в більшості розвинених країн світу.

Якісно новим етапом розвитку ТК є формування таких напрямків, як теплова **дефектометрія і томографія**. На відміну від дефектоскопії, що ставить своєю задачею виявлення (виявлення) дефекту, метою дефектометрії є визначення параметрів дефекту за експериментальними даними з використанням алгоритмів розв'язання обернених задач.

Теплова томографія націлена на отримання просторового зображення внутрішньої структури об'єкта як розподілу за координатами його теплофізичних характеристик.

Опис процесу визначення технічного стану радіоелектронних систем.

Термографічний аналіз – метод, при якому інфрачервона камера або пристрій використовується для фотографування температур поверхні деталі машини або всього обладнання, заснований на випущенні випромінювання з поверхні об'єкту. Термографічний аналіз є безконтактним і детальним засобом моніторингу стану електричного і електромеханічного устаткування [3].

Головне завдання термографії – відстеження інфрачервоного теплового випромінювання від об'єкта. Розвиток цієї технології полягає у відповіді на відмінності між температурами на поверхні об'єкта та їх відображенням в чорно-білих або кольорових зображеннях, які відображаються на моніторі, РК-екрані або телевізорі [3]. Ці зображення, або термограми, можуть бути копійовані, сфотографовані або записані для подальшого аналізу картин отримання або віддачі тепла.

Термографічний аналіз – ефективний засіб попереджувального обслуговування.

Розвиток термографії та обґрунтування методології технічної діагностики РЕС

Використання безконтактних засобів моніторингу стану електричного і електромеханічного устаткування зручно в силу наступних причин [3]:

– контакт між поверхнями виключено;

– безпечно для навколишнього середовища;

– стійкість до магнітного шуму ;

– допустимо застосування у вибухонебезпечному середовищі ;

– передає інформацію в реальному часі ;

– надійно завдяки практично необмеженому терміну служби.

Таблиця 1 показує список станів, що виявляються при теплової оцінці.

Відображення можливостей вимірювання

Таблиця 1

Несправності електричних та електронних систем	*Температура*
Відмови заземлення, ізоляція	X
Струморозподілювачі, щітки і контакти	X
Запобіжники, реле, розподільний пристрій, трансформатори, нещільності з'єднань, перевантаження і незбалансоване навантаження	X
Окремі компоненти РЕС, електронні плати, ТЕЗи	X

Таким чином, використовуючи тепловий МНК для моніторингу стану електричного і електромеханічного устаткування е можливість побудови універсальної високо продуктивної та безпечної автоматизованої системи діагностування технічного стану РЕС.

ЛІТЕРАТУРА

1. Стороженко В.А., Малик С.Б. Применение термографии для контроля тепловых режимов печатных плат/ „Техническая диагностика и неразрушающий контроль", Киев, № 1, 2007, стр. 28 – 31.

2. ГОСТ 16504-81 „Система державних випробувань продукції. Випробування і контроль якості продукції. Основні терміни та визначення" №5297 (зі змінами від 10.10.2003 р.) – К.: Держспоживстандарт України, 2003. – (Національний стандарт України).

3. Стороженко В.А.Термография в диагностике и неразрушающем контроле/ Стороженко В.А., Маслова В.А.. – Харьков: Компания СМИТ. – 2004. – 160 с.

к.т.н. Волков О.В. (ВІТІ ДУТ)
Волкова Ю.О. (РТФ НТУУ „КПІ”)

ОЦІНКА ЕФЕКТИВНОСТІ РАДІОМЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ЩОДО УСУНЕННЯ ВПЛИВУ РАДІОЗАВАД

При веденні сучасних військових конфліктів сформувалась стійка тенденція до радіоелектронного впливу на системи управління військами (зброєю) противника, успішність якого значною мірою забезпечується ефективним використанням радіозавад. Тому оцінка ефективності функціонування радіомереж спеціального призначення (РМСП) щодо можливості усунення впливу радіоперешкод є важливим завданням на етапах розробки, виробництва та розгортання сучасних радіомереж спеціального призначення так і оцінки та приведення у відповідність вимогам забезпечення інформаційного обміну вже існуючих РМСП.

Ефективності функціонування РМСП щодо усунення впливу радіозавад визначається багатьма факторами, головними з яких є рівень технічної оснащеності та структурної побудови РМСП та складністю завдань виявлення засобів радіоелектронної боротьби та визначення їх технічних можливостей. В цьому випадку кількісною оцінкою ефективності функціонування РМСП може служити величина $Z_{\text{завад}}$, що визначається відношенням кількості усунутих випадків дії радіозавад $S_{\text{усун}}$ до загальної кількості випадків застосування радіозавад $S_{\text{завад}}$ з врахуванням часових (нормативних) термінів виконання заходів протидії [1]. Величину $Z_{\text{завад}}$ можливо визначити за формулою

$$Z_{\text{завад}} = \sum_{r=1}^{R} \frac{T_{\text{норм}_r}}{T_{\text{усун}_r}} \cdot \frac{S_{\text{усун}_r}}{S_{\text{завад}_r}},$$

де R – загальна кількість радіотехнологій, які використовуються для створення РМСП та для яких виконуються заходи по усуненню впливу завад;

$T_{\text{норм}}$ – часові (нормативні) терміни виконання заходів протидії одинокому випадку радіозавад для r–ї радіотехнології,

$T_{\text{усун}}$ – час, що затрачений на усунення одиночного випадку радіозавад для r–ї радіотехнології.

У випадку $T_{\text{норм}} > T_{\text{усун}}$ перевищує 1, то значення даного відношення приймається рівним 1.

Узагальнена оцінка ефективності функціонування РМСП може бути проведена на основі часткових коефіцієнтів, тобто завдання „вагових” коефіцієнтів, що враховують різний вклад часткових показників. В зв’язку з значною евристичністю значень „вагових” коефіцієнтів визначення узагальненої оцінки ефективності функціонування РМСП потребує визначення характеристик засобів радіоелектронної боротьби противника, стратегій їх застосування, а також, можливості впливу на засоби РМСП, що створені з використанням радіотехнологій.

В зв’язку з апріорною невизначеністю в застосуванні противником стратегій та засобів радіоелектронної боротьби в оцінці ефективності функціонування РМСП, показник $Z_{\text{завад}}$ неможливий для визначення потенційних можливостей РМСП по нівелюванню випадків застосування завад противником без використання методів прогнозування і має стати предметом подальших досліджень.

ЛІТЕРАТУРА

1. Слободянюк П.В., Благодатний В.Г. Радиомониторинг: вчера, сегодня, завтра (Теория и практика построения системы радиомониторинга) / Под общ. ред. П.В. Слободянюка. – Прилуки: ООО „Издательство „Аір-Поліграф”, 2010. – 296 с.

Волощук А.В. (ВІТІ ДУТ)
д.т.н. Самохвалов Ю.Я. (ВІТІ ДУТ)

ПІДСИСТЕМА ОРГАНІЗАЦІЇ НАВЧАЛЬНОЇ СТРАТЕГІЇ ІНТЕЛЕКТУАЛЬНОЇ КОМП'ЮТЕРНОЇ ТРЕНАЖЕРНОЇ СИСТЕМИ НАВЧАННЯ

На сьогоднішній день підготовка висококваліфікованих кадрів є актуальною задачею для будь-якої організації або установи. Сучасний навчальний процес складно уявити без використання комп'ютерних підручників, тренажерів, лабораторних практикумів, тестуючих, контролюючих та інших комп'ютерних систем навчання. Одним з перспективних напрямків розвитку комп'ютерних систем навчання є розробка інтелектуальних комп'ютерних тренажерних систем навчання (ІКТСН), що для свого проектування використовують методи та засоби штучного інтелекту (ШІ).

ІКТСН складається з трьох підсистем – підсистеми конструювання навчально-тренажних задач, тренажно-імітаційної підсистеми та підсистеми інтерфейсу. Кожна з підсистем тісно взаємодіє одна з одною, використовуючи для цього модуль організації і управління навчальною стратегією.

Для організації роботи підсистеми конструювання навчально-тренажних задач та тренажно-імітаційної підсистеми використана продукційна модель представлення знань. Вона отримала найбільше поширення серед інших моделей представлення знань.

Продукційна модель або модель, заснована на правилах, дозволяє представити знання у вигляді виразів типу „ЯКЩО (умова), ТОДІ (дія)".

Під „умовою" (антецедентом) розуміється деякий вираз-зразок, по якому відбувається пошук в базі знань, а під „дією" (консеквентом) – дію, виконувану при успішному результаті пошуку (вони можуть бути проміжними, виступаючими далі як умови, і термінальними або цільовими, які завершують роботу системи.

При використанні продукційної моделі база знань складається із набору правил. Програма, яка керує перебором правил, називається машиною виводу. В ІКТСН її роль виконує тренажно-імітаційна підсистема.

Машина виводу (інтерпретатор правил) виконує дві функції: по-перше, перегляд існуючих фактів із робочої пам'яті (бази даних) і правил із бази знань і додавання (по мірі можливості) в робочу пам'ять нових фактів, і по-друге, визначення порядку перегляду і застосування правил. Цей механізм керує процесом консультації, зберігаючи для користувача інформацію про отримані висновки, і запитує у нього інформацію, коли для спрацювання чергового правила в робочій пам'яті знаходиться недостатньо даних.

Інтерпретатор продукцій працює циклічно. В кожному циклі він переглядає всі правила, щоб виявити те, умова якого співпадає з відомими на даний момент фактами із робочої пам'яті. Після вибору правило спрацьовує, його висновок заноситься в робочу пам'ять, і потім цикл повторюється знову.

Для забезпечення максимальної інформативності і об'єктивності результатів контролю було запропоновано впровадити в логіку роботи модулю конструювання програмної логіки навчально-тренувальної задачі ІКТСН *адаптивні алгоритми*.

Запропонований алгоритм оцінки рівня засвоєння навчального матеріалу за результатами практичної роботи в інтелектуальній комп'ютерній тренажерній системі навчання підвищує якість підготовки спеціалістів з інформаційних технологій за рахунок інтеграції адаптивних моделей теорії *IRT*, що визначає наукову новизну роботи.

Відмінністю запропонованого рішення від існуючих є застосування методів параметричної моделі IRT для визначення ступеня засвоєння навчального матеріалу та методу збалансованості М. Челишкової для вирішення завдання калібровки коефіцієнтів тестових завдань.

Волянюк І.І. (ВІТІ ДУТ)
к.т.н. Правило В.В. (ВІТІ ДУТ)

НАПРЯМИ ВДОСКОНАЛЕННЯ ВІДОМЧИХ ТРАНСПОРТНИХ МЕРЕЖ ЗВ'ЯЗКУ

На сьогоднішній день ні одна із силових структур України, у тому числі і Збройні Сили України, крім окремо реалізованих фрагментів телекомунікаційної мережі, не має єдиної стаціонарної мережі, що охоплює всю територію України.

Тому на даний час війська зв'язку орендують канали зв'язку у комерційних структур, таких як „Укртелеком".

Вони мають достатню ефективність, але не задовольняють сучасним вимогам захищеності та не являються рентабельними для нас на сьогоднішній день.

З метою вирішення цієї проблеми та задля забезпечення Збройних Сил України надійними та швидкісними каналами зв'язку, необхідне створення стаціонарної транспортної телекомунікаційної мережі Збройних Сил України.

Одним із шляхів реалізації проекту являється розгортання на території України волоконно-оптичних систем передачі та оптичного кабелю. Враховуючи ситуацію обмеженого фінансування і високих вимог до проектованої мережі, одним з ефективних варіантів є використання технології WDM та її різновидів.

Застосування WDM технології при побудові мережі, в першу чергу диктується необхідністю збільшення ефективності використання оптичного волокна без збільшення його фізичної кількості. Темпи зростання обсягів переданої інформації призводять до швидкого зниження запасів „вільного" волокна.

У деяких випадках багато утворених каналів повністю задіяні і фізичне збільшення ємності оптичного волокна практично неможливе.

Швидке впровадження нових телекомунікаційних сервісів можливе тільки за рахунок збільшення ємностей оптичного волокна, тобто використання систем спектрального ущільнення (CWDM або DWDM). Але крім цієї, існують й інші причини використання в основі відомчої телекомунікаційної мережі CWDM або DWDM.

По-перше, це необхідність передачі високошвидкісних сигналів, таких як 10 G Ethernet на великі відстані (близько 100 км і більше), оскільки дальність сучасних широкосмугових XFP трансиверів обмежена через хроматичну дисперсію.

По-друге, застосування WDM дозволяє використовувати функції швидкого відновлення на рівні оптичної, а не пакетної IP/Ethernet мережі.

По-третє, з'являється можливість реалізації довільної топології мережі поверх WDM. Наприклад, організація топології зірка між Ethernet комутаторами.

Ще одна можливість надається WDM простота і швидкість нарощування ємності мережі в майбутньому. Це дуже важливий момент! Критерії оцінки WDM систем при її виборі простота, гнучкість, надійність і ціна (яка набуває особливої актуальності зараз, у часи економічних труднощів).

Таким чином, запропоноване впровадження технології WDM дозволить передавати цифрову інформацію по існуючим каналам зв'язку у більших об'ємах, на більших швидкостях та з підвищеною захищеністю, а також підвищити ефективність передачі інформації в умовах мирного часу та особливого періоду.

Воробйов А.О. (ВІТІ ДУТ)
к.т.н. Макарчук О.М. (ВІТІ ДУТ)

ЗАДАЧА ДІАГНОСТИКИ ЯКОСТІ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Останнім часом спостерігається значне зростання кількості комп'ютерних мереж. Таке зростання провокує прояву факторів, які впливають на якість їх функціонування. Будь-яка організація, яка дбає про надійність та стійкість своєї комп'ютерної мережі, повинна вчасно діагностувати такі систем. Тому доцільно розглянути деякі фактори, які впливають на якість функціонування мережі:

1. Прямий доступ до пам'яті: дані безпосередньо передаються з буфера плати мережного адаптера в пам'ять комп'ютера, не зачіпаючи при цьому центральний процесор.
2. Розділювана пам'ять адаптера (*shared memory*): плата мережного адаптера має власну оперативну пам'ять, яку вона використовує спільно з комп'ютером. Комп'ютер сприймає цю пам'ять як частину власної.
3. Розділювана системна пам'ять: процесор плати мережного адаптера використовує для обробки даних частину пам'яті комп'ютера.
4. Управління шиною: до плати мережного адаптера тимчасово переходить керування шиною комп'ютера. Без використання ЦП плата передає дані безпосередньо в системну пам'ять комп'ютера. При цьому підвищується продуктивність комп'ютера, оскільки його процесор в цей час може вирішувати інші завдання. Подібні плати досить дороги, але вони здатні підвищити продуктивність мережі на 20-70%. Архітектури *EISA*, *MCA* і *PCI* підтримують цей метод.
5. Буферизація: для більшості плат мережного адаптера сучасні швидкості передачі даних по мережі занадто високі. Тому на платі мережного адаптера встановлюється буфер за допомогою мікросхем пам'яті. У разі, коли плата приймає даних більше, ніж здатна обробити, буфер зберігає дані до тих пір, поки вони не будуть оброблені адаптером. Буфер підвищує продуктивність плати, не даючи їй стати вузьким місцем системи. Розмір буфера істотно варіюється від одного виробника мережевих адаптерів до іншого. Зазвичай мережеві плати мають буфер, що вміщає один або кілька повних кадрів. У цьому випадку мережева плата не перериває роботу процесора в момент, коли вона може почати передачу.
6. Вбудований мікропроцесор: з таким мікропроцесором платі мережного адаптера для обробки даних не потрібна допомога комп'ютера. Більшість мережевих плат має свої мікропроцесори, які збільшують швидкість мережевих операцій звільнивши ЦП від виконання функцій з підтримки протоколів канального рівня. Потужний мікропроцесор може забезпечити функції щодо встановлення з'єднань і безпомилкової передачі даних, істотно розвантаживши ЦП сервера. У *PCI* системах це не дає помітного виграшу в продуктивності, оскільки вони не орієнтовані на паралельну обробку даних декількома швидкими контролерами шини, якими є ЦП, дискова і відео підсистеми.
7. Сервери: з серверами пов'язана значна частина мережевого трафіку, тому вони повинні бути обладнані платами мережного адаптера з найбільшою продуктивністю.
8. Робочі станції: робочі станції можуть використовувати менш дорогі мережеві плати, якщо їх робота з мережею обмежена додатками, генеруючими невеликий обсяг мережевого трафіку (наприклад, текстовими процесорами). Інші програми (наприклад, бази даних або інженерні програми) досить швидко перенавантажуватимуть мережеві плати, що не відповідають їх вимогам. Слід зазначити, що приведені не всі фактори, які потребують особливої уваги. А з подальшим розвитком комп'ютерних мереж, їх кількість стрімко зростає. Таким чином, перспективними стають системи діагностики та контролю комп'ютерних мереж, які будуть сучасними та значно підвищують рівень надійності, що є особливо важливим для військових систем.

Восколович О.І. (ВІТІ ДУТ)
к.т.н. Бортнік Л.Л. (АСВ)

РОЗРОБКА БЛОКУ ОЦІНКИ СТАНУ КАНАЛІВ ЗВ'ЯЗКУ ДЛЯ СТРУКТУРНОЇ СХЕМИ ВІЙСЬКОВИХ БАГАТОАНТЕННИХ РАДІОЗАСОБІВ З ППРЧ

При проектуванні і розробці перспективних військових засобів радіозв'язку (ЗРЗ) невід'ємним етапом є розробка їх структурних схем [1].

Схема приймально-передавального пристрою програмованої радіостанції із MIMO та ППРЧ побудована за схемою із пристроєм аналізу стану каналу на приймальному боці. Така побудова дозволяє здійснювати контроль завадозахищеності з урахуванням характеристик каналу зворотнього зв'язку. Наявність зворотнього зв'язку при передачі повідомлень дозволяє здійснити послідовну процедуру аналізу стану каналу, а також дає можливість одержати на передавальній стороні дані про стан завадозахищеності програмованої радіостанції із MIMO та ППРЧ [2].

Блок виявлення та оцінки характеристик каналу зв'язку функціонує згідно методу ітеративної оцінки стану каналів зв'язку системи MIMO [3].

Сутність методу полягає в оцінці відношення значення сигнал-завада в каналах системи MIMO та параметра канальних характеристик в основних алгоритмах декодування турбокодів з використанням ітеративного принципу декодування.

Алгоритм реалізації методу складається з етапів визначення дисперсії завад, розрахунку параметру канальних характеристик, обчислення рекурсій, обчислення вихідного логарифмічного відношення функцій правдоподібності, перевірки необхідності ітеративної оцінки. Як критерій ефективності розробленого методу використовується точність оцінювання, яку можна кількісно виразити нормованим середньоквадратичним відхиленням, визначеним в дБ. Новизна розробленого методу полягає в введенні допоміжної процедури розрахунку дисперсії завад з використанням ітеративного принципу декодування та інформації про логарифмічне відношення функції правдоподібності про передані біти та врахуванні її в основних алгоритмах декодування турбокодів системи MIMO.

Слід зазначити, що оцінка каналу може проводитись для схеми, коли використовується один ТК для всіх каналів системи MIMO, так і для схеми, коли ТК використовується в кожному каналі системи MIMO. Запропонований метод дозволяє підвищити точність оцінки стану каналів зв'язку системи MIMO з ППРЧ та турбокодуванням до 0,3 дБ в порівнянні з відомими.

Перспективні програмовані радіостанції, що використовують розглянуту схему приймально-передавального пристрою програмованої радіостанції із MIMO та ППРЧ можуть бути реалізовані програмно-апаратним способом на ЦСП *ADSP*-21261 із плаваючою крапкою і пам'яттю 1Мб, тактова частота якого дорівнює 150 МГц.

Використання даної структурної схеми при розробці перспективних ПРС дозволить підвищити завадозахищеність засобів радіозв'язку тактичної ланки управління Збройних Сил України.

ЛІТЕРАТУРА

1. Шаров А. Н. Сети радиосвязи с пакетной передачей информации / А. Н. Шаров, В. А. Степанец, В. И. Комашинский; под ред. А. Н. Шарова. – СПб.: ВАС, 1994. – 216 с.

2. Восколович О. І. Методика управління параметрами радіозасобів MIMO з псевдовипадковою перестройкою робочої частоти / О. І. Восколович // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2011. – Вип. 2 – С. 21 – 27.

3. Патент на корисну модель 62638, МПК H03M 13/37. Пристрій ітеративної оцінки стану каналів зв'язку систем з технологією MIMO / Восколович О.І., Кувшинов О.В., Зайцев С.В.; заявл. 19.01.11; опубл. 12.09.11, Бюл. №17.

Галушко С.О. (УІТ МОУ)

ДОСВІД ЗБРОЙНИХ СИЛ США ЩОДО ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА: ДЕЯКІ УРОКИ ДЛЯ УКРАЇНИ

Питання розвитку форм та способів інформаційного протиборства займає важливе місце в діяльності органів військового управління збройних сил США на всіх рівнях. Зазначене в повній мірі підтверджує досвід збройних конфліктів сучасності, до участі в яких активно залучалися сили та засоби інформаційно-психологічної боротьби, що стали суттєвим чинником результатів збройного протистояння. При цьому заслуговує уваги те, що до проведення заходів інформаційного впливу на війська та населення противника активно залучалися не лише відповідні підрозділи та частини інформаційно-психологічних операцій Сил спеціальних операцій ЗС США, а й інші сили та засоби всіх видів збройних сил.

Одним з успішних прикладів ефективного впливу на особовий склад збройних сил та населення Республіки Ірак в операціях багатонаціональних сил проти цієї країни було активне розповсюдження на її території радіоприймачів, які були налаштовані на фіксовані частоти. Не маючи можливості вільного вибору цивільних радіостанцій для прослуховування та відчуваючи потребу в задоволенні „інформаційного голоду", іракці були змушені використовувати зазначені радіоприймачі.

Для Збройних Сил України в умовах створення та подальшого функціонування Системи забезпечення інформаційної безпеки є актуальним використання досвіду збройних сил провідних країн світу з зазначених питань, у т.ч. в частині щодо застосування технічних засобів для виконання завдань інформаційного протиборства.

Можна прогнозувати, що у випадку виникнення прикордонного збройного конфлікту або іншої кризової ситуації воєнного характеру на території нашої держави буде порушена критична інформаційна інфраструктура, що значно зменшить або навіть унеможливить трансляцію в тих чи інших регіонах держави передач українського радіо- та телемовлення.

Відповідно, населення держави в зазначених районах буде значно обмежене в можливості отримувати достовірну ситуацію про події в державі та навколо неї. Крім того, будуть зменшені можливості щодо інформування населення про загрозу або виникнення надзвичайних подій природного/техногенного характеру, які можуть бути спричинені в результаті збройного конфлікту. Цілком очевидно, що антидержавні деструктивні сили будуть намагатися використати такий „інформаційний вакуум" для поширення інформаційно-психологічного впливу антиукраїнського спрямування.

Таким чином, існує проблема щодо відсутності у розпорядженні центральних та місцевих органів влади, Збройних Сил України ресурсів (сил та засобів), за допомогою яких в короткий термін може бути створена система керованого надання інформації та оповіщення населення в тому чи іншому регіоні (районі кризової ситуації).

Для вирішення зазначеної проблеми є доцільним використання досвіду ЗС США, про який йшла мова вище в частині щодо розповсюдження серед населення та використання радіоприймачів, які налаштовані на фіксовані частоти.

При цьому розглядаються три взаємопов'язані складові: залучення техніки радіозв'язку військових частин та підрозділів Збройних Сил України для розгортання мереж радіомовлення на визначеній території; завчасне замовлення, закупівля та утримання на зберіганні для використання в умовах особливого періоду (правового режиму надзвичайного стану тощо) необхідної кількості радіоприймачів з частотним діапазоном, який може приймати передачі військових радіостанцій. У випадку виникнення необхідності – їх оперативне розповсюдження серед користувачів; завчасна та оперативна підготовка інформаційних матеріалів.

Таким же чином, але вже іншого спрямування можна вести радіомовлення на населення суміжної держави у випадку виникнення конфлікту з нею.

Слід зазначити, що реалізація запропонованого варіанту застосування окремих технічних засобів для виконання завдань інформаційного протиборства є доцільною з огляду на потребу в мінімальних фінансових та інших ресурсах на його реалізацію.

Гізун Ю.В. (ВІТІ ДУТ)
к.т.н. Горбенко В.І. (ВІТІ ДУТ)
Мужеський К.К. (ВІТІ ДУТ)

МОДУЛЬ АВТОМАТИЧНОГО СКАНУВАННЯ ІНФОРМАЦІЙНОЇ МЕРЕЖІ

Для успішного адміністрування мережі необхідно знати стан кожного її елемента з можливістю змінювати параметри його функціонування. Зазвичай мережа складається з пристроїв різних виробників, і керувати нею було б нелегким завданням, якби кожне з мережевих пристроїв розуміло тільки свою систему команд.

Сьогодні *SNMP* є найпопулярнішим протоколом управління різними комерційними, університетськими і дослідницькими об'єднаними мережами. Діяльність по стандартизації, пов'язана з *SNMP*, триває в міру того, як постачальники розробляють і випускають сучасні прикладні програми управління, що базуються на *SNMP*.

Основною концепцією протоколу є те, що вся необхідна для керування пристроєм інформація зберігається на самому пристрої, сервері, модемі або маршрутизаторі – у так званій адміністративній інформаційній базі (*MIB - Management Information Base*).

Використовуючи даний підхід до вирішення проблем адміністрування було розроблено модуль автоматичного сканування, робота якого значно полегшить адміністрування інформаційної мережі. В основу роботи програмного модуля покладено зчитування інформації з елементів інформаційної мережі за допомогою протоколу *SNMP*.

За допомогою програмного модулю, посилаючи запити за протоколом *SNMP*, відображено інформацію про стан кожного із елементів мережі, яка записана в інформаційній базі (*MIB*), та порівнюються із записами, що знаходяться в базі даних на сервері, де зберігаються дані про інформаційну мережу.

Даний програмний модуль забезпечує автоматичне оновлення записів в базі даних або додавання нових, та зменшення помилок при ручному заповненні полів в базі даних, враховуючи людський фактор.

Для додавання відомостей про новий елемент або оновлення інформації про вже існуючий, необхідно внести *IP* – адресу та *community* – пароль для певного елементу інформаційної мережі. Після цього з легкістю можемо додати всю інформацію з самого пристрою до бази даних.

Програмний модуль, що керований протоколом *SNMP*, складаються з двох невід'ємних ключових компонентів:

– керований пристрій;

– система мережевого управління (*Network Management System, NMS*) – програмне забезпечення, що взаємодіє з програмним модулем для підтримки комплексної структури даних, що відбиває стан мережі.

Даний програмний модуль взаємодіє з *MIB*, що описують структуру керованих даних на підсистемі пристроїв, вони використовують ієрархічний простір імен, що містить ідентифікатори об'єктів (*OID*-и). Кожен *OID* визначає змінну, яка може бути зчитана або встановлена за допомогою *SNMP*.

Як висновок, розроблений програмний модуль з використання протоколу *SNMP* та власною базою даних *(MIB)* є достатнім для вирішенням задач адміністрування. Його використання надасть з легкістю маніпулювати даними про стан елементів інформаційної мережі, робота програмного модулю автоматично порівнює дані в інформаційній базі *(MIB*), на самому пристрої та в базі даних, де знаходиться вся інформація про елементи інформаційної мережі.

Головін А.Ю. (в/ч К–1410)
к.т.н. Головін Ю.О. (ІСЗЗІ)

КАНАЛИ ПРИХОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ В МЕРЕЖАХ TCP/IP

Глобальна мережа Інтернет та більшість сучасних локальних мереж та мереж спеціального призначення функціонують на базі протоколів *TCP* та *IP*. При розробці архітектури протоколів враховувались наступні фактори: можливість майбутнього зростання об'єму інформаційних потоків, неоднорідності характеристик системи передачі, застосування глибоко розгалуженої топології мережі тощо. Але при цьому не було приділено достатньої уваги питанням забезпечення безпеки інформації в мережі, зокрема проблемі несанкціонованої передачі інформації прихованими каналами.

В загальному випадку, під терміном „прихований канал" (*covert channel*) передачі розглядається комунікаційний канал, у якому інформація передається в такий спосіб (або напрям), який заздалегідь не був передбачений для передачі [4]. Таким чином, канал називається прихованим, якщо він не проектувався і не передбачався для передачі інформації в електронній системі обробки даних.

Згідно критеріїв стандарту *TCSEC* [3] виділяють 2 типи прихованих каналів:

– приховані канали по пам'яті, коли системи взаємодіють між собою оперуючи із даними (доповнення, модифікація), що передаються [1, 2];

– приховані канали по часу – системи взаємодіють між собою кодуючи інформацію шляхом використання часових затримок [2].

При організації прихованого каналу по часу приймач (*receiver*) і передавач (*sender*) узгоджують часовий інтервал (*timing interval*) та початковий відлік часу. Під час кожного часового інтервалу передавач передає пакет даних або не передає його. Приймач відслідковує часові інтервали і в залежності від того прийшов пакет від передавача (подія відповідає бінарній 1) чи ні (подія відповідає бінарному 0) декодує повідомлення. Прихований канал по пам'яті організовується використовуючи службові поля *IP* та *TCP* пакетів, а також поля із даними протоколів верхніх рівнів (*DNS, HTTP, FTP* та ін.). Несанкціонована передача інформації через мережу, використовуючи приховані канали може здійснюватися шляхом встановлення спеціального несанкціонованого програмного закладення або за допомогою осіб, що мають доступ до в середину організації (інсайдери).

В роботі розглянуті основні характеристики прихованих каналів передачі інформації обох типів.

Характеристика	**Канали по пам'яті**	**Канали по часу**
Прихованість	Задовільна	Відмінна
Ефективна швидкість передачі	Добра	Задовільна
Завадостійкість	Відмінна	Задовільна

Проаналізувавши наведені характеристики прихованих каналів були виділені основні особливості їх функціонування та можливого застосування тих чи інших методів прихованої передачі інформації у мережах спеціального призначення, а також наведено основні сценарії їх використання.

ЛІТЕРАТУРА

1. R.A. Kemmerer – A Practical Approach to Identifying Storage and Timing Channels: Twenty Years Later. – Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC'02). – IEEE, 2002.

2. S. Cabuk , C.E. Brodley , C. Shields – IP Covert Timing Channels: Design and Detection. – Proceedings of the CCS'04. – ACM, 2004.

3. 5200.28-STD, Trusted Computer System Evaluation Criteria (Orange Book).

4. http://www.nestor.minsk.by/sr/2003/01/30111.html.

к.т.н. Головін Ю.О. (ІСЗЗІ)
Павелко Є.І. (ІСЗЗІ)

АЛГОРИТМИ ПОПЕРЕДЖЕННЯ ПЕРЕВАНТАЖЕННЯ В СУЧАСНИХ МАРШРУТИЗАТОРАХ

У зв'язку із збільшення обсягу обміну інформації в інформаційно-телекомунікаційних мережах, в тому числі і в мережах спеціального призначення збільшується ризик додаткового навантаження на мережі, що призводить до перевантаження та значного зменшення пропускної здатності мережі, аж до виникнення колапсу, результатом якого є втрата інформації. Для зниження ймовірності виникнення перевантажень та колапсів мережі в сучасних пристроях маршрутизації використовуються алгоритми попередження перевантажень. В роботі проаналізовано найбільш розповсюджені алгоритми попередження перевантажень, а саме *Tail Drop* („відкидання хвоста"), метод випадкового раннього виявлення – *RED* (*Random Early Detection*) [1], та похідні від нього – *ARED* і *WRED*, метод справедливих (зважених) черг – *WFQ* (*Weighted Fair Quiuing*) [2], а також метод випадкового експотенціального маркування – *REM* (*Random Expotential Marki*ng). Результати показують (табл.1), що при використання механізму Drop Tail значні втрати через переповнення буфера припадають на короткі HTTP з'єднання, а при використання активних методів управління TCP з'єднання мають незначні втрати. Механізм RED допускає найменші загальні втрати. Алгоритми A-RED і RED при правильному налаштуванні здатні поліпшити якість передачі пакетів.

Значення параметрів якості для різного трафіку в залежності від методу обслуговування черги

Таблиця 1

Алгоритм	Трафік FTP		Трафік CBR/UDP		Трафік HTTP		
	Втрати пакетів, %	Середня швидкість, Мбіт/с	Втрати пакетів, %	Затримка/ джиттер, мсек	Втрати пакетів, %	Тривалість сесії: середня/ СКЗ	Середня швидкість, Мбіт/с
RED	0,12	11,7	3,1	260/5,8	0,63	1,44/3,3	3,15
A-RED	0,2	11,7	3,3	265/5,7	0,89	1,48/3,5	3,15
Drop Tail	2,52	11,7	2,9	348/5,4	3,5	1,89/3,8	3,28

Серед пристроїв компанії *Cisco* було проаналізовано маршрутизатори серії *Catalyst* 29xx… 35xx, які підтримують алгоритми управління чергами *WRED*, *Strict Priority*, *Shaped Round Robin*, а також магістральні маршрутизатори *Cisco* серій 7000 та 12000, *Huawei* серії S57xx, в яких кожний порт підтримує до восьми черг і широкий набір алгоритмів управління чергами: *WRR, DRR, SP, WRR+SP* і *DRR+SP*, завдяки чому гарантується висока якість передачі даних. Огляд алгоритмів попередження перевантаження, що використовуються в операційних системах маршрутизаторів та комутаторів відомих виробників (*Cisco*, *HP* та *Huawei*) дозволяє зробити наступні висновки: застосування адаптивних методів маршрутизації дозволяє в деякій мірі прогнозувати виникнення черг, але не гарантують стовідсоткову протидію перевантаженням мережі; повністю дослідити алгоритм попередження перевантаження досить важко, оскільки є велика кількість факторів, що впливають на результати моделювання різні сценарії моделювання та початкові умови, різні мережеві конфігурації і передача різної за об'ємом та призначенням інформації, тощо.

ЛІТЕРАТУРА

1. Ningning Hu, Liu Ren, Jichuan Chang: A Comparison of Active Queue Management Algorithms Using OPNET Modeler – Course Project Report for *15-744* Computer Networks

2. G.F. Ali Ahammed, Reshma Banu: Analyzing the Performance of Active Queue Management Algorithms – International journal of Computer Network & Communications (IJCNC),Vol.2, No2, March 2010.

Головко Д.О. (ВІТІ ДУТ)
к.т.н. Сілко О.В. (ВІТІ ДУТ)

МОДЕЛЬ МАНДАТНОГО РОЗМЕЖУВАННЯ ДОСТУПУ ДЛЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ СУПРОВОДУ НАВЧАЛЬНОГО ПРОЦЕСУ

Основною проблемою інформаційних систем супроводу навчального процесу (ІС СНП) є розподіл прав доступу. Права доступу до інформації – сукупність встановлених правовими документами чи власниками інформації правил, що регламентують порядок і умови доступу суб'єкта до інформації. Права доступу визначають набір прав (читання, запис, виконання), дозволених суб'єктам (наприклад, користувачам системи) дій над об'єктами даних. Аналіз сучасних ІС СНП показав, що в більшості з них застосовується контроль прав доступу на рівні типів об'єктів системи. Такий механізм реалізується розробником ІС СНП в коді програми. Перспективним вважається застосування в ІС СНП мандатного управління доступом, для якого обов'язкове виконання наступних умов:

– всі суб'єкти і об'єкти повинні бути однозначно ідентифіковані;

– заданий лінійно упорядкований набір позначок таємності ;

– кожному об'єкту системи привласнена позначка таємності, яка визначає рівень таємності в ІС;

– кожному суб'єкту системи привласнена позначка таємності, яка визначає рівень довіри до нього в ІС, яка визначає рівень доступу до об'єкта.

Для аналізу систем захисту з мандатним розмежуванням доступу пропонується застосувати класичну модель Белла-Лападула. Формальний опис моделі: S – множина суб'єктів ІС СНП, O – множина об'єктів ІС СНП, $S \subset O$; $R = \{r, w\}$ – множина прав доступу, r – доступ суб'єкта ІС СНП на читання об'єкта, w – доступ на запис; $L = \{U, SU, S, TS\}$ – множина рівнів таємності, U – нетаємно, SU – для службового користування, S – таємно, TS – цілком таємно; $\wedge = (L, \leq, \bullet, \otimes)$ – решітка рівнів таємності, де: $\leq$ – оператор, який визначає часткове відношення порядку для рівнів таємності; $\bullet$ – оператор найменшої верхньої межі, $\otimes$ – оператор найбільшої верхньої межі; V – множина станів системи у вигляді набору упорядкованих пар (F, M), де: $F : S \cup O \to L$ функція рівнів таємності, яка ставить у відповідність кожному об'єкту і суб'єкту в системі певний рівень таємності; M – матриця поточних прав доступу.

Оператор відношення „$\leq$" має такі властивості:

$\forall \alpha \in L : \alpha \leq \alpha$ – рефлективність, означає, що між суб'єктами та об'єктами одного рівня безпеки передача інформації дозволена;

$\forall \alpha_1, \alpha_2 \in L : ((\alpha_1 \leq \alpha_2) \& (\alpha_2 \leq \alpha_1)) \to \alpha_2 = \alpha_1$ – анти симетричність, означає, що якщо інформація може передаватися від суб'єктів і об'єктів рівня *A* до суб'єктів і об'єктів рівня *B*, так і від суб'єктів і об'єктів рівня *B* до суб'єктів і об'єктів рівня *A*, то ці рівні еквівалентні;

$\forall \alpha_1, \alpha_2, \alpha_3 \in L : ((\alpha_1 \leq \alpha_2) \& (\alpha_2 \leq \alpha_3)) \to \alpha_1 = \alpha_3$ – транзитивність, означає, що якщо інформації може передаватися від суб'єктів і об'єктів рівня *A* до суб'єктів і об'єктів рівня *B*, і від суб'єктів і об'єктів рівня *B* до суб'єктів і об'єктів рівня *C*, то вона може передаватися від суб'єктів і об'єктів рівня *A* до суб'єктів і об'єктів рівня *C*.

Оператор найменшої верхньої границі $\bullet$ визначається наступним відношенням:

$$\alpha = \alpha_1 \bullet \alpha_2 \Leftrightarrow (\alpha_1, \alpha_2 \leq \alpha) \& (\forall \alpha' \in L : (\alpha' \leq \alpha) \to (\alpha' \leq \alpha_1 \vee \alpha' \leq \alpha_1)).$$

Оператор найбільшої нижньої межі „$\otimes$" визначається наступним відношенням:

$$\alpha = \alpha_1 \otimes \alpha_2 \Leftrightarrow (\alpha \leq \alpha_1, \alpha_2) \& (\forall \alpha' \in L : (\alpha' \leq \alpha_1 \,\&\, \alpha' \leq \alpha_1) \to (\alpha' \leq \alpha)).$$

Виходячи з визначення цих двох операторів можна показати, що для кожної пари $\alpha_1, \alpha_2 \in L$ існує єдиний елемент найменшої верхньої межі і єдиний елемент найбільшою нижньої межі. Система $\Sigma = (\nu_0, R, T)$ в моделі Белла-Лападули складається з наступний

елементів: ν_0 – початковий стан системи; R – множина прав доступу; $T: V \times R \to V$ – функція переходу, яка в ході виконання запитів переводить систему з одного стану в інший.

Визначення стану згідно моделі: Стан безпеки ν називається досяжним в системі $\Sigma = (\nu_0, R, T)$, якщо існує послідовність $\{(r_0, \nu_0), \ldots, (r_{n-1}, \nu_{n-1}), (r_n, \nu_n)\}: T(r_i, \nu_i) = \nu_{i+1} \forall_i = = 0, n-1$. Початковій стан (F, N) називається безпечним за читанням, якщо для кожного суб'єкта, що здійснює в цьому стані доступ до об'єкта, рівень безпеки суб'єкта домінує над рівнем безпеки об'єкта: $\forall_s \in S, \quad \forall_0 \in O, \quad r \in M[s, o] \to F(o) \le F(s)$. Стан системи *(F, M)* називається безпечним по запису у разі, якщо для кожного суб'єкта, що здійснює в цьому стані доступ по запису до об'єкта, рівень безпеки об'єкта домінує над рівнем безпеки суб'єкта: $\forall_s \in S, \quad \forall_0 \in O, \quad w \in M[s, o] \to F(s) \le F(o)$.

Стан *(F, M)* називається безпечним, якщо воно безпечне за читанням та записом. Система $\Sigma = (\nu_0, R, T)$ називається безпечною, якщо її початковий стан ν_0 безпечний, і всі стани, досяжні з ν_0 шляхом застосування кінцевої послідовності запитів з *R* безпечні.

Таким чином, всі елементи, що входять до складу ІС СНП, поділені на дві категорії – суб'єкти та об'єкти. Кожному суб'єкту присвоюється свій рівень доступу. Аналогічно, об'єкту присвоюється рівень таємності. Перехід між станами ІС СНП описується функціями переходу. ІС СНП знаходиться в безпечному стані в тому випадку, якщо у кожного суб'єкта є доступ тільки до тих об'єктів, до яких дозволений доступ на основі поточної політики безпеки. Для визначення, чи має суб'єкт права на отримання певного виду доступу до об'єкта, рівень таємності суб'єкта порівнюється з рівнем таємності об'єкта, і на основі цього порівняння вирішується питання, надати чи ні запитуваний доступ. Набори рівень доступу рівень секретності описуються за допомогою матриці доступу.

Запропонована модель мандатного розмежування доступу розширює можливості користувачів ІС СНП призначення. За рахунок цього з'являється можливість максимально природним чином обмежити область дії наданих користувачеві повноважень. Це дозволяє зменшити необхідну кількість ролей і спростити схеми доступу до об'єктів ІС СНП. Розроблене програмне забезпечення дозволяє створювати легку в адмініструванні політику безпеки для ІС СНП.

ЛІТЕРАТУРА

1. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. – Р.: Феникс, 2008. С. 40 – 44.

2. Девянин П.Н. Модели безопасности компьютерных систем: Учебное пособие для студентов высших учебных заведений. – М.: Издательский центр „Академия", 2005. С. 55 – 66.

3. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агентства „Яхтсмен", 1996. С 52 – 55.

4. А.П. Баранов, Н.П. Борисенко, П.Д. Зегжда, А.Г. Ростовцев, Корт С.С. – Математические основы информационной безопасности. – М.: Издательство Агентства "Яхтсмен", 1997. С 22 – 36.

к.т.н. Горбенко В.І. (ВІТІ ДУТ)
Вовкогон О.О. (ВІТІ ДУТ)
Картавих В.Ю. (ВІТІ ДУТ)

МЕТОД ПОБУДОВИ ГРАФУ БАЗИ ІНФОРМАЦІЇ УПРАВЛІННЯ МЕРЕЖЕВОГО ЕЛЕМЕНТУ ІНФОРМАЦІЙНОЇ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

З розвитком мережевих технологій з'являються нові задачі щодо управління інформаційними мережами. Чим складнішою є технологія тим складнішим являється організація управління нею. Тобто в наш час актуальною темою являється вирішення задач щодо якісної організації управління мережою. Одною з основних складових управління мережою являється моніторинг даної мережі.

Інформаційна мережа військового призначення будується на основі стеку протоколу TCP/IP в зв'язку з цим стандартом для моніторингу цих мереж дефакто став протокол моніторингу SNMP. Параметри, що доступні для збору за допомогою визначеного протоколу, розміщуються в базі інформації управління (Management Information Base – MIB).

MIB складається з модулів, які в свою чергу описуються в текстововому документі, з чітко визначеним синтаксисом в якому описані об'екти MIB.

Для побудови системи моніторингу мережевого елементу необхідно використовувати інформаційну модель мережевого елементу, яка містить динамічні параметри мережевого елементу.

При побудові інформаційної моделі мережевого елементу необхідно побудувати граф-дерево об'єктів,що містяться в базі інформації управління даного елемента враховуючи структуру MIB модулів та всіх залежностей які в ньому відображаються, а також типів даних об'єктів. Подальша обробка граф-дерева MIB дозволяє отримати інформаційну модель мережевого елемента

Метод побудови граф-дерева об'єктів складається з двох етапів .

Перший етап :полягає в пошуку залежностей між MIB модулями, та побудова орієнтованого графа залежностей між цими модулями,а також побудова графа наслідування типів параметрів.

Даний етап реалізовується шляхом аналізу структури файлів MIB модулів. В кожному описовому файлі, який поданий як текстовий файл, містяться посилання на інші модулі, у випадку коли даний модуль будь-яким чином використовує їх об'єкти . Тобто при аналізу всіх вкладень MIB файлу можливо побудувати граф залежностей між модулями.

Всі параметри які описані в MIB модулях поділяються на три множини по типам, та типи які в них містяться. Необхідно визначити ці множини по типам. Множини визначаються трьома основними типами, які можуть уточнюватися шляхом створення типів нащадків або текстовим представленням. Дана процедура можлива за умови детального та структурованого аналізу всіх параметрів об'єктів які представлені у текстовому вигляді.

Другий етап: Після проведення аналізу MIB файлів , який здійснюється починаючи від аналізу кореневих модулів до нижнього рівня модулів, та побудови вищезазначених графів , будується загальний граф бази інформації управління мережевого елементу.

В доповіді детально описується алгоритм методу, та наводиться приклад його застосування.

Таким чином для побудови граф–дерева бази інформації управління здійснюється в два етапи, на першому етапі необхідно проаналізувати залежності між MIB модулями та наслідування типів об'єктів в MIB модулях, та побудувати відповідні графи. На другому етапі будується загальний граф бази інформації управління мережевого елементу на основі результатів першого етапу.

Ієрархічний граф всіх типів параметрів буде використаний при побудові інформаційної моделі мережевого елементу.

к.т.н. Горбенко В.І. (ВІТІ ДУТ)
Картавих В.Ю. (ВІТІ ДУТ)
Бандура А.В. (ВІТІ ДУТ)

МЕТОДИКА ПОБУДОВИ ІНФОРМАЦІЙНОЇ МОДЕЛІ МЕРЕЖЕВОГО ЕЛЕМЕНТУ

Інформаційна мережа військового призначення будується на основі стеку протоколів *TCP/IP*. Для здійснення моніторингу мережевих елементів застосовується *SNMP* протокол. Параметри, що доступні для збору за допомогою визначеного протоколу, розміщуються в базі інформації управління (*MIB*). Інформація управління елементами мережі описується в міжнародних стандартах і рекомендаціях Інженерної ради Інтернету (*IETF ISOC*). Вони є обов'язковими для всіх виробників телекомунікаційного обладнання та програмного забезпечення. Це забезпечує єдиний підхід до структури *MIB* для будь-якого мережевого елементу.

Для забезпечення масштабованості *MIB* розділяється на модулі. Кожний модуль має чітку деревовидну структуру і унікальний ідентифікатор під'єднання до загальної MIB. Завдяки цьому, незалежно від множини підтримуємих модулів, *MIB* будь-якого мережевого елементу об'єднується в єдину деревовидну структуру, яку можна представити у виді граф-дерева. Основа дерева єдина для будь-яких мережевих елементів і затверджена відповідними стандартами.

Кожна вершина дерева має свою унікальну символічну назву та номер, який ідентифікує вершину серед усіх вершин, які виходять з старшої вершини. Для ідентифікації вершини в усьому дереві використовується ідентифікатор об'єкту(*OID*), що визначає послідовність вершин від кореня дерева до відповідної вершини. *OID* може представлятися, як послідовністю символічних назв вершин розділених через крапку, так і через послідовність номерів вершин. Виходячи з аналізу структури дерева *MIB*, задачею методики побудови інформаційної моделі мережевого елементу є визначення множини об'єктів дерева *MIB*, що динамічно змінюються на протязі роботи мережевого елементу на основі існуючих формалізованих описів піддерев *MIB*, апаратних характеристик мережевого елементу і його конфігурації. Формалізовано задача представляється наступним чином: первинні дані методики, обмеження моделі, кінцеві дані методики.

Виходячи з аналізу структури дерева *MIB* і синтаксису представлення *MIB* модулів, побудова інформаційної моделі мережевого елементу складається з двох етапів. Перший етап забезпечує автоматичну обробку дерева MIB.

Другий етап являє собою обробку кінцевих даних першого етапу на основі конфігураційних параметрів і тактико-технічних характеристик певного мережевого елементу.

Першочерговим кроком автоматичного етапу побудови інформаційної моделі мережевого елементу є крок побудови дерева *MIB*. При аналізі кожного із існуючих модулів визначаються: залежності між модулями, множина модулів, яких не вистачає для побудови дерева, множину макросів, які використовуються в кожному модулі.

Отже, у зв'язку з залежністю кількості динамічних параметрів від конфігураційних і тактико-технічних характеристик мережевого елементу вирішення задачі побудови інформаційної моделі лише в автоматичному режимі неможливе.

Тому, для отримання інформаційної моделі слід застосовувати методи експертного оцінювання. Використання автоматичного етапу обробки, дозволяє зменшити початкові дані для експертної оцінки.

к.т.н. Горбенко В.І. (ВІТІ ДУТ)
Картавих В.Ю. (ВІТІ ДУТ)
Гіль А.В. (ВІТІ ДУТ)

МОДУЛЬ МОНІТОРИНГУ КАНАЛІВ ПЕРЕДАЧІ ДАНИХ

На теперішньому етапі розвитку інформаційних систем Збройних сил України застосовуються передові технології та стандарти передачі даних: *Fast Ethernet* – набір стандартів передачі даних в комп'ютерних мережах по технології *Ethernet* зі швидкістю 100 Мбіт/с; *MPLS(multiprotocol label switching)* – механізм у високопродуктивній телекомунікаційній мережі, що здійснює передачу даних від одного вузла мережі до іншого за допомогою міток. Він є масштабованим та незалежним від будь-яких протоколів та процедур передачі даних. В мережі заснованій на *MPLS* пакетам даних присвоюються мітки, рішення про подальшу передачу пакету даних іншому вузлу мережі реалізується тільки на основі значення присвоєної мітки без необхідності вивчення самого пакета. За рахунок цього можливо створення віртуального каналу, незалежного від середовища передачі і застосовуючого будь-який протокол предачі даних; *HDSL(high data rate digital subscriber line)* – високошвидкісна цифрова абонентська лінія, може забезпечувати швидкість передачі даних відповідно за стандартами Т1 – 1,544 Мбіт/с та Е1 – 2 Мбіт/с, менші швидкості обслуговуються використанням 64 Кбіт/с каналів у середині Т1/Е1 пакету, через необхідність забезпечення симетричної передачі даних максимальна швидкість передачі даних забезпечується на відстані до 4,5 км; *E1* – європейська версія цифрової лінії зв'язку з часовим розділенням каналів, на відміну від американської Т1 (24 канали по 64 кбіт/сек) – Е1 має 32 канали кожен по 64 кбіт/сек, з яких 30 каналів використовуються для голосу або даних і 2 канали для сигналізації. Загальна пропускна спроможність 2,048 Мбіт/сек в повно-дуплексному режимі.

Для здійснення моніторингу каналів передачі даних пропонується застосовувати протокол *SNMP(simple network management protocol)* з додатковим використанням баз керуючої інформації – бази *MIB(management information base)*. Бази *MIB* описують структуру керованих даних на підсистемі пристрою, вони використовують ієрархічний простір імен, котрий містить ідентифікатори об'єктів – *OID(object id)*. Кожний *OID* визначає змінну, котра може бути зчитаною або встановлена за допомогою *SNMP*.

Провівши аналіз предметної області можна зробити висновок, що за своєю специфікою, усі параметри, занесені в базу керуючої інформації (*MIB*), поділяються на статичні, тобто фіксовані, які напряму визначаються або самою системою, або вводяться безпосередньо адміністратором системи, та динамічні, тобто ті, що змінюються в залежності від часу та впливу на систему внутрішніх або зовнішніх чинників. Моніторинг статичних параметрів являється недоцільною витратою програмних та людських ресурсів, а тому підсистема моніторингу каналів передачі даних має бути орієнтованою перш за все на збір динамічних параметрів, їх аналіз та графічне представлення адміністратору системи. Запропонована підсистема моніторингу каналів передачі даних дозволяє значно зменшити об'єм службової інформації, що циркулює в інформаційній системі, за рахунок зменшення кількості опитувань пристроїв за допомогою протоколу *SNMP*, та звернень до бази керуючої інформації.

У доповіді також розглядається типова структура бази керуючої інформації маршрутизатора та проводиться аналіз існуючих програмних реалізацій. Визначаються їх сильні та слабкі сторони а також основні динамічні параметри та функції, що дозволяють здійснювати повноцінний моніторинг каналів передачі даних на основі технології *Fast Ethernet*. Отримані результати пропонується реалізувати практично.

Гудзь С.М. (ЖВІ ДУТ)
к.т.н. Шуренок В.А. (ЖВІ ДУТ)

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ НА ЗАСТОСУВАННЯ ЗАСОБІВ РАДІОМОНІТОРИНГУ СИСТЕМ СУПУТНИКОВОГО ЗВ'ЯЗКУ

Аналіз використання систем супутникового зв'язку (ССЗ) показав, що постійно розширюється сфера їх використання, збільшується орбітальне угруповання космічних апаратів зв'язку, зростає кількість абонентів, що утруднює виконання завдань радіомоніторингу.

Однак на сьогоднішній день на постах радіомоніторингу ССЗ розподіл ресурсу на пошук та спостереження супутникових каналів виконується емпіричним методом, і тому залежить від досвіду та кваліфікації особи, що приймає рішення. Такий спосіб прийняття рішення не відповідає вимогам достовірності та своєчасності, крім того відбувається в умовах невизначеності стосовно відповідності супутникових каналів об'єктам радіомоніторингу, параметрів їх функціонування, режимів, інтенсивності роботи та інформативності.

Оскільки прийняття рішення на радіомоніторинг відбувається в умовах невизначеності, а темп зміни оперативної обстановки та завдань є високим, то актуальним є застосування алгоритмів прийняття рішення на планування на посту радіомоніторингу ССЗ, які ґрунтуються на теорії нечіткої логіки.

Підвищення достовірності своєчасного і правильного прийняття рішень на розподіл сил і засобів радіомоніторингу ССЗ можна реалізувати шляхом автоматизації процесу обробки інформації та формування рекомендацій, що приведе до зменшення часу на підготовку прийняття рішення.

Через велику кількість ССЗ охоплення їх усіх спостереженням практично не можливе. Тому при розподілі сил та засобів радіомоніторингу на спостереження для ефективного виконання завдань потрібно відібрати з них найбільш інформативні та цінні.

Критерієм відбору є показник важливості, що для ССЗ можливо описати системою частинних показників. Виходячи з аналізу літератури обрано наступні частинні показники, які необхідно враховувати при оцінюванні важливості каналів передачі даних під час ведення радіомоніторингу ССЗ: кут місця антени станції радіомоніторингу, ступінь втрат енергії сигналу за рахунок впливу атмосферних опадів; ступінь розкриття виду модуляції каналу, ступінь визначення несучої частоти каналу, ступінь визначення швидкості передачі каналу, ступінь визначення параметрів кодування каналу; ступінь доступу до смислової інформації, завантаженість каналу; ступінь пріоритетності завдання, в інтересах якого ведеться радіомоніторинг; ступінь змістовної інформаційної цінності каналу; ступінь оперативної цінності каналу.

Для визначення важливості каналів ССЗ запропоновано методику оцінювання важливості каналів передачі даних ССЗ, що заснована на використанні багаторівневого ієрархічного дерева нечіткого логічного висновку та сукупності нечітких логічних правил *якщо* <*вх.*> *то* <*вих.*>. Результатом застосування запропонованої методики є ступінь важливості каналу передачі даних ССЗ.

Для планування радіомоніторингу ССЗ розроблено методику розподілу сил та засобів поста радіомоніторингу ССЗ, що заснована на використанні методу нечіткого динамічного програмування. Застосування даного методу обумовлено використанням ступеню важливості каналу передачі даних ССЗ, що заданий у вигляді нечітких множин з відповідними функціями належності.

Описані методики пропонується реалізувати у вигляді інформаційної системи підтримки прийняття рішення, яку використовувати при плануванні роботи на постах радіомоніторингу ССЗ.

к.т.н. Гуржій П.М. (НЦЗІ ВІТІ ДУТ)
Гуржій І.А. (НЦЗІ ВІТІ ДУТ)

ОЦІНКА ЗАВАДОСТІЙКИХ ВЛАСТИВОСТЕЙ КОДОВИХ КОМБІНАЦІЙ

Для додаткового підвищення коефіцієнта стиску відеоданих у роботах [1 – 2] був запропонований метод стиску зображень на основі змішаного поліадичного кодування масивів довжин серій і кольорових координат. Проведемо оцінку завадостійких властивостей кодових комбінацій які були сформовані розробленим методом стиску, та порівняємо їх з існуючими методами стиску [3 – 4]. Розглянемо двійково-симетричний канал, що змінює в результаті дії завад значення переданого двійкового розряду на зворотне з імовірністю **p**, та зберігає це значення незмінним з імовірністю 1-**p**. Модель включає припущення про те, що помилки у двійкових розрядах виникають незалежно друг від друга. Для оцінки результатів впливу перешкод на правильність відновлення прийнятого зображення, ми також будемо використовувати двійково-симетричний канал (ДСК) .

При впливі перешкоди на зображення яке стиснуте розробленим методом відбувається два типи основних помилок: помилка типу „зсув” та помилка типу „забивання”. При цьому помилка типу „зсув” характерна для масивів довжин серій, у випадку виникнення даної помилки відбувається помилкове зменшення або збільшення довжини серії, що у свою чергу при відновленні початкового зображення веде до появи більшої (чи меншої відповідно) кількості елементів певного кольору. Однак оскільки вихідне зображення обробляється построчно, а масиви довжин серій L формуються для одного рядка, до складу одного масиву не можуть увійти елементи іншого рядка. Таким чином, якщо в масиві довжин серій L виникає помилка, вона веде до „зсуву” тільки в одному рядку вихідного зображення, не роблячи впливу на наступні рядки.

Помилка типу „забивання” характерна для масивів колірних координат C, у випадку виникнення даної помилки відбувається підміна кольору для деякої кількості елементів що входять у серію.

В ході експерименту також було з’ясовано, що поліадичні коди мають властивості самокорекції та локалізації. Властивість локалізації означає те, що розмір помилки (погрішності), при відновленні кодових комбінацій які піддалися впливу перешкод, не буде перевищувати верхньої та нижньої границі поліадичних чисел. Властивість самокорекції означає те, що певна кількість початкових елементів буде відновлена без помилок, таким чином відбувається локалізація кількості помилок.

ЛІТЕРАТУРА

1. Баранник В.В., Гуржій П.М. Полиадическое кодирование массивов длин серий в смешанной системе оснований // Авиационно-космическая техника и технология. – 2005. – Вип. 5 (21). – С. 47 – 51.

2. Баранник В.В., Гуржий П.М. Кодирование массивов цветовых координат в разностном полиадическом пространстве // Радіоелектронні і комп’ютерні системи. – 2005. – Вип. 1 (9). – С. 44 – 49.

3. Гуржий П.М., Процюк Ю.О., Петросян І.А., Криховецький В.Я. Аналіз можливостей зменшення кодового представлення статичних цифрових зображень // VI-й науково-практичний семінар [„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”], К.: ВІТІ НТУУ „КПІ”. – 20 жовтня 2011 року.

4. Ватолин В.И., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ – МИФИ, 2002. – 384 с.

5. Gonzalez, Rafael C; Woods, Richard E. Digital Image Processing, 2nd ed. – published by Pearson Education, Inc. publishing as Prentice Hall., 2002. – 793 p.

к.т.н. Гурський Т.Г. (ВІТІ ДУТ)
Постригань О.М. (ВІТІ ДУТ)
Волкова Ю.О. (РТФ НТУУ „КПІ”)

ЗАДАЧА ТЕРИТОРІАЛЬНО-КОДОВОГО ПЛАНУВАННЯ РАДІОМЕРЕЖІ З КОДОВИМ РОЗПОДІЛОМ КАНАЛІВ

Однією з найбільш перспективних для створення перспективних систем рухомого радіозв’язку (СРРЗ) є технологія кодового розподілу каналів (CDMA), що використовує сигнали з розширеним спектром і дозволяє багатьом абонентам одночасно працювати в одній загальній смузі частот. Розширення спектра відбувається за рахунок перемноження вузькосмугового інформаційного сигналу на псевдовипадкову послідовність (ПВП), що є унікальною для кожного абонента мережі. Безумовною перевагою систем з розширеним спектром для військових СРРЗ є, безумовно, висока завадозахищеність, що залежить від величини бази сигналу, характеристик ПВП та ін.

Визначальним при проектуванні мережі рухомого радіозв’язку з кодовим розподілом каналів є планування радіомережі, яке являє собою ітеративний процес з виконанням наступних кроків:

синтез структури мережі;

прогнозування напруженості поля сигналу в зоні дії мережі радіозв’язку;

аналіз зони обслуговування для кожного стільника та мережі в цілому;

оцінка внутрішньосистемної електромагнітної сумісності;

призначення частот і розподіл фазових зсувів ПВП;

аналіз функціонування мережі з урахуванням взаємних завад.

Часова та логічна послідовність дій при плануванні містить ряд етапів:

1) отримання вихідних даних;

2) уточнення математичної моделі розповсюдження радіохвиль на основі вимірювань напруженості поля в найбільш характерних точках зони обслуговування мережі;

3) побудова першого наближення радіомережі;

4) прив’язка ділянок розгортання базових станцій, визначених планом побудови мережі, до місцевості, і ітеративна оптимізація при широкому використанні програмного забезпечення, що підтримує функції синтезу мережі та аналізу експлуатаційних характеристик.

На результати планування істотний вплив здійснюють системні чинники, підсилюючи складність і неоднозначність рішення задачі синтезу мережі радіозв’язку, яка може бути сформульована як завдання пошуку такої мережі радіозв’язку S'', яка задовольняє вихідним вимогам (обмеженням), і володіє при цьому значенням сукупності (вектора) показників якості $\overline{K}(S'')$, найкращим в сенсі безумовного критерію переваги: $\overline{K}(S') \leq \overline{K}(S'')$.

Якщо виконується дана умова, то кожен з показників якості $k_i(S''),\ i=\overline{1,m}$ оптимізованої мережі S'' не гірше ніж у вихідній мережі S', в тому числі, щонайменше, один з цих показників якості краще, чим у мережі S'.

Успішно вирішити вище поставлене завдання синтезу мережі можна лише шляхом поєднання методів математичного синтезу, пов’язаного з істотною ідеалізацією мережі, з евристичним синтезом, під яким розуміється важкий творчий процес, що полягає у знаходженні задовільних рішень на основі використання накопичених даних та інженерного досвіду.

Таким чином, подальшим напрямком досліджень є розробка методики територіально-кодового планування радіомережі з кодовим розподілом каналів, призначену для проектування нових та розвитку існуючих мереж рухомого радіозв’язку.

Діянчук І.М. (ВІТІ ДУТ)
Клименко М.О. (ВІТІ ДУТ)

СПОСОБИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ЗОНДОВИХ МЕТОДІВ МАРШРУТИЗАЦІЇ В МОБИЛЬНИХ РАДІОМЕРЕЖАХ

Основною проблемою управління мобільними радіомережами (MANET) є маршрутизація інформаційних повідомлень. В умовах динамічної топології переважні зондові методи маршрутизації: DSR, AODV тощо.

Функціонування зондових методів маршрутизації (ЗММ) включає два основних етапи: побудова маршруту і його підтримка.

Основними недоліками ЗММ (на відміну від таблично-орієнтованих) є значний службовий трафік (хвильовий спосіб розсилки зондів-запитів) та затримка при побудові маршруту.

Для зменшення кількості зондів-запитів пропонується використовувати наступні способи: локальне зондування і селективний вибір вузлів для ретрансляції.

1. Локальне зондування – обмеження зони розсилки зондів граничним значенням числа ретрансляцій або обмеження геометричної відстані (координат зони розсилки при наявності системи позиціонування у вузлах).

На етапі побудови маршруту вузол може використовувати спосіб локального зондування k-раз із змінною глибиною ($TTL_1 = 2$, $TTL_2 = 4$, ..., $TTL_k = 2k$). Це вигідно в ситуації коли адресат знаходиться в декількох ретрансляційних ділянках від відправника. Однак даний спосіб може збільшити час побудови маршруту при значній відстані до адресата.

2. Селективний вибір вузлів для ретрансляції зондів за рахунок застосування різних хвильових алгоритмів передачі. Вибір конкретного ретранслятора визначатиме за різними правилами залежно від ситуації в мережі.

3. Побудова маршрутів (зондування) адресатом.

4. Навчання маршрутами та їх оптимізація.

5. Інтелектуалізація процесу побудови і підтримки маршруту.

Зменшення часу побудови (підтримання) маршруту може бути досягнуто наступними способами:

1. Двоетапна побудова адресатом маршруту заданої якості (Quality and Service). У цій ситуації для зменшення часу побудови адресату необхідно посилати зонд-відповідь на перший прийнятий зонд-запрос (навіть якщо отриманий маршрут не задовольняє необхідної якості) і після цього очікувати (обчислювати) маршрут заданої якості .

2. Попереджуюча побудова нового маршруту – прогнозування часу існування маршруту і випереджаюча побудова нового маршруту. Рішення про упереджувальну побудову нового маршруту може здійснюватися кожним проміжних вузлом в первинному маршруті або відправником.

3. Застосування багатопараметричної маршрутизації.

Проведені дослідження з використанням імітаційного моделювання показали, що розглянуті способи підвищення ефективності функціонування ЗММ дозволяють значно знизити обсяг службового трафіка (до 50 %) і скоротити час побудови (підтримання) маршрутів (в 2 – 3 рази).

Дука В.В. (ВІТІ ДУТ)
к.т.н. Нестеренко М.М. (ВІТІ ДУТ)

ОСНОВНІ ВИМОГИ ЩОДО ПОБУДОВИ ПАКЕТНИХ МЕРЕЖ НА БАЗІ NGN

Створення єдиної, ефективної, універсальної мультисервісної структури мережі за рахунок застосування „плоскої" архітектури із застосуванням технологій пакетної передачі голосової інформації, що служить основою для впровадження будь-яких послуг зв'язку в необхідній кількості і є шляхом еволюційного переходу від традиційних мереж з комутацією каналів до мереж з комутацією пакетів. До основних параметрів яким повинні задовольняти мультисервісні мережі наступного покоління *NGN(Next Generation Networks)* відносять:

– мультисервісність − незалежність технологій надання послуг від транспортних технологій;

– широкополосність − можливість гнучкого й динамічного змінювати швидкість передачі інформації залежно від потреби користувача;

– мультимедійність − здатність мережі одночасно передавати різноманітну інформацію;

– інтелектуальність − можливість управління послугою з боку оператора або користувача;

– доступність − можливість організації доступу до послуги незалежно від використовуваної технології доступу;

– мобільність − можливість отримання послуг незалежно від географічного місцезнаходження користувача;

– розподілене управління − термін виражає можливість участі декількох операторів у процесі надання послуги і поділ їх відповідальності відповідно до їх обласної діяльності.

Для побудови мультисервісної мережі необхідні наступні засоби:

– транспортні канали і протоколи, здатні підтримувати доставку інформації будь-якого типу (мова, відео, дані);

– обладнання доступу до такої мережі;

– різноманітні термінальні пристрої, тобто кінцеві пристрої мережі(комп'ютер).

До складу транспортної мережі *NGN* можуть входити наступні компоненти:

– транзитні вузли , що виконують функції переносу і комутації ;

– кінцеві (граничні) вузли, що забезпечують доступ абонентів до мультисервісної мережі;

– контролери сигналізації, що виконують функції обробки інформації сигналізації, управління викликами і з'єднаннями ;

– шлюзи, що дозволяють здійснити підключення традиційних мереж зв'язку.

Архітектура мереж *NGN* складається з *IP*-ядра і кількох мереж доступу, що використовують різні технології. Обмін інформацією між джерелом і пунктом призначення здійснюється по одному і тому ж принципу незалежно від виду з'єднання. Прикладний рівень логічно і фізично відділений від транспортного рівня, що дозволяє незалежно розвивати різні сегменти мережі. За різні послуги відповідають різні сервери, відокремлені від транспортного рівня. Для впровадження нової послуги необхідно додати новий сервер, який завдяки транспортному рівню стає доступним для всіх підключених до мережі користувачів.

Отже, основне завдання мереж нового покоління полягає в забезпеченні безперервної взаємодії існуючих і нових телекомунікаційних мереж, що підтримуються єдиною інфраструктурою для передачі будь-яких видів інформації. Основу мережі *NGN* становить універсальна транспортна мережа, яка реалізує функції транспортного рівня, рівня управління комутацією і передачею. Призначенням транспортної мережі являється надання послуг перенесення. Загальна інфраструктура NGN, що використовується для надання різних послуг реалізується на транспортному рівні, що заснований на пакетній технології.

Єрмолов В.В. (ВІТІ ДУТ)

АНАЛІЗ ПІДВИЩЕННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ ВОЛОКОННО-ОПТИЧНИХ ЛІНІЙ ЗВ'ЯЗКУ ВІДОМЧИХ МЕРЕЖ

Явища хроматичної та поляризаційної модової дисперсії в оптичному волокні ставлять обмеження на швидкість і дальність передачі сигналу. Для компенсації їх негативного впливу використовують різні методи компенсації: попереднє чірпування лазерного джерела, інверсію спектра в середині ділянки, волоконні браггівских решітки з постійною лінійною складовою що змінюється (чірпування), волокно з компенсацією дисперсії і пристрої компенсації дисперсії.

На відміну від однохвильових систем передачі, в системах WDM актуальною стає компенсація дисперсії не на одній довжині хвилі, а в робочому діапазоні довжин хвиль, так звана компенсація нахилу дисперсії.

Оптичні волокна транспортних мереж є анізотропним середовищем під впливом статичних і динамічних факторів (механічних спотворень), що призводить до різних швидкостей поширення поляризаційних складових і виникнення диференціальної групової затримки, та як наслідок, поляризаційної модової дисперсії. Основним завданням при створенні підсистеми моделювання оптичного волокна з двозаломленням було збереження адекватної залежності диференціальної групової затримки від довжини хвилі оптичної несучої, тому для опису поширення світла через такі структури було вибрано багатосегментну структуру волокна і модифікований метод Джонса, що полягає у визначенні матриць для кожного із сегментів, що характеризується азимутом і затримкою.

Створена підсистема моделювання оптичного волокна з двозаломленням використовує також методи статистичного моделювання, що дозволяє досліджувати залежність диференціальної групової затримки від еліпса поляризації вхідного сигналу, довжини хвилі оптичної несучої і ширини смуги випромінювання оптичного джерела, а кількість сегментів і їх параметри безпосередньо пов'язати з коефіцієнтом ПМД і довжиною оптичного волокна.

Нелінійні ефекти виникають через нелінійну залежність індексу рефракції матеріалу оптичного волокна від потужності сигналу, що ним передається, і можуть викликати шуми і спотворення оптичних імпульсів, що накладає обмеження на максимальну швидкість передавання і пропускну здатність ОВ, а також на довжину регенераційної ділянки.

Перехресна фазова самомодуляція (XPM) виникає тоді, коли потужність однієї хвилі, що поширюється у волокні, викликає зміну показника заломлення середовища поширення і призводить до самомодуляції фази іншої хвилі.

Чотирихвильове змішування FWM (Four-Wave Mixing) виникає в системах передавання зі спектральним ущільненням каналів і полягає у виникненні паразитних хвиль, що призводить до втрати потужності сигналу і виникнення паразитних впливів в інших каналах системи. Для реалізації адекватної моделі оптичної транспортної системи необхідно виміряти її характеристики і параметри, для чого були вибрані методики і розроблені схеми експериментів з вимірювання диференціальної групової затримки в широкому спектральному діапазоні і джиттера (фазового тремтіння), що має місце в системах такого класу, а також проведені вимірювання коефіцієнта бітової помилки. Результати вимірювань лягли в основу реалізації відповідних підсистем моделювання оптичних транспортних систем (ОТС), а також були використані для перевірки адекватності розробленої моделі.

Один із найефективніших методів аналізу параметрів цифрової системи передавання є ОКО-діаграма, тому саме цей метод і ліг в основу створення моделі ОТС. Запропонований метод дозволяє аналізувати як енергетичні, так і часові параметри цифрового сигналу.

Око-діаграмою є результат багатократного накладання бітових послідовностей, що відображається на екрані осцилографа у вигляді діаграми розподілу амплітуди сигналу в часі.

Показником якості цифрових систем передачі є коефіцієнт помилок BER. Робота цифрових систем передачі вважається нормальною тільки в тому випадку, якщо BER не перевищує певне допустиме значення, що відповідає використовуваному мережевому стандарту.

Для оцінки розподілу джиттера, що призводить до часового зсуву оптичних імпульсів, визначають точку синхронізації і зміщення імпульсів, що передавалися через послідовність пристроїв і оптичних волокон відносно цієї точки. В результаті отримуємо такі параметри джиттера, як його середньоквадратичне значення і максимальний розмах. Шляхом детальнішого аналізу отриманих значень можна встановити деякі закономірності виникнення джиттера, що дозволить реалізувати схему зменшення його негативного впливу.

В основу розробленого методу компенсації ПМД покладено той факт, що диференціальна групова затримка (ДГЗ) залежить від еліпса поляризації світлового випромінювання, що подається в оптичне волокно.

Найбільш вигідною стала схема DWDM-системи передачі з по канальною компенсацією ПМД, основними компонентами якої є одномодові лазери, підсилювачі потужності, лінійні підсилювачі, попередні підсилювачі потужності, фотодетектори, WDM MUX – мультиплексори спектрального ущільнення; WDM DMX – демультиплексори спектрального ущільнення; STM, ATM, Ethernet – можливі види трафіка, модулятори – пристрої для зміни еліпса поляризації вхідного випромінювання, аналізатори – пристрої для визначення ДГЗ і для керування модуляторами через зворотній канал.

Лазер випромінює лінійно-поляризоване світло, причому може використовуватися як лазер з внутрішньою модуляцією інтенсивності, так і передавальний оптичний модуль з зовнішнім модулятором. Випромінювання подається на модулятор, далі сигнали всіх спектральних каналів подаються на оптичний WDM – мультиплексор, після якого груповий сигнал спектральних каналів передається в оптичне волокно через широкосмуговий підсилювач потужності.

Схема компенсації ПМД, дозволяє оперативно реагувати на зміну ДГЗ. Замість модулятора використовується електрооптичний кристал. Під дією керуючої напруги кристал змінює двозаломлення, причому різниця показників заломлення швидкої і повільної осей залежить від величини прикладеної напруги. Для схеми компенсації ПМД потрібно, щоб модулятор дозволяв реалізувати різницю часу поширення швидкої і повільної складових в межах від 0 до $2\pi/\omega$, де ω – кутова частота оптичного сигналу. Для різної довжини хвилі оптичної несучої буде і різне значення прикладеної напруги для отримання однакової різниці ходу. Аналізатор на виході ОВ вимірює значення ДГЗ в даний момент. Якщо значення ДГЗ перевищує максимально допустиме, то по зворотному каналу передається сигнал на зміну вхідного еліпса поляризації. На модулятор в покроковому режимі подаються фіксовані значення напруги, а на виході аналізатора визначається ДГЗ сигналу. Передача даних ведеться неперервно на кожному еліпсі поляризації вхідного сигналу. Після проходження одного циклу вимірювань (зміна відносного зсуву фаз кристала від 0 до 2π з заданою кількістю кроків) на модуляторі встановлюється таке значення напруги, при якому ДГЗ на виході волокна приймало мінімальне значення, і цей вхідний стан поляризації зберігається до того моменту, поки значення ДГЗ знову не перевищить допустимого. Такий алгоритм компенсації використовується для кожного спектрального каналу окремо, незалежно один від одного.

Таким чином, метод компенсації поляризаційної модової дисперсії в волоконно-оптичних лініях відомчих мереж зі спектральним ущільненням каналів дозволяє зменшити вплив нелінійних ефектів, міжмодової дисперсії, джиттера та підвищити пропускну здатність і швидкість передачі цифрових потоків інформації оптичних транспортних систем.

ЛІТЕРАТУРА:

1. Гітин В.Я. Волоконно-оптичні системи передачі: Навч. посіб. для техн. закладів / Гітин В.Я., Кочановский Л.Н. − М.: Радіо і зв’язок, 2003. − 128 с.

Єсаулов М.Ю. (ВІТІ ДУТ)

НАПРЯМКИ РОЗВИТКУ СТАЦІОНАРНОЇ КОМПОНЕНТИ СИСТЕМИ ЗВ'ЯЗКУ ТА АВТОМАТИЗАЦІЇ ЗБРОЙНИХ СИЛ УКРАЇНИ

Аналіз бойових дій останніх десятиліть показує, що потрібно реформування способів ведення бойових дій, а також організації підтримки військ на полі бою з урахуванням останніх досягнень в області інформаційних комунікацій. Це означає, що в комплексі заходів щодо забезпечення обороноздатності держави поряд з підтриманням високої бойової готовності військ пріоритетним напрямком є розвиток і вдосконалення системи військового управління та її технічної основи – системи зв'язку Збройних Сил України як найважливішого елемента державної та військової інфраструктури, визначає ефективність застосування військ та зброї.

Система зв'язку Збройних Сил України технічно базується переважно на застарілих системах радянського виробництва 70 – 80-х років минулого століття. Це переважно аналогові засоби в яких реалізовані технічні рішення, які вже не підтримуються виробниками засобів зв'язку. У свою чергу утримання застарілих аналогових систем призводить до надмірних (зайвих) витрат коштів.

У той же час протягом 2006-2012 років у Збройних Силах виконувались заходи щодо переоснащення системи зв'язку цифровими засобами. Співвідношення стаціонарних цифрових систем до аналогових складає приблизно 25% на 75%. За вказаний період апробовані типові технічні рішення щодо забезпечення сучасними послугами зв'язку (захищений обмін голосом, даними, відео), які забезпечують відповідним вимогам щодо відкритості, комплексності та модульності їх побудови.

Нажаль динаміка розвитку системи зв'язку залежить від рівня фінансування, наявності цифрових систем спеціального призначення, які прийнято на озброєння або подвійного використання, а також від структури системи управління, погляди на яку доволі часто змінюються.

Реформування системи зв'язку Збройних Сил України планується здійсненням наступних основних заходів:

визначення оптимального складу військ зв'язку, які забезпечать розгортання та функціонування системи зв'язку з метою якісного управління військами (силами);

забезпечення надання послуг зв'язку органам державного і військового управління Міністерства оборони та Збройних Сил України;

переоснащення стаціонарної та польової компоненти системи зв'язку новітніми цифровими засобами (комплексами);

виведення з експлуатації, списання та утилізація морально застарілої техніки зв'язку.

Аналізуючи досвід провідних світових державам щодо здійснення формування глобальних інформаційних мереж військового призначення на основі наявних і перспективних систем зв'язку, можливо зробити висновок, що розвиток системи зв'язку Збройних Сил України планується здійснювати на основі створення єдиного інформаційно-телекомунікаційного середовища із впровадженням сучасних інформаційно-телекомунікаційних технологій, протоколів обміну інформацією (IP, VPN MPLS, E1), комплексів та систем зв'язку спеціального призначення, яке забезпечить обмін всією інформацією (голос, данні, відео) між органами та пунктами управління (всіх ланок) з відповідною пропускною спроможністю, достовірністю та надійністю.

Отже, в якості шляхів розвитку стаціонарної компоненти системи зв'язку та автоматизації Збройних Сил України можливо визначити наступні:

застосування технології MPLS для потреб Збройних Сил України;

переоснащення телекомунікаційної мережі на цифрові засоби;

розроблення та провадження асу системою зв'язку;

створення стаціонарної автоматизованої системи радіозв'язку;

створення інтегрованої системи супутникового зв'язку ЗС України;

впровадження апаратури засекречування IP-шифрування вітчизняного виробництва.

В основі переоснащення стаціонарної компоненти системи зв'язку Збройних Сил України цифровими засобами є підключення та використання телекомунікаційної мережі спеціального призначення Державної служби спеціального зв'язку та захисту інформації.

З метою такого переоснащення планується виконати наступні заходи:

розгортання відомчої мережі Збройних Сил України з використанням IP-технологій, впровадження сучасних телекомунікаційних та інформаційних систем, апаратно-програмних комплексів;

розгортання стаціонарної компоненти захищеної системи обміну інформацією Збройних Сил України зі швидкістю обміну інформацією до 70 Мбіт/с у кожному напрямку (передача даних, мовної інформації, відео);

розгортання системи захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах Збройних Сил України;

створення системи супутникового зв'язку Збройних Сил України на базі національного супутника;

створення цифрової мережі радіозв'язку, у тому числі транкінгової;

удосконалення технічної складової системи оповіщення Збройних Сил України;

поступове скорочення послуг аналогового зв'язку, відмова від використання застарілих систем зв'язку та виведення їх з експлуатації.

Таким чином, у стаціонарній компоненті системи зв'язку Збройних Сил України буде виконане наступне: переоснащено на цифрові засоби усі інформаційно-телекомунікаційні вузли стаціонарної компоненти; відмова від використання системи відкритого телеграфного зв'язку за рахунок впровадження засобів передачі даних; створення системи супутникового зв'язку з використанням новітніх засобів для резервування наземної компоненти системи зв'язку та збільшення рівня її гнучкості й мобільності; функціонування захищеної системи обміну інформацією, в усіх ланках управління, з виведенням з експлуатації окремих типів апаратури засекречування телеграфного зв'язку виробництва колишнього СРСР та повне виведення з експлуатації комутаторів засекреченого зв'язку; створення засобів, що дозволяють формувати єдину картину "поля бою" на основі одержуваної від різних джерел інформації, доведення її до керівництва в зручному для ухвалення рішення вигляді, а також забезпечування планування бойового застосування військ (сил) і зброї в близькому до реального масштабі часу.

В результаті переоснащення стаціонарна компонента системи зв'язку Збройних Сил України буде мати цільну структуру в усіх ланках управління, яка забезпечить якісний відкритий та закритий цифровий зв'язок (голос, дані, відео) зі швидкостями:

до 300 Мбіт/с – в стратегічній;

до 155 Мбіт/с – в оперативній;

до 34 Мбіт/с – в тактичній ланках управління.

Враховуючи, що в якості основи буде використовуватися телекомунікаційна мережа спеціального призначення Державної служби спеціального зв'язку та захисту інформації проблема щодо взаємосумісності систем зв'язку буде практично вирішена.

ЛІТЕРАТУРА

1. Стратегічний оборонний бюлетень України, 2012 року.

2. Концепція реформування і розвитку Збройних Сил України на період до 2017 року.

3. Щорічне видання „Біла книга-2012. Збройні Сили України", 2012 року.

4. Замисел переоснащення системи зв'язку Збройних Сил України цифровими засобами в період 2013 – 2017 років та шляхи його реалізації.

Жаханович Р.О. (ВІТІ ДУТ)
Гусєв О.І. (ДУТ)

ДОСЛІДЖЕННЯ ВПЛИВУ НЕЛІНІЙНИХ СПОТВОРЕНЬ НА ЗАВАДОСТІЙКІСТЬ ПРИЙМАННЯ СИГНАЛУ З ОРТОГОНАЛЬНОЮ ЧАСТОТНОЮ МОДУЛЯЦІЄЮ

Сьогодні технологія ортогонального частотного мультиплексування – OFDM (Orthogonal Frequency Division Multiplex) широко застосовується в мережах безпроводового доступу стандартів IEEE 802.11 та IEEE 802.16, системах цифрового радіомовлення T-DAB та DRM, цифрового телебачення DVB-T, xDSL-модемах (рекомендація ITU G.992).

Проведений аналіз існуючих систем радіозв'язку з OFDM показав, що поряд зі своїми перевагами сигнал з OFDM має недоліки, одним з яких є висока чутливість до нелінійних спотворень, які виникають у радіотрактах радіозасобів. При проходженні групового сигналу OFDM через нелінійні тракти порушується ортогональність піднесучих, що призводить до їх взаємного впливу і, в остаточному підсумку, до зниження завадостійкості приймання сигналів. Тому виникає необхідність дослідження впливу нелінійних спотворень на завадостійкість OFDM-модемів при довільній кількості піднесучих.

При OFDM груповий сигнал модему на інтервалі передачі одного символу може бути поданий у вигляді

$$A_{\text{вих}}(t) = \sum_{j=0}^{n} \mu_j \left[\sum_{p=0}^{N-1} A_p \cos\left[2\pi f_0 t + \left(p - \frac{N-1}{2} \right) \Delta f_{\text{р}} t + \varphi_p \right] \right]^j ,$$

де μ_j – коефіцієнт, що визначає нелінійні спотворення n-го порядку; f_0 – центральна частота групового сигналу; N – кількість піднесучих; p – номер піднесучої; $\Delta f_{\text{р}}$ – рознесення частот між піднесучими; A_p – амплітуда p-ї піднесучої; φ_p – поточна фаза p-ї піднесучої. Вплив нелінійних спотворень на кожну піднесучу групового сигналу з OFDM може бути виражений еквівалентним відношенням сигнал/шум (ВСШ), під яким розуміють відношення енергії корисної складової сигналу OFDM до сумарної енергії продуктів нелінійних спотворень для певної піднесучої.

Відношення сигнал/шум для кожної піднесучої групового сигналу з OFDM можна розрахувати за наступними формулами:

$$Q^2 = 10 \lg \left(\frac{1}{2N^2 + N(7+4p) - 4p(1+p) + 6} \left(\frac{N}{2} 10^{-\frac{K_3}{20}} + \left(\frac{N}{2} - 1 \right) \text{sign}(\mu_3) \right)^2 \right)$$

при парних значеннях N, і

$$Q^2 = 10 \lg \left(\frac{1}{2N^2 + N(7+4p) - 4p(1+p) + 5 + 2\,\text{mod}(p,2)} \left(\frac{N}{2} 10^{-\frac{K_3}{20}} + \left(\frac{N}{2} - 1 \right) \text{sign}(\mu_3) \right)^2 \right)$$

при непарних значеннях N, де K_3 – коефіцієнт нелінійних спотворень третього порядку, μ_3 – коефіцієнт, що визначає спотворення амплітудної характеристики радіотракту.

Отримані точні аналітичні вирази дозволяють розрахувати еквівалентне відношення сигнал/шум для кожної піднесучої сигналу з OFDM при довільній кількості піднесучих.

к.т.н. Жук О.Г. (ВІТІ ДУТ)
Оліфір Д.Ю.(ВІТІ ДУТ)
Давиденко Л.С. (ДУТ)

МЕТОДИ ОПТИМІЗАЦІЇ ПАРАМЕТРІВ ГРУПОВОГО СИГНАЛУ СИСТЕМ ПЕРЕДАЧІ З ТЕХНОЛОГІЄЮ OFDM

Серед задач оптимізації характеристик *OFDM*-систем, що можуть розв'язуватися в процесі адаптації системи до умов передачі по каналу зв'язку в реальному масштабі часу, суттєве значення мають задачі оптимізації параметрів сигналу за різноманітними критеріями.

Основна задача оптимізації параметрів сигналу формулюється наступним чином: знайти такий розподіл потужності сигналу та кількості інформації, що передається, по підканалах *OFDM*-системи, при якому швидкість передачі інформації по каналу зв'язку з лінійними частотними спотвореннями та адитивним шумом буде максимальною. При цьому припускають, що характеристики каналу зв'язку відомі, потужність сигналу обмежена і забезпечується потрібна ймовірність помилки на виході приймача. Кількість несучих визначається в процесі виконання процедури оптимізації та визначає ширину спектра сигналу. Очевидно, сформульована задача є практичним варіантом відомої в теорії зв'язку задачі оптимізації спектра сигналу, що передається по каналу зв'язку з лінійними частотними спотвореннями та адитивним шумом.

Мають зміст і інші задачі оптимізації, наприклад, мінімізація потужності сигналу, що передається при заданій швидкості передачі інформації, а також мінімізація ширини спектра сигналу при заданій швидкості передачі інформації та обмеженні на випромінювану потужність.

Методи оптимізації параметрів сигналу *OFDM* базуються на співвідношенні, що пов'язує кількість бітів інформації, яка передається протягом посилки на кожній несучій, із співвідношенням сигнал/шум у смугах частот цих несучих та з ймовірністю помилки на виході приймача, яку необхідно забезпечити.

Для розв'язання задачі максимізації швидкості передачі інформації при обмеженні потужності групового сигналу *OFDM*-системи розроблено два алгоритми. Ідея першого полягає в тому, що на кожному кроці оптимізації для приросту потужності вибирається та несуча, яка потребує мінімального приросту її потужності для збільшення кількості інформації, що передається протягом однієї посилки на один біт. Процес оптимізації продовжується до тих пір, поки не буде досягнуто значення заданої потужності сигналу.

Ідея другого алгоритму полягає в побудові функції, що задає сумарну кількість бітів, які передаються протягом однієї посилки з використанням k кращих несучих (вибраних за критерієм мінімуму рівня шуму на вході каналу зв'язку), та знаходженню максимуму цієї функції. При обчисленні відношення сигнал/шум припускається, що потужність передавача рівномірно розподіляється між k несучими. Пошук оптимального значення кількості несучих здійснюється методом золотого перетину, завдяки чому забезпечується малий час оптимізації. Розроблені також алгоритми оптимізації *OFDM*-систем з передспотвореннями сигналу на передачі та з корекцією сигналу на прийомі. Ці алгоритми відрізняються від розглянутих вище тим, що на всіх несучих використовуються одинакові сигнальні сузір'я. В *OFDM*-системі з передспотвореннями сигналу на передачі потужність у кожному каналі задається прямо пропорційною до приведеного до входу каналу зв'язку шуму (еквівалентного шуму) в цьому каналі. В *OFDM*-системі з корекцією на прийомі потужність у всіх каналах однакова, а на прийомі здійснюється вирівнювання частотних спотворень, які вносяться каналом зв'язку.

Результати комп'ютерного моделювання алгоритмів оптимізації підтверджують їх ефективність. Причому з ростом лінійних частотних спотворень ефективність оптимізації зростає.

к.т.н. Жук П.В. (ВІТІ ДУТ)
Проненко Є.В. (ВІТІ ДУТ)
Стойчев М.І. (ВІТІ ДУТ)

МЕТОДИКА РОЗРАХУНКУ ЕЛЕКТРИЧНИХ ХАРАКТЕРИСТИК ШИРОКОСМУГОВИХ ДЗЕРКАЛЬНИХ АНТЕН

Протягом всього часу свого розвитку радіорелейний зв'язок завжди займав важливе і невід'ємне місце серед інших родів зв'язку. Його використовують коли прокладання кабельних ліній нерентабельне, або для встановлення зв'язку в найкоротші терміни.

На практиці всі важливі параметри антен для радіорелейного зв'язку значною мірою залежать від параметрів опромінювача, тому від його вибору залежить ефективність усієї антенної системи в цілому.Сучасні радіорелейні станції повинні функціонувати в широкому діапазоні частот, тому актуальним є завдання розробки широкодіапазонних антен. Доцільно його вирішувати використовуючи логарифмічно-періодичні антени (ЛПА) вібраторного типу. В дециметровому діапазоні довжин хвиль постає можливість виконати ЛПА в печатному вигляді, що значно спрощує процес їх виготовлення.

Розрахунок електричних характеристик антенного пристрою будь-якого типу проводиться виходячи з заданих вихідних даних, які звичайно отримують з енергетичного розрахунку конкретної радіолінії:

коефіцієнт підсилення чи коефіцієнт направленої дії (КНД);

ширина діаграми направленості (ДН) в двох ортогональних площинах;

рівень бічних та задніх пелюстків ДН;

поляризаційна характеристика;

діапазон робочих частот;

вхідний опір антени.

Методика розрахунку електричних характеристик широкосмугової дзеркальної антени складається з наступних етапів.

1. Розрахунок геометричних параметрів параболічного дзеркала. На цьому етапі визначаються всі параметри, які дозволяють реалізувати заданий коефіцієнт підсилення в діапазоні робочих частот.

2. Розрахунок зовнішніх та внутрішніх характеристик опромінювача. Початковими даними для розрахунку геометричних та електричних характеристик ЛПА вібраторного типу є: смуга робочих частот (коефіцієнт перекриття); КНД; вхідний опір; потужність, яка підводиться до антени, величина якої визначається вимогами до її електричної міцності.

На цьому етапі визначаються кут та період структури ЛПА, довжина та кількість вібраторів. В залежності від кута розкриву параболоїда $2\Psi_0$ підбирається необхідна характеристика спрямованості опромінювача. Вона вибирається таким чином, щоб потужність сигналу на кромці параболоїда зменшувалась на 10 дБ. Це дозволяє отримати достатньо великий коефіцієнт підсилення та зменшити рівень бічного випромінювання.

3. Розрахунок електричних характеристик дзеркальної антени.

3.1. Визначення поля в розкриві параболоїдного дзеркала. Поле в розкриві визначається методом геометричної оптики за відомою нормованою ДН опромінювача.

3.2. Визначення поля випромінювання параболоїдного дзеркала.

Теоретичний розрахунок електричних характеристик широкосмугової дзеркальної антени за запропонованою методикою продемонстрував зменшення обчислювальної складності розрахунку та показав необхідність використання в якості основного дзеркала усічений параболоїд з перфорованою решітчастою конструкцією для зменшення ваги антенної конструкції та вітрових навантажень та в якості первинного джерела випромінювання (опромінювача) – логоперіодичної антени в печатному виконанні для дециметрового діапазону довжин хвиль.

к.т.н. Жук О.Г. (ВІТІ ДУТ)
Рубцов І.Ю. (ВІТІ ДУТ)

МЕТОД ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМИ РАДІОЗВ'ЯЗКУ З OFDM

Однією з головних проблем у системах радіозв'язку в декаметровому та НВЧ діапазоні є передача сигналу в умовах багатопроменевого розповсюдження. За рахунок неідеальної передаточної характеристики каналу зв'язку виникають частотно-селективні завмирання переданого сигналу. Для стандартних методів передачі цифрової інформації на одній несучій частоті повні завмирання окремих частотних компонентів у спектрі призводять до незворотних спотворень сигналу, і відповідно до необмеженого росту помилок.

Одним з напрямків вирішення цієї проблеми є застосування багаточастотного методу передачі сигналів – методу ортогонального частотного розділення з мультиплексуванням (Orthogonal Frequency Division Multiplexing – OFDM). Основними перевагами даного методу є висока стійкість відносно селективних завмирань, а також висока частотна ефективність. У системах радіозв'язку застосовується різновид сигналів OFDM – COFDM (Coded OFDM). Сигнали COFDM використовують кодування інформації на кожній піднесучій і між піднесучими. Завадостійке кодування дозволяє додатково підсилити корисні властивості OFDM-сигналу. При всіх перевагах багаточастотних систем, метод COFDM має суттєвий недолік – велике відношення пікової потужності сигналу до його середньої потужності (великий пікфактор сигналу), що значно знижує ефективність функціонування засобів радіозв'язку. Виділяють три основних напрямки вирішення даної проблеми. Перший та найпростіший – амплітудне обмеження сигналу, що дозволяє суттєво знизити величину пікфактора. Але при цьому виникають неконтрольовані спотворення сигналу, що призводить до погіршення якості зв'язку та зростання рівня позасмугового випромінювання.

Другим напрямком є додаткове кодування та введення надлишкових несучих, корекція параметрів яких дозволяє зменшити значення пікфактора. При цьому погіршується спектральна ефективність, оскільки суттєве зменшення пікфактора спостерігається тільки при швидкості кодування 1/2, тобто половина несучих частот використовується для корекції.

Третій напрямок – використання додаткових ортогональних (або неортогональних) перетворень, а також використання замість Фур'є-базису інших ортогональних базисів (Hadamard basis, wavelet-basis та ін.). Недоліком усіх цих підходів є спотворення структури OFDM-сигналу, що призводить до того, що сигнал стає неінваріантним по відношенню до циклічних зсувів, тобто чутливим до багатопроменевості каналу.

Усе вище розглянуті методи лише частково вирішують проблему зниження пікфактора багаточастотних сигналів, при цьому або погіршуючи ймовірність помилкового приймання сигналів, або знижуючи пропускну спроможність каналу та ускладнюючи системи кодування і декодування.

Значний пікфактор багаточастотних сигналів обумовлює застосування лінійних каскадів посилення. Лінійні підсилювачі потужності достатньо складні у виготовленні, мають велику вартість і дуже низький коефіцієнт корисної дії, у зв'язку із цим неминучі додаткові енергетичні витрати на побудову передавальних трактів, тому потрібний розгляд і аналіз нових методів обробки сигналу OFDM для підвищення не тільки енергетичної ефективності, але й завадостійкості подібних систем.

Для зменшення пікфактора запропоновано використати додаткову частотну модуляція несучої частоти багаточастотним сигналом (COFDM-ЧМ).

Використання сигналів з постійною обвідною дозволяє застосовувати високоефективні нелінійні підсилювачі потужності у вихідних каскадах передавачів з резонансним навантаженням з максимальним теоретичним коефіцієнтом корисної дії величиною до 78,5%. Трансформація в області амплітуда-частота дозволяє одержати енергетичний виграш і спростити схеми передавальних каскадів для багаточастотних сигналів.

Порівняльний аналіз COFDM і COFDM-ЧМ сигналів в умовах шумових завад показав енергетичний виграш останньої мінімум на 1,5-2 дБ при інших рівних системних параметрах.

к.т.н. Жук П.В. (ВІТІ ДУТ)
Хоменко П.В. (ВІТІ ДУТ)
Пікуль Р.В. (ВІТІ ДУТ)

ЗАВАДОЗАХИЩЕНІСТЬ СИСТЕМ РАДІОЗВ'ЯЗКУ З ПСЕВДОВИПАДКОВОЮ ПЕРЕБУДОВОЮ РОБОЧОЇ ЧАСТОТИ

Системам радіозв'язку відведена важлива роль у функціонуванні систем військового зв'язку в різних ланках управління. Удосконалення систем зв'язку тактичної ланки управління (ТЛУ) спрямоване, в першу чергу, на забезпечення оперативного, стійкого й прихованого управління військами й зброєю.

Одним з шляхів вирішення цієї задачі є використання широкосмугових систем радіозв'язку (СРЗ), які базуються на застосуванні широкосмугових сигналів (ШСС) [1]. Широкосмугові сигнали, на відміну від вузькосмугових, мають більш високу розвід- та завадозахищеність. Серед методів формування ШСС широкого практичного застосування отримав метод псевдовипадкової перебудови робочої частоти (ППРЧ), при якому розширення спектру в межах заданої смуги частот здійснюється за допомогою стрибкоподібної зміни частоти сигналу за псевдовипадковим законом, невідомим постановнику завад. Для роботи необхідно виділяти не одну частоту, а пакет частот, що потребує грамотного частотного планування та призначення законів перебудови для окремих радіоліній СРЗ таким чином, щоб вони не створювали взаємних завад одна одній.

Найбільш ефективною при подавленні радіоліній з ППРЧ є ретрансльована завада (завада у відповідь). Коли радіолінія переходить на нову робочу частоту система радіоелектронного подавлення повинна її визначити та створити заваду. Потужність передавача завад у цьому випадку використовується більш ефективно, у порівнянні з широкосмуговою загороджувальною завадою, а бо шумовою завадою в частині смуги.

Успішність постановника завад залежить від часу спрацьовування, який необхідний на визначення поточної частоти та створення завади, та часу запізнення, який витрачається на розповсюдження радіохвиль від передавача СРЗ до станції завад та від останньої до приймача СРЗ. Якщо час роботи радіозасобу з ППРЧ на одній частоті $\Delta t_{\text{р}}$, менший за сумарний час спрацьовування $\Delta t_{\text{спр}}$ і час запізнення завад $\Delta t_{\text{з}}$ ($\Delta t_{\text{р}} \le \Delta t_{\text{спр}} + \Delta t_{\text{з}}$), то ретрансльована завада виявляється неефективною. На сьогоднішній день відомі СРЗ зі швидкістю перебудови до 20 тис. стрибків за секунду (комплекс „Абзац", Російська Федерація).

Нескладний аналіз показує, що при відстані до постановника завад від 5 до 15 км, та прийнявши, що $\Delta t_{\text{спр}} = 0$, щоб повністю позбутися впливу завади необхідно забезпечити швидкість перебудови, відповідно, від 60 до 20 тис. стр/с. Враховуючи можливість використання противником малогабаритних, „одноразових" постановників завад, що можуть „заккидуватись" якомога ближче до радіозасобів, а також можливість застосування постановників завад на безпілотних літальних апаратах [2], виникає необхідність розробки та впровадження у радіозасоби з ППРЧ додаткових засобів завадозахисту. Серед них найбільш перспективними є багатоантенні системи (MIMO), адаптивні антенні решітки (ААР), що можуть формувати мінімум діаграми направленості у напрямку приходу завади [3]. Тому напрямком подальших досліджень є розробка методики управління діаграмоутворенням ААР.

ЛІТЕРАТУРА

1. Борисов В. И. Помехозащищенность систем радиосвязи. Вероятностно-временной подход. Изд. 2-е, исправленное / В. И. Борисов, В. М. Зинчук.– М.: Радиософт, 2008. – 260 с.

2. Гурський Т.Г. Перспективи використання безпілотних літальних апаратів для радіоелектронного подавлення систем радіозв'язку / Т.Г. Гурський, Л.Л. Бортнік, О.М. Макарчук // Збірник наукових праць ВІТІ НТУУ „КПІ". – №1. – 2010. – С. 15 – 23.

Жуковський Т.Я. (ВІТІ ДУТ)
Паламарчук С.А. (ВІТІ ДУТ)
Рехлицький Д.С. (ВІТІ ДУТ)
Самелюк О.С. (КНУТД)

КОРЕКТНІСТЬ РЕАЛІЗАЦІЇ ПОСЛУГ БЕЗПЕКИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Сучасні користувачі автоматизованих систем (АС) поряд з гарантованим доступом до інформаційних ресурсів потребують належного і достатнього забезпечення захисту інформації, і в першу чергу від несанкціонованого доступу (НСД). Механізми управління доступом є основою захисту ресурсів АС, забезпечують вирішення задач розмежування доступу суб'єктів (користувачів з різними повноваженнями, процесів) до інформаційних і технічних ресурсів (об'єктів) та визначаються правилами розмежування доступу (ПРД).

На сьогодні, найбільш чітко визначено й відпрацьовано два типи ПРД, які реалізуються за допомогою політик безпеки на основі виборчого (дискреційного) розмежування доступу (дискреційна політика безпеки) та повноважного (мандатного) розмежування доступу (мандатна політика безпеки). Якщо враховувати загальний підхід щодо визначення мінімального кола осіб, які мають право на ознайомлення з інформацією, то переваги віддаються дискреційній політиці безпеки, але вона складніша в реалізації. Керування організацією розмежування доступу відповідно до вимог нормативних документів системи технічного захисту інформації (НД ТЗІ) поділяється на „довірче" та „адміністративне". В результаті аналізу коректності реалізації механізмів розмежування доступу в автоматизованих системах, вимог НД ТЗІ, слідує що, більш доцільне для застосовування адміністративне керування доступом. Довірче керування доступом можливе при розмежуванні доступу для груп користувачів з однаковими повноваженнями стосовно конфіденційної інформації і лише в межах цих груп [НД ТЗІ 2.5-008-2002].

На даний час використання операційних систем (ОС) сімейства Windows (XP SP2, Windows 7), як тих, що мають позитивні експертні висновки Державної служби спеціального зв'язку та захисту інформації України, дозволяє реалізувати згадані підходи з розмежування доступу при створенні захищених АС, у вигляді різноманітних послуг безпеки, рівень яких залежить від вимог до забезпечення захищеності інформації в АС. Для реалізації ПРД до ресурсів автоматизованих систем можливо використовувати вбудовані в ОС засоби захисту та поряд з вбудованими, додаткові механізми захисту (сукупність програмно-апаратних засобів), які забезпечують реалізацію політики безпеки інформації та складають основу комплексу засобів захисту від НСД до інформації (КЗЗ від НСД). Однак, складність сучасних ОС ускладнює проведення експертного оцінювання механізмів захисту ОС в сфері ТЗІ.

Підсистема захисту ОС сімейства Windows забезпечує рівень гарантій Г2 (з існуючих 7-ми рівнів) та реалізує однорівневу автентифікацію користувачів (послуга НИ-2 згідно НД ТЗІ 2.5-004-1999, в якій перевірка ключової інформації здійснюється після завантаження ОС), що коректно для забезпечення безпеки конфіденційної та службової інформації, однак не достатньо для захисту таємної інформації, як наслідок, перевага повинна віддаватися комплексам засобів захисту від НСД („Лоза-1" (рівень гарантій Г3), „Лоза-2" (рівень гарантій Г3), „Рубіж-РСО" (рівень гарантій Г3), „Гриф" (рівень гарантій Г4), „Гриф-Мережа" (рівень гарантій Г4)). Загалом, для захисту таємної інформації пропонується удосконалення прийнятих механізмів розмежування доступу за рахунок моделі безпеки звернень, що реалізує процедуру двохрівневої автентифікації користувачів, послуга НИ-3 згідно НД ТЗІ 2.5-004-1999. Хоча дана послуга вимагає додаткової реалізації достовірного каналу (послуги НК-1, неможливість прослуховування або перегляду ключової інформації під час самої автентифікації), що потребує рішень на рівні технічної платформи. Подальші дослідження потрібно спрямувати на реалізацію послуги безпеки НК-1 під час автентифікації.

Залужний О.В. (ВІТІ ДУТ)
Залужна С.В. (ВІТІ ДУТ)
Волкова Ю.О. (РТФ НТУУ “КПІ”)

МЕТОДИКА РОЗРАХУНКУ ДОВЖИНИ КОДОВОЇ ПОСЛІДОВНОСТІ ДЛЯ ОДНОСТОРОННЬОЇ РАДІОПЕРЕДАЧІ КОМАНД І КОРОТКИХ ПОВІДОМЛЕНЬ

В умовах сьогодення все частіше виникає необхідність у використанні різних дистанційно керованих електромеханічних пристроїв, систем збору інформації, систем оповіщення та доведення повідомлень особливої важливості і терміновості. При цьому невід’ємною складовою таких комплексних систем є використання високонадійних командних радіоліній управління. Існуючі рішення, що забезпечують обмін інформацією з об’єктом управління в двосторонньому режимі адаптовані до умов використання в цивільних системах, але не завжди задовольняють потребам при виникненні надзвичайних ситуацій та при веденні бойових дій. В таких випадках доречним є застосування одностороннього режиму, що дає можливість зменшити час та затрати на розгортання, знизити вартість обладнання, значно збільшити тривалість автономної роботи окремих пристроїв, зменшити масогабаритні показники, унеможливити викриття місцязнаходження приймача, застосувати більш складні та ефективні алгоритми обробки сигналів, що в свою чергу призводить до підвищення стійкості до завад, живучості та скритності вказаних систем. Основним недоліком односторонньої передачі є відсутність можливості отримання підтвердження про прийом команди (повідомлення) та передачі запиту на уточнення її достовірності. Тому важливим завданням є максимізація надійності прийому повідомлення та достовірності прийнятої інформації. Відомо, що завадостійкість радіоліній управління оцінюється двома основними критеріями, що характеризують приймання команди при наявності корисного сигналу – ймовірність прийому вірної команди $P_к$, та при його відсутності – ймовірність прийому хибної команди $P_х$. Останнє ускладнюється можливістю наявності імітаційної завади. Одним із шляхів підвищення завадостійкості є визначення необхідної довжини кодової послідовності для передачі повідомлення із одночасним врахуванням спільних вимог до $P_к$ та $P_х$. Запропонована методика дає змогу здійснювати такі розрахунки і на відміну від існуючих способів, навіть на тривалих інтервалах часу коли імітаційна команда повторюється довільно велику кількість разів.

Суть даної методики полягає у виборі потрібної довжини кодової послідовності шляхом поступового її збільшення та підбору порогового значення кількості правильно прийнятих елементарних двійкових символів до тих пір поки ймовірності $P_к$ та $P_х$ будуть відповідати заданим вимогам. Вихідні дані для розрахунку та обмеження залежать від вказаних вимог до ймовірнісних характеристик радіолінії, технічних характеристик системи та завадової обстановки. Припускається, що атакуючій стороні відомі неінформаційні параметри сигналу та час очікування повідомлення, двійкові стани елементів імітаційної команди є рівноймовірними та взаємонезалежними.

Методика дозволяє обчислити мінімальнонеобхідну довжину кодової послідовності, а також необхідне значення $N_{пор}$, при заданих вимогах до надійності прийому вірної команди та імовірності хибного спрацювання. Вона може бути застосована у випадках висування безпрецедентно надвисоких вимог до імовірнісних характеристик радіолінії управління систем і комплексів різного призначення, узагальнена для будь-якого радіоканалу і виду обробки (демодуляції) сигналу, що вплине лише на розрахунки ймовірності помилки на біт. Методика не накладає обмежень на можливість використання завадостійкого кодування та перемеження.

Можливим напрямком подальших досліджень є розробка методики вибору довжини повідомлення при передачі команди одночасно на різних частотах та із застосуванням конкретних кодових послідовностей.

к.т.н. Зінченко А.О. (НУОУ ім. Івана Черняховського)

МЕТОД ВИЗНАЧЕННЯ ВІДСТАНЕЙ НА ОСНОВІ ФАЗОВИХ ВИМІРІВ В MIMO-СИСТЕМАХ ЗВ'ЯЗКУ ТА РАДІОЛОКАЦІЇ

У переліку завдань, що можуть бути покладені на інтегровані MIMO-системи зв'язку та радіолокації, важливе місце відводиться виміру відстаней до джерел сигналів, в якості яких слід розглядати рухомих кореспондентів на суші, в повітрі, на водній поверхні, а також повітряні цілі, у тому числі засоби повітряного нападу. У разі застосування неперервних сигналів, таких як OFDM та N-OFDM (з неортогональним частотним дискретним мультиплексуванням), заслуговує на увагу багаточастотний фазовий метод виміру дальності. Попередньо було усунено основний недолік зазначеного методу – відсутність розрізнювальної здатності по дальності, що створює умови для більш широкого застосування фазової дальнометрії при сумісному вирішенні завдань радіолокації та зв'язку в багатопозиційних мобільних MIMO системах.

Метою доповіді є розгляд особливостей багаточастотного фазового методу виміру відстаней та його адаптація до застосування в багатопозиційній інтегрованій системі зв'язку та радіолокації. Сутність методу фазового виміру дальності полягає у визначенні різниці фаз між сигналами що передається та відбитим від цілі. На основі різниці фаз розраховується дальність до цілі. Однозначність виміру дальності фазовим багаточастотним методом у рамках розглянутих алгоритмів вимагає компенсації паразитного набігу фаз сигналів після ШПФ по значеннях частот допплерівського зрушення, а також після процедури цифрового фільтру формування квадратур.

Особливістю OFDM (NOFDM) сигналів є можливість утворення значної кількості частотних пар для виміру дальності, що дозволяє не тільки отримати великий діапазон однозначності виміру відстаней та здійснити розрізнення багатьох об'єктів, що не розрізнюються за іншими параметрами, а й досягти високої точності дальнометрії. Щоб забезпечити одночасне виконання завдань передачі даних та виміру відстаней до малорухомих об'єктів шляхом фазової дальнометрії доцільно використовувати пілот-сигнали, що інтегровані в пакет OFDM (N-OFDM).

За допомогою методів спектрального оцінювання у вимірювальній системі забезпечується вимір допплерівських зрушень частот сигналів і розрізнення цілей за швидкістю з точністю до 0,1 – 0,25 ширини фільтра ШПФ. При цьому точність виміру швидкості залежно від відношення сигнал-шум досягає 0,01 ширини фільтра ШПФ. Однозначність виміру швидкості визначається періодом дискретизації АЦП. З огляду на максимальну швидкість руху об'єкту до 1000 м/с, час накопичення може скорочуватися до величини 1 мс, що буде відповідати зсуву по дальності близько 1,5 м. Саме з такою дискретністю (1,5 м) можна на практиці здійснювати оцінку дальності до об'єктів фазовим багаточастотним методом. Удосконалення методу полягає в його узагальненні на обробку OFDM (N-OFDM) сигналів по виходах цифрової антенної решітки (ЦАР) з оптимізацією вимірювальної процедури, наприклад, за методами максимальної правдоподібності чи найменших квадратів. Ключовим етапом у синтезі відповідного варіанту фазового методу виміру дальності є формування аналітичного опису відгуку ЦАР. Оскільки при фазових вимірах інформація про відстань закладена у фазах сигналів, то кінцевою метою відповідної обробки сигнальних напруг є оцінка їх квадратурних складових. Це завдання збігається за своєю сутністю з демодуляцією повідомлень, що передаються каналом зв'язку. У зазначений спосіб нескладно узагальнити фазовий вимір відстаней на випадок багатопозиційної системи приймальних мультисекційних ЦАР, яка дозволяє максимально використати потенційні можливості інтегрованої системи зв'язку та радіолокації.

Подальші дослідження доцільно зосередити на аналізі потенційної точності вимірів відстаней до множини об'єктів фазовим методом, підставивши вирази для сигнальних матриць в інформаційну матрицю Фішера та здійснивши її обернення.

к.т.н. Іванченко С.О. (ІСЗЗІ НТУУ „КПІ”)

ЕФЕКТИВНА СПЕКТРАЛЬНА ЩІЛЬНІСТЬ ШУМОВИХ ЗАВАД ТА ЇЇ ДОСТОВІРНІСТЬ ДЛЯ ГАРАНТУВАННЯ ЗАХИЩЕНОСТІ ДЖЕРЕЛ ВИТОКУ ІНФОРМАЦІЇ

Як відомо, в даний час, що характеризується стрімким розвитком науки і техніки, технологій і технічних можливостей їх реалізації, все більше і більше зростає актуальність захисту інформації від витоку при її обробці сучасними, переважно цифровими технічними засобами і системами. Інтеграція інформаційних і телекомунікаційних систем та виникнення потреб в обробці відкритої і закритої інформації в одному і тому ж інформаційному середовищі ставлять нові, все більш жорсткі вимоги щодо захисту від випромінювань і наведень; збільшення швидкісних показників обробки даних істотно розширює частотний спектр циркулюючого в електричних ланцюгах сигналу, де значущими стають другий і наступні пелюстки спектру; застосування новітніх технологій і засобів прийому та обробки сигналів дозволяють на сьогоднішній день реалізувати для перехоплення інформації оптимальний, майже ідеальний приймач і т.д. Очевидно, що забезпечення безпеки вимагає відповідного розвитку методів і засобів захисту і, більше того, розвитку методичного апарату з оцінки захищеності з необхідним обґрунтуванням його методологічних основ, обмежень і припущень. Одним з питань забезпечення безпеки та оцінки ефективності захисту інформації від витоку є використання маскуючих завад – шумів, які в ідеалі мають бути білими з відповідними статистичними та енергетичними характеристиками. Бажано щоб завади представляли собою нормально розподілений ергодичний процес з рівномірним розподілом спектральної щільності по частоті. При цьому близько розташовані відліки часу повинні бути не корельованими, або, принаймні, мінімально корельованими з відомою функцією кореляції. Реальні ж шумові завади далеко не ідеальні. Вони мають недоліки та відхилення від вище зазначених вимог, що надає можливість противнику у здобутті ефективних методів та застосування засобів обробки шумів та перехоплених сигналів. Неврахування ж зазначених дефектів реальних завад може призвести до зниження та невідповідності гарантування захищеності джерел витоку інформації.

Для вирішення вказаної проблеми наряду з іншими підходами щодо обґрунтування еквівалентів білого шуму та оцінювання їх показників, що забезпечують маскуючі властивості реальних завад, обґрунтовано метод оцінювання ефективної спектральної щільності. Сутність цього методу полягає в тому, що досліджуваний шумовий процес за допомогою певної перевірки діагностують на предмет придатності щодо використання його в якості завади та при позитивному результаті визначають його відповідні статистико-енергетичні характеристики. Так результуючою характеристикою, яку оцінює метод, є еквівалентна спектральна щільність, що представляє собою таку щільність, яка з точки зору маскування забезпечить такий же ефект, що і білий шум, але з меншою потужністю. При цьому очевидно, що доведення ефективної щільності реального шуму до потрібної можливе шляхом створення його енергетичного запасу по відношенню до небезпечного сигналу в точці перехоплення.

Оцінювання зазначеної характеристики передбачає також і оцінювання її достовірності, яка є необхідним елементом у розрахунку гарантії захисту джерел витоку та безпеки інформації в цілому. Показано, що вона повністю визначається достовірностями статистично досліджених всіх складових результатів методу: визначення функції кореляції шумового процесу, перевірки його на стаціонарність та ергодичність, на нормальність розподілу та визначення звичайної спектральної щільності, що має бути перерахованою в ефективну.

Використання зазначеного підходу, оцінювання ефективної спектральної щільності маскуючих завад та її достовірності дозволить підвищити адекватність оцінювання захищеності джерел витоку інформації та забезпечити її потрібну гарантію.

к.т.н. Ільїнов М.Д. (ВІТІ ДУТ)
Ошурко В.М. (ВІТІ ДУТ)
Воробйов А.О. (ВІТІ ДУТ)

СПОСІБ ПОКРАЩЕННЯ АНТЕННОГО ПРИСТРОЮ БАЗОВИХ СТАНЦІЙ СИСТЕМ МОБІЛЬНОГО РАДІОЗВЯЗКУ

Аналізуючи принципи роботи системи зв'язку з рухомими об'єктами необхідно відмітити, що не залежно від її побудови, найважливішим елементом таких систем є стаціонарні базові станції, а відповідно і їх антенно-фідерний пристрій, який визначає загальну ефективність функціонування системи радіозв'язку.

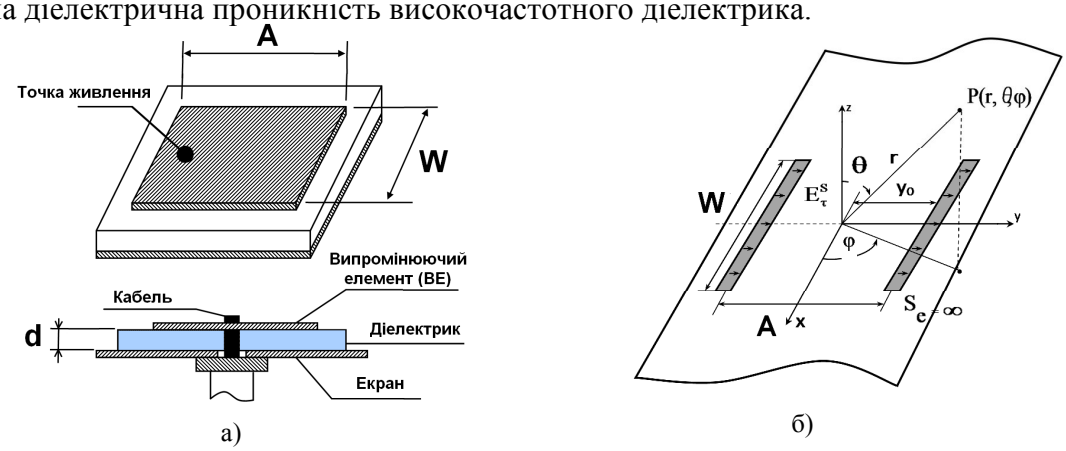
Тому задачі, що пов'язані з розробкою нових конструктивних рішень, щодо побудови антенно-фідерних пристроїв, чи модернізації вже існуючих, мають велику практичну цінність та актуальність.

В даний час, враховуючи особливості поширення радіохвиль на лініях радіозв'язку з рухомими об'єктами та принципи побудови систем мобільного радіозв'язку, в якості основних антен базових станцій використовуються панельні антени.

В переважній більшості випадків, у якості випромінюючих елементів таких антен виступають симетричні вібратори, розташовані над плоскою відбиваючою поверхнею (екраном) і орієнтовані під деяким кутом α відносно осі антенної решітки.

Одним із варіантів реалізації таких антен, є антенні решітки з низькопрофільними випромінювачами. Конструктивно, низькопрофільні антені решітки (далі – НПА) являють собою дві металеві пластини, що рознесені між собою на відстань $d << \lambda$ (Рис. 1 а), одна з яких виконує функцію випромінюючого елемента, а друга, більших розмірів, слугує екраном. Між пластинами розміщується вузол збудження електромагнітних хвиль. На практиці найбільш широкого застосування набули НПА з простою формою верхньої пластини (випромінюючого елемента): прямокутною, квадратною та круговою.

Особливістю таких антен, є те, що при введенні в простір між пластинами діелектричного матеріалу, можна зменшити розмір випромінювача в $\sqrt{\varepsilon'}$ разів, де ε' – відносна діелектрична проникність високочастотного діелектрика.



а) б)

Рис. 1. Випромінюючий елемент НПА та апертурна модель для його розрахунку

Антени даного типу володіють рядом переваг порівняно з вібраторними:

Перш за все, це зменшення розмірів самої антени, за рахунок використання у якості їх випромінювачів низькопрофільних пластин. В свою чергу, зменшення розмірів антени призводить до підвищення надійності роботи системи зв'язку в цілому, через зменшення вітрового навантаження антен та підвищення економічних показників при виготовленні.

По-друге, такі антени є простими у виготовленні, мають високу стабільність параметрів і жорстку конструкцію, можуть працювати як з лінійною так і з круговою поляризацією поля.

Згідно із теоретичними дослідженнями електричних характеристик НПА, такі антени розраховуються за допомогою теорії хвилеводів [1]. Кожний випромінюючий елемент НПА ставиться у відповідність циліндричному хвилеводу, поперечний переріз якого дорівнює поперечному перерізу випромінюючої низькопрофільної пластини.

Так, наприклад, для НПА з прямокутною верхньою пластиною апертурна модель має вигляд антенної решітки з випромінювачами у вигляді двох щілин довжиною W, рознесених на відстань A і прорізаних в металевому екрані S_e (рис. 1 б). Достатньою умовою для даних розрахунків є обмеження: $d \le 0{,}1\lambda$, де λ - довжина хвилі.

Для підвищення рівня сигналу в точці прийому, запропоновані антени доцільно компанувати у вигляді антенних решіток (рис. 2). Вираз для розрахунку характеристик направленості таких антенних решіток має наступний вигляд:

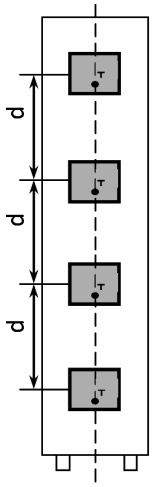


Рис. 2. Чотирьохелементна НПА

$$F(\theta,\varphi)=\frac{1}{N}\left|\cos\left(\frac{\pi}{2\sqrt{\varepsilon'}}\sin\varphi\sin\theta\right)\times\frac{\sin\left(\frac{\pi}{2\sqrt{\varepsilon'}}\cos\varphi\sin\theta\right)}{\frac{\pi}{2\sqrt{\varepsilon'}}\cos\varphi\sin\theta}\times\frac{\sin\left(\frac{N}{2}kd\sin\varphi\sin\theta\right)}{\frac{1}{2}kd\sin\varphi\sin\theta}\times\sqrt{\sin^2\varphi+\cos^2\theta\cos^2\varphi}\right|$$

В якості розрахунку була обрана чотирьохелементна НПА. Діаграми направленості (ДН) такої антени в ортогональних площинах з діелектриком та без діелектрика в просторі між пластинами ($\varepsilon' = 7{,}2$ і $\varepsilon' = 1$ відповідно) представлені на рис. 3. Згідно з отриманими результатами видно, що ДН та коефіцієнт направленої дії (КНД) таких антен змінюється зі зміною значень параметра ε'.

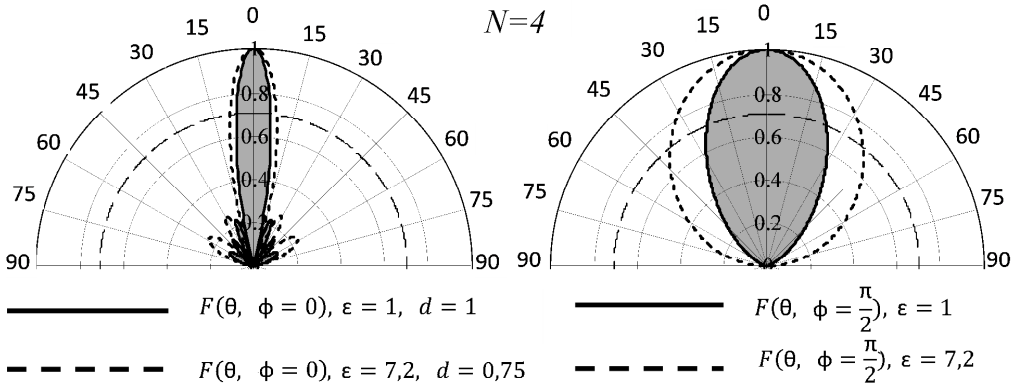


Рис. 3. ДН чотирьохелементної НПА з діелектриком та без діелектрика між пластинами

При збільшені параметра ε', значення КНД поступово зменшується, що пояснюється розширенням ширини діаграми направленості яв в меридіальній, так і в азимутальній площинах, за рахунок зменшення розмірів антени.

Результати розрахунків електричних характеристик НПА дають змогу говорити про перспективність компоновки даних пристроїв. Такі випромінювачі та антенні решітки, на їх основі, не поступаються електричними характеристиками антенам з випромінювачами вібраторного типу, та вирізняються компактністю, що дозволяє суттєво зменшити габаритні розміри антени. НПА можуть бути успішно застосовані в якості антен базових станцій систем мобільного радіозв'язку.

ЛІТЕРАТУРА

1. *Уэйт Д.* Электромагнитное излучение из цилиндрических систем.– М.: Сов. Радио, 1963 – 312 с.

д.в.н. Ільяшов О.А. (в/ч А1906)
Білан Г.А. (в/ч А1906)

МЕТОДИКА ІНТЕРАКТИВНОГО УПРАВЛІННЯ ПРОЦЕСАМИ ПОШУКУ ТА СПОСТЕРЕЖЕННЯ ЗА ОБ'ЄКТАМИ ПРИ ВИКОНАННІ СПЕЦІАЛЬНИХ ЗАВДАНЬ

На сьогодні в системі воєнної розвідки складається ситуація, коли розвідувальні завдання ускладнюються і їх кількість зростає, а розвідувальний ресурс обмежений, що призводить до зниження ефективності виконання завдань за призначенням. До того ж, проблемним питанням є низький рівень автоматизації виконання вказаних завдань, відсутність спеціалізованих програмно-технічних комплексів. Отже, виникає протиріччя, що зумовлено зростанням кількості завдань, відсутністю автоматизації та обмеженим ресурсом для їх виконання. Це протиріччя можна вирішити інтенсивним, або екстенсивним шляхом. Тобто шляхом нарощування ресурсу, або оптимальним його розподілом. Нарощування ресурсу є нераціональним. Його альтернативою є оптимізація розподілу обмеженого ресурсу шляхом інтерактивного управління процесом виконання спеціальних завдань. Тому існує необхідність розробки ефективних методик, математичних моделей та створення на їх основі процедур, методів і алгоритмів, які стануть основою для реалізації автоматизованих програмно-технічних комплексів, призначених для ефективного управління виконанням спеціальних завдань.

Метою методики інтерактивного управління процесами пошуку та спостереження за об’єктами є підвищення ефективності виконання спеціальних завдань за допомогою розроблених на її основі технічних засобів.

Алгоритм реалізації методики складається з таких кроків: формування функціоналу вхідних даних (вибір критеріїв ефективності пошукових дій, встановлення функцій обмежень); здійснення пошукових дій на основі вдосконалених математичних моделей пошуку та спостереження за об’єктами; збір, обробка, аналіз оперативних даних та формування динамічної оперативної обстановки на засобах візуалізації; надання динамічної оперативної обстановки для прийняття рішення з урахуванням реструктуризації кластерних утворень в разі руйнування інформаційних елементів в обраній області контролю; приймання ґрунтовних рішень на основі наданої динамічної обстановки та визначення показників для розподілу сил та засобів в процесі інтерактивного управління пошуковими діями; доведення команд управління за допомогою спеціального програмного забезпечення і засобів комунікації та зв’язку; організація отримання реакцій (зворотного зв’язку) від об’єктів управління (в разі потреби). В доповіді зазначається, що методика інтерактивного управління процесами пошуку та спостереження за об’єктами відрізняється від відомих застосуванням удосконалених математичних моделей пошуку та спостереження за об’єктами і розробленої процедури адаптації методів реструктуризації даних, необхідних для прийняття ґрунтовних рішень. Розроблена методика дає можливість використовувати її для створення алгоритмічного забезпечення при розробці автоматизованих комплексів, розподілу сил та засобів в інтерактивному режимі і обґрунтованого обрання стратегій пошуку та спостереження за об’єктами.

ЛІТЕРАТУРА:

1. Гасов В.М. Отображение информации. Гасов В.М., Коротаев А.И., Сенькин С.И. – М.: Высшая школа, 1990. – 111 с.

2. Карлин С. Математические методы в теории игр, программировании / Карлин С. – М.: Мир, 1994. – 102 с.

3. Петросян Л.А. Теория игр. Учебное пособие (для математических специальностей университетов) / Петросян Л.А., Зенкевич Н.А., Семина Е.А. – М.: Совместное издание: Изд-ва „Высшая Школа” и „Книжный дом ”Университет”, 1998. – 300 с.

Каламбет О.Ю. (ІТС НТУУ „КПІ”)
д.т.н. Сундучков К.С. (ІТС НТУУ „КПІ”)

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ WI-FI ДЛЯ ОРГАНІЗАЦІЇ В ЕКСПРЕС-ПОТЯЗІ КАНАЛУ ЗАПИТУ В МЕРЕЖІ МОБІЛЬНОГО ЗВ’ЯЗКУ

Актуальність напрямку роботи. На даний момент новітні розробки в сфері телекомунікацій обіцяють користувачам стабільну послугу 3G, проте в найближчому майбутньому цього буде вже недостатньо. Робота, що виконана в цій статті спрямована на те, щоб будь-хто міг користуватися високоякісною послугою, що відповідає стандартам 4G у вагоні потягу [1]. „China Mobile” є оператором зв’язку, який у 2012 році надавав інформацію щодо послуги 4G для пасажирів потягу, що рухається зі швидкістю до 350 км/год, проте насправді, використовуючи заявлені технології, досягти високоякісної послуги неможливо.

Основна інформація про загальну структуру.

Основною відмінністю запропонованої структури від стандартних технологій є те, що канал запиту і прямий канал є рознесеними за частотою. Це дає можливість досягти більших швидкостей шляхом реалізації цих каналів на різних технологіях. В поданій роботі розглянемо лише канал запиту. Базові станції для прийому і передачі сигналу є спрощеними. БС складається з 2-х оптоволоконних кабелів; діоду, що виступатиме у ролі змішувача; і рупора. По одному з кабелів надходить модульований сигнал, по іншому – піднесуча. Така БС коштує 8$. Це дає можливість поставити велику кількість БС, наприклад, через кожні 500 метрів залізничного шляху. Канал запиту між потягом і БС можна забезпечувати за допомогою технологій WIMAX або LTE. До мобільних терміналів користувача послуга надходить через технологію Wi-Fi.

Постановка задачі. В експресі 10 вагонів. В кожному вагоні 10 абонентів.

Мінімальна швидкість каналу запиту для кожного абонента – 100 кбіт/с, позначимо *B*.

Оскільки канал запиту в нашому випадку буде являти собою досить просту систему, метою якої є передача коротких повідомлень користувача про заявлену послугу, то надто великої швидкості він, відповідно, не потребує. Для передачі коротких команд абонентів мережі достатньо 100 кбіт/с.

На кожному вагоні розташовано дві точки доступу. Трафік каналу запиту кожних двох вагонів надходить на ретранслятори, які в свою чергу збирають всі запроси абонентів до головної станції за допомогою технології Wi-Fi. Головна станція надсилає їх до БС за допомогою технології WIMAX або LTE (рис 1).

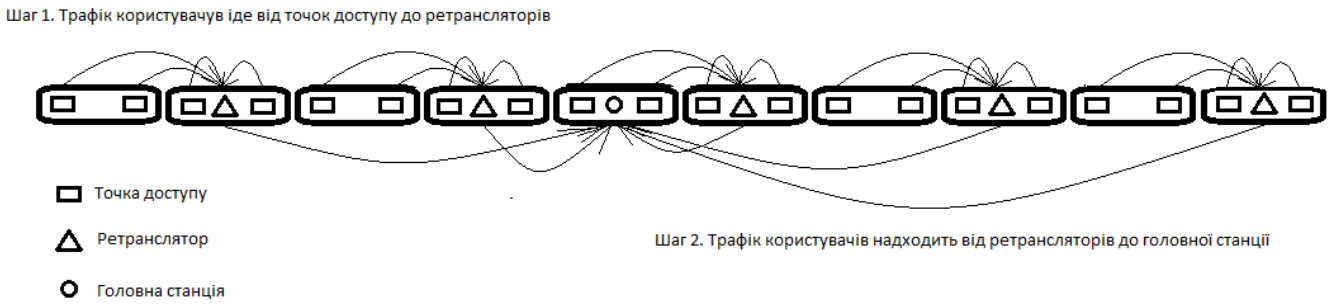


Рис. 1. Схема передачі запиту

Розрахунок поданої схеми. Дано:

Кількість вагонів від 1 до 10 (*M*).

Кількість абонентів у вагоні від 1 до 10 (*K*).

Кількість роутерів на вагон – 2 шт.

Кількість ретрансляторів – 1шт на 2 вагони.

Головна станція – 1шт. на 5-му вагоні.

Швидкість каналу запиту для одного абонента – не менше 100 Кбіт/с (*B*).

Швидкість, яка може бути досягнута, використовуючи технологію – не більше 100 Мбіт/с (*B*мах).

Коефіцієнт втрат – до 60% (*I*мах).

Розрахуємо для максимального навантаження системи весь трафік на потяг – *B*заг ≤ *B*мах.

Середня пропускна здатність, яку має підтримувати кожна точка доступу

*B*тд = 0,5M**B* = 0,5*10*100 = 500 Кбіт/с

Середня пропускна здатність кожного ретранслятору

*B*р = 4**B*тд = 4*500 = 2000 Кбіт/с = 2 Мбіт/с

Загальна пропускна здатність.

*B*заг = *M***K***B*

*B*заг = 10*10*100 = 10000 Кбіт/с = 10 Мбіт/с.

*в розрахунку подано ідеальні значення, без врахування втрат на обладнанні, інтерференції та інше. Вважатимемо, що максимальний коефіцієнт втрат *I*мах = 60%.

Таблиця 1

Теоретична і реальна пропускна здатність в мережах на основі технології Wi-Fi [2, 3]

Стандарт	Максимальна теоретично розрахована швидкість (Мбіт/с)	Максимальна реальна швидкість (Мбіт/с)
IEEE 802.11a	До 54	До 36
IEEE 802.11g	До 54	До 36
IEEE 802.11n*	До 150	До 50
IEEE 802.11n	До 300	До 100

*мається на увазі використання точок доступу, які підтримують неповноцінний стандарт IEEE 802.11n.

Висновок. Згідно даним розрахунку необхідної швидкості і з урахуванням можливих втрат при передаванні інформації точки доступу на вагонах можуть бути реалізовані через стандарти IEEE 802.11a і IEEE 802.11g. Реалізовувати їх через стандарт IEEE 802.11n не має сенсу, бо це не є необхідно і економічно невигідно.

На головну станцію подається сигнал швидкістю 10 Мбіт/с. Такий сигнал можна реалізувати за допомогою стандартів WiFi IEEE 802.11n або IEEE 802.11n* (табл. 1).

ЛІТЕРАТУРА

1. Ильченко М.Е., Сундучков К.С., Волков С.Э., Ящук А.С. Новые технические решения проблемы повышения скорости движения мобильных терминалов на автобане при приёме сигналов услуг 4G // Науково-технічний журнал „Электроника и связь”, 2011.

2. http://www.gogoair.com/.

3. http://ru.wikipedia.org/wiki/Wi-Fi.

Карловський І.В. (ВІТІ ДУТ)
к.т.н. Штаненко С.С. (ВІТІ ДУТ)

СУЧАСНІ МЕТОДИ ДІАГНОСТИКИ ЗРАЗКІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

На сьогоднішній день одним з найбільш перспективних методів підвищення ефективності функціонування систем діагностики озброєння і військової техніки (ОВТ) є застосування інтелектуальних комп'ютерних технологій – систем, що базуються на різнорідних експертних знаннях [1]. До таких систем відносяться експертні системи (ЕС), які нададуть допомогу при оцінці технічного стану ОВТ, визначенні оптимального способу дій при управлінні технологічними процесами в умовах дефіциту часу на прийняття рішення, неповноті та невизначеності інформації про технічний стан зразка ОВТ.

В архітектурі ЕС можна виділити три основні компоненти: базу знань, машину логічного висновку і інтерфейс користувача. База знань містить факти, правила і евристики, що представляють собою експертні знання про предметну область. Машина логічного висновку містить стратегії та управляючі структури, які використовуються для застосування знань, що містяться в базі знань для вирішення поставленої проблеми. Інтерфейс користувача управляє взаємодією з користувачем. До нього відносяться управління екраном, організація діалогу, пояснювальні здатності системи тощо.

Завдання діагностики ОВТ, по суті, вимагають певного припущення, яке не завжди можна здійснити, використовуючи ймовірнісний підхід. Серед таких завдань найбільш складними є завдання діагностики. Їх складність визначається тим, що серед множини несправностей зразка ОВТ, що мають спільні ознаки, треба вибрати найбільш ймовірні. В ідеалі можна обчислити вірогідність $P(d_i|E)$, де $d_i - i$-та діагностична категорія, E представляє всі необхідні додаткові умови, використовуючи тільки ймовірності $P(d_i|S_j)$, де S_j є j-м симптомом. Формула Байєса дозволяє виконати такі обчислення тільки в тому випадку, якщо, по-перше, доступні всі значення $P(S_j|d_i)$, а, по-друге, правдоподібним є припущення про взаємної незалежності симптомів. У деяких ЕС застосований альтернативний підхід на основі правил впливу, які таким чином пов'язують наявні дані (свідоцтва) з гіпотезою рішення: Якщо в зразку ОВТ спостерігаються симптоми (несправності) $S_1 \wedge ... \wedge S_k$ та мають місце певні фонові умови $f_1 \wedge ... \wedge f_m$ (наприклад, режими роботи), то можна з упевненістю t зробити висновок, що в об'єкті присутня певна несправність d_i. Коефіцієнт впевненості t приймає значення в діапазоні $[-1; +1]$. Якщо $t = +1$, то це означає, що при дотриманні всіх обумовлених умов упорядник правила абсолютно впевнений у правильності висновку d_i, а якщо $t = -1$, значить, що при дотриманні всіх обумовлених умов існує абсолютна впевненість в хибності цього висновку.

Відмінні від $+1$ позитивні значення коефіцієнта вказують на ступінь впевненості в правильності висновку d_i, а негативні значення – на ступінь впевненості в його помилковості. Основна ідея полягає в тому, щоб за допомогою породжуючих правил такого виду спробувати замінити обчислення точного значення ймовірності $P(d_i|S_1 \wedge ... \wedge S_k)$ наближеною оцінкою, і, таким чином, зімітувати процес прийняття рішення людиною – експертом.

ЛІТЕРАТУРА

1. Герасимов Б.М. Системы поддержки принятия решений: проектирование, применение, оценка еффективности / Б.М Герасимов, М.М. Дивизинюк, И.Ю. Субач – Севастополь, 2004. – 320 с.

Картавих В.Ю. (ВІТІ ДУТ)

МЕТОДИКА РОЗРАХУНКУ ОПОРНОЇ МАТРИЦІ МОНІТОРИНГУ ДОМЕНУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

На сучасному етапі розвитку інформаційної мережі спеціального призначення Збройних сил України актуальною є задача побудови системи управління даною мережею. Підтвердженням даного факту є завдання, що ставляться керівним складом перед військами зв'язку та наукових підрозділів ЗСУ. Аналіз сучасних наукових публікацій показує, що одним з основних етапів управління є процес моніторингу об'єктів управління. В сучасних інформаційних мережах спеціального призначення моніторинг мережевих елементів здійснюється постійно. На основі аналізу результатів роботи підсистеми моніторингу визначається стан інформаційної мережі, виявляються або прогнозуються критичні ситуації. Однак, оскільки підсистема моніторингу для отримання значень параметрів мережевих елементів використовує транспортні можливості мережі, існує загроза виведення з ладу мережі шляхом перевантаження її службовим трафіком. Ситуація можлива при неправильному проектуванні підсистеми моніторингу. Таким чином, при проектуванні підсистеми моніторингу, актуальними стають наступні задачі:

– визначення множини параметрів, за якими здійснюється моніторинг мережевого елементу;

– визначення оптимального місця підключення підсистеми моніторингу до інформаційної мережі;

– визначення оптимальних періодів моніторингу параметрів мережевих елементів.

Для визначення оптимальних періодів моніторингу в першу чергу слід визначити опорну матрицю моніторингу, що містить у собі періоди моніторингу мережевих елементів із урахуванням обмеження, що будь-який параметр одного мережевого елементу опитується з рівною періодичністю. Опорна матриця моніторингу повинна задовольняти заданому коефіцієнту співвідношення службового трафіку до пропускної здатності каналів передачі даних між мережевими елементами. В доповіді представлена методика, що складається з трьох етапів. Перший етап побудова графу інформаційної мережі. В даному графі враховується структура інформаційної мережі. Ваги вершин дорівнюють кількості параметрів, що характеризують роботу мережевого елементу в будь-який момент часу. Ваги ребер дорівнюють пропускній здатності каналів передачі даних між мережевими елементами. Коренем графа є підсистема моніторингу.

Другий етап методики є побудова системи лінійних нерівностей на основі графу створеного на першому етапі. При побудові системи нерівностей застосовується інформаційно-часова модель процесу моніторингу і враховується коефіцієнт співвідношення між службовим трафіком та пропускною здатністю каналів передачі даних.

Третій етап методики полягає у розв'язанні системи лінійних нерівностей. Для цього застосовується метод послідовного зменшення невідомих. При застосуванні даного методу слід враховувати області значень невідомих. Результатом вирішення нерівностей є проміжки значень періодів моніторингу кожного мережевого елемента, що задовольняють вимогу співвідношення між пропускною здатністю каналів передачі даних та службовим трафіком. Крайні ліві значення відповідають мінімально можливим періодам моніторингу параметрів мережевих елементів. Таким чином, дані періоди складають опорну матрицю моніторингу інформаційної мережі. За результатами доповіді можна зробити висновки: 1) для отримання оптимальних періодів моніторингу параметрів мережевих елементів слід вирішити оптимізаційну задачу; 2) першим етопом вирішення оптимізаційної задачі є отримання опорної матриці моніторингу; 3) методика визначення опорної матриці моніторингу складається із трьох етапів і застосовує методи теорії графів та теорії систем лінійних нерівностей. 4) результатом методики є опорна матриця моніторингу, яка задовольняє поставленому завданню.

Клевцов С.В. (ВІТІ ДУТ)
Шкіцький В.В. (ВІТІ ДУТ)

ОБГРУНТУВАННЯ ВИБОРУ ТЕХНОЛОГІЇ ІНТЕРАКТИВНОЇ ВЗАЄМОДІЇ З 3D-МОДЕЛЛЮ ПРОГРАМНОГО ТРЕНАЖЕРУ

В даний час дуже актуальним є питання навчання військовослужбовців та здобуття ними нових навичок. Це дуже ресурсоємний та тривалий процес. З метою зменшити вартість та підвищити результативність розроблюють тренажери. Застосування сучасних інтерактивних 3D-тренажерів дозволяє вирішити такі завдання:

– економія коштів за рахунок отримання практичної навички за відсутності обладнання;

– економія часу за рахунок доступності тренажера для великої кількості навчаємих одночасно;

– вироблення навичок в процесі навчання, в областях, де немає можливості провести тренування в реальних умовах.

Основні етапи створення комп’ютерного імітаційного тренажера: аналіз моделюємого технологічного процесу; визначення об'єктів, що підлягають 3D – візуалізації; визначення необхідних елементів управління реальних технічних систем; розробка 3D - моделей об’єктів технологічного процесу; розробка елементів управління (при необхідності); впровадження комп’ютерного імітаційного тренажера; проведення випробувань; розгортання комп’ютерного імітаційного тренажера. Перші три етапи виконують підготовчу роль у розробці тренажеру та виконуються при проведенні аналізу предметної області, командою розробників та фахівців в сфері використання імітуємого обладнання. Розробка 3D-моделей виконується на редакторах тривимірної графіки (Autodesk 3d Max, Maya). Про аналізувавши процес створення імітаційного тренажера виявили, що мінімальний набір технік і механізмів повинен включати:

– полігональне моделювання;

– моделювання на основі неоднорідних раціональних B-сплайнів, NURBS;

– моделювання на основі поверхонь Безьє – підходить для моделювання тіл обертання;

– моделювання з використанням вбудованих бібліотек стандартних параметричних об’єктів (примітивів) і модифікаторів;

– моделювання на основі сплайнів (Spline) з подальшим застосуванням модифікатора Surface – примітивний аналог NURBS, зручний, проте, для створення об'єктів зі складними формами. Для розробки елементів управління та повного розгортання імітаційного тренажера існує декілька підходів. Розглянемо підхід з використанням стандарту WebGL. Стандарт створений на базі OpenGL, що дозволяє розробникам веб-контенту вбудовувати у веб-оглядачі, що підтримують HTML5, повноцінну 3D-графіку, не вдаючись до посередництва плагінів. Бібліотеки побудовані на основі OpenGL забезпечують API(розшифруй) для 3D-графіки, використовують елементи HTML5, також оперують програмним інтерфейсом DOM., при цьому автоматичне управління пам’яттю здійснюється мовою JavaScript. Основні переваги застосування стандарту WebGL: крос-браузерні і крос-платформної сумісності;тісна інтеграція з HTML контентом, включаючи шарову композицію, взаємодія з іншими HTML елементами; апаратне прискорення 3D-графіки для середовища браузера; середа сценаріїв, яка дозволяє легко створити прототип 3D-графіки.

WebGL підтримується наступними браузерами: Mozilla Firefox 4.0, Google Chrome 9, Safari 6.0, Opera 12.00. Підтримка WebGL з’явиться в IE 11. Отже, розробка візуального 3D-тренажеру на WebGL має наступні переваги: взаємодія з тренажером буде проходити централізовано, це дозволить одночасно навчати велику кількість слухачів у різних підрозділах (маштабованість), без необхідності розгортання тренажеру на ПЕОМ (гнучкість). Централізований підхід також надасть можливість резервування даних (надійність) та полегшить налаштування політик безпеки (безпека). Основним недоліком є залежність від доступності та працездатності серверу.

Клімович С.О. (ВІТІ ДУТ)
Волкова Ю.О. (РТФ НТУУ „КПІ”)

МЕТОДИКА ВИБОРУ ПАРАМЕТРІВ ШИРОКОСМУГОВИХ ЗАСОБІВ РАДІОЗВ'ЯЗКУ ПРИ ВПЛИВІ НАВМИСНИХ ЗАВАД

Однією з основних вимог до систем військового радіозв’язку є забезпечення високого рівня завадозахищеності – здатності успішно функціонувати в умовах активної радіоелектронної протидії противника.

Ефективним методом боротьби з навмисними завадами є технології розширення спектра сигналів, яке здійснюється двома основними методами:

псевдовипадкової перебудови робочої частоти (ППРЧ);

прямого розширення спектра (ПРС).

Крім цього, відомі надширокосмугові методи розширення з використанням ультракоротких імпульсів без гармонійної несучої.

В телекомунікаційних системах з кодовим розподілом каналів (КРК) загального призначення використовуються широкосмугові сигнали (ШСС) прямого розширення спектра, наприклад, у стандартах cdmaOne, cdma 2000, WCDMA. Проте вказані стандарти, хоч і забезпечують вищу завадозахищеність у порівнянні з вузькосмуговими системами, розроблені для мирного часу і не здатні ефективно боротися з впливом навмисних завад. В першу чергу, це пов’язано з відносно невеликими значеннями бази сигналу.

У даний час у військових ЗРЗ Збройних Сил України для забезпечення захисту від навмисних завад у деяких типах радіозасобів використовується режим ППРЧ, але, на жаль, зі швидкістю перебудови лише 312,5 стрибків за секунду. Сигнали прямого розширення не використовуються.

Кожна із технологій розширення спектра має свої переваги та недоліки. Слід зазначити, що основною перевагою ШСС з ПРС порівняно з ППРЧ є значно вища прихованість, оскільки остання, по суті, у фіксований момент часу є вузькосмуговою системою зі значною спектральною щільністю потужності (СЩП) сигналу (що у кілька разів перевищує шум в кагналі).

Тому актуальним завданням є створення широкосмугових ЗРЗ з ПРС та розробка методики вибору їх параметрів при впливі навмисних завад.

Для цього на етапі проектування мережі проводиться аналіз вихідних даних та вибираються раціональні межі можливих змін їх значень. До вихідних даних, як для переносних, так і базових станцій, відносяться: діапазони частот на передачу та прийом, тип антен, потужності передавачів та чутливість приймачів, види завадостійких кодів, види модуляції, види псевдовипадкових послідовностей для розширення спектра та реалізації КРК та ін. Зупинимось детальніше на параметрах, значення яких змінюється під час ведення зв’язку з метою забезпечення максимальної пропускної спроможності при забезпеченні необхідної завадостійкості.

База ШСС. Значення бази повинне бути максимально можливим, але воно обмежується наступними факторами:

чутливість приймача (яка, в свою чергу, залежить від смуги пропускання, а значить – ширини спектра сигналу);

широкосмуговість антенно-фідерного тракту;

широкосмуговість підсилювачів потужності та інших каскадів приймально-передавального тракту.

ПВП. В теорії інформації та кодування є відомою достатньо велика кількість різних типів кодів та послідовностей. Проте, лише обмежена кількість із них може використовуватися для розширення спектра сигналів та організації множинного доступу з кодовим розділенням каналів. Перший тип послідовностей, що використовується тільки для

розширення спектра сигналів, володіє АКФ з низьким рівнем бокових пелюстків та вузьким центральним пелюстком. Цей тип послідовностей використовують для вимірювання часових запізнень, селективного відбору радіосигналів. До них належать послідовності Баркера, m-послідовності, послідовності Лежандра, тощо.

Послідовності, які використовують для розширення спектра сигналів та організації кодового розділення каналів мають слабкий взаємний кореляційний зв'язок. Прикладами таких послідовностей є послідовності Уолша, ансамблі послідовностей Голда, множини Касамі, тощо. Відомо, що у послідовностей, АКФ яких є близькою до ідеальної, наявний сильний взаємний кореляційний зв'язок, а у послідовностей зі слабким взаємним кореляційним зв'язком автокореляційна функція містить великі бокові пелюстки та широкий центральний пелюсток.

Військові СРЗ, очевидно, мають меншу абонентську ємність, тому менш критичні до ВКФ послідовностей. У той же час, у разі виявлення факту передачі інформації й запису її відрізка противник може створити ретрансльовану заваду у напрямку кореспондента. У цьому випадку, для мінімізації її впливу саме АКФ повинна бути мінімальною. У той же час, якщо стратегія противника буде спрямована на визначення структури регістра формування ПВП та постановку імітаційної завади, на перший план виходить забезпечення мінімальної ВКФ. Тому в процесі ведення зв'язку необхідно передбачити можливість зміни виду ПВП, а також структури регістрів для їх формування.

Адаптивне регулювання потужності. Важливим параметром, що визначає ефективність мережі в цілому є використання алгоритмів адаптивного регулювання потужності. На вході приймача сигнали кореспондентів мережі не повинні значно перевищувати сигнал кореспондента, в іншому випадку робиться неможливим виділення корисної інформації. Така ситуація можлива і при постановці ретрансльованих або імітаційних навмисних завад. Тому в процесі ведення зв'язку слід передбачити адаптивне підвищення потужності корисного сигналу станцією кореспондента у випадку погіршення зв'язку для протидії навмисним завадам.

Таким чином, методика вибору параметрів широкосмугових засобів радіозв'язку при впливі навмисних завад складається з наступних етапів.

1. Визначення вихідних даних.
2. Оцінка завадової обстановки в каналі: визначення наявності, типу та інтенсивності навмисних завад, визначення рівня внутрішньосистемних завад.
3. Визначення величини бази сигналу.
4. Оптимізація ансамблю послідовностей. У сприятливій завадовій обстановці обираються ПВП для максимізації ВКФ, а отже – мінімізації внутрішньосистемних завад. При недостатній завадостійкості реалізується зміна виду ПВП.
5. Зменшення швидкості передачі інформації при перевищенні коефіцієнта помилки порогового значення. Зменшення швидкості може реалізуватися двома способами. При першому збільшується база (для отримання більшого виграшу від обробки сигналу). При другому – збільшується швидкість коригувального коду. Конкретний спосіб визначається в залежності від його ефективності в конкретній завадовій обстановці.
6. Збільшення потужності передавача станції кореспондента при блокуванні приймача через велику потужність сигналу завади і адаптивне її зменшення при покращенні завадової обстановки.

Новизна методики полягає у раціональному виборі для кодового розподілу каналів такого ансамблю ПВП із обраної множини, який забезпечує максимальну завадостійкість для конкретної завадової обстановки в каналі зв'язку.

Напрямком подальших досліджень є розробка імітаційної моделі та проведення дослідження ефективності запропонованої методики для різних завадових ситуацій.

Коваленко І.Г. (НЦЗІ ВІТІ ДУТ)
Феріма Ю.В. (НЦЗІ ВІТІ ДУТ)

АНАЛІЗ МЕТОДИК ПРОГНОЗУВАННЯ ПОСЛАБЛЕНЬ РІВНІВ РАДІОСИГНАЛІВ ЗА РАХУНОК РОЗПОВСЮДЖЕННЯ

При плануванні побудови систем радіозв'язку актуальною є задача оцінки послаблень рівнів радіосигналів за рахунок територіального рознесення радіоелектронних засобів (РЕЗ). Рівень радіосигналів, прийнятих після проходження по трасі розповсюдження, залежить від характеристик місцевості, погодних явищ, стану тропосфери та іоносфери в залежності від пори року, часу доби тощо. Внаслідок цього радіосигнал на вході приймача має паразитні амплітудно-фазові випадкові зміни (завмирання) [1]. В залежності від умов розповсюдження радіосигналів завмирання мають окремі назви: мерехтіння, загальні завмирання, частотно-селективні завмирання тощо. Існує декілька видів розповсюдження радіохвиль, а саме: через тропосферний хвилевід, за допомогою земних хвиль, через іоносферні хвилі, просторовими хвилями (що складаються з прямих та відбитих хвиль), за рахунок дифракції, шляхом тропосферного розсіювання, в межах прямої видимості та через розсіювання гідрометеорами [2]. На рис. 1 показані основні довгострокові види розповсюдження радіохвиль, які обумовлюють величину послаблення рівнів радіосигналів (як корисних, так і завад). На рис.2 показані основні короткострокові види розповсюдження, які призводять до створення радіозавад, але, в деяких випадках, призводять до підвищення рівня корисних радіосигналів [2].

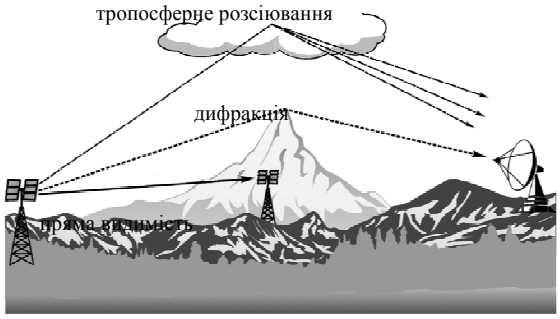


Рис.1 Довгострокові види розповсюдження радіосигналів

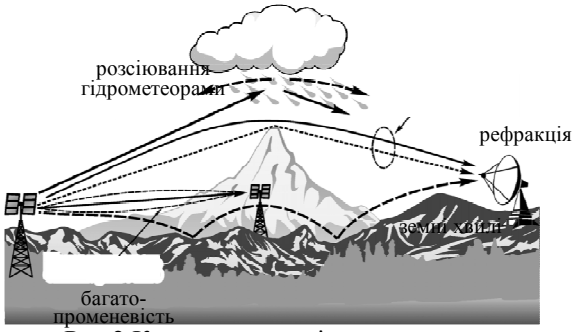


Рис.2 Короткострокові види розповсюдження радіосигналів

В залежності від діапазону частот основне значення мають окремі види розповсюдження радіохвиль – табл.1 [2].

Таблиця 1

Діапазон частот	Дальність радіозв'язку	Види розповсюдження
3...30 кГц	тисячі км	Хвилевід
30..300 кГц	тисячі км	Земна хвиля, іоносферна хвиля
0,3...3 МГц	тисячі км	Земна хвиля, іоносферна хвиля
3...30 МГц	сотні-тисячі км	іоносферна хвиля
30...300 МГц	сотні км	Просторова хвиля, тропосферне розсіювання, дифракція
0,3...3 Гц	до 100 км	Просторова хвиля, тропосферне розсіювання, дифракція, в межах прямої видимості
3...30 Гц	до 30 км земля-космос	В межах прямої видимості
30...300 Гц	до 20 км земля-космос	В межах прямої видимості

Завади між станціями різних систем радіозв'язку можуть створюватись на основі як довгострокових, так і короткострокових механізмів розповсюдження [2]. Середовища розповсюдження радіосигналів від джерел і завад можуть мати різні характеристики, тому проблема надійного прогнозування рівнів завад пов'язана зі складністю врахування великої кількості типів і параметрів трас та умов розповсюдження в них. При цьому в окремі періоди часу на визначеної відстані від передатчика можуть бути ключовими різні механізми розповсюдження радіохвиль. Найбільш повні та загальноприйняті дані про розповсюдження радіохвиль представлені в більше ніж 20-ти рекомендаціях Міжнародного союзу

електрозв'язку (МСЕ) (серія Р) [3]. Основні методики прогнозування розповсюдження радіохвиль для наземних радіослужб представлені в таблиці 2. В запропонованих методиках використовуються окремі параметри середовища розповсюдження радіохвиль, які визначаються (або розраховуються) за допомогою додаткових рекомендацій МСЕ-R (Р. 839, 837, 1511, 836, 1510, 453, 840 та інші).

Таблиця 2

Мето-дики	Результат	Частота	Відстань	Висота термінала	Вхідні дані	Примітки
Р.368	Напруженість	10кГц-30МГц	1-10000км	Земля	Частота, провідність земної поверхні	Всі радіослужби
Р.452	Втрати на трасі	0,7-30ГГц	Радіогори-зонтідалі	Земля	Профіль траси, частота, %часу, висоти антен, координати передавача/ приймача, метеодані	Станції на поверхні Землі; завади
Р.530	Втрати	0,15-40ГГц	До2000км	Пряма видимість	Відстань, частота, висоти, %часу, перешкоди, метеодані, профіль траси	Фіксований зв'язок прямої видимості
Р.533	Параметри ЕМС	3-30МГц	0-40000км	–	Координати, число сонячних плям, часовий період, потужність, тип антен	Радіомовна, фіксована та рухома служби
Р.534	Напруженість	30-100МГц	0-4000км	–	Відстань, частота	Фіксована, рухо-ма, радіомовна служби
Р.684	Завмирання	0,8-20Гц	0-4000км	–	Координати, відстань, потуж-ність, частота, період часу, кількість плям на сонці	Фіксована та рухома служби
Р.1147	Напруженість	0,15-1,7МГц	50-12000км	–	Координати, відстань, кількість плям на сонці, потужність, частота	Радіомовна служба
Р.1410	Зона покриття	3-60ГГц	0-5км	–	Частота, розмір чарунки, висота термінала, параметри забудови	Широкосмуговий доступ
Р.1546	Напруженість	30-3000МГц	1-1000км	0-3000м	Характеристики траси, відстань, висоти антен, частота, %часу	Наземні служби з пункту в зону
Р.1812	Напруженість	30-3000МГц	До радіогори-зонту і далі	0-3000м	Профіль і характеристики траси, відстань, висоти антен, частота, % часу, метеодані	Наземні служби з пункту в зону

Зміст запропонованих МСЕ рекомендацій відображає складність моделювання та розрахунків параметрів розповсюдження радіохвиль для визначення електромагнітної сумісності (ЕМС) РЕЗ. Крім того для підвищення точності розрахунків параметрів ЕМС необхідна точна інформація щодо профілів та характеристик місцевості, забудови та інше. Відсутність цієї інформації або її неточність може привести к отриманню неправильного результату розрахунків. Вказані фактори додатково ускладнюють використання запропонованих методик. Для засобів радіозв'язку військового призначення висуваються підвищенні вимоги з надійності, розвідзахищеності та протидії засобам радіоелектронної боротьби супротивника. В цих умовах застосування запропонованих МСЕ методик, при наявності неточних вихідних даних, невиправдано ускладнює розрахунки параметрів та призводить до отримання невірних результатів оцінки ЕМС РЕЗ військового призначення.

Тому постає актуальною задача розробки методик по визначенню електромагнітної сумісності радіоелектронних засобів спеціального призначення на основі рекомендацій МСЕ, які б враховували особливості технічних характеристик та особливостей застосування РЕЗ військового призначення, наявність та точність вихідних даних.

ЛІТЕРАТУРА

1. Электромагнитная совместимость радиоэлектронных средств / Седельников Ю.Е. – Казань. ЗАО „Новое знание", 2006 – 304 с.

2. Управление радиочастотным спектром и электромагнитная совместимость радиосистем. / Под ред. д.т.н., проф. М.А.Быховского. – М.: Эко-Трендз, 2006.– 376 с.

3. Рекомендация МСЭ-R Р.1144-5, 2009. Руководство по использованию методов прогнозирования распространения радиоволн.

Козій С.О. (ВІТІ ДУТ)

ЕВОЛЮЦІЯ ТЕХНОЛОГІЇ LTE (RELEASE 11, 12) ТА ЇЇ ВАРІАНТИ ВПРОВАДЖЕННЯ У ВІДОМЧУ МЕРЕЖУ

Поряд з підготовкою більшості країн до впровадження 3G– стандартів передачі даних в GSM – мережах, в світі вже почалося впровадження 4G – технології четвертого покоління, захищених і ефективних , призначених для обміну даними на надвисоких швидкостях

Широке розповсюдження мобільних пристроїв стає поштовхом до розробки нових версій технології, а саме LTE release 11 та 12 – наступних версій стандарту, які наразі перебувають у завершальній стадії розробки. У поточних планах організації 3GPP 2013 рік означено як рік остаточного затвердження 11 версії.

Після остаточного затвердження у 2010 році release 10 стандарту LTE розробники ведуть активну роботу над 11 та 12 версіями, які мають вирішити наступні проблеми:

1) Перехід до діапазонів більш високих частот: 3 ГГц і вище (зазначено у стандарті 3GPP TR 36.932v12.0.0(2012-12));

2) Підвищення швидкості передачі даних завдяки технології багатоточкової відправки та прийому даних (вимоги до швидкості описані у вищезгаданому стандарті 3GPP TR 36.932 v12.0.0 (2012.12));

3) Розширену підтримку IPv6 (вимоги зазначені у стандарті 3GPP TS 23.402 v11.5.0 (2012-12));

4) Поєднання технологій Wi-Fi та 4G;

5) Можливість прямого з'єднання двох абонентських 4G-пристроїв.

Важливим напрямом розвитку є поєднання технологій 4G та Wi-Fi, що дозволить ще більше підвищити швидкість передачі даних на відносно невеликих відстанях. Наразі така інтеграція підтримується на теоретичному рівні. Головна ідея полягає у тому, що пристрій здійснює пошук не лише базових станцій 4G, але й точок доступу Wi-Fi. Якщо пристрій знаходить Wi-Fi з високим рівнем сигналу, то він перемикається на нього і таким чином значно додає у швидкості. Ще одним аспектом розвитку технології 4G LTE є можливість прямого з'єднання двох абонентських 4G-пристроїв, без використання базової станції. Її сутність полягає у пошуку одним пристроєм іншого у зоні прийому та відправленні запиту, чи підтримує інший пристрій пряме з'єднання. Якщо так, то з'єднання буде встановлено напряму. Для впровадження технології LTE у відомчу мережу потрібно вирішити основну проблему, це правильний вибір частотного діапазону. У нижньому діапазоні важко знайти смугу частот необхідної ширини. У верхньому ж діапазоні необхідна велика кількість БС. Можливо, що більшість мереж LTE, аналогічно GSM, будуть 2-діапазонні.

Можливі три архітектурні варіанти по впровадженню технології LTE у мережу:

– радіосистема кожного оператора буде підключатися до загальної опорної мережі;

– перехресне підключення радіосистем до опорних мереж по схемі „кожний з кожним";

– оператори виділяють сегмент опорної мережі для спільного користування і підключають до загальної частини свої індивідуальні мережі.

Таким чином, в роботі розглянуті основні проблеми бездротових технологій та запропоновані стандарти, які зможуть це вирішити (LTE release 11 та 12). Вони легко конвергуються із стандартами 3G, нададуть змогу користуватися більш швидким, якісним, безпечним та дешевим мобільним Інтернетом, і в той же час прямого з'єднання 4G-пристроїв, що задовольняє вимогам сучасних відомчих мереж.

ЛІТЕРАТУРА

1). 3GPP LTE release 11 overview / Mobile Broadband Standart. – Rel-11_description_20130121.zip. – 30.01.2013;

2). Тихвинський В.О., Терентьєв С.В., Юрчук А.Б. Сети мобильной связи LTE, технология и архитектура. – М.: Еко-Трендз, – 2010.

к.т.н. Корольов А.П. (ВІТІ ДУТ)
к.т.н. Труш О.В.(ДУТ)

МАГНІТООПТИЧНІ ЗАСОБИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Інтерес до носіїв магнітного запису багато в чому визначається тим, що, не дивлячись на наявність альтернативних носіїв (оптичні диски, флеш-пам'ять і ін.), вони володіють істотними перевагами і, очевидно, застосовуватимуться ще достатньо довго.

У міру зростання об'ємів інформації, яка реєструється на магнітних носіях, усе більшу актуальності набувають питання вдосконалення методів і засобів її технічного захисту. В зв'язку з цим представляють інтерес технології, які забезпечують доступ на фізичному рівні до зареєстрованої інформації, тобто до характеру розподілу неоднорідних магнітних полів над носієм. Найбільш поширені методи візуалізації полів магнітними частинками (метод порошкових фігур; візуалізація в колоїдному розчині; візуалізацію на феромагнітній плівці і метод деформації (пластифікації) робочого шару) носять якісний характер. Застосування електронно-оптичних методів, які володіють субмікронним просторовим дозволом, істотно обмежене їх унікальністю і складністю технічної реалізації. Мініатюрні датчики, вживані для топографування магнітних полів (Холла, індукційні і магніторезистивні), володіють невисоким просторовим дозволом і позбавлені властивостей візуалізації.

Порівняно недавно розроблений і успішно розвивається магнітооптичний метод (МО) візуалізації і топографування просторово-неоднорідних магнітних полів монокристалічними плівками вісмутоскладових феррогранатів під впливом полів розсіяння досліджуваних магнітних сигналограм (МС), і задаючих полів зсуву (компенсації).

Існує ряд прикладних завдань технічного захисту інформації (ТЗІ), вирішення яких вимагає візуалізації і топографування полів розсіяння, контроль за знищенням інформації, контроль наявності несанкціонованих записів, апаратне кодування (захист) інформації; ідентифікація носіїв інформації, контроль достовірності і цілісності МС, відновлення частково знищеної інформації, класифікація, ідентифікація і діагностика апарату магнітного запису за наслідками аналізу МС і ін. Зупинимося детальніше на проблемі контролю за знищенням інформації, зафіксованої на магнітних носіях. Джерелами утворення залишкової інформації є:

1. Недостатній рівень (нижче за насичення магнітного носія магнітного поля стирання магнітної головки).
2. Неспівпадання форматів запису і стирання МС.
3. Неспівпадання форматів запису і відтворення МС.

Якщо як критерій норми контролю наявності залишкової інформації прийняти мінімальний фізичний помітний рівень залишкової намагніченості магнітних сигналограм, який перевищує шуми носія, то нормою повинен бути визнаний рівень відтворного сигналу порядку – 77 дБ. Існують різні варіанти розташування магнітних доріжок запису і відтворення, які можуть виникати в процесі дослідження залишкової інформації. Це: повний збіг доріжок, частковий збіг доріжок, частковий збіг доріжок при сегментності доріжки запису, неспівпадання доріжок.

1. *Проблема знищення конфіденційної інформації.* Достатньо гострою є проблема знищення конфіденційної інформації (стирання з магнітних носіїв), без знищення самого носія. Ступінь знищення інформації істотно залежить від вживаної апаратури і методів стирання, і у ряді випадків не є достатньою. Так, застосування штатних засобів стирання – апаратури магнітного запису – для розмагнічування сигналограми і подальше застосування штатних засобів відтворення для контролю якості стирання, у ряді випадків, може привести до помилкових виводів про повне знищення інформації. Найбільш вірогідними причинами виникнення залишкової (нестертої) інформації можуть бути:

– засмічення, порушення регулювання, або дефекти магнітної головки стирання, які приводять до стирання запису не по всій ширині доріжки запису;

– поперечні переміщення магнітного носія в стрічкопротяжних механізмах, що не мають магнітної головки стирання (схема „запис по запису”, вживаний у ряді диктофонів, автовідповідачів і бортових реєстраторів) (рис 1);

– неспівпадання форматів запису і стирання (рис. 2).

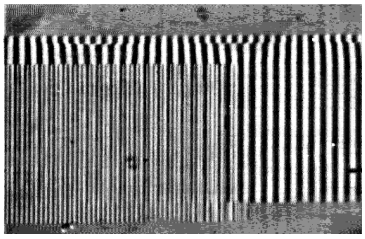


Рис.1

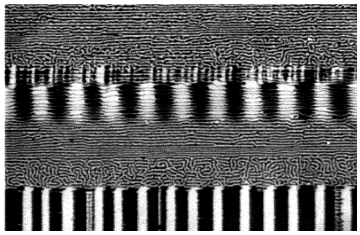


Рис.2

Магнітооптика у вигляді датчика контролю залишкової інформації максимально використовує своє призначення та може відчувати і відображати двовимірні магнітні поля розсіяння на рівні шумів магнітного носія з просторовим дозволом менш 1мкм .

2. *Магнітооптичний контроль несанкціонованих записів на магнітних носіях.*

Під „несанкціонованими” маються на увазі приховані записи, які не відтворюються стандартною апаратурою відтворення. При цьому маскуючий запис, який не представляє таємності, відтворюється стандартними засобами і створює враження єдиного запису на даному носієві.

3. *Магнітооптичні дослідження достовірності магнітних сигналограм.*

Якщо складний і важливий технічний об’єкт управляється апаратурою, де інформація про управління записана на магнітний носій, виходить з ладу, то важливо знати, чи була зареєстрована інформація цілісним оригіналом, або вона була змінена шляхом монтажу, а також на якому апараті була змонтована і записана магнітна сигналограма.

4. *Магнітооптичне кодування і ідентифікація магнітних носіїв.*

Одному з найважливіших завдань при вирішенні проблем ТЗІ є завдання захисту від несанкціонованого доступу до інформації, а також від несанкціонованого доступу до систем, які використовують запис інформації, – особливо до стратегічно важливих систем.

Як варіант вирішення цієї проблеми може служити магнітне кодування магнітних носіїв інформації з використанням магнітооптичної візуалізації.

5. *Магнітооптичне відновлення частково знищеної (зіпсованою) інформації.*

В процесі зберігання і використання інформації трапляються випадки її часткового або повного знищення в результаті помилок, халатності або яких-то обставин. При цьому ступінь збитку від втрати інформації іноді може бути дуже високим. Тому завдання відновлення частково знищеної інформації часом буває вельми актуальним. Проведені дослідження показали можливість відновлення змісту мовного повідомлення при залишковій ширині доріжки запису до 5мкм (менше 1% стандартної ширини доріжки аудіокасети). Іншими словами, відновлення мовного повідомлення попереднього і пред-попереднього запису автовідповідача з технічної точки зору не складає проблеми.

Всі описані технічні засоби на основі магнітооптики успішно пройшли апробацію і підтвердили свою конкурентоспроможність і ефективність при вирішенні практичних завдань ТЗІ.

ЛІТЕРАТУРА

1. *Levy S.V., Ostrovsky A.S., Agalidi Yu.S.* Magnetic field topographical survey by space-time light modulators. SPIE Proceedings Vol. 2108 (2007).

2. *Губенберг В. Візуалізация* магнітному запису. Техніка магнітного відеозапису. М.: Іноземна література, 1982, с. 314.

3. *Лайфер М.В. Крижановський І.А.* Теоретичні основи магнітного запису сигналів на рухомий носій. К.: Віща школа, 1992, с.270.

д.т.н. Кравченко Ю.В. (ДУТ)
к.в.н. Микусь С.А. (НУОУ)

ПІДХІД ЩОДО ОПТИМІЗАЦІЇ ТОПОЛОГІЇ СИСТЕМИ ЗВ'ЯЗКУ І АВТОМАТИЗАЦІЇ УПРАВЛІННЯ ВІЙСЬКАМИ

При синтезі складних технічних систем, до яких повною мірою відноситься і система зв'язку і автоматизації управління військами (АУВ), виникає необхідність рішення задач дискретної оптимізації. Для цих задач, як відомо, важлива боротьба за точність. Дослідження показали, що в багатьох випадках тільки повний або направлений перебір можуть дати точне рішення. Як завжди, повний перебір не можливий через проблему великої розмірності. Відомо, що серед методів та алгоритмів направленого перебору найкращим є той, для якого до його початку або в період його виконання можливо відкинути як можна більше неперспективних варіантів (елементів множини допустимих рішень). Для складних систем множина припустимих рішень при завданні оптимізації структури є комбінаторним об'єктом, а цільова функція визначається алгоритмічно. У таких умовах актуальною є розробка найбільш ефективних методів пошуку точного рішення. Існуюча теорія дискретної оптимізації, яка досить повно описана у багатьох наукових роботах, вимагає розвитку щодо конкретних технічних завдань. Це пов'язано з тим, що основою процедури, яка дозволяє зменшити область припустимих рішень, є апріорна інформація, яка безпосередньо залежить від конкретної ситуації або технічної системи [1 – 4].

Метою доповіді є доведення результатів досліджень щодо розробки методу поетапного зменшення потужності бази *k*-однорідного матроіда для організації направленого перебору в задачах дискретної оптимізації на прикладі оптимізації топології системи зв'язку і автоматизації управління військами.

Введено поняття матроіда топології системи зв'язку і АУВ.

Визначення 1. Матроід – комбінаторний об'єкт, що представляє собою пару $M = (E, \varepsilon)$, де E – кінцева непуста множина елементів матроіда, а ε – непуста множина його підмножин (назвемо їх базами), які задовольняють наступним двом умовам:

В1). Ніяка з баз не міститься в іншій базі.

В2). Якщо B_1 і B_2 – бази, то для будь-якого елемента $b \in B_1$ існує такий елемент $c \in B_1$, що $(B_1 \setminus b) \cup c$ – також база.

$|Y \cup Z| = |X|$.

Визначення 2. Матроідом топології системи зв'язку і АУВ називається пара $M = (E, \varepsilon)$, де E – кінцева непуста множина елементів матроіда, що представляють собою зв'язки між елементами, а ε – непуста множина його підмножин (названих базами).

Матроід топології системи зв'язку і АУВ є *k-однорідний* матроід на E, базами якого є всі незалежні між собою підмножини множини E, що містять рівно k елементів.

У роботі [2] запропоновано комбінаторний підхід у дискретній оптимізації, що для синтезу складної технічної системи розглядається як сукупність методу часткових порядків, концепції опуклості в частково впорядкованих множинах і схеми побудови серії градієнтних алгоритмів. Доведено, що на матроіді градієнтні алгоритми знаходять, як правило, оптимальне рішення. В основі доказу лежить ідея широко відомої для передгеометрії теореми Радо-Едмонса [3]. Жадібні алгоритми і їхні властивості досліджено досить добре, та їхнє знання при рішенні оптимізаційних задач є важливим. Якщо вдається звести подібну задачу до того, що множина допустимих рішень є матроідом, то в більшості випадків варто застосовувати жадібний алгоритм, оскільки він досить ефективний у практичному змісті. Якщо ж виявиться навпаки, і множина можливих варіантів не утворить матроід, тоді, швидше за все, градієнтний алгоритм не буде ефективний.

Ідея застосування градієнтних алгоритмів при оптимізації топології системи зв'язку і АУВ заснована на особливостях функціонування системи. Тому як градієнтом виступає відношення мажоризації. Дійсно, для такої системи збільшення кількості елементів (зв'язків між елементами) однозначно веде до росту (або не до зниження) значення показників ефективності її функціонування. Пропонується здійснювати пошук рішення за принципом послідовного зменшення кількості надлишкових елементів і зв'язків структури для забезпечення відновлення максимальних функціональних можливостей при мінімальному використанні ресурсу. На всіх етапах занурення множини допустимих рішень в частково впорядковану множину здійснюється на основі відношення мажоризації. Спочатку формується *k*-однорідна топологія системи зв'язку і АУВ з елементів і зв'язків, множина баз яких є множиною всіх можливих структур з максимальної кількості елементів і зв'язків $M = (E, \varepsilon); A \subseteq \varepsilon; \rho(A) = |A|$. Далі застосування жадібного алгоритму дозволяє знайти найкраще рішення, для якого розраховується значення показника ефективності. Слід зазначити, що перебір варіантів здійснюється за всіма видами надмірності $\alpha^* = \arg\max P(\alpha) \; \forall \alpha \in A_1$ при $P(\alpha^*) \geq P_{ЗАД}$.На наступному етапі відбувається зменшення потужності бази матроіда на одиницю і попередня процедура повторюється із застосуванням градієнтного алгоритму і розрахунком значення показника функціональної стійкості. Далі за показником функціональної стійкості виконується порівняння знайденого рішення із заданим рівнем функціональної стійкості.

Для рішення, що задовольняє за показником ефективності, послідовно перевіряються варіанти, включені за допомогою відношень часткового порядку в даний варіант, із метою пошуку рішення з мінімальним застосуванням надмірності і заданим рівнем функціональної стійкості. Процедура поетапного зменшення потужності бази матроіда буде тривати доти, поки рішення не вийде за межі потрібної ефективності. У цьому випадку оптимальним буде рішення, отримане на попередньому етапі $\alpha^* = \arg\max P(\alpha) \; \forall \alpha \in A$. Даний метод класифікується як точний метод дискретної оптимізації, а саме градієнтний метод направленого перебору. Ефективність розробленого методу оцінино за кількістю звернень до *f-оракула* і визначено значний виграш у порівнянні з повним перебором.

Таким чином, у доповіді запропоновано метод поетапного зменшення потужності бази (базиса) матроіда, який класифікується як точний метод дискретної оптимізації, побудований за принципом направленого або неявного перебору. В основі методу є науково-обґрунтоване положення про те, що область допустимих рішень асоціюється з таким комбінаторним об'єктом, як матроід, та про те, що максимальна за включенням незалежна підмножина множини допустимих рішень, тобто база (базис) матроіда, відображає мінімально-необхідний склад топології системи. Запропонований метод є основою методики оптимізації топології системи зв'язку і АУВ.

ЛІТЕРАТУРА

1. Емеличев В. А. Многогранники, графы, оптимизация (комбинаторная теория многогранников/ В. А. Емеличев, М. М. Ковалев, М. А. Кравцов. – М.: Наука, Главная редакция физико-математической литературы, 1981. – 344 с.

2. Ковалев М. М. Матроиды в дискретной оптимизации / М. М. Ковалев. – Минск : Изд-во „Университетское", 1987.– 222 с.

3. Большие технические системы: проектирование и управление / Л. М. Артюшин, Ю. К. Зиатдинов, И. А. Попов, А. В. Харченко / Под ред. И. А. Попова. – Харьков: Факт, 1997. – 284 с.

4. Кравченко Ю. В. Методология многокритериальной дискретной оптимизации сложных технических систем на матроидных структурах / Ю. В. Кравченко, В. В. Афанасьев // Збірник наукових праць ІПМ в Е ім. Г. Є. Пухова. – Вип. 22 – 1. – К. : ІПМЕ ім. Г. Є. Пухова – 2003. – С. 73 – 78.

Краснощок Я.О. (ВІТІ ДУТ)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТА РОЗВИТКУ ГІБРИДНИХ СИСТЕМ ПЕРЕДАЧІ НА БАЗІ ТЕХНОЛОГІЙ FSO ТА WIMAX

В гібридних системах передачі на базі технологій FSO (Free Space Optics, Безпровідна оптика) та WiMax, для утворення основного каналу використовується обладнання FSO, а в якості резервного WiMax.

Для передачі даних, голосу та відео від однієї точки доступу до іншої у системах FSO застосовують технології організації високошвидкісних каналів зв'язку за допомогою інфрачервоного випромінювання по повітрю в діапазонах 780–850 нм та 1520–1600 нм.

До основних переваг FSO можна віднести

− не потрібно отримувати дозвіл на використання частотного діапазону;

− висока захищеність каналу від несанкціонованого доступу і скритність;

− можливість встановити FSO там, де важко прокласти проводову лінію зв'язку)

− швидкість і простота розгортання FSO-мережі.

− висока швидкість і якість цифрового зв'язку;

− високий рівень завадостійкості і перешкодозахищеності;

Поряд з основними перевагами систем FSO добре відомі і їх головні недоліки:

− залежність доступності каналу зв'язку від погодних умов;

− необхідність забезпечення прямої видимості між випромінювачем і приймачем;

− обмежена дальність зв'язку.

Серед зазначених недоліків найбільший вплив на систему мають погодні умови, а саме туман, сніг та дощ. Тому, було вирішено використовувати резервний радіоканал передачі даних організований WiMax–маршрутизатором для якого дані погодні умови не несуть суттєвого впливу.

Високоефективні гібридні системи, засновані на використанні технології FSO, є реальною альтернативою, якщо мережному розробнику необхідно враховувати вплив погодних умов, протяжність лінії безпроводового зв'язку, вимоги до смуги пропускання і потенційну можливість використання системи FSO в якості допоміжних резервних каналів зв'язку.

Завдяки своїм перевагам, гібридні системи передачі – дозволяють вирішувати проблеми „останньої милі", розвивати міські мережі передачі даних і голосу, здійснювати підключення домашніх мереж або офісів до мережі Інтернет, а також організовувати резервні канали зв'язку або розширювати існуючі канали при високому ступені захищеності.

Крім того, технологія використовується для комунікацій між космічними апаратами. Застосування даної системи має місце в будівлях які мають історичну цінність, чи там де необхідно максимально захистити дані, що передаються по лазерному каналу.

Таким чином, галузі для застосування технології, можуть бути різними, в залежності від сфери застосування, та завдань, що будуть вирішуватись. Особливу увагу слід звернути на управління ризиками, що має критичне значення для установ та будівель, які повинні дотримуватися законодавства, що вимагає від них збереження державної таємниці та конфіденційності.

В тих місцях де прокладання кабелів недоцільне, чи має суттєві труднощі через особливості рельєфу, чи там де лінія зв'язку була втрачена через стихійне лихо і необхідно в короткі строки відновити зв'язок гібридні системи передачі будуть найкращим варіантом.

Кримець Б.В. (НУОУ ім. І.Черняховського)

ПРОБЛЕМНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ ВІЙСЬКАМИ ВІД ВИТОКУ КАНАЛАМИ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ТА НАВЕДЕНЬ

Автоматизована система управління військами (АСУ)призначена для автоматизації всіх етапів процесу управління – збору інформації, планування та організації підготовки та проведення військових операцій контролю за виконанням прийнятих рішень. В системі обробляється інформація що стосується організації, чисельності, дислокації, озброєння та матеріально-технічного забезпечення підрозділів, військових частин та угрупувань військ, що становить держану таємницю та в обов'язковому порядку підлягає захисту від витоку каналами побічних електромагнітних випромінювань та наведень (ПЕМВН). Для захисту інформації від витоку каналами ПЕМВН в АСУ створюється комплекс технічного захисту інформації який повинен включати організаційні заходи, пасивні або активні методи захисту інформації [1, 5].

В складі АСУ Збройних Сил України здебільшого використовуються офісні не захищені персональні комп'ютери, ноутбуки та оргтехніка, а для захисту від витоку каналами ПЕМВН застосовуються активні засоби – генератори високочастотного шуму. Виробниками цих засобів приведенні наступні технічні характеристики: спектральна щільність напруженості електромагнітного поля шуму – до 60 дБ, робоча смуга частот від 10 кГц до 2500 МГц [2].

Аналіз значень напруженості та частот ПЕМВН сучасних складових АСУ показує, що генератор високочастотного шуму не спроможний створити достатню напруженість електромагнітного поля на частотах більше 2500 МГц, для таких елементів як послідовний інтерфейс SATA-3 – 30 дб на частоті 6000 МГц; процесор – 20 дб на частоті більше 3 МГц, відеоадаптер – 20 дб на частотах до 6500 МГц та активне обладнання оптоволоконних обчислювальних мереж 20 дб на частотах до 5000 МГц [3,4].

Можливості радіоелектронних засобів розвідки з використанням параболічних антен (ширина діаграми направленості від 1 градусу та коефіцієнт направленої дії до 30 дб) дозволяють отримати просторову селекцію інформативного сигналу ПЕМВН на відстані від 100 м., якщо інформативні елементи АС знаходяться за 2 метра від генератора високочастотного шуму.

Разом з тим випромінювання високочастотного генератора (більше 8 ват) є демаскуючою ознакою АСУ. Сучасні засоби розвідки можуть виявити це випромінювання, визначити його точне місцезнаходження, та надати дані для подальшого знищення, тощо.

До організаційних методів захисту інформації від витоку каналами ПЕМВН відноситься збільшення контрольованої зони, встановлення обмежуючих режимів роботи, виключення обробки критичної інформації в АСУ. Використання тільки даних методів обмежує функціональність та інформаційну діяльність в АСУ.

До пасивних методів захисту відноситься: екранування, зниження потужності випромінювань і наведень, зниження інформативності сигналів. [5]

Екранування є одним з найефективніших методів захисту від електромагнітних випромінювань. Для мінімізації інформативних ПЕМВН необхідне комплексне екранування елементів схем, блоків, пристроїв що входять в АСУ та приміщення (об'єкта). Застосуванням комплексного екранування можливо досягти необхідного мінімального рівня ПЕМВН в АСУ. Екранування дозволяє також зменшити вплив електромагнітних шумів на роботу пристроїв, зменшити можливість ураження складових АСУ спеціальним впливом потужного електромагнітного випромінювання (електромагнітної зброї). Недоліком екранування є складність його реалізації.

Зниження потужності ПЕМВН включає: зміну електричних схем; використання оптичних каналів зв'язку; зміна конструкції; використання фільтрів; гальванічна розв'язка в системі живлення.

Зниження інформативності сигналів ПЕМВН включає: впровадження спеціальних (нестандартних, змінних) схемних рішень та кодування інформації.

Найбільш ефективним буде комплексне застосування всіх доступних методів пасивного захисту елементів схем, блоків та пристроїв що будуть входити до АСУ. Реалізувати в повному обсязі пасивні методи захисту можливо тільки при їх врахування на етапі проектування та виробництва елементів, блоків, пристроїв при створенні АСУ, або визначенням вимог до них при їх закупівлі.

Порівняння переваг та недоліків методів захисту інформації від витоку каналами ПЕМВН наведені в таблиці 1

Таблиця 1

Метод захисту	**Недоліки**	**Переваги**
Активний	– Невідповідність характеристик засобів активного захисту, вимогам сьогодення – технічне відставання; – Демаскуюча ознака високочастотного випромінювання – Можливість створення каналів витоку в зв'язку з підвищення характеристик засобів радіол електронної розвідки.	– Простота реалізації та використання
Пасивний	– Складність виготовлення компонентів АСУ та екранування приміщень (об'єктів)	– Відсутність демаскуючих факторів – Захист АС від спеціального впливу
Організаційні заходи	– Обмеження функціональності АС	– Відсутність демаскуючих факторів

Аналіз переваг та недоліків методів захисту показує, що тільки пасивний захист від ПЕМВН має суттєві переваги та не має ознак, які негативно впливають на роботу АСУ. Реалізувати в повному обсязі пасивні методи захисту можливо тільки при їх врахуванні на етапі проектування та виробництва елементів (складових) АСУ, або визначенням вимог (допустима величина ПЕМВН) до них при їх закупівлі.

ЛІТЕРАТУРА

1. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05 – (Нормативний документ технічного захисту інформації).

2. Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України (станом на 23 вересня 2013 року) [Електронний ресурс] Режим доступу: www.dsszzi.gov.ua, вільний.

3. Сорокин А.Д. Побочные электромагнитные излучения (ПЭМИ) компьютера [Електронний ресурс] Режим доступу: http://www.electrosad.ru/Processor/RFI.htm, вільний.

4. Семенов Ю.А. Телекоммуникационные технологи [Електронний ресурс] – ИТЭФ-МФТИ, 2013. Режим доступу: http://book.itep.ru/preword.htm, вільний.

5. Завгородний В.И. Комплексная защита информации в компьютерных системах [Електронний ресурс] Режим доступу: http://www.eusi.ru/lib/savgorodnij_kompleksnaja_sasita_informacii_v/index.shtml, вільний.

Кротов В.Д. (НЦЗІ ВІТІ ДУТ)
Панченко С.М. (НЦЗІ ВІТІ ДУТ)
Шемендюк О.В (НЦЗІ ВІТІ ДУТ)

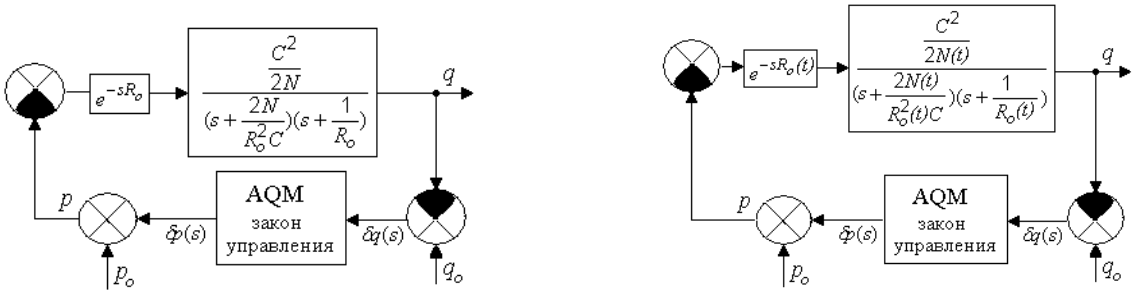
МАТЕМАТИЧНА МОДЕЛЬ AQM-РЕГУЛЯТОРА СЕСІЙ В МЕРЕЖАХ TCP/IP

В останні роки, з високим активним ростом Інтернету, все більш актуальна проблема боротьби з перевантаженнями в мережах. Більшість існуючих маршрутизаторів Інтернету відіграють пасивну роль в управлінні перевантаженнями і мають назву droptail routers, тобто маршрутизатори з відкиданням хвоста. AQM-система – система активного керування чергою в TCP/IP. Динамічна модель поведінки (режиму роботи) TCP отримана шляхом використання потоків, що протікають, інформації й аналізу стохастических диференціальних рівнянь у роботах [1, 2]. Результати моделювання показують, що ця модель точно охоплює динаміку TCP.

Традиційно обробка перевантаження здійснюється через протокол TCP, який передає сигнал перевантаження, відкидає вхідні пакети, коли черга вузла переповнена і маршрутизатор перевантажен (політика відкидання хвоста Tail Drop – TD). На відміну від традиційного управління чергою, яке починає відкидати вхідні пакети тільки тоді, коли черга вже переповнена, при активному управлінні чергою (Active Queue Management – AQM) відкидання вхідних пакетів здійснюється насамперед, коли черга буде повна.

Система керування AQM може бути представлена блок-схемою, наведеної на рис.1(а).

У цій системі автоматичного керування об'єкт керування описується передатною функцією (δ), а блок AQM-Алгоритму являє собою регулятор. Завдання регулятора – забезпечити стійкість і якісні показники системи керування. По-перше, у системи повинен бути прийнятний перехідний процес. По-друге, регулятор повинен забезпечити робастність системи до варіацій параметрів моделі.



(а) (б)

Рис.1. Загальна схема AQM-системи, скоректованої AQM-регулятором

Коефіцієнт навантаження (число TCP сесій) $N(t)$ і час проходження туди й назад – round trip time RTT $R(t)$ є змінними при роботі мережі, тому математична модель AQM-Системи, скоректованої AQM-регулятором, повинна представляти нестаціонарну систему зі змінними в часі параметрами. Загальна схема такий AQM-системи, скоректованої AQM-Регулятором, представлена на рис.1(б).

У роботі [3] досліджені AQM системи з PID, PI, RED і нечіткими регуляторами як системи зі змінними параметрами при випадковій зміні навантаження трафіка (випадковій зміні числа сесій TCP і випадковій зміні часу проходження туди й назад – round trip time RTT) на основі інтерактивної системи MATLAB.

В інтерактивній системі MATLAB можна представити модель об’єкта керування з’єднанням ланок з мінливими випадковим образом параметрами $N(t)$ і $R_0(t)$ й структурну схему AQM системи, скоректованої AQM-регулятором, зображену на рис.1(б), змоделювати в системі MATLAB, використовуючи потужний засіб моделювання й дослідження систем

керування зі зворотним зв'язком Simulink. Як приклад на рис. 2 наведена конкретна модель AQM-системи з нечітким AQM-регулятором (Fuzzy controller).

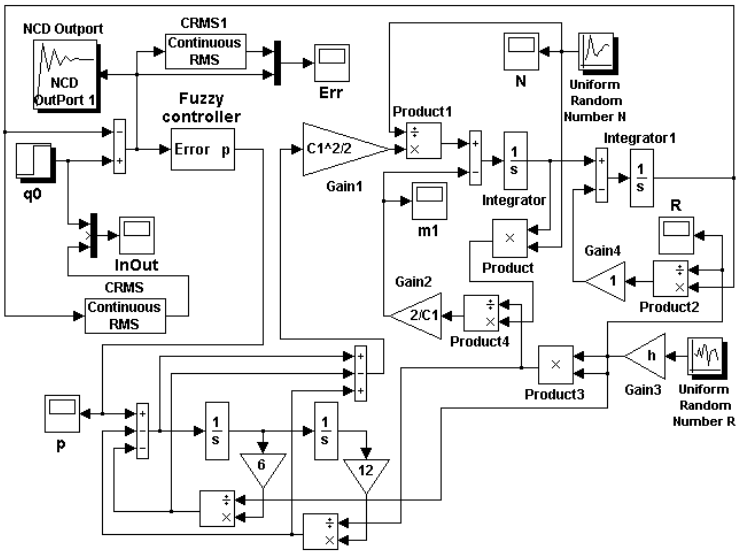


Рис. 2. Модель AQM системи, яка скоректована нечітким регулятором у системі MATLAB

Найбільш складним завданням для системи, показаної на рис. 2, є завдання функцій $R_0(t)$ і $N(t)$. Справа в тому, що час проходження туди й назад $R_0(t)$ і навантаження трафіка $N(t)$ змінюються в часі випадковим образом і в теж час ці функції визначають змінні параметри у відповідних ланках системи. Крім того, ці функції слід задавати як „типові збурюючи впливи" на різні „збурюючи впливи" на системи „збурюючи впливи" на AQM-системи для порівняння AQM-регуляторів, використовуваних у цих системах. Наприклад, можна задати, що час проходження туди й назад $R_0(t)$ змінюється випадковим образом у межах від 220 мс до 300 мс, а навантаження трафіка $N(t)$ змінюється також випадковим образом у межах від 40 до 80. Ще раз підкреслимо, що в реальних мережах і час проходження туди й назад, і навантаження трафіка може змінюватися випадковим образом у різних межах, але для порівняння роботи AQM-регуляторів слід вибирати однакові „збурюючи впливи".

Таким чином, застосування розробленого регулятора**,** який працює з протоколом TCP, є ефективним тому, що позволяє утримувати довжину черги, близько до бажаної, при високій швидкодії і достатню для практичного використання ефективну швидкість передавання даних.

ЛІТЕРАТУРА

1. Hollot C.V. On Designing Improved Controllers for Routers Supporting TCP Flows // C.V. Hollot, V. Misra, D. Towsley, W.B. Gong, IEEE INFOCOM'2001, April 2001, 1726 – 1734.

2. Hollot C.V. Analysis and design of controllers for AQM routers supporting TCP flows // C.V. Hollot, V. Misra, D. Towsley, W.B. Gong, IEEE/ACM Transactions on Automatic Control, vol. 47, no.6, pp. 945-959, June 2002.

3. Гостев В.И., Скуртов С.Н. Фаззи–системы активного управления очередью в сетях TCP/IP: монография. – Нежин: ООО „Видавництво "Аспект-Поліграф", 2011. – 464 с.

к.т.н. Крючкова Л.П. (ДУТ)
Філімонов М.І. (ДУТ)

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ

В часи, коли діє принцип – хто володіє інформацією, той володіє світом, існує стійкий попит на інформацію, отриману несанкціонованим шляхом.

„Високочастотне нав'язування" (ВЧН) є одним з ефективних методів несанкціонованого отримання інформації з віддалених від спостерігача об'єктів, тому створення високоефективних засобів захисту інформації від витоку каналами ВЧН є актуальною задачею.

Метод ВЧН базується на реєстрації змінювань параметрів високочастотного зондуючого сигналу, спрямованого для взаємодії на контрольований об'єкт.

Якість перехоплення інформації каналами ВЧН залежить від ряду факторів:

– характеристик та просторового положення джерела сигналу;

– наявності у контрольованому приміщенні нелінійного елемента (пристрою), параметри якого (геометричні розміри, положення у просторі, індуктивність, ємність, опір, т. і.) змінюються з інформаційним сигналом;

– характеристик зовнішнього джерела, яке опромінює цей елемент (пристрій);

– типу приймача відбитого сигналу.

При проведенні захисних заходів використовуються пасивні та активні методи захисту.

В публікації [1] авторами запропоновано новий метод технічного захисту інформації від витоку по каналах ВЧН, сутність якого полягає в формуванні комбінованої активної завади, що змінює властивості зондуючого сигналу. При цьому блокується перехоплення інформації при використанні як амплітудної, так і частотної та фазової модуляції (АМ, ЧМ, ФМ) зондуючого коливання небезпечним сигналом. В основі методу лежить відоме фізичне явище виникнення биття між коливаннями близьких частот. Новизна рішення підтверджується патентом на винахід №95365 „Спосіб захисту інформації", який у 2011 році зайняв перше місце на конкурсі в системі МВС України у номінації „Патенти".

Головними задачами наукового дослідження є забезпечення максимальної ефективності запропонованого методу, визначення максимального рівня цієї ефективності та визначення оптимальних параметрів системи.

Для вирішення цих задач необхідно створити модель аналітичного опису процесу биття, здатну описувати поведінку амплітуди, частоти і фази результуючого коливання в широкому діапазоні змінювання параметрів періодичних сигналів, що складаються, та визначити критерій ступеню ефективності запропонованого методу при проведенні експериментальних досліджень.

Основні параметри системи, які визначаються експериментально:

1. Смуга частот максимально ефективного впливу для кожного виду модуляції, що використовується при перехопленні інформації.

2. Рівні сигналів максимально ефективного впливу для кожного виду модуляції.

ЛІТЕРАТУРА

1. Ленков С.В., Рыбальский О.В., Хорошко В.А., Крючкова Л.П. Принципы блокирования съема информации методами ВЧ-навязывания // Науковий вісник Національного університету ім. Т. Шевченко. – К., №, 2009.

Кувшинова А.О. (НТУУ „КПІ”)

ОСОБЛИВОСТІ СИТУАЦІЙНОГО УПРАВЛІННЯ ПІДПРИЄМСТВОМ

В сучасних умовах одним із важливих завдань управління підприємством є забезпечення його розвитку. Необхідність цілеспрямованого змістовного розвитку підприємства зумовлює доцільність відповідних управлінських дій. Підприємства, які своєчасно усвідомили роль інформаційних ресурсів і переваги інформаційних технологій в організації та веденні своєї діяльності, які стали використовувати їх в управлінні, не тільки оптимізували виробництво та реалізацію своїх продуктів, а й забезпечили конкурентні переваги, що дозволило їм вижити в умовах кризи.

Під управлінням підприємством розуміють всі дії, які відносяться до планування, створення та експлуатації (функціонування) підприємства, які роблять більш економічним використання її ресурсів при забезпеченні необхідної якості послуг. Основне призначення системи управління підприємством полягає в забезпеченні найкращих значень характеристик функціонування підприємства або значень основного критерію оцінки роботи підприємства в процесі експлуатації.

Збільшити ефективність планування та управління підприємством можливо за допомогою автоматизації цих процесів. До автоматизованої системи планування разом з посадовими особами та іншими засобами забезпечення входить автоматизована система інформаційної та обчислювальної підтримки, яка представляє собою інтерактивну людино-машинну систему, призначену реалізовувати інформаційну та обчислювальну підтримку процесів планування підприємства.

Процес управління може бути представлений сукупністю функцій управління. В свою чергу кожна функція може бути розділена на окремі задачі управління. Кількість і конкретні задачі управління визначаються характеристиками і умовами функціонування підприємства, а також прийнятими рішеннями на етапі його проектування.

Особливості функціонування і умов застосування підприємства потребують створення такої системи управління (СУ) ним, яка б характеризувалася високим ступенем адаптивності, надійності і якості функціонування в умовах невизначеності.

Необхідність забезпечення вимог до якості функціонування підприємства і створення множини функціональних можливостей СУ по формуванню доцільної поведінки і плануванню послідовності операцій управління з активною адаптацією до впливів зовнішнього середовища і варіаціях поточного стану підприємства обумовлюють розробку засобів і методів інтелектуального управління, заснованих на комплексному застосуванні технологій обробки знань. Запропоновані форми представлення знань, способи їх вилучення і поповнення, варіанти організації логічного виводу успішно реалізується в широкому спектрі різноманітних практичних застосувань експертних і діагностичних системах, системах планування і підтримки прийняття рішень та інших.

Базовою основою такого підходу є концепція ситуаційного управління. Виходячи із ключових положень цієї концепції кожному класу ситуацій, виникнення яких вважається допустимим в процесі функціонування підприємства, ставиться у відповідність деяке рішення по управлінню (вибір методу, алгоритму, процедури управління). Тоді ситуація, яка виникла, і яка визначається поточним станом як самого підприємства (чи його елемента), так і зовнішнього середовища, та за результатами ідентифікації може бути віднесена до деякого класу, для якого необхідне управління уже вважається відомим.

Таким чином, необхідність забезпечення вимог до якості функціонування підприємства і створення множини функціональних можливостей системи управління підприємством обумовлюють розробку засобів і методів інтелектуального управління, заснованих на комплексному застосуванні технологій обробки знань. Реалізація концепції ситуаційного управління в СУ підприємством на основі сучасних інтелектуальних технологій передбачає наявність в підсистемі формування рішень бази знань про принципи побудови, цілі функціонування підприємства, а також про особливості використання різних методів і алгоритмів управління підприємством.

Куцаєв В.В. (НЦЗІ ВІТІ ДУТ)
Живило Є.О. (НЦЗІ ВІТІ ДУТ)

ДОПОВНЕННЯ ДО ТЕРМІНОЛОГІЇ СТОСОВНО СУЧАСНОГО КІБЕРПРОСТОРУ

У зв'язку із актуальністю питання щодо кібернетичної загрози сучасним інформаційним телекомунікаційним системам військового призначення (ІТС ВП) останнім часом іде активне обговорення термінів притаманних сучасному кіберпростору.

Перспектива подальших досліджень така, що потребує уточнення в трактуванні технічного кіберпростору та обґрунтуванні існування аналогового інформаційного простору, як основи для виникнення технічного кіберпростору та подальшій перехід до об'єднаного кібер-біо-простору в кібер-ноо-сфері („антропосфера", „біосфера" та „біотехносфера").

Сучасні терміни вживаються в такому значенні:

кібернетичний простір (кіберпростір) – середовище утворене організованою сукупністю інформаційних процесів на основі взаємо поєднаних за єдиними принципами та правилами інформаційних телекомунікаційний та інформаційно-телекомуніуаційних систем [проект Закону про кібернетичну безпеку України];

кібернетична безпека (кібербезпека) – стан захищеності життєво важливих інтересів людини і громадянина суспільства та держави в кіберпросторі [проект Закону про кібернетичну безпеку України];

кіберзагрози – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [проект Закону про кібернетичну безпеку України];

кіберінцидент – подія пов'язана з порушенням належного функціонування інформаційних телекомунікаційних та інформаційно телекомунікаційних систем – обумовлена впливом програмно математичного характеру.

У зв'язку з необхідністю врахувати взаємодію між користувачем кіберпростору та технічним компонентом кіберпростору пропонуємо наступні додаткові терміни:

технічний кіберпростір – технічне середовище утворене організованою сукупністю інформаційних процесів на основі взаємо поєднаних за єдиними принципами та правилами інформаційних телекомунікаційний та інформаційно-телекомуніуаційних систем;

аналоговий біо-простір – взаємопов'язані аналогові інформаційні процеси, які відбуваються у головному мозку однієї людини за допомогою аналогової комунікаційної системи аксонових зв'язків між нейронами;

аналоговий кібер-біо-простір – множина аналогових людино кібернетичних одиниць (біо-просторів), яка за допомогою громадсько-вербального спілкування та формування динамічної наукової картини знань поєдналась в аналоговий суспільний простір;

кібер-біо-простір – поєднання та взаємодія аналогового кібер-біо-простору та технічного кіберпростору в єдиній кібер-ноо-сфері [В. І. Вернадський].

Висновки. Обговорювання та розширення термінології щодо кіберпростору дозволить суспільству більш якісно та безпечно планувати свої дії в сучасному кіберпросторі. Додаткові терміни дозволяють лаконічно пояснити, що людська (суспільна) думка це є аналоговий кібер-біо-простір, який за допомогою технічних засобів перетікає у технічний кіберпростір там накопичується, багаторазово копіюється, обробляється та перетікає назад у аналоговий кібер-біо-простір у новому більш розвинутому та перевіреному всім суспільством вигляді, але вже для масового використання та розвитку суспільства на новому вищому рівні. Ще далі коло в кібер-біо-просторі замкнулось та циклічно запрацював синтез нових знань та взаємний обмін інформацією між технічним кіберпростором та аналоговим кібер-біо-простором.

Лазаренко М.О. (ВІТІ ДУТ)
к.т.н. Хусаінов П.В. (ВІТІ ДУТ)

ВИБІР ПАРАМЕТРІВ СИНТЕЗУ СИСТЕМ ІНФОРМАЦІЙНОЇ ПІДГОТОВКИ КІБЕРНЕТИЧНОГО ВПЛИВУ

В контексті інформаційного протиборства сторін одна з можливих форм отримання інформаційної переваги є кібернетичний вплив. Він досягається шляхом нав'язування обчислювальним процесам інформаційних служб, які виступають об'єктами кібернетичного впливу, спеціальної послідовності даних (вектору атаки) використовуючи засоби віддаленої комп'ютерної взаємодії.

Практичним вирішенням даної задачі пропонується розробка розподіленого програмно-технічного комплексу, де буде відбуватись розподілення частин роботи щодо проведення кібернетичного впливу між кількома вузлами мережі та їх паралельне виконання. Ключовим елементом являється проведення розподілення навантаження між частинами програмного модулю. Реалізація розподіленої системи імітації вимагає розробки алгоритмів синхронізації об'єктів (або процесів), що функціонують на різних вузлах обчислювальної системи. Ефективність реалізації цих алгоритмів, у свою чергу, залежить від рівномірності розподілу (балансування) обчислювального навантаження по вузлах під час функціонування розподіленої програмної системи, якою є, зокрема, розподілена система інформаційної підготовки кібернетичного впливу. Мета балансування завантаження може бути сформульована таким чином:

Виходячи з набору задач, що включають обчислення і передачу даних, і мережі комп'ютерів певної топології, знайти такий розподіл завдань з комп'ютерів, яке забезпечує приблизно рівну обчислювальну завантаження комп'ютерів і мінімальні витрати на передачу даних між ними. Завдання балансування ставиться як завдання відображення не ізоморфних зв'язкових графів. Таким чином, безліч графів завдань повинні бути оптимальним чином відображено на безліч графів обчислювальної системи. Слід розрізняти статичну і динамічну балансування.

Статичне балансування виконується до початку виконання розподіленого додатку.

Динамічне балансування передбачає перерозподіл обчислювальної навантаження на вузли під час виконання програми. Програмне забезпечення, що реалізує динамічне балансування, визначає :

– завантаження обчислювальних вузлів ;
– пропускну спроможність ліній зв'язку;
– частоту обмінів повідомленнями між логічними процесами розподіленого додатка.

На підставі зібраних даних як про розподіленому додатку, так і обчислювальної середовищі) приймається рішення про перенесення логічних процесів з одного вузла на інший. Зазвичай практичне і повне рішення задачі балансування завантаження складається з чотирьох кроків:

– Оцінений завантаження обчислювальних вузлів.
– Ініціація балансування завантаження.
– Прийняття рішень про балансуванню.
– Переміщення об'єктів.

Доповідь присвячена висвітленню варіанта розподілення навантаження при оцінці об'єкта кібернетичного впливу.

к.т.н. Мазулевський О.Є. (ВІТІ ДУТ)
Загребельний О.Ю. (ВІТІ ДУТ)
Толстих В.А. (ВІТІ ДУТ)

МОДЕЛЬ СИСТЕМИ МАСКУВАННЯ ТАФІКУ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ВІЙСЬКОВОГО ЗАСТОСУВАННЯ

Обов'язковою умовою досягнення успіху в діях сучасних збройних сил є наявність функціонуючої системи управління. Тому слід приділяти велику увагу питанням функціонування та різностороннього захисту системи управління в цілому та її складовим частинам. Одним із питань такого захисту є приховання обсягу інформаційного обміну в інформаційно-телекомунікаційній мережі (ІТМ) та перекриття прихованих параметричних каналів витоку інформації. Виконання таких задач можливо за рахунок застосування трафіку маскування. Тому дослідження методів синтезу трафіку для приховання обсягів інформаційного обміну (маскуючого трафіку) та порушення прихованих каналів передачі інформації в сучасних військових телекомунікаційних мережах є актуальною науковою задачею.

Нехай вузли зв'язку позначимо v_i, $i=\overline{1,N}$ за умови що всі вони належать множині військових вузлів зв'язку $\{V\}$. Інформаційний обмін $Q_{ij}(t)$, $i=\overline{1,N}$, $j=\overline{1,N}$, $i\neq j$, в кожен момент часу t в напрямку від i-го вузла до j-го вузла складається із складових: трафіку забезпечення роботи системи управління R_{ij} (робочого обміну) та маскуючого трафіку M_{ij}. Для раціонального приховання роботи системи управління та перекриття прихованих каналів витоку інформації, для однокрокових вузлів ІТМ, кожному вузлу необхідно вирішити наступну задачу:

$$\boldsymbol{Q_{ij}(t)=R_{ij}(t)+M_{ij}(t)\rightarrow g_{ij}},$$

де g_{ij} елемент матриці (G) робочих навантажень з однокроковими сусідами.

Модель взаємодії вузлів телекомунікаційної мережі (граф моделі представлено на рис.1) має однонаправлені зв'язки в зв'язку з тим, що в кожному інформаційному напрямку рішення у виборі параметрів маскуючого трафіку приймаються тільки в напрямку передачі інформації. В зв'язку з тим, що передбачити зміну параметрів трафіку в короткостроковій перспективі неможливо (присутня невизначеність) то рішення на вибір параметрів маскуючого трафіку пропонується заснувати на основі теорії нечітких множин та нечіткого висновку. Початкове значення елементів матриці (G) робочих навантажень з однокроковими сусідами визначається в ході розгортання мережі шляхом визначення максимально доступної пропускної здатності ліній зв'язку і в подальшому можуть бути уточнені шляхом статистичного аналізу трафіку забезпечення роботи системи управління. Цей аналіз та виробка методів управління маскуючим трафіком будуть подальшими науковими задачами.

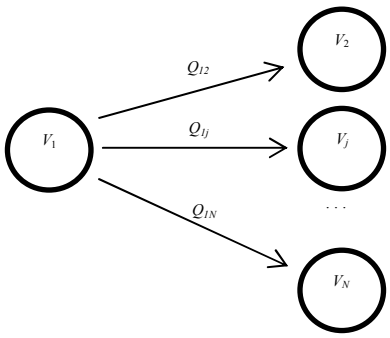


Рис. 1. Модель взаємодії вузла ТКМ із взаємодіючими вузлами

Таким чином застосування маскування робочого трафіку системи управління в ІТМ дозволить позбутися деяких демаскуючих ознак та значно ускладнити роботу засобам, що використовують приховані параметричні канали витоку інформації із захищеної мережі. Також залишається можливість провести введення в оману супротивника шляхом зміни елементів матриці (G) робочих навантажень з однокроковими сусідами.

Макарчук О.М. (ВІТІ ДУТ)
Макарчук В.І. (ВІТІ ДУТ)

РОЗБІРЛИВОСТЬ МОВИ ПРИ ПЕРЕДАЧІ В СИСТЕМАХ РАДІОЗВ'ЯЗКУ З ППРЧ

Якість передачі мови в системах радіозв'язку (СРЗ), в першу чергу, визначається інтенсивністю і характеристиками як ненавмисних, так і організованих завад. Застосування СРЗ з використанням принципу псевдовипадкової перебудови робочої частоти (ППРЧ) дозволяє підвищити завадостійкість передачі інформації. При цьому виникає задача оцінки розбірливості мови, що, в загальному випадку, залежить від швидкості перебудови та параметрів мовного кодера (МК).

В СРЗ спеціального призначення, як правило, використовуються вокодерні методи для аналого-цифрового перетворення мови, що дозволяють зменшити швидкість передачі при збереженні прийнятної розбірливості мови.

При використанні радіостанцій з режимом ППРЧ, слідування декількох уражених робочих частот підряд може стати причиною спотворення кадру передачі вокодера, що призведе до зниження розбірливості переданої мови.

Групування уражених частот призводить до появи на вході приймальної частини вокодерів пакетів помилок. При накладенні ураженої частоти на переданий кадр вокодера можливі кілька варіантів: спотворення кодової комбінації, що відповідає основному тону, і призводить до спотворення сигналу збудження (тембру мови); спотворення кодової комбінації тон-шум, що призводить до помилок в тональному або шумовому заповненні спектра мовного сигналу; спотворення кодових комбінацій амплітуд формант, в результаті чого на прийомі будуть спостерігатися стрибки амплітуди мови.

Нехай кадри МК і ППРЧ синхронізовані за часом, і тривалість кадру МК дорівнює 25 мс, а кадру ППРЧ – 10 мс (швидкість перебудови дорівнює 10000 стр/с). Тоді співвідношення кадрів МК і ППРЧ буде дорівнювати 5/2 (тобто на 2 кадри МК накладається 5 кадрів ППРЧ). Тому, при накладенні уражених частот на передані кадри МК, ураження завадою однієї частоти призведе до спотворення двох кадрів вокодера. У силу того, що тривалість ураженої частоти, що накладається на обидва кадри, невелика в порівнянні з тривалістю кадру, такі кадри підлягають відновленню при прийомі.

У доповіді пропонується визначення якості кадру здійснювати за наступними критеріями: „добрий – *а*" – у кадрі відсутні уражені частоти; „поганий – *в*" – у кадрі МК присутня хоча б одна уражена частота; „середній – *с*" – одна уражена частота присутня в обох кадрах.

Таким чином, на підставі подібного розподілу з використанням теорії інформації було проведено розрахунок розбірливості формант для розглянутого прикладу. На підставі розрахунку отримано залежності правильно прийнятих і уражених кадрів МК та правильно прийнятих фрагментів мови від відносної частоти появи уражених частот для УКХ-радіостанції з режимом ППРЧ.

Аналіз отриманих залежностей показує, що для довгих фрагментів мови ймовірність і відсоток спотворення вище, ніж для коротких. В реальному зв'язку це призводить до більшого спотворення довгих голосних звуків і проявляється у виникненні характерного „пробулькування" сигналу.

Ґрунтуючись на отриманих залежностях, можна розрахувати формантну і складову розбірливість мови для вокодерів різних типів.

Тому напрямком подальших досліджень є визначення оптимального поєднання алгоритмів аналого-цифрового перетворення мови та методів завадостійкого кодування, що дозволить для конкретної завадової обстановки мінімізувати спотворення мовних сигналів (максимально підвищити розбірливість).

Марилів О.О. (ВІТІ ДУТ)
к.т.н. Сілко О.В. (ВІТІ ДУТ)

РОЗРОБКА ПРОГРАМНОГО ІНСТРУКТОРА-ТРЕНАЖЕРА

Розгортання в Збройних Силах України цифрової телекомунікаційної системи потребує підвищення рівня професійної підготовки фахівців щодо експлуатації сучасних цифрових засобів інформаційно-телекомунікаційних мереж. Для забезпечення навчання військових фахівців новій техніці безпосередньо у військових частинах пропонується застосовувати спеціальне програмне забезпечення інструктора-тренажера, яке дозволить набути уміння певної практичної діяльності.

На даний час відомі два підходи до побудови програмних тренажерів: тренажери на базі ПЕОМ, які призначені тільки для інтелектуального тренажу операторів та тренажери на базі ПЕОМ, які з'єднані із макетами пультів та індикаторів реальних пристроїв.

Цікавим з точки зору мінімізації матеріальних, ресурсних та часових витрат є застосування програмних інструкторів-тренажерів. Загальну структуру процесу взаємодії оператора з тренажером цього типу в процесі навчання можливо представити у вигляді орієнтованого графа $G(H, w)$, де H – множина елементів або дій оператора, w – множина відповідних відображень (рис.1).

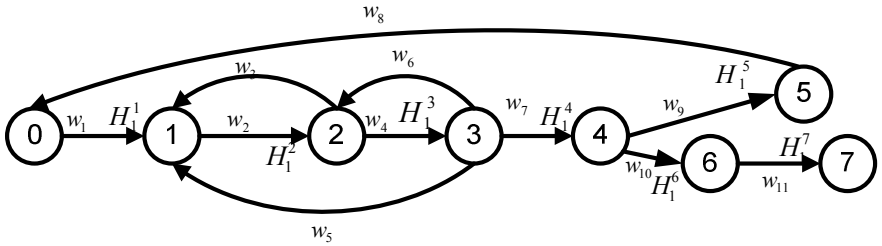


Рис. 1. Граф алгоритму роботи інструктора-тренажера

Етап навчання	Формальне представлення	Зміст етапу	Спосіб реалізації
H_0	$w_1 : H_0 \to H_1^1$	Формування інформаційної моделі	Засоби відображення
	$w_2 : H_1^1 \to H_1^2$	Сприйняття інформаційної моделі	Оператор
	$w_3 : H_1^2 \to H_1^1$	Реалізація окремих операцій управління відображенням	Оператор, засоби відображення
H_1	$w_4 : H_1^2 \to H_1^3$	Розпізнавання конфліктних ситуацій	Оператор
	$w_5 : H_1^3 \to H_1^1$	Контроль оточення при відсутності конфліктних ситуацій	Оператор
	$w_6 : H_1^3 \to H_1^2$	Коректування для деталізація інформації	Оператор
	$w_7 : H_1^3 \to H_1^4$	Визначення цілей та критеріїв	Оператор
H_2	$w_8 : H_1^5 \to H_1^1$	Затвердження і перехід до реалізації	Оператор
	$w_9 : H_1^4 \to H_1^5$	Генерація альтернатив і оцінка результатів рішення	Оператор
H_3	$w_{10} : H_1^4 \to H_1^6$	Реалізація	Оператор, ПЕОМ
	$w_{11} : H_1^6 \to H_1^7$	Оцінка результатів і запам'ятовування результатів	Оператор, ПЕОМ

Наведений граф є абстрактним, однак дозволяє описати послідовність етапів навчання та моделювати діяльність оператора. Таким чином, для реалізації програмного інструктора-тренажера необхідно запрограмувати функції розпізнавання ситуацій, управління інформаційною моделлю з метою відбору необхідної для навчання інформації та оптимізації умов її сприйняття, планування рішень та накопичення досвіду.

Мельник А.О. (ВІТІ ДУТ)
Голубенко І.А. (ДУТ)
Дубина В.О. (ВІТІ ДУТ)

МЕТОДИКА ВИБОРУ ПАРАМЕТРІВ БАГАТОПОЗИЦІЙНИХ СИГНАЛІВ В СИСТЕМАХ ШИРОКОСМУГОВОГО ДОСТУПУ

Технічне оснащення існуючої системи зв'язку (СЗ) має досить низький рівень. За основними можливостями технічного рівня комплекси та засоби зв'язку інформатизації поступаються відповідним зразкам провідних країн світу. Значна кількість засобів і комплексів морально і фізично застаріли і потребують змін. Одним з варіантів підвищення якісних показників системи зв'язку є використання широкосмугових сигналів (ШСС). Вони широко застосовуються в системах багатостанційного доступу з кодовим розподілом каналів, які безпечніші в порівнянні з іншими стільниковими системами з точки зору конфіденційності інформації. Кодування мовних сигналів із змінною швидкістю дозволяє мовним бітам передаватися з тією швидкістю, яка необхідна для забезпечення високої якості мови. Це економить заряд батареї та приводить до пониження потужності мобільної станції.

Але для вирішення задачі підвищення ефективності системи радіозв'язку рекомендується керуватися методикою вибору параметрів багатопозиційних сигналів, яка дозволяє здійснити перехід від системи із незмінною структурою до адаптивної системи.

Основні етапи реалізації цієї методики:

1. Аналіз характеристик існуючої системи радіодоступу.
2. Формування цілей системи радіодоступу, що розробляється.
3. Вибір технологій використовуваних в системі радіодоступу.
4. Розробка сценарію на підставі вибраних технологій.
5. Розрахунок характеристик системи радіодоступу відповідно обраного сценарію.
6. Розрахунок економічної обгрунтованості даної мережі.
7. Запис отриманих результатів розрахунків в базу даних.
8. Вибір раціонального сценарію побудови мережі відповідно висунутих умов.

Використовуючи різні типи модуляції, застосовуючи їх разом з фазовою і квадратурною фазовою модуляцією для збільшення інформаційної швидкості при передачі широкосмугових сигналів у діапазоні 2,4 ГГц, можна досягти швидкості передачі інформації до 11 Мбіт/с, приймаючи до увагу обмеження, що накладаються МСЕ на роботу в цьому діапазоні. Для зменшення взаємної інтерференції характеристики сигналів обмежуються. Даними типами модуляції є різні форми М-ичної ортогональної модуляції, фазоімпульсна модуляція, квадратурна амплітудна модуляція. До широкосмугових можна віднести також сигнали, одержувані при одночасній роботі по декількох паралельних каналах, з розділенням по частоті і/або за часом. Більш ефективного використання випромінюваної потужності чим при ФМ-*M* і КАМ-*M* можна досягти комбінуючи сукупність амплітуд і фазових зсувів при формуванні сигналів. Порівняння кривих завадостійкості сигналів КАМ і ФМ показує, що при однаковій імовірності помилки при КАМ необхідно менше відношення сигнал/шум. При багатопозиційній ФМ сигнальні точки розташовані на окружності і простір сигналів використовується неефективно. Сигнали з КАМ характеризуються більш щільним і рівномірним розташуванням сигнальних точок на сигнальному просторі, що при однаковій середній енергії сигналу E забезпечує більші значення мінімальної відстані d і більш високу завадостійкість. У порівнянні з системами, які використовують багатопозиційну ЧМ, перевагою систем з багатопозиційною ФМ, ВФМ і КАМ, є те, що в них збільшення швидкості передачі інформації досягається без розширення смуги частот каналу зв'язку в обмін на зниження коефіцієнта використання потужності сигналу.

Таким чином, застосовуючи методику вибору параметрів БПС можна обрати оптимальний вид модуляції для застосування в конкретній системі радіозв'язку, яка задовольнятиме всім умовам та відповідатиме вимогам, які до неї висуваються.

Мельничук І. В. (ВІТІ ДУТ)
к.т.н. Хусаінов П. В. (ВІТІ ДУТ)

КЛАСИФІКАЦІЯ РОЗПОДІЛЕНИХ СИСТЕМ КІБЕРНЕТИЧНОГО ВПЛИВУ

Останнім часом спостерігається значне зростання кібернетичного впливу. Він здійснюється за допомогою систем нав'язування кібернетичного впливу. Будь-яка держава, яка дбає про свою обороноздатність, повинна мати власні зразки такої кібернетичної зброї. Тому доцільно розглянути види систем нав'язування кібернетичного впливу, та деякі задачі, що ставляться при їх побудові.

В таких системах слід виділити наступні елементи:

1. активний елемент або бот (від англ. bot) – вузол, що безпосередньо здійснює нав'язування кібернетичного впливу;
2. центр управління, або командний центр – елемент, що управляє кінцевими ботами. Таких центрів може бути декілька.

По типу управління можна виділити наступні системи кібернетичного впливу :

– системи з єдиним центром управління;
– системи з декількома центрами управління;
– розподілені децентралізовані системи.

Системи з єдиним центром управління історично виникли першими. До переваг таких систем слід віднести відносну простоту побудови, максимально повний контроль над системою. Недоліком є наявність лише одного центру управління. Відповідно, знищення такого центру управління призводить до утрати управління над мережею. Також, із зростанням розміру мережі зростає навантаження на командний центр. Тому мережі із єдиним центром управління мають обмеження на максимальний розмір. На даний час такі системи досі використовуються, але втрачають свої позиції.

Наступними є системи з декількома центрами управління. Такі системи мають декілька командних центрів, які частково дублюють один одного. Такий підхід дозволяє тримати контроль над системою навіть у випадку знищення одного чи декількох центрів. Іншою перевагою є можливість контролю різними центрами різних частин системи – це дозволяє зменшити навантаження на окремі командні центри, і, відповідно, зняти обмеження на розмір мережі. Надійність всієї системи також значно вища – пропорційно кількості командних центрів. До недоліків слід віднести складність синхронізації між окремими командними центрами, більшу складність побудови ботів, які повинні враховувати можливість наявності декількох центрів управління. Останнім часом значна увага звертається на розподілені децентралізовані системи. У таких системах не можна виділити окремий центр управління, кожний елемент може бути як активним елементом нав'язування кібернетичного впливу, так і командним центром, так і простим ретранслятором команд. При підключенні нового вузла в систему він отримує список сусідніх вузлів – але не всієї системи. Така структура певним чином нагадує організацію „шпигунських клітинок", де ніхто не знає структури всієї організації, а лише найближчих сусідів. Таким чином, розкриття і знищення окремого елемента призводить до розкриття лише декількох інших елементів – але не всієї системи. Переваги такої системи наступні: немає обмеження на розмір системи, немає вразливих центрів управління. За рахунок цього досягається висока надійність системи. Іншою перевагою є висока скритність – розкриття окремого вузла не дає ніякого уявлення про розміри мережі. Недоліком є висока складність побудови такої системи. На даний час такі системи вважаються найперспективнішими.

Слід зазначити, що приведена класифікація не є вичерпною. Існують гібридні системи, які об'єднують наведені вище підходи. Такий гібридний підхід дозволяє об'єднати переваги декількох систем – за рахунок ускладнення побудови такої системи. Як висновок, найперспективнішими являються розподілені децентралізовані системи за рахунок їхньої підвищеної живучості та скритності.

к.т.н. Могилевич Д.І. (ВІТІ ДУТ)
к.т.н. Климович О.К. (НЦСВ АСВ)
к.т.н. Пащетник О.Д. (НЦСВ АСВ)

АНАЛІЗ СУЧАСНИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ УПРАВЛІННЯ ПІД ЧАС ПРОВЕДЕННЯ БАГАТОНАЦІОНАЛЬНИХ ВІЙСЬКОВИХ НАВЧАНЬ

Міжнародне співробітництво як складова зовнішньої політики держави посідає ключове місце в діяльності Міністерства оборони. У 2013 році розвинені і посилені системні надбання у сфері міжнародних відносин із провідними міжнародними організаціями та країнами світу, налагоджене з ними конструктивне воєнно-політичне, військово-технічне і військове співробітництво на взаємовигідних умовах, а також розвинене добросусідське співробітництво з країнами-сусідами під час проведення багатонаціональних військових навчань [1].

Участь у багатонаціональних військових навчаннях дає можливість військам (силам) провідних країн світу посилити тактико-бойовий потенціал підрозділів під час спільних дій, удосконалити бойову майстерність особового складу, підтримати партнерські відносини своїх збройних сил зі збройними силами інших країн світу. Під час проведення навчань підготовка штабів здійснюється з використанням комп'ютерних технологій, активно використовується навчальна матеріально-технічна база підготовки, наявні імітаційні засоби та тренажерні комплекси. В той же час постає питання удосконалення системи управління військовими навчаннями за рахунок використання сучасних інформаційних технологій у вигляді інтелектуальних систем.

В залежності від процедур, за допомогою яких інтелектуальна система оволодіває новими знаннями та новими видами діяльності, планує та реалізує свою поведінку, застосовуються гібридні інтелектуальні системи, в тому числі інтелектуальні системи планування та оперативного управління в системах військового призначення під час проведення багатонаціональних військових навчань. Гібридні інтелектуальні системи представляють собою комбінацію експертних систем, системи імітаційного моделювання, системи, яка навчає, розрахункового блоку та інших систем, тобто даний клас систем об'єднує можливості вказаних вище типів систем [2 – 4].

Пропонується і в подальшому використовувати сучасні гібридні інтелектуальні системи під час проведення багатонаціональних військових навчань з метою підвищення оперативності та якості управління. Об'єднання можливостей використання всіх інформаційних, програмних, обчислювальних ресурсів для забезпечення взаємозв'язку учасників навчань та отримання достатньої інформації на протязі необхідного часу в незалежності від розташування та відстані дозволить удосконалити систему управління під час проведення міжнародних навчань.

ЛІТЕРАТУРА

1. Біла книга – 2012. Збройні Сили України. – К.: Міністерство оборони України, 2013. – 74с.

2. Тарасов В.О., Герасимов Б.М., Левін І.О., Корнійчук В.О. Інтелектуальні системи підтримки прийняття рішень: Теорія, синтез, ефективність. – К.: МАКНС, 2007. – 336 с.

3. Теория управления в системах военного назначения / Под редакцией И.В. Котенко. – М.: МО, 2001. – 320 с.

4. Ткачук П.П., Могилевич Д.І., Климович О.К. Застосування перспективних інтелектуальних систем управління під час створення Єдиної автоматизованої системи управління Збройних Сил України – Л.: Військово-технічний збірник Академії сухопутних військ, 2013. – с. 38-41.

к.т.н. Москаленко А.О. (ПНТУ)
к.т.н. Івко С.О. (АСВ)
к.т.н. Мазулевський О.Є. (ВІТІ ДУТ)

МАТЕМАТИЧНА МОДЕЛЬ ДИСКРЕТНОГО КАНАЛУ ЗВ'ЯЗКУ З МОДУЛЯЦІЄЮ ЦИКЛІЧНИМ ЗСУВОМ КОДУ В УМОВАХ БАГАТОПРОМЕНЕВОГО РОЗПОВСЮДЖЕННЯ РАДІОХВИЛЬ

Використання вузькосмугових сигналів обумовлює ряд недоліків сучасних систем військового радіозв'язку: низька перешкодостійкість, низька структурна та енергетична скритність, неефективне використання частотного ресурсу. Суттєво покращити ці характеристики можливо шляхом використання сигналів з розширенням спектру.

За результатами порівняльного аналізу перспективних методів широкосмугової модуляції (MBOK, CCSK, OCDM, OFDM) встановлено, що найкращим методом є MBOK (M-ічна двоортогональна модуляція) завдяки високій стійкості до радіоперешкод та багатопроменевого розповсюдження радіохвиль [1]. Іншим перспективним методом є CCSK (Cyclic Code Shift Keying, модуляція циклічним зсувом коду) [2], що поступається M-ічній двоортогональній модуляції внаслідок використання неортогонального алфавіту сигналів та вразливості до багатопроменевого розповсюдження радіохвиль.

В роботі [3] показано, що змінюючи методи формування алфавіту сигналів CCSK-модуляції можливо усунути вказані недоліки. В результаті чого, модуляція циклічним зсувом коду, у порівнянні з MBOK, отримує перевагу за рахунок забезпечення більш високої швидкості передачі інформації та простоти кореляційної обробки. Для підтвердження висунутої в [3] гіпотези, необхідно проведення математичного моделювання каналу зв'язку з CCSK-модуляцією в умовах багатопроменевого розповсюдження радіохвиль. Проте, в існуючих моделях відсутня реалізація CCSK-модуляції з можливістю вибору методу формування алфавіту сигналів. Тому актуальним завданням є розробка математичної моделі дослідження перешкодостійкості сигналів з модуляцією циклічним зсувом коду в умовах багатопроменевого розповсюдження радіохвиль. В програмному середовищі Matlab, було розроблено математичну модель дискретного каналу зв'язку. Основні складові моделі: підсистема „Generator", що формує код розширення спектру сигналу; підсистема „Seredov. rozpovs", моделює явище багатопроменевого розповсюдження радіохвиль; підсистема „Receiver", реалізує алгоритми кореляційної обробки сигналу, підрахунок переданих та помилково прийнятих інформаційних біт. Фізична адекватність моделі підтверджена співпадінням результатів моделювання з теоретичними відомостями для відомих кодів (кодів Уолша).

Таким чином, розроблена математична модель дискретного каналу зв'язку відрізняється від існуючих реалізацією модуляції циклічним зсувом коду з можливістю вибору методу формування алфавіту сигналів. Модель призначена для дослідження перешкодостійкості сигналів з розширенням спектру в умовах багатопроменевого розповсюдження радіохвиль.

ЛІТЕРАТУРА

1. M. Webster et al., "Proposal for a high speed PHY for the 2.4 GHz band," IEEE P802.11-98/47, Jan. 1998.

2. G.M. Dillard et all., Cyclic Code Shift Keying: A Low Probability of Intercept Communication Technique // IEEE Trans. Aerosp. Electron. Systems., vol. AES-39, July 2003, pp. 786 – 798.

3. Гепко И.А. Новый класс ортогональных кодов для телекоммуникационных систем CDMA и метод их корреляционного приема, минимизирующий вычислительную сложность цифрового сигнального процессора /И.А. Гепко, А.А.Москаленко// Зв'язок. – 2007. – № 6. – С. 33 – 39.

Мусієнко В.А. (НЦЗІ ВІТІ ДУТ)
Малишкін В.В. (НЦЗІ ВІТІ ДУТ)
Савченко О.М. (НЦЗІ ВІТІ ДУТ)
Ткач В.О. (НЦЗІ ВІТІ ДУТ)

СУЧАСНИЙ СТАН СИСТЕМИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ І РЕМОНТУ ТЕХНІКИ ЗВ'ЯЗКУ ТА АВТОМАТИЗАЦІЇ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ ТА ШЛЯХИ ЇЇ УДОСКОНАЛЕННЯ

Сучасний стан системи технічного обслуговування та ремонту техніки зв'язку та автоматизації свідчить про необхідність вирішення певних проблем щодо технічного обслуговування та ремонту новітніх зразків техніки зв'язку, що уже надійшла у війська Збройних Сил України, або буде надходити під час виконання основних напрямів державної політики у сферах безпеки і оборони України, а саме:

1. Відсутность на нову техніку зв'язку робочої конструкторської документації із-за чого неможливо своєчасно провести обслуговування і ремонт її в ремонтних підрозділах та базах зв'язку ЗС України (відповідно до вимог ГОСТ 2.102 в комплект конструкторської документації на вироби усіх отраслей промисловості повинна входити експлуатаційна документація – документи, призначені для використання виробу при експлуатації, обслуговуванні та ремонті в процесі його експлуатації).

2. Відсутність експлуатаційних документів (відповідно до вимог ГОСТ 2.102 – „Руководства по эксплуатации. Инструкции по монтажу, пуску, регулированию и обкатке изделия, Формуляра, Паспорта, Этикетки, Каталога деталей и сборочных единиц, Норм расхода запасных частей, Норм расхода материалов. Ведомости комплекта запасных частей, инструмента та інш.принадлежностей (ЗИП) Учебно-технических плакатов. Ведомости эксплуатационных документов").

3. Невиконання вимог ГОСТ 2.601 замовником перед початком ДКР щодо проробки, узгодження з виконавцем та затвердження відповідного „Переліку документації, яка розробляється під час виконання ДКР", в якому конкретно необхідно вказувати – яка конструкторська та експлуатаційна документація обов'язково розробляється.

Іноді невиконання виробником в повному обсязі вимог ГОСТ, які є складовою системи розробки та поставлення на виробництво озброєння та військової техніки (далі – СРПВ ОВТ), щодо порядку розробки експлуатаційної і ремонтної документації.

Розроблена згідно вище зазначених вимог відповідних ГОСТ ремонтна документація повинна поставлятися в ремонтні організації, бази, заводи Збройних Сил України з метою підготовки ремонтного виробництва, проведення ремонту та контролю відремонтованої техніки і її складових частин в стаціонарних і рухомих ремонтних підрозділах. Вона має бути не тільки розроблена, а і обов'язково перевірена відповідним органом, а визначатися це повинно в окремому договорі, або в договорі на ДКР, чи в договорі на поставку техніки серійного виробництва відповідно до вимог ГОСТ СРПВ ОВТ щодо постановки техніки на серійне виробництво.

4. Невизначеність в повному обсязі питань щодо прийняття на озброєння розробленої або модернізованої техніки.

Відповідно до вимог наказу про постановку на озброєння (наказ МОУ від 10.08.10 р. №416) прийняття на озброєння – це включення в склад Зройних Сил розробленої або модернізованої техніки. Але ж яким чином повинна ставитися на озброєння куплена техніка або та, яка закуповується – точніше не розроблена за заказом МОУ, в нормативних документах не визначено. Гарантійне обслуговування визначеної техніки здійснюється постачальником в визначений термін, а по його закінченні техніку, яка потребує ремонту, за окремі кошти необхідно здавати в ремонт.

У відповідних серіях ГОСТ СРПВ ОВТ задані вимоги до військової техніки та визначено випробування цих вимог. В них чітко прописано, що для військової техніки повинна бути система вбудованої діагностики, а ремонт повинен проводиться агрегатним методом в бойових умовах швидко за рахунок ЗІП. Закуплена техніка не задовольняє цим вимогам. Вона, як правило, знаходиться на стаціонарі, але її планується застосовувати ще й в польових умовах. Переробка, а по суті створення нових польових апаратних, використовуючи КУНГИ й автомобілі від старих апаратних та наповнення їх покупними на ринку засобами, – це не визначений нормативним законодавством та недосконалий шлях, який призведе до того, що все обладнання рано чи пізно вийде з ладу. Наприклад, техніка, яка була розроблена в результаті проведення ДКР шифр „Скіф-КАЗ", „Світязь", „Простір" за рахунок державних оборонних замовлень підприємством „Телекарт-прилад", має в своєму складі елементи, які були прийняті на озброєння, але ж технічне обслуговування та ремонт на них зовсім не організовані у військах. У разі виникнення потреби проведення ремонту виникає необхідність відправляти цю техніку на завод, який її розробив, або запрошувати спеціалістів від виробника за окремі кошти, що визначено в окремому договорі на поставку. В договорі на виконання ДКР визначено, що по закінченню ДКР розроблена техніка приймається на озброєння. А далі наступають комерційні відносини (договори на поставку) – закуповується обладнання, рік воно обслуговується, а по закінченню гарантійного терміну визначені вище роботи повинні проводитися за гроші – але це вже прирегатива Департаменту розробок і закупівель Міністерства оборони України (далі – ДРіЗ МОУ). Тобто начальник військ зв'язку Збройних Сил України планує оснащення військ новими засобами, цей план затверджує, подає в загальний план за Міністерство оборони України, а ДРіЗ МОУ згідно цього плану закуповує техніку та поставляє її у війська через бази. Таким чином, Управління технічного забезпечення ГУЗІС ЗС України може тільки організовувати роботу, але ж для цієї роботи потрібні ЗІП, витратні матеріали та документація з обслуговування та ремонту. А якщо виробник заздалегідь цього не надає, в ДКР не розробляє та при поставці не надсилає – у війська буде поставлятися непридатна щодо ремонту техніка зв'язку та автоматизації військовими засобами. На заводі-виробнику вона придатна, але ж завод не є власністю держави та веде свою особисту ринкову політику щодо вигідних комерційних відносин, та не відомо, яким чином буде ремонтуватися військова техніка при скороченні виробничих потужностей виробника, скрутному становищі, банкрутстві тощо.

5. Відсутність вимог (або їх наявність, але не вповному обсязі) у відповідній документації (технічні завдання, робочо-конструкторська документація тощо) щодо технічного обслуговування, ремонту та ремонтопридатності до техніки зв'язку та автоматизації, яка розробляється в результаті проведення ДКР за державними оборонними замовленнями та поставляється у війська.

6. Необхідність удосконалення структури та складу системи технічного обслуговування і ремонту техніки зв'язку та автоматизації в умовах реформування Збройних Сил України.

Основними напрямками щодо удосконалення системи технічного обслуговування та ремонту техніки зв'язку та автоматизації є:

поступовий перехід від планового ремонту засобів зв'язку на ремонт за технічним станом, застосування агрегатного методу поточного та відновлюваного ремонту;

створення регіональних сервісних центрів на базі ремонтних установ, військових частин із залученням представників виробників сучасних та перспективних засобів зв'язку з її технічного обслуговування і ремонту;

забезпечення військових ремонтних органів зв'язку ремонтною та експлуатаційною документацією на сучасні засоби зв'язку, спеціальними засобами вимірювальної техніки та проведення навчання особового складу щодо навичок та методів ремонту відповідної техніки.

к.т.н. Нестеренко М.М. (ВІТІ ДУТ)
Висоцький Г.В. (ВІТІ ДУТ)

МОДЕЛІ ЗАБЕЗПЕЧЕННЯ *QOS* НА БАЗІ МЕХАНІЗМІВ *TRAFFIC ENGINEERING*

Для сучасних інформаційно-телекомунікаційних мереж характерним є необхідність передачі повідомлень різного типу, при цьому існує тенденція збільшення об'ємів передачі мультимедійного трафіка. Одним з основних завдань управління такою мережею є організація ефективної доставки інформації, а саме забезпечення якості обслуговування (*Quality of Service – QoS*), для всіх видів трафіку. Тому питанням оптимального управління трафіком в мультисервісних мережах являється досить актуальним питанням.

Для забезпечення виконання показників *QoS* в *IP*-мережах використовуються наступні методи: резервування ресурсів; пріоритизація трафіку; динамічна перемаршрутизація.

Також у сучасних *IP*-мережах для забезпечення якості обслуговування використовуються: моделі інтегрованого сервісу – *Integrated Service* (*IntServ*); моделі диференційних послуг – *Differentiated Service* (*DiffServ*); гібридні моделі для надання *QoS* з кінця в кінець *IntServ-DiffServ,* що включають механізми вище перерахованих методів.

Одним із перспективних підходів забезпечення необхідного рівня якості обслуговування в *IP*-мережах являються механізми *Traffic Engineering. Traffic Engineering* (*TE*) – здатність динамічного управління потоками вхідного трафіку з метою виконання необхідних показників *QoS*.

На теперішній час, найбільш гнучкою мережевою технологією, яка підтримує протоколи забезпечення *QoS* є *MPLS* (*Multiprotocol label switching*). Причому, головною особливістю даної технології є заміна процесу маршрутизації кожного пакета на комутацію пакета на основі міток.

Для реалізації комутації по міткам використовуються наступні протоколи сигналізації *LDP* (*Label Distribution Protocol*), *CR-LDP* (*Constraint-Routing*) та *RSVP-TE* (*Resource Reservation Protocol – Traffic Engineering*), однак не всі вони забезпечують виконання показників *QoS*. Наприклад, протокол розподілу міток *LDP* являє собою набір процедур і службових повідомлень, за допомогою яких маршрутизатори (комутатори) *LSR* (*Label Switching Router*) організовують тракти комутації по мітках *LSP* (*Label-switched path*), обмінюючись інформацією про прив'язку міток по *FEC* (*Forwarding Equivalence Class*), а саме об'єднують в один потік пакети з однаковими вимогами до передачі. Даний протокол здатен агрегувати потоки даних, від різних джерел передачі на основі *FEC*, але не підтримує забезпечення показників якості обслуговування.

В свою чергу, протокол *CR-LDP* має всі властивості *LDP*, однак додатково в ньому визначені механізми створення і підтримки трактів *LSP* з явно заданим маршрутом. *CR-LDP* застосовується для таких додатків *MPLS*, як *TE* (*Traffic Engineering*) – управління трафіком і *QoS*, де потрібна додаткова інформація про маршрути. *CR-LDP* володіє досить широкими можливостями інжинірингу трафіку в мережах *MPLS* і не вимагає реалізації в обладнанні додаткового протоколу, а лише розширення вже існуючого. Однак, недолік протоколу полягає в тому, що він не може динамічно перерозподіляти навантаження мережі.

Наступний протокол сигналізації *RSVP-TE* має значні доопрацювання. Першою з двох функцій, покладених на *RSVP-TE* технологією *MPLS*, є розподіл міток (замість протоколу *LDP*). Друга, традиційна для *RSVP* роль полягає у підтримці *QoS* в мережі *MPLS*, за рахунок використання механізмів *TE* в режимі тунелювання. Тобто, маршрутизатори *LSR* повинні узгодити між собою параметри *QoS* для кожного *FEC*.

Таким чином, на основі проведеного аналізу можна зробити висновок, що найбільш перспективним із розглянутих протоколів сигналізації, що реалізує розподіл міток та забезпечує механізми *QoS* є *RSVP-TE*.

к.т.н. Нестеренко М.М. (ВІТІ ДУТ)
Потапенко І.В. (ВІТІ ДУТ)

СТАНДАРТИ ВІДЕОКОНФЕРЕНЦЗВЯЗКУ В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

На теперішній час перспективною послугою, що використовується в багатьох в держаних та приватних організаціях установах є відеоконференцзв'язок, який являється технологією інтерактивної взаємодії двох або більше віддалених абонентів та дозволяє здійснювати обмін аудіо- і відеоінформацією в режимі реального часу з врахуванням передачі повідомлень управління. В свою чергу, відеоконференція може застосовується як технічний засіб, для підтримки або підвищення ефективності оперативного прийняття рішення в випадку нештатних та надзвичайних ситуацій, проведення судових процесів, а також може виступати як елемент технологій телемедицини, дистанційного навчання і.т.д. Також необхідно відмітити економічний виграш в результаті використання даної технології за рахунок скорочення витрат на відрядження в територіально розподілених організаціях.

До основних вимог забезпечення необхідного рівня якості обслуговування при організації відеоконференцзв'язку необхідно віднести: затримка доставки аудіо-відео пакетів між транслюючими пристроями – не більше 300 мілісекунд; різниця в часі доставки аудіо-відео пакетів (джиттер) між транслюючими пристроями – не більше 50 мілісекунд; втрата аудіо-відео пакетів, для забезпечення зображення *FullHD*-якості – не більше 1%.

Однак, бурхливий розвиток мережевих технологій, конвергенція різнорідних мереж та широкий спектр протоколів, що забезпечують відеоконференцзв'язок вимагають створення універсальних підходів та архітектури побудови для організації передачі інформації та підтримки заданого рівня якості надання послуги, на всіх ділянках мережі.

На теперішній час в системах відеоконференцзв'язку використовуються наступні протоколи: *h*.320 – стандарт для мереж типу *ISDN*; *h*.321 – стандарт для мереж Ш-ЦСІО і *ATM*; *h*.322 – для мереж з комутацією пакетів з гарантованої пропускною спроможністю; *h*.323 – стандарт для мереж з комутацією пакетів з негарантованої пропускною здатністю; *h*.324 – стандарт для телефонних мереж загального користування; *h*.324/С –для мереж стільникового звязку; *h*. 239 – підтримка двох потоків від різних джерел, зображення учасника і даних (інша камера або презентація) виводиться на два різних дисплеї (або на один дисплей в режимі *PIP*); *h*.460.17/.18/.19 – підтримка проходження аудіо і відео трафіка через *NAT* и *Firewall*; *SIP* (*Session Initiation Protocol*) – протокол передачі даних, який описує спосіб встановлення і завершення інтернет-сеансу користувачів, який включає обмін мультимедійним вмістом (відео-та аудіоконференція, миттєві повідомлення). Даний протокол визначає тільки спосіб узгодження між клієнтами про порядок відкриття каналів обміну на основі інших протоколів, які можуть використовуватися для безпосередньої передачі інформації. Тобто, *SIP* – сигнальний протокол що дозволяє встановити з'єднання і узгодити параметри мультимедійної сесії користувачів.

Однак, провівши аналіз функціональних можливостей вище розглянутих протоколів, можна зробити висновок, що *SIP* має ряд переваг щодо його використання в сучасних телекомунікаційних мережах, які орієнтуються на використання комутацію пакетів на всіх рівнях. А саме: персональна мобільність (відслідковується та фіксується переміщення користувачів); масштабованість мережі (за рахунок використання серверної структури); розширення функціональних можливостей (доповнення протоколу при появі нових послуг та його адаптація з різними додатками); інтеграція в стек існуючих *IP*-протоколів; взаємодія з іншими протоколами сигналізації.

Таким чином, *SIP* може виступати як універсальний протокол сигналізації для організації передачі мультимедійного трафіка на всіх ділянках телекомунікаційної мережі.

Нікіфоров С.В. (ДУТ)

АНАЛІЗ ПІДХОДІВ ЩОДО КІЛЬКІСНОЇ ОЦІНКИ ОСНОВНИХ ВЛАСТИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ

Інформаційна система – це взаємопов'язана сукупність інформаційних, технічних, програмних, математичних, організаційних, правових, ергономічних, лінгвістичних, технологічних та інших засобів, а також персоналу, що призначені для збору, обробки, зберігання, видачі інформації та прийняття управлінських рішень.

Властивості інформаційної системи:

– складність – система залежить від множини вхідних до неї компонентів, їх структурної взаємодії, а так само складності внутрішніх і зовнішніх зв'язків;

– подільність – система складається з ряду підсистем або елементів, що виділені за певними ознаками і відповідають конкретним цілям і завданням;

– цілісність системи – означає те, що всі елементи системи функціонують як єдине ціле;

– різноманіття елементів системи і відмінність їх природи – властивість пов'язана з функціонуванням елементів, їх специфікою і автономністю;

– структурність – визначає наявність встановлених зв'язків і відносин між елементами всередині системи, розподіл елементів системи за рівнями та ієрархією;

– адаптивність системи – означає пристосованість системи до умов конкретної предметної області;

– інтегрованість – означає можливість взаємодії системи із знову підключеними компонентами або підсистемами.

Якість інформаційної системи – це сукупність властивостей системи, що обумовлюють можливість її використання для задоволення визначених, відповідно до її призначення, потреб. Кількісні характеристики цих властивостей визначаються показниками. Основними показниками якості інформаційних систем є:

1. Надійність системи – властивість системи зберігати в часі у встановлених межах значення всіх параметрів, що характеризують здатність виконувати необхідні функції в заданих режимах і умовах застосування.

2. Достовірність функціонування інформаційної системи – властивість системи, яка обумовлює безпомилковість вироблених нею перетворень інформації. Достовірність функціонування інформаційної системи повністю визначається і вимірюється достовірністю її результативної інформації.

3. Безпека інформаційної системи – властивість системи, що полягає в здатності забезпечити конфіденційність і цілісність інформації, тобто захист інформації від несанкціонованого доступу з метою її розкриття, зміни або руйнування.

Ефективність системи – це властивість системи виконувати поставлену мету в заданих умовах використання і з певною якістю. Показники ефективності характеризують ступінь пристосованості системи до виконання поставлених перед нею завдань і є узагальнюючими показниками оптимальності функціонування інформаційної системи, залежними від локальних показників, якими є надійність, достовірність, безпека.

Економічна ефективність системи – узагальнюючий показник, що характеризує доцільність зроблених на створення і функціонування системи витрат.

Для кількісної оцінки основних властивостей інформаційних систем можуть використовуватися комплексні показники надійності та достовірності.

Комплексні показники надійності:

1. Коефіцієнт готовності – імовірність того, що система опиниться в працездатному стані в довільний момент часу, крім планованих періодів, протягом яких застосування системи за призначенням не передбачається.

2. Коефіцієнт оперативної готовності – ймовірність того, що система опиниться в працездатному стані в довільний момент часу, крім планованих періодів, протягом яких застосування системи за призначенням не передбачається, і, починаючи з цього моменту, працюватиме безвідмовно протягом заданого часу.

3. Коефіцієнт технічного використання – відношення математичного очікування інтервалів часу перебування системи в працездатному стані за деякий період експлуатації до суми математичних очікувань інтервалів часу перебування системи в працездатному стані, простоїв, обумовлених технічним обслуговуванням, і ремонтів за той же період експлуатації.

4. Коефіцієнт збереження ефективності – відношення значення показника ефективності за певну тривалість експлуатації до номінального значення цього показника, обчисленому за умови, що відмови в системі протягом того ж періоду експлуатації не виникають.

Комплексні показники достовірності:

1. Коефіцієнт інформаційної готовності – ймовірність того, що інформаційна система виявиться здатною до перетворення інформації в довільний момент часу того періоду, який планувався для цього перетворення, тобто того, що в даний момент часу система не буде перебувати в стані позапланового обслуговування, викликаного усуненням відмови або ідентифікацією та виправленням помилки.

2. Коефіцієнт інформаційного технічного використання – відношення математичного сподівання планованого часу роботи системи на перетворення інформації, за вирахуванням часу відновлення, контролю, ідентифікації та виправлення помилок, до суми планованого часу роботи системи та профілактичного обслуговування.

В якості показників економічної ефективності зазвичай використовуються:

1. Річний економічний ефект.

2. Коефіцієнт економічної ефективності капітальних вкладень.

3. Термін окупності проекту (в роках) капітальних вкладень.

Оскільки розрахунок величини річної ефективності викликає звичайно серйозні труднощі, на практиці часто використовуються інші економічні показники, а саме:

1. Показник річних приведених витрат.

2. Показник „повної вартості володіння”.

Дані критерії є критеріями порівняльної економічної ефективності, тобто вони дозволяють проводити вибір кращої системи з декількох порівнюваних між собою.

ЛІТЕРАТУРА

1. Белых А.А., Горлов Ю.Г., Калинин Н.П., Харитонов В.А. Отношение объективного и субъективного в моделях поддержки принятия решений / Под научной редакцией В.А. Харитонова: Монография. – Пермь: ПГСХА, 2008. – 230 с.

2. Белых А.А. Модели и методы синтеза противосбойных систем цифровой аппаратуры управления сложных технических комплексов. Препринт. - Пермь: Институт механики сплошных сред УрО РАН, 2000.– 76 с.

3. Белых А.А., Харитонов В.А. Архитектурно-ориентированный подход к оценке сбоеустойчивости специализированных вычислительных комплексов. // Приборы и системы. Управление, контроль, диагностика, № 11, 2000. С. 51 – 55.

4. Белых А.А. Методика функционального контроля цифровых устройств систем управления объектами агропромышленного комплекса на основе взвешенных алгебраических соотношений // Труды Кубанского государственного аграрного университета. Выпуск № 3. – Краснодар: КубГАУ, 2006. – С. 28– 37.

5. Белых А.А., Винокур И.Р., Харитонов В.А. Функциональные возможности механизмов комплексного оценивания с топологической интерпретацией матриц свертки // Управление большими системами. Сб. трудов. Вып. 18. М.: ИПУ РАН, 2007. – С. 129 – 140.

к.т.н. Овсянніков В.В. (ВІТІ ДУТ)
Паламарчук С.А. (ВІТІ ДУТ)
Процюк Ю.О. (ВІТІ ДУТ)
Черниш Ю.О. (ВІТІ ДУТ)

КАНАЛИ ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ ПО ВОЛОКОННО-ОПТИЧНИМ ЛІНІЯМ ЗВ'ЯЗКУ

Високі вимоги до сучасних систем телекомунікацій (висока швидкість передачі інформації, надійність, захищеність від несанкціонованого доступу), призводять до визнання переваг волоконно-оптичних ліній зв'язку (ВОЛЗ). В найближчому майбутньому, можна очікувати, що ВОЛЗ замінять всі існуючі магістральні лінії передачі інформації.

ВОЛЗ широко використовуються для передачі інформації, як аналогової (в тому числі і мовної), так і цифрової при побудові телекомунікаційних мереж (насамперед, локально-обчислювальних). Це зумовлено якісними характеристиками волоконно-оптичної лінії, як лінії зв'язку. З точки зору захисту інформації, волоконно-оптична лінія, також вважається ідеальною, оскільки в цих лініях відсутні випромінювання в радіотехнічному діапазоні частот. Перехоплення інформації можливе тільки у випадку фізичного доступу безпосередньо до самої лінії, і не обов'язкове порушення її цілісності. При вигині оптичного волокна відбувається зміна кута падіння електромагнітної хвилі на межі серцевина-оболонка. Кут падіння стає менше граничного кута, що значить вихід частини електромагнітного випромінювання із світловоду (Рис.). Вигин оптичного волокна призводить до сильного побічного випромінювання в місці вигину, що дає можливість несанкціонованого зняття інформації в локалізованій області.

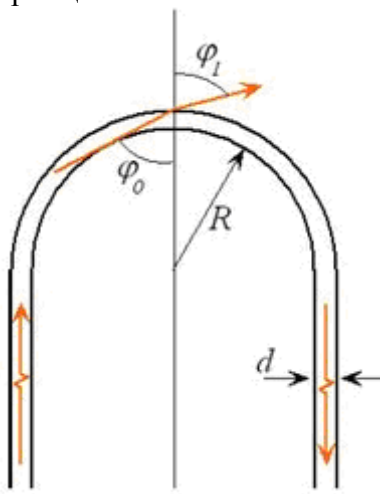


Рис. Формування каналу витоку інформації при вигині оптоволокна радиусом *R*
де, *d* – діаметр серцевини,
φ_0 – кут падіння,
φ_1 – кут переломлення

Мінімальний радіус вигину R, при якому виникає побічне випромінювання в точці вигину світловоду з діаметром серцевини d, повязане з порушенням повного внутрішнього відбиття визначається як в [1]:

$$R \le d \frac{n_2}{n_1 - n_2},$$

n1, n2– показники переломлення серцевини та оболонки світловода.

Наприклад, оцінка радіусу вигину для волокна з діаметром серцевини d=50 мкм та оптичної оболонки – D=125 мкм (n1=1,481, n2=1,476) пояснює, що при R≤3,5 см спостерігається інтенсивне проходження випромінювання в точці вигину (до 80% значення інтенсивності основного світлового потоку в ВОЛ).

Виробники оптичного волокна, як одну з його характеристик приводять мінімальний радіус вигину, допустимий при прокладанні кабелю. Цей радіус, як правило витримується, але вигин волокна з малим радіусом може здійснюватися спеціально, з метою зняття інформації.

Порушення внутрішнього відбиття при механічному впливі можливе не лише при вигині волокна, але і при здійсненні локального тиску на оптоволокно, що викликає

неконтрольване розсіювання (на відміну від вигину) в точці деформації. Розміри оптичного волокна прирівняні до довжини хвилі світлового потоку. В наслідок цього, мікроскопічні зміни положення або вигину цього волокна, навіть під дією акустичних коливань, можуть призвести до зміни шляху проходження світлових хвиль.

Зміна шляху проходження світлових хвиль, призводить до зміни фази випромінювання, яке перехоплюється. Це означає, що навіть при передачі інформації в зашифрованому вигляді, якщо лінія зв'язку прокладена всередині об'єкту інформаційної діяльності, де озвучується мовна інформація, світловий потік, за допомогою якого передається інформація в цій лінії зв'язку, буде промодульований мовною інформацією. Ця модуляція не впливає на передачу цифрових сигналів, але дозволяє перехопити мовну інформацію. Таким чином, у ВОЛЗ, в силу їх конструктивних особливостей, завжди присутній канал витоку інформації за рахунок акустоелектричних перетворень (перетворення акустичних сигналів в електричні), виражений в модуляції світлового потоку акустичним сигналом. При прокладанні ВОЛЗ, одночасно з інформаційними волоконно-оптичними лініями зв'язку, як правило прокладаються так звані „темні волокна". Це резервні лінії, які не підключені до апаратури і необхідні для швидкого відновлення системи у випадку виходу із ладу основних волокон. Оскільки, в цих волокнах відсутній світловий потік, то перехоплення інформації неможливе, однак ефект зміни шляху можливого проходження світлового потоку, так званий „параметричний ефект" присутній. Параметричний ефект сам по собі не є загрозою, але коли подати у волоконно-оптичну лінію оптичне випромінювання, за допомогою лазерного або навіть світлодіодного випромінювача, формується параметричний канал витоку інформації.

Таким чином, волоконно-оптичні лінії зв'язку, які проходять через об'єкт інформаційної діяльності (та мають вихід за межі контрольованої зони) є елементами, в яких присутній канал витоку мовної інформації за рахунок акустоелектричних перетворень або можливий параметричний канал витоку мовної інформації. Канали витоку інформації в електронних пристроях можуть бути повністю або частково нейтралізовані. В волоконно-оптичних лініях розглянуті канали витоку усунути неможливо, оскільки вони обумовлені їх конструктивними особливостями. Для реалізації розглянутих вище каналів витоку інформації, створюється локальна неоднорідність у волоконно-оптичній лінії зв'язку. Одночасно з випромінюваням у місці неоднорідності, в цих місцях виникає значне зворотнє розсіювання світла. За допомогою рефлектометрії зворотнього розсіяного світла, такі підключення легко детектуються з високим просторовим і часовим розділенням. Це дозволяє, при наявності спеціальної апаратури, виявити, як факт встановлення апаратури зйому інформації, так і місце її встановлення.

ЛІТЕРАТУРА

1. Введение в интегральную оптику. Под ред. М. Барноски, пер. с англ. под ред. Т.А. Шмаонова // М.: Мир, 1977.– 368 с.

2. А.Г. Сивцов ВОСП и защита информации. Фотон-Экспресс / №18, 2000, С. 16 – 20.

3. В.Г. Годный Вопросы информационной безопасности в волоконно-оптических линиях связи. Системы безопасности. / №2(44), 2002. С.44 – 47.

4. К.Е. Румянцев, И.Е. Хайров Передача конфиденциальной информации по волоконно-оптическим линиям связи, защищённая от несанкционированного доступа. Информационное противодействие угрозам терроризма: Научн.-практ.журн., №1, 2003. С. 72 – 79.

5. В.И. Бусурин, Ю.Р. Носов Волоконно-оптические датчики: Физические основы, вопросы расчёта и применения. //М.: Энергоатомиздат, 1990. – 256 с.

6. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам.– М.: Горячая линия – Телеком, 2005.

7. Хорев А.А., Макаров Ю.К. Методы защиты речевой информации и оценка их эффективности. // Защита информации. Конфидент. – №4. – 2001.

Ольшанський В.В. (ВІТІ ДУТ)

ОЦІНКА ПРОСТОРОВО-ЧАСОВИХ МОЖЛИВОСТЕЙ СТАНЦІЙ ЗАВАД У ВІДПОВІДЬ ПО ПОДАВЛЕННЮ РАДІОЗАСОБІВ З ППРЧ

До радіозасобів, які функціонують в умовах апріорної невизначеності щодо умов ведення зв'язку, сигнальної і завадової обстановки, пред'являються високі вимоги по завадозахищеності та пропускної здатності. Постійне вдосконалення засобів радіорозвідки та радіозавад, впровадження автоматизованих комплексів радіоелектронного подавлення (РЕП) призвело за останні роки до істотного підвищення можливостей по радіоподавленню засобів радіозв'язку.

Одним з ефективних методів підвищення завадозахищеності радіозасобів (РЗ) при впливі навмисних завад є застосування псевдовипадкового перестроювання робочої частоти (ППРЧ). У РЗ з ППРЧ розширення спектра в межах заданої смуги частот здійснюється за допомогою стрибкоподібної зміни частоти сигналу за псевдовипадковим законом, який невідомий постановнику завад.

Для подавлення РЗ з ППРЧ можуть застосовуватися різні види організованих завад. Слід зазначити, що при використанні режиму ППРЧ для радіозасобів однією із самих несприятливих завад є ретрансльована завада (завада у відповідь).

Негативний вплив навмисних завад в системах і засобах радіозв'язку з ППРЧ може бути значно послаблений за рахунок застосування адаптивних алгоритмів формування та обробки сигналів, які дозволяють підвищити енергетичну ефективність радіозасобів. При цьому, важливим є завдання оцінки рівня спотворення сигналів з ППРЧ в умовах навмисних завад.

Тому актуальним є завдання дослідження можливостей станцій завад у відповідь по подавленню радіозасобів з ППРЧ. В разі присутності на вході станції завад великої кількості сигналів радіозасобів з ППРЧ одного типу передавач завад, маючи обмежену потужність, не в змозі подавити кожен перехоплений сигнал. У зв'язку з цим зменшується ймовірність перехоплення і, відповідно, ймовірність подавлення частотних елементів сигналів радіозасобів. В таких умовах вирішення задачі подавлення певної кількості радіозасобів з ППРЧ використовуються різні види селекції, наприклад, просторовій селекції по направленню приходу. Проте при цьому виникає трудність в тому, що через просторове рознесення приймача і передавача РЗ немає можливості визначити напрями (пеленги) на приймачі раіозасобів. Тому з метою забезпечення необхідної ймовірності подавлення приймачів РЗ потужність передавача станції завад у відповідь має бути розподілена по заданому певним чином кутовому сектору.

Станція завад у відповідь, яка має у своєму складі апаратуру радіотехнічної розвідки, для вирішення задач по подавленню РЗ з ППРЧ повинна забезпечувати: виявлення сигналів радіозасобів по всьому робочому діапазоні частот за можливо короткий час; вимірювання частоти і напрямку приходу перехопленого сигналу з заданою точністю; настроювання передавача завад на частоту сигналу, що подавлюється; випромінювання завади в заданому просторовому секторі.

Проведений аналіз показав, що ефективність станції завад у відповідь залежить як від енергетичних характеристик радіозасобів (відношення сигнал-завада), так і часових можливостей, які визначаються топологією РЗ та станції завад, а також часом спрацьовування станції завад.

Перспективним напрямом подальших досліджень є розробка методів та методик управління параметрами радіозасобів з ППРЧ на основі отриманих оцінок нижньої межі часу спостереження, потрібного для оцінювання із заданою ймовірністю і точністю частоти перехоплених сигналів з ППРЧ та необхідної кількості завад для подавлення сигналів декількох радіозасобів з ППРЧ при використанні в апаратурі радіотехнічної розвідки селекції за напрямом приходу сигналів РЗ.

к.т.н. Перегуда О.М. (ЖВІ ДУТ)
Горнін М.А. (ЖВІ ДУТ)

ДВОКОНТУРНА МОДЕЛЬ ЖИТТЄВОГО ЦИКЛУ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

В Україні створення автоматизованих систем (АС) регламентовані ГОСТ, насамперед серії 34 та 15 (для військової сфери) [1, 2]. Однак окремі положення цих ГОСТів вже застаріли, а зміст деяких етапів життєвого циклу АС викладено недостатньо повно. Застосування міжнародного стандарту (ISO/IEC 12207) [3] обмежене через його орієнтацію перш за все на програмне забезпечення АСУ, він не пропонує конкретної моделі життєвого циклу (ЖЦ) й методів розробки, його рекомендації є загальними для будь-яких моделей життєвого циклу. Авторами пропонується варіант поєднання двох найпоширеніших на даний час моделей ЖЦ: каскадної та спіральної. В рамках запропонованого підходу експлуатація АСУ повинна передбачати застосування набору спеціальних модулів – комплекту конфігурування та модернізації (ККМ). Основне призначення ККМ – забезпечення високого рівня адаптаційних властивостей АСУ. ЖЦ АСУ пропонується організувати з двох контурів. Перший контур включає переважну більшість визначених у нормативних документах етапів (процесів) життєвого циклу АСУ (планування та аналіз вимог, проектування, реалізація, впровадження, експлуатація), але при цьому головним об'єктом, на модернізацію та зміну якого спрямовані заходи даного контуру, є ККМ, який призначений для конфігурування (модернізації) самої АСУ. Другий контур використовується для конфігурування АСУ при підготовці до безпосереднього застосування за призначенням (переважно за рахунок ККМ) з метою забезпечення визначеного (максимально можливого за конкретних обставин) рівня ефективності АСУ в різних умовах її застосування. Основним завданням, яке вирішується в першому контурі, є визначення кількісного та якісного складу набору (комплекту) модулів ККМ, призначених для конфігурування (модернізації) АСУ. Основне завдання другого контуру – конфігурування (модернізація) самої АСУ. Тривалість виконання етапів першого контуру може складати від декількох тижнів до декількох років, а послідовність їх виконання має ітераційний не завжди детермінований характер. Завершення певного циклу роботи в першому контурі є умовним (при досягнені певних характеристик ККМ і як наслідок характеристик АСУ), взагалі заходи даного контуру здійснюються безперервно. У другому контурі етапи виконується згідно жорсткого алгоритму (каскадна модель), а його загальна тривалість може складати від десятків хвилин до десятків днів, вона чітко регламентується та точно прогнозується. Заходи другого циклу повинні бути обов'язковою складовою етапу підготовки АСУ до застосування за призначенням, а також можуть виконуватись для оперативного конфігурування АСУ під час безпосереднього виконання завдань за призначенням. Відповідальність за виконання заходів (етапів) першого контуру несе розробник АСУ (ККМ) або організація, що здійснює науково-технічне супроводження АСУ, за виконання заходів другого контуру – командир (начальник), у розпорядженні якого знаходиться АСУ. Перший контур доцільно організовувати у відповідності до спіральної моделі ЖЦ, другий – у відповідності до каскадної моделі.

Реалізація обох контурів повинна передбачати використання положень концепції CALS (Continuous Acquisition and Life cycle Support, безперервна інформаційна підтримка життєвого циклу продукту).

ЛІТЕРАТУРА

1. ГОСТ 34.601 – 90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
2. ГОСТ В 15.203 – 79 Порядок выполнения опытноконструкторских работ по созданию образцов.
3. ISO/IEC 12207:2008 „System and software engineering – Software life cycle processes".

Поліщук Л.І. (НЦСВ АСВ)
к.т.н. Пащетник О.Д. (НЦСВ АСВ)

ПРОПОЗИЦІЇ ЩОДО МОЖЛИВИХ НАПРЯМКІВ РЕФОРМУВАННЯ СУЧАСНОЇ СИСТЕМИ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

Відповідно до концепції реформування і розвитку Збройних Сил України (ЗСУ) на період до 2017 р., з метою підвищення ефективності та оперативності управління військами (силами) заплановано перерозподіл на законодавчому рівні завдань і функцій між органами військового управління щодо створення трирівневої системи управління (СУ), яка включає: Генеральний штаб, до якого будуть інтегровані штаби видів ЗС; Оперативні командування „Північ" і „Південь" та командування Військово-морських сил, як міжвидові органи військового управління з підпорядкуванням військ (сил); Управління бригад, полків, інших військових частин і військових навчальних закладів, установ і організацій.

Основними напрямками створення і удосконалення запропонованої трирівневої СУ ЗСУ, на наш погляд можуть бути: як найшвидше законодавче закріплення прийнятих рішень на створення і удосконалення запропонованої СУ ЗСУ з виключенням із законів всіх недоліків, на які повинні вказати відповідні експерти, а також виділення на це реальних і достатніх коштів; створення єдиного органу управління, сектором безпеки і оборони (СБО) для розгортання і впровадження новітніх технологій у СУ державою з метою послідовності прийняття рішень з визначення пріоритетів щодо проведення наукових досліджень та розроблення окремих складових системи, а також створення узгодженого із суб'єктами національної безпеки і оборони держави документа та опису структури інформаційної безпеки, яка б забезпечила взаємодію та інтеграцію інформаційних систем, які використовуються в різних функціональних підрозділах, у різному географічно-розділеному організаційному середовищі, тобто узгодженням між собою розробки СУ суб'єктами СБО держави; визначенням конкретних вітчизняних і зарубіжних науково-промислових комплексів і організацій з укладанням відповідних договорів, які будуть залучені до створення єдиної автоматизованої системи управління (ЄАСУ) ЗСУ з гарантованими замовленнями і фінансуванням; удосконалення і оптимізація організаційно-штатної структури органів управління всіх ланок ЗСУ, опираючись при цьому на наукові розробки, а не суб'єктивні бажання окремих керівників і уточнення в зв'язку з цим функцій та процесів, які вони будуть виконувати; створення органів управління інформаційної боротьби; здійснення оптимізації інфраструктури існуючих стаціонарних пунктів управління (ПУ) у всіх ланках управління ЗСУ, модернізацію систем життєдіяльності, здійснення прив'язки до державної цифрової мережі зв'язку ВАТ „Укртелеком", а також забезпечення всім необхідним для обладнання сучасних автоматизованих робочих місць (АРМ) на визначених стаціонарних ПУ, створивши тим самим мережу універсальних, багатофункціональних ПУ, спроможних забезпечити роботу оперативного складу різних органів управління; переведення техніки рухомих ПУ і засобів вузлів зв'язку на єдину, удосконалену, уніфіковану транспортну базу вітчизняного виробництва обладнану сучасними цифровими засобами зв'язку і автоматизації; створення нових, сучасних повітряних ПУ; створення на базі прийнятих на озброєння нових засобів зв'язку і автоматизації АСУ в тактичній ланці управління, яка в подальшому інтегрується в АСУ оперативного командування і у майбутньому – в ЄАСУ ЗСУ, а також створення АСУ, в першу чергу, розвідки, зв'язку, оповіщення, оперативного (бойового) чергування; здійснення заходів щодо створення комплексної системи захисту інформації.

Все це повинно бути направлено на те, щоб структура і склад системи управління ЗСУ мирного часу забезпечили надійне управління військами (силами) без суттєвої перебудови та організаційних заходів в особливий період, а її рівень готовності був вищим за рівні готовності підпорядкованих військ (сил).

Поправко Ю.Ю. (ВІТІ ДУТ)
Бугера М.Г. (ЦНДІ ОВТ ЗС України)

АЛГОРИТМ ВИБОРУ ФОРМИ ПРАВОВОЇ ОХОРОНИ РЕЗУЛЬТАТІВ ІНТЕЛЕКТУАЛЬНОЇ ДІЯЛЬНОСТІ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Результатом інтелектуальної діяльності (РІД) є нематеріальний комерційний продукт, що підлягає використанню, якому відповідно до чинного законодавства надається правова охорона. Результати інтелектуальної діяльності, яким відповідно до чинного законодавства надається правова охорона, є об'єктами інтелектуальної власності (ОІВ). Правова охорона ОІВ побудована на принципі надання виключних прав на цей об'єкт. Вибір форми правової охорони РІД відноситься до класу задач, у яких найважливіші системні відносини носять неявний характер і не можуть бути виміряні за допомогою стандартних статистичних процедур.

Особливість прийняття рішень щодо форми правової форми РІД для озброєння та військової техніки (ОВТ) полягає в необхідності врахування аспектів, що лежать як в науково-технічній області вирішуваної проблеми, так і в правовій.

Для визначення доцільності і форми правової охорони РІД застосовують наступні критерії:

- науково-технічний рівень;
- можливість підвищення тактико-технічних характеристик ОВТ;
- можливість рішення принципово нових військово-технічних завдань;
- вклад в зниження витрат на експлуатацію і бойове застосування ОВТ;
- можливість застосування подвійних технологій.

При цьому, можливими альтернативами, можуть виступати наступні форми правової охорони РІД:

- отримання документів у формі патенту на винахід;
- отримання документів у формі патенту на корисну модель;
- отримання документів у формі патенту і деклараційного патенту на секретний винахід;
- отримання документів у формі деклараційного патенту на секретну корисну модель;
- правова охорона не можлива (виняткове авторське право) або недоцільна.

Для вирішення проблеми вибору форми правової охорони РІД пропонується застосувати метод аналізу ієрархій, який ґрунтується на ієрархічному представленні елементів, які визначають суть проблеми. Мета дослідження розташовується у вершині ієрархії, проміжними рівнями виступають критерії, альтернативи формують самий нижній ієрархічний рівень.

Для порівняння альтернатив застосовується метод оцінки погодженості даних, представлених у виді обернено симетричної матриці попарних порівнянь, розробленої Сааті Т.Л. Чисельне значення показника погодженості (*OS*), який характеризує погодженість множини суб'єктивних оцінок, отримується способом парного порівняння властивостей. Значення показника погодженості менше чи рівне 0,1 (10%), вважається припустимим, а по вихідним даним можуть бути отримані рішення, якщо значення *OS*, перевищує припустимий рівень, то вихідна інформація неприпустимо перекручена особою, що приймає рішення. У цьому випадку прийняті рішення щодо форми правової охорони РІД будуть характеризуватися великою неточністю і дуже низькою якістю. Отже, потрібний перегляд вихідної інформації чи залучення додаткових джерел її одержання.

На основі наведених міркувань сформовані рекомендації щодо алгоритму визначення конкретного типу форми правової охорони РІД, який повинен встановлювати форму патентної охорони в співвідношенні з нормативними актами Державної служби інтелектуальної власності України.

к.т.н. Правило В.В. (ВІТІ ДУТ)
Іванченко В.А. (ВІТІ ДУТ)
Кривенко О.В. (ВІТІ ДУТ)

НЕЧІТКИЙ КОНТРОЛЛЕР ПІДСИСТЕМИ УПРАВЛІННЯ МАРШРУТИЗАЦІЄЮ ДЛЯ МЕРЕЖІ З ДИНАМІЧНОЮ ТОПОЛОГІЄЮ

Сучасний бій характеризується високим ступенем мобільності та тісною взаємодією окремих підрозділів та частин, що в свою чергу зумовлює використання високо мобільної системи зв'язку, яка здатна задовольняти вимоги розвід захищеності, імітостійкості, завадостійкості, забезпечувати широкий маневр засобами зв'язку у всіх ланках управління, особливо в тактичній ланці. Задовольнити такі вимоги можуть мобільні радіомережі з механізмами самоорганізації.

Складність зовнішніх умов, таких як багатопроменеве розповсюдження радіохвиль, завмирання сигналів, робота з пониженою потужністю, динамічність топології, а також складність задач які вирішуються даними мережами не дозволяє застосовувати на даних мережах один конкретний протокол, або навіть конкретний клас протоколів. Дослідження показали що для мереж з різною інтенсивністю змін топології оптимальними є різні методи маршрутизації, такі як таблична, зондова, волнова. Крім того для різних умов розповсюдження радіохвиль оптимальними є різні методи доступу до середовища та різні види модуляції та кодування.

Виходячи з вищезазначеного перед нами постає актуальне завдання правильного вибору протоколу маршрутизації та технології доступу до середовища. Вирішити дану проблему в змозі інтелектуальна система управління з підсистемою управління маршрутизації реалізованою на базі нечіткого контролера, який зможе за допомогою апарату нечіткої логіки на базі неповної та недостовірної контрольної інформації про стан інформаційних напрямків, чітко приймати рішення по вибору певного протоколу маршрутизації, або ж певної технології.

Нечіткий контролер в складі підсистеми управління маршрутизацією, враховуючи зовнішні чинники (завадова обстановка, умови розповсюдження радіохвиль для конкретної ділянки місцевості, ємність мережі, кількість ретрансляторів, потужність передавачів, ємність батарей, забезпечення зв'язку в радіо напрямку чи радіомережі, з гарантованою доставкою повідомлень чи без, на основі терміновості доставки повідомлень та ін.) повинен виконувати наступні функції:

1) Вибір цільової функції управління маршрутами
2) Вибір типу маршрутизації
3) Вибір кількості маршрутів
4) Вибір способу розсилки службової інформації та способу управління мережею

Таким чином, даний підхід дозволяє створити ефективну мобільну радіомережу, що буде в змозі вирішувати завдання по зв'язку за призначенням в різних умовах обстановки, між портативними низько потужними та возимими високо потужними радіостанціями, між низько мобільними піхотними підрозділами та високо мобільними літальними апаратами, між пунктами управління та підрозділами що діють на найбільш віддалених напрямках з повноцінними можливостями по обміну інформації та по управлінню мережею.

ЛІТЕРАТУРА

1. Бунин С.Г., Войтер А.П., Ильченко М.Е., Романюк В.А/. Самоорганизующиеся радиосети со сверхширокополосными сигналами. – К.:НПП «Издательство «Наукова думка» НАН Украины. – 2012. 444 с.

2. Миночкин А.И., Романюк В.А. Маршрутизация в мобильных радиосетях – проблема и пути ее решения. // Зв'язок – 2006. – №3 – С.42– 50.

к.т.н. Правило В.В. (ВІТІ ДУТ)
Крисюк А.Ю. (ВІТІ ДУТ)

ПРОЕКТУВАННЯ МУЛЬТИСЕРВІСНОЇ ВІДОМЧОЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ GOOGLE API

Планування та побудова мультисервісної відомчої мережі з використанням широкосмугових безпроводових технологій є досить нелегкою в плані розрахунків, адже мережа повинна відповідати вимогам, які задані в вихідних даних, та нормам стандартів побудови безпроводових мереж (ISO, IEC, ITU та ін.). Причина в тому, що ряд факторів (тип місцевості, розподіл несучих частот, вибір технології і т.д.), які ускладнюють розрахунки, не дають вивести ідеальної методики, яка могла б задовольнити планування та розрахунок будь-якої мережі.

Так, як при розрахунку мережі, людина може припуститись помилки, яка критично вплине на подальший розрахунок та проектування, слід автоматизувати алгоритм розрахунку та мінімізувати втручання людини у проектування мережі.

Методика проектування мультисервісної відомчої мережі з використанням платформи Google API (Application Programming Interface) передбачає використання сторонніх бібліотек Google в програмному забезпеченні для вирішення задач, пов'язаних з проектуванням мережі.

Метою проектування мультисервісної відомчої мережі являється кінцеве представлення результатів розрахунків даної мережі та її графічне відображення у вигляді зон покриття базових станцій на карті шляхом застосування програмних технологій Google API.

Постановка задачі: Змоделювати мультисервісну відомчу мережу з графічною прив'язкою до місцевості (карти), а також виведення основних та проміжних розрахунків мережі та графіків їх залежностей.

Основні етапи реалізації задачі:

1. Використання існуючих методик розрахунку безпроводової мережі із застосуванням моделі Окамура-Хата та COST 231-Хата, їх модернізація та комбінування.

2. Розробка програмного продукту із використанням платформи Google API, який дозволяє автоматизовано розрахувати та проектувати мультисервісну відомчу мережу при обмеженнях, які задані в вихідних даних.

3. Графічне представлення основних та проміжних розрахунків у вигляді таблиці (Google Tables API).

4. Вивід графіків залежностей розрахованих характеристик (Google Charts API) та проектування розрахованої мережі на карті (Google Maps API).

Висновки:

Використання платформи Google API при проектуванні мультисервісної відомчої мережі дозволяє застосовування сторонніх бібліотек Google та отримання необхідних даних для подальшої маніпуляції з ними.

Графічне проектування безпроводової мультисервісної відомчої мережі на місцевості можливе в будь-якій точці нашої планети, що визначає гнучкість програмного забезпечення.

Використання платформи Google API мінімізує втручання людини у складні математичні розрахунки, що дозволяє уникнути помилок, які можуть трапитися в ході проектування мережі.

Пузиренко О.Г. (ВІТІ ДУТ)
Соколов О.В. (ВІТІ ДУТ)

ВИЗНАЧЕННЯ ПОКАЗНИКІВ КОМПЛЕКСНИХ ІНФОРМАЦІЙНИХ ЗАГРОЗ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ МЕТОДОМ ЕКСПЕРТНИХ ОЦІНОК

На етапі розвитку Збройних Сил України, під час побудови сучасної системи управління Збройних Сил України, захист від загроз інформаційної безпеки в інформаційно-телекомунікаційних системах спеціального призначення набуває важливого значення.

Інформаційно-телекомунікаційні системи спеціального призначення являють собою комплекс інформаційних та телекомунікаційних засобів, призначених для обробки та обміну усіма видами інформації, яка циркулює безпосередньо у Збройних Силах України.

Звичайно, виникають питання захисту інформації в інформаційно-телекомунікаційних системах спеціального призначення від загроз інформаційної безпеки.

Насамперед, в загальному контексті, загрози інформаційної безпеки [information security threat] – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері.

Сучасні системи управління створюються і функціонують за безпосередньою допомогою інформаційно-телекомунікаційних засобів і технологій. Протиправні дії в комп'ютерно-телекомунікаційному середовищі вже сьогодні реально загрожують національній безпеці держави, оскільки можуть порушити керування державними та військовими структурами.

Розглянемо можливості визначення показників комплексних інформаційних загроз методом експертних оцінок.

Експертне оцінювання здійснюється за кожним показником воєнної сфери національної безпеки ψ_i , де $i \in \{1, k\}$, що характеризується відповідним набором показників ψ_{ij}, де $j = 1,2,3,\ldots$ Кожний показник ψ_{ij} оцінюється за допомогою шкали важливості та шкали значень.

Перша шкала характеризує ступінь важливості показника ψ_{ij} і передбачає присвоєння йому експертом відповідного рангу φ_{ij}:

$$\varphi_{ij} = \begin{cases} 5 – украй важливий; \\ 4 – дуже важливий; \\ 3 – важливий; \\ 2 – не дуже важливий; \\ 1 – неважливий. \end{cases}$$

Друга шкала відображає відносну величину показника ψ_{ij}, що експертно оцінюється певним значенням δ_{ij}:

$$\delta_{ij} = \begin{cases} 5 – максимальне; \\ 4 – вище за середнє; \\ 3 – середнє; \\ 2 – нижче середнього; \\ 1 – мінімальне. \end{cases}$$

Експертне оцінювання проводиться наступним чином. Спочатку, на основі емпіричних оцінок показників загроз, експертами за шкалою важливості здійснюється присвоєння кожному з них відносного рангу φ_{ij}. Після цього здійснюється експертна оцінка за шкалою значень δ_{ij}, яка визначає внесок кожного показника в загальну характеристику стану

відносної сфери національної безпеки. Далі розраховуються відносні значення показників загроз за співвідношенням:

$$\lambda_{ij} = [\delta_{ij}/\varphi_{ij}] \leq 1 \text{ для усіх } i \in \{1,k\} \text{ та } j = 1,2,3,\ldots$$

відносні значення показників визначають ступінь небезпеки кожної загрози у будь-якій сфері національної безпеки Ψ_i. Загальний стан інформаційної безпеки в цілому у кожній сфері доцільно оцінювати за мінімальним значенням усіх її показників ψ_{ij}.

Таким чином, емпіричні значення показників комплексних інформаційних загроз перетворюються у відносну форму. На цій основі оцінюються узагальнені відносні показники загроз для кожної сфери Ψ_i національної безпеки:

$$\Psi_i = \Sigma_j=1,2,3, \alpha_{ij} \cdot \lambda_{ij},$$

де α_{ij} – нормуючий ваговий коефіцієнт ($0 \leq \alpha_{ij} \leq 1$), що визначається експертним шляхом для кожного показника в окремій сфері.

Відповідно, узагальнений відносний показник загроз інформаційній безпеці в цілому Ω визначатиметься як лінійно зважена сума узагальнених відносних показників усіх сфер національної безпеки:

$$\Omega = \sum_{i=1}^{k} \beta_i \cdot \psi_i,$$

де β_i – нормуючий ваговий коефіцієнт i-тої сфери інформаційної безпеки ($0 \leq \beta_i \leq 1$), що також визначається шляхом експертної оцінки. Наприклад, узагальнюючий відносний показник загроз інформаційній безпеці у воєнній сфері визначатиметься співвідношенням:

$$\Psi_i = \alpha_{11} \cdot \lambda_{11} + \alpha_{12} \cdot \lambda_{12} + \alpha_{13} \cdot \lambda_{13} + \alpha_{14} \cdot \lambda_{14} + \alpha_{15} \cdot \lambda_{15}.$$

Відповідно формується матриця оцінювання стану інформаційної безпеки у воєнній сфері (див. табл.)

Таким чином, запропонований підхід до визначення показників комплексних інформаційних загроз дозволяє:

– практично оцінювати стан інформаційної безпеки за кожною сферою національної безпеки;

– цілеспрямовано формувати і розвивати моніторинг зовнішніх і внутрішніх загроз інформаційній безпеці на основі системи показників цих загроз;

– більш обґрунтовано приймати рішення щодо підвищення рівня інформаційної безпеки за всіма сферами національної безпеки.

Матриця оцінок показників інформаційних загроз у воєнній сфері

Сфера національної безпеки	Емпіричні оцінки	Оцінки за шкалою значень	Оцінки за шкалою важливості	Відносні значення показників	Вагові коефіцієнти
Ψ_1	ψ_{11}	δ_{11}	φ_{11}	λ_{11}	α_{11}
	ψ_{12}	δ_{12}	φ_{12}	λ_{12}	α_{12}
	ψ_{13}	δ_{13}	φ_{13}	λ_{13}	α_{13}
	ψ_{14}	δ_{14}	φ_{14}	λ_{14}	α_{14}
	ψ_{15}	δ_{15}	φ_{15}	λ_{15}	α_{15}

У рамках запропонованого підходу доцільно провести подальші дослідження за наступними напрямами:

– розробка методів і засобів системного моніторингу загроз інформаційній безпеці, що дозволяють не лише контролювати, а й підтримувати такий стан інформаційної безпеки, за якого її показники перебуватимуть у допустимих межах;

– визначення взаємозв'язків відносних показників загроз інформаційній безпеці за всіма сферами національної безпеки;

– обґрунтування вибору нормуючих вагових коефіцієнтів для оцінювання стану інформаційної безпеки в цілому.

к.т.н. Радзівілов Г.Д. (ВІТІ ДУТ)
Бєляков Р.О. (ВІТІ ДУТ)

МЕТОД УСУНЕННЯ ПРОТИРІЧЧЯ КОЄФІЦІЄНТА ПІДСИЛЕННЯ І СЕРЕДНЬОКВАДРАТИЧНИХ ПОМИЛОК СИСТЕМИ АВТОМАТИЧНОГО УПРАВЛІННЯ ДІАГРАМОЮ НАПРАВЛЕНОСТІ ФАР

Як відомо, існуюча система зв'язку ланок управління різного рівня має ряд недоліків [1]. Вирішення цих недоліків можливо при використанні MANET (MobileAdHoc Networks) [2].

У якості антен таких мереж пропонуються фазовані антенні решітки (ФАР), та активні фазовані антенні решітки (АФАР), що набули широкого використання у сучасних системах мобільного, супутникового, та транкінгового зв'язку. Антенні системи з ФАР дозволяють формувати задану діаграму направленості при швидкому скануванні одночасно в широкому спектрі частот [3, 4, 5], що є їх вагомою перевагою.

Але побудову мереж з використанням ФАР з адаптивною системою управління діаграмою направленості, доцільно здійснювати у відповідності до вимог по направленності об'єкта зв'язку. Для викнання цих вимог необхідно забезпечити постійне високоточне супроводження антенної системи за об'єктом. Сучасні антенні системи зв'язку не завжди забезпечують необхідну точність, що призводить до погіршення енергетичних показників каналу зв'язку і збільшення вірогідності помилки приймаємого сигналу [1, 6].

Підвищення якості автосупроводження об'єкта антенною системою об'єкта зумовлено необхідністю безперервного взаємного орієнтування прийомної та передаючої станції протягом всього сеансу зв'язку. Орієнтування повинно відбуватися так, щоб антени ретранслятора (АР) та антени об'єктів приймали максимально можливу частину сигналу [1, 7]. Формування діаграми направленості ФАР залежить від системи автоматичного управління цих антен. У ході дослідження залежності коєфіцієнта підсилення системи, середньоквадратичних помилок (СКП) і квадратичної інтегральної оцінки системи автоматичного управління ФАР, обгрунтовано необхідність компромісного вибору коефіцієнта підсилення у зв'язку з протиріччям між умовами перехідних процесів. Для вирішення поставленої задачі розглянуто принцип побудови САУ ФАР на прикладі системи по відхиленню, з передаточними функціями системи управління $K_1(p)$ об'єкта управління, $K_2(p)$ – функція запасу стійкості (комплексна передаточна функція системи з помилкою), T – час встановлення заданого режиму.

$$K_1(p)=\frac{k_1}{T_1p+1}=\frac{D_1(p)}{F_1(p)}\quad K_2(p)=\frac{k_2}{(T_2p+1)p}=\frac{D_2(p)}{F_2(p)}$$

Виходячи із отриманих результатів аналізу системи автосупроводження АФАР, для усунення протиріччя між умовами мінімізації середньоквадратичних помилок та квадратичної інтегральні оцінки, що характерні для систем управління з принципом за відхиленням, що заключається у введенні похідних від задаючого (орієнтування діаграми направленості на абонента) та збурюючого (реального положення ФАР) впливів на систему автоматичного управління діаграмою направленості ФАР [8].

Метод усунення протирічча коєфіцієнта підсилення і середньоквадратичних помилок системи автоматичного управління діаграмою направленості ФАР полягає у розрахунку передаточних функцій по збурюючому впливу процесів системи автоматичного управління діаграмою направленості з урахуванням мінімізації СКП, визначення умов еквівалентності систем автоматичного упраління.

Для рис. 1 $\theta(p)=\alpha(p)-\beta(p);U_1(p)=K_1(p)\theta(p);$

$\beta(p)=K_4(p)[K_2(p)K_3(p)U_1(p)-K_5(p)L(p)]$

отримані передаточні функції системи:

$$K_{\theta\alpha}(p)=\frac{(T_1p+1)(T_3p+1)p}{(T_1p+1)(T_3p+1)p+k_p}=\frac{D_{\theta\alpha}(p)}{F_{\theta\alpha}(p)}\quad;\quad K_{\theta L}(p)=\frac{(T_1p+1)k_4k_5}{(T_1p+1)(T_3p+1)p+k_p}=\frac{D_{\theta L}(p)}{F_{\theta L}(p)}\quad.$$

Отримано підтвердження, що система управління з принципом управління по відхиленню є астатичною по відношенню до задаючого впливу $\alpha(p)$ та статичною по відношенню до збурюючого впливу $L(p)$.

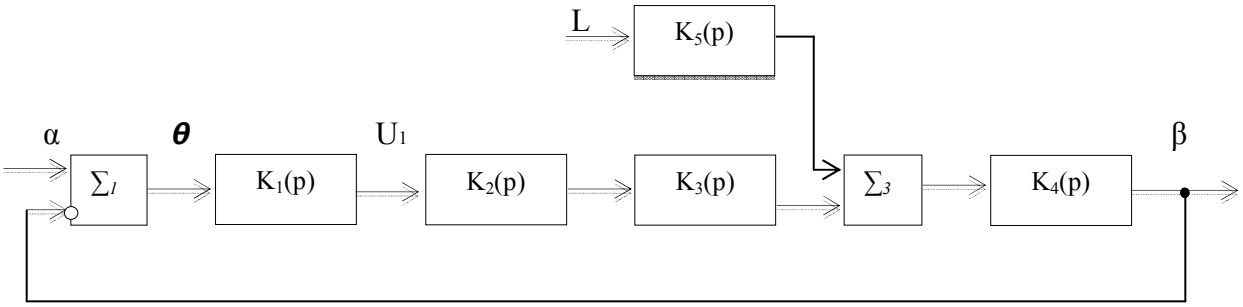


Рис. 1 Структурна схема системи управління з принципом управління по відхиленню

Спектральна щільність системи з астатизмом першого порядку

$$S_{\theta L}(\omega)=\left|\frac{K_{\theta\alpha}(j\omega)}{j\omega}\right|^2 S_{\dot\alpha}(\omega)\,.$$

Отримано та проаналізовано умови еквівалентності системи автоматичного упраління діаграмою направленості ФАР з диференційним зв'язком та системи з комбінованим управлінням. Встановлено, що дана система при k_p=12 має запас стійкості по фазі $\gamma=80^0$ і по амплітуді σ = 25 дБ. Для мінімізації СКП необхідно збільшувати коєфіцієнт підсилення, що призводить до виводу системи з рівноваги. При збільшенні k_p=300 запас стійкості по фазі зменьшується до $\gamma=8^0$. Для компенсації випадкового збурюючого впливу що надходить не на вхід системи, необхідно ввести зв'язок по заданому впливу. У подальшому необхідна розробка методу синтезу диференціального зв'язку системи автоматичного управління діаграмою направленості ФАР у відповідності із умовами мінімізації СКП та, динамічних помилок, що викликані збурюючими (зовнішніми) впливами.

ЛІТЕРАТУРА

1. Фортушенко А.Д. Основы технического проектирования систем связи через ИСЗ. – М.: Связь, 1990. – 322с.

2. Романюк В.А. Мобильные радиосети – перспективы беспроводных технологий // Сети и телекоммуникации. – 2003. – № 12. – С. 62 – 68.

3. Super Capacity Solution. The World's First GSM Adaptive Array Solution. – www.airnetcom.com.

4. Радиоавтоматика. Т.1./Г.Ф.Зайцев, Г.Н.Арсеньев, В.Г.Кривуца, В.Л. Булгач. – К.: ООО „Д.В.К." 2004. – 504с.

5. Воскресенский Д.И. Активные фазированые антенные решетки. – М.: Радиотехника, 2004.С.24 – 31.

6. Кровин В.В. Информационно – управляющие космические радиолинии: В2ч. – М.: НИИЭИР. – Ч.1. – 1993. – 229с.

7. Покрас А.М., Цирлин В.М., Кудеяров Г.И. Системы наведения антенн спутниковой связи. – М.: Связь, 1978. – 152с.

8. Радзівілов Г.Д., Бєляков Р.О. Системи автоматичного регулювання процесів прийомопередаючого тракту модулів активної фазованої антенної решітки. – К: Вісник Державного університету інформаційно – комунікаційних технологій. – 2012. – Т.1, №3. – С. 9 – 17.

д.т.н. Романенко І.О. (ВІТІ ДУТ)
Івахненко Т.О. (ВІТІ ДУТ)

СТРУКТУРА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ОЦІНКИ ЕФЕКТИВНОСТІ АВТОМАТИЗОВАНОЇ СИСТЕМИ ПЛАНУВАННЯ БОЙОВОЇ ПІДГОТОВКИ

У теперешній час актуальним є створення автоматизованої системи планування підготовки ЗС України. У доповіді представлена структура інформаційної технології оцінки ефективності планування бойової підготовки військовослужбовців у разі застосування автоматизованої системи планування підготовки рис.1. Такий підхід дозволив вирішити завдання оцінки ефективності планування підготовки із зменшенням витрат часу на неї , а також знайти оптимальний режим планування при заданих обмеженнях, досягаючи при цьому , необхідного рівня приросту навику в бойовій підготовці . Пропозиція нечіткої моделі оцінки ефективності планування підготовки за рівнем приросту навику, згідно цільової функції підготовки, дозволить сформулювати метод оцінки ефективності планування підготовки військовослужбовців, згідно функціональних обов'язків, на основі апарату нечітких множин та відійти від формального підходу у плануванні і оцінки бойової підготовки.

Запропонована інформаційна технологія оцінювання дозволить підвищити точність і зменшити витрати часу на планування бойової підготовки військовослужбовців .

Рис.1. Структура інформаційної технології оцінки ефективності пла військовослужбовців

Романенко С.О. (ВІТІ ДУТ)
к.т.н. Соколов В.В. (ВІТІ ДУТ)

ФОРМИ ЗАХИСТУ АВТОРСЬКИХ ПРАВ ПРОГРАМНОГО ПРОДУКТУ

Питання правової охорони та захисту комп'ютерного програмного забезпечення є найбільш суперечливим та конфліктним у юридичній практиці. Здійснюючи значний обсяг роботи по створенню програмного продукту (розробка програм, здійснення заходів щодо збереження конфіденційної інформації та комерційної таємниці тощо), перше про що повинні подбати розробники програмного продукту – захист авторських прав.

На сучасному етапі розвитку інформаційних технологій існує декілька форм захисту авторських прав програмного продукту. Доволі часто такі форми захисту на програмне забезпечення містять різні заборони.

Обмеження на комерційне використання дозволяє безплатне використання програмних продуктів в некомерційних цілях для приватних осіб, однак вони вимагають оплати в разі використання програмного продукту з метою отримання прибутку.

Обмеження на розповсюдження супроводжує зазвичай великі програмні проекти, коли правовласник вимагає оплати за кожну копію програми. Забороняється відтворення та розповсюдження програми та окремих частин програмного забезпечення. Зазвичай з таким обмеженням використовуються програмні продукти, орієнтовані на вузький «професійний» сегмент ринку або у програмному забезпеченні, потрібному великому числу користувачів. Прикладом може служити пакет програм *Adobe Creative Suite* або операційна система *Microsoft Windows.*

Прив'язка до апаратної чи програмної платформи визначає, що власник забороняє використовувати свої програми, які можуть навіть бути відкриті, поза своєю апаратною чи програмною платформою. Така бізнес модель типова для монополістів, таких як *Apple* чи *Microsoft.*

Обмеження на модифікацію використовується як правило в програмних пакетах із закритим кодом і може забороняти або обмежувати будь-яку модифікацію програмного коду, дизасемблювати і декомпілювати, забороняється реверсний інжиніринг і вивчення коду програмного забезпечення. Деякі виробники дозволяють партнерам вивчати сирцевий код для ефективної побудови своїх застосунків на його основі, але забороняють вносити зміни у свій код.

У доповіді розглянуто вирішення питання про можливість протидії незаконного використання ПЗ та форм захисту авторських прав програмного продукту.

Аналіз показує, що кожна окрема форма захисту авторського права програмного продукту певною мірою забезпечує надійність захисту ПЗ і дозволяє здійснити його захист у визначених межах. Однією з основних проблем авторського права є те, що воно встановлює захист лише форми вираження об'єкта. Проблеми патентного захисту програмного забезпечення пов'язані з пошуком аналогів заявленого алгоритму, із встановленням юридичного механізму виявлення його прототипу, з умінням описати формулу алгоритму, із визначенням його новизни, з наявністю класифікації алгоритмів подібно до міжнародної класифікації винаходів.

Таким чином, використання різних форм захисту програмного продукту свідчить про те, що існуюча на сьогодні юридична підтримка захисту авторських прав програмного продукту є недостатньою. В Україні автори і власники програмних продуктів досить рідко вдаються до судового захисту своїх виключних прав на програмне забезпечення, причинами чого є недосконаліть законодавства, відсутність досвіду боротьби з такими порушеннями.

д.т.н. Романюк В.А. (ВІТІ ДУТ)
к.т.н. Сова О.Я. (ВІТІ ДУТ)
Симоненко О.А. (ВІТІ ДУТ)

АНАЛІЗ ІСНУЮЧИХ АГЕНТНИХ ПЛАТФОРМ ДЛЯ ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ ВУЗЛАМИ МОБІЛЬНИХ РАДІОМЕРЕЖ КЛАСУ MANET

Сучасні системи безпроводового зв'язку розвиваються у напрямку забезпечення мобільності їх абонентів та організації зв'язку між абонентами за принципом „у будь-якому місці, у будь-який час". Прикладом реалізації даного принципу є мобільні радіомережі (МР), що будуються за технологією MANET (*Mobile Ad-Hoc Networks*). Особливості функціонування МР вимагають наявності в складі кожного вузла системи управління (СУ), здатної приймати рішення в умовах невизначеності. В ході попередніх досліджень показано, що реалізація підсистем вузлової СУ можлива шляхом використання агентів.

Під агентом розуміється деяка автономна програма, яка знаходиться в середовищі, від якого отримуються дані про події, що відбуваються, інтерпретує їх і виконує команди, що впливають на це середовище, в залежності від поставленої мети.

Зважаючи на особливості функціонування СУ вузлами МР, які, з одного боку передбачають відносну автономність при вирішенні завдань з управління вузловими ресурсами, а з іншого боку – повинні враховувати стан вузлів-сусідів при прийнятті управлінських рішень (поодинці вузлові СУ не зможуть вирішити всіх завдань поставлених перед ними), запропоновано для побудови структурних елементів СУ вузлами радіомереж класу MANET використовувати технологію інтелектуальних агентів, з можливістю їх об'єднання в багатоагентну систему.

Базовим інструментом розробки інтелектуальних багатоагентних систем, що дозволяє створювати, знищувати, інтерпретувати, запускати і переміщати агентів є агентна платформа. Основними функціями агентних платформ є:

– організація взаємодії агентів;
– передача повідомлень між агентами всередині платформи (на різних рівнях: на рівні мережевих пакетів, повідомлень будь-якої мови реалізації, протоколів передачі) і між різними платформами;
– підтримка онтологій;
– управління агентами, їх життєвими циклами;
– пошук агентів і даних про них всередині системи;
– забезпечення безпеки агентів.

Найбільш відомі наступні агентні платформи для розробки:

– JADE (*Java Agent Development Framework*);
– *Coguaar* (*Cognitive Agent Architecture*) – найпотужніший проект, підтримується DARPA (*Defense Advanced Research Projects Agency* – агентство передових оборонних дослідницьких проектів);
– *Aglobe* – володіє недостатньою підтримкою *FIPA* (*Foundation for Intelligent Physical Agents*) – організації стандарту *IEEE*, яка сприяє розвитку технології на основі агентів і взаємодії їх з іншими технологіями;
– *Jason* (*multi-agent systems development platform*) – для розробки багатоагентних систем, має багато функцій, що можна налаштовувати;
– *Jack* – одна з небагатьох платформ, де використовуються модель логіки агента, що заснована на принципах переконаннях-бажаннях-наміри (*Belief-desire-intention software model* – BDI) і вбудовані формально-логічні планування роботи агента.

Крім агентних платформ для програмування агентів можуть застосовуватися:

– універсальні мови (*Java*, C++, *Visual Basic*, C#);
– мови представлення знань (SL, KIF);

– мови комунікацій та обміну знаннями (KQML, *AgentSpeak*, *April*);
– мови сценаріїв (TCL/TK, Python, Perl 5);
– спеціалізовані мови (*TeleScript*, COOL, *Agent*0, *Agent*K);
– символьні мови та мови логічного програмування (Oz, *ConGolog*, IMPACT, *Dylog*, *Concurrent* METATEM);
– а також інші мови і засоби розробки агентів.

В якості критеріїв вибору засобів розробки багатоагентних систем для використання при побудові СУ вузлами радіомереж класу MANET можна використовувати, наступні:
– a-критерій: здатність до самоорганізації;
– b-критерій: здатність до функціонування в режимі реального часу;
– c-критерій: наявність правил поведінки та моделей реакцій на основі даних, отриманих з зовнішнього середовища;
– d-критерій: активізації інших ІА у разі зміни параметрів зовнішнього середовища чи після надходження команд з ІСУ;
– e-критерій: забезпечення самонавчання ІСУ на основі зібраної інформації про стан навколишнього середовища та стан самої системи управління;
– f-критерій: визначення (зміна, у разі необхідності) пріоритетів функціонування ІА в залежності від доступних йому внутрішніх ресурсів, що дозволить уникнути ситуації, за якої прийняття управляючих рішень буде покладене на ІА з недостатніми внутрішніми ресурсами;
– g-критерій: виконання функцій тимчасового координатора МР, при втраті зв'язку з вузлом, який координує роботу МР, в залежності від визначеної в процесі функціонування пріоритетності.

Порівняння засобів програмування агентів показано в табл. 1.

Таблиця 1

Порівняння засобів реалізації агентів за критеріями

Засоби розробки агента/ мова реалізації	***Критерії***						
	a	**b**	**c**	**d**	**e**	**f**	**g**
Mscrosoft.NET/C#	+	+	-	+	+	+	+
NetStepperPro 1.0/Java	+	+	-	+	+	+	+
JADE/Java	+	+	-	+	+	+	+
Aglobe/Java	+	+	-	+	+	+	+
Jason/Java	+	+	-	+	+	+	+
Jack/Java	+	+	+	+	–	+	–

Таким чином, при застосуванні агентів в МР класу MANET, задоволення зазначених вище критеріїв є важливою умовою для їх успішної реалізації з використанням того чи іншого програмного засобу чи платформи. Як видно з таблиці, цим критеріям задовольняють багато програмних засобів реалізації агентів, однак переважна більшість платформ використовує мову програмування *Java*, як таку, що дозволяє реалізувати агенти, задовольняючи всі вище зазначені критерії.

Руденко Д.М. (ВІТІ ДУТ)

АНАЛІЗ ЕФЕКТИВНОСТІ ОСНОВНИХ МЕТОДІВ АДАПТАЦІЇ В ЗАСОБАХ РАДІОЗВ'ЯЗКУ НА ФІЗИЧНОМУ РІВНІ

Ієрархічна структура системи радіозв'язку, як різновиду адаптивної системи, що автоматично змінює структуру, алгоритми роботи і параметри радіоапаратури з метою забезпечення необхідного показника якості зв'язку при зміні зовнішніх умов однозначно визначають рівні управління її адаптацією. На системному рівні процедури адаптації забезпечують управління прикладними процесами, терміналами, адміністративне управління мережею. На мережевому рівні процедури адаптації забезпечують вибір маршруту доставки повідомлень, управління потоками повідомлень, протоколами і обміном даними, процедури конфігурації мережі. На рівні каналу зв'язку процедури адаптації забезпечують управління вибором робочої частоти, зондування середовища поширення радіохвиль і дослідження якості частотного каналу, спостереження за інтенсивністю використання частотного каналу, множинний доступ абонентів до ресурсу каналу. На рівні фізичної передачі процедури адаптації забезпечують управління швидкістю передачі даних, видом модуляції, завадостійким кодуванням, управління потужністю передавача, типом і діаграмою спрямованості випромінювання антени, тобто управляє параметрами сигналу, що передається по каналу зв'язку. *Управління швидкістю передачі.* При високій якості каналу зв'язку, швидкість передачі даних повинна бути встановлена максимально можливою. Проте за несприятливих умов для забезпечення необхідної надійності передачі даних в процесі адаптації швидкість передачі даних може бути знижена. Відповідно, адаптивна система автоматизованого управління апаратурою радіолінії повинна будуватися так, щоб спроби встановлення зв'язку починалися з максимальної швидкості передачі, а потім система знижує швидкість передачі даних у спробі надійно закінчити процедуру передачі.

Управління видом модуляції. Вибір виду модуляції в складній радіоелектронній обстановці є критичним для радіозв'язку через нестаціонарність каналу зв'язку. Вид модуляції при зміні пропускної спроможності каналу повинен вибиратися оптимальним чином для забезпечення заданої ймовірності помилки. При зниженні якості каналу, тобто при зростанні контрольованої ймовірності помилок, для підвищення надійності демодуляції кратність модуляції може бути понижена, що також призводить до зниження загальної пропускної спроможності каналу передачі інформації.

Управління параметрами завадостійкого коду. Розглядаючи управління завадостійкістю кодування, відзначимо, що способи кодування з виправленням помилок забезпечують різні ступені надійності передачі даних і безпеки передачі. Залежно від стану каналу можуть бути вибрані ті або інші способи завадостійкого кодування. Адаптивне управління (за критерієм забезпечення заданої ймовірності помилки) структурою завадостійкістю коду дозволить забезпечити в конкретних умовах максимальну пропускну здатність каналу зв'язку. *Управління потужністю*. Важливою є процедура адаптивного управління рівнем потужності канального сигналу. Техніка стеження за ефективністю потужності випромінювання дозволяє оцінити достатність її рівня для забезпечення заданої дальності і надійності радіозв'язку. Адаптивне зниження потужності випромінювання є досить ефективним для системи з погляду електромагнітної сумісності, електромагнітної безпеки і розвідзахищеності. *Управління діаграмою спрямованості антени*. Адаптивне управління діаграмою спрямованості антени також є ефективним способом підвищення якості радіозв'язку. Адаптивні антени відповідно до встановленої методики можуть бути оперативно перебудовані головним пелюстком діаграми спрямованості по заданим напрямом роботи, а нулями – по напрямах заважаючих випромінювань. Підводячи підсумки виконаного аналізу способів адаптації на фізичному рівні, відзначимо, що для забезпечення надійної роботи системи радіозв'язку, найбільш ефективними виявляються процедури управління потужністю передачі, видом модуляції та завадостійкого коду.

Садиков О.І. (ВІТІ ДУТ)

РОЗРАХУНКОВА МОДЕЛЬ ПОКАЗНИКІВ ЯКОСТІ ОБСЛУГОВУВАННЯ АБОНЕНТІВ ТРАНКІНГОВИХ РАДІОМЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

При проектуванні телекомунікаційних мереж, в тому числі і радіомереж транкінгового зв'язку спеціального призначення, попередній розрахунок показників якості обслуговування QoS абонентів являється важливим моментом. Точний розрахунок необхідної кількості каналів (канальної ємності) для обслуговування плануємої загрузки абонентів з необхідною якістю допоможе: з однієї сторони – забезпечити прийняту якість обслуговування абонентів, з другої сторони – уникнути планування „зайвих" ресурсів системи, включаючи дефіцитний частотний ресурс, що природно позбавляє замовника від надлишкових фінансових вкладень в систему. Для розрахунку показників обслуговування нагрузки в радіомережах транкінгового зв'язку спеціального призначення, на даний час найбільш перспективного стандарту TETRA, пропонується метод, який ґрунтується на більш реалістичних імовірних припущеннях розподілу часу обслуговування абонентів, що дозволяє краще апроксимувати навантаження на мережу й досягти більшої точності проведених розрахунків. Обраний стандарт TETRA беремо як приклад, метод може використовуватися для розрахунків показників якості обслуговування абонентів транкінгових мереж інших стандартів.

Для розрахунків показників якості обслуговування абонентів транкінгових радіомереж аналітичними методами теорії масового обслуговування звичайно ухвалюється наступний підхід – кожна зона обслуговування базової станції (сота) моделюється як система масового обслуговування із чергою, тобто:

– канали базової станції є обслуговуючими пристроями;

– виклики користувачів (абонентів) моделюється вхідним процесом запитів на обслуговування;

– час заняття каналу радіозв'язку являє собою час обслуговування запиту (заявки);

– у випадку зайнятості всіх обслуговуючих приладів виклики абонентів стають у чергу на обслуговування.

Час заняття каналу (у цьому випадку радіоканалу) – це час, на який виклик абонента займає радіоканал у зоні обслуговування базової станції. Природно, цей час є випадковою величиною і її розподіл апроксимується законами вірогідних розподілів.

Представляю наступні моделі:

– аналітична модель з експоненціально розподіленим часом обслуговування;

– модель з гіперекспоненціальним розподілом часу обслуговування.

Аналітична модель з експоненціально розподіленим часом обслуговування позначається в теорії масового обслуговування як M/M/S/K/N. При проведенні розрахунків, можемо прорахувати рівняння рівноваги системи з накладенням нормуючої умови:

$$P \times Q = 0; \quad \sum_{i=0}^{N} p(i) = 1$$

p(i)-імовірність стану системи.

імовірність постановки виклику користувача на очікування (імовірність очікування) буде дорівнюватися:

$$Роч = \sum_{i=S+1}^{N} p(i)$$

N-кількість обслуговуємих абонентів;

S-кількість каналів радіозв'язку, предоставляющей однією базовою станцією;

Експоненційне розподілення не в повному обсязі описує час обслуговування абонентів. Як відомо, що характеристики експоненціального розподілу визначаються параметром μ, відповідно коефіцієнт варіації експоненціальної випадкової величини дорівнює одиниці. Однак статистична обробка результатів виміру часу обслуговування у багатьох телекомунікаційних системах показує, що розподілення часу обслуговування не

рідко має значення коефіцієнта варіації більше одиниці. При використанні системи, з коефіцієнтом варіації часу обслуговування більшим за одиницю, з застосуванням експоненціального розподілу, розрахункові показники якості обслуговування можуть бути недооцінені, та сплановані мережеві ресурси можуть виявитися недостатніми для обслуговування абонентів з заданою якістю.

Виходячи з цього багатьма винахідниками був запропонований гіперекспоненціальний розподіл часу обслуговування для моделювання часу обслуговування абонентів (часу заняття каналу радіозвязку). Визначення в теорії масового обслуговування M/H2/S/K/N. При проведенні розрахунків, розподіли що входять до розкладу являються експоненціальними, тому відсутність послідовності зберігається, що дозволяє використовувати, для моделювання системи, ланцюги Маркова. Так як всі стани багатомірної марковської моделі (крім стану i=0) представлені двома або декількома станами еквівалентної марковського ланцюга, то змінюючи межі складання отримуємо імовірність очікування:

$$Роч=\sum_{m=2^s}^{(N-S+1)2^s-1} p(m)$$

Підбором параметрів гіперекспоненціального розподілу можно моделювати розподіл нагрузки загального типу, отриманого по результатам статистичних вимірювань в мережі зв'язку. Єдине обмеження складається в тому, що коефіцієнт варіації часу обслуговування (часу заняття каналу) не може бути меньшим за одиницю, так як являється властивістю гіперекспоненціальногорозподілу.

Запропонована аналітична модель для розрахунків параметрів якості обслуговування абонентів у транкінгових мережах радіозв'язку спеціального призначення дає більш точну оцінку в порівнянні з формулами Єрланга, оскільки:

– ураховує неекспонентний характер розподілу часу обслуговування викликів абонентів;

– ураховує кінцеву популяцію (число) користувачів, що характерно для мереж транкінгового професіонального радіозв'язку;

– дозволяє враховувати різні сценарії навантаження на мережу;

– може апроксимувати розподілення часу обслуговування абонентів загального виду, отримане статистичною обробкою результатів вимірів у реальній мережі зв'язку.

Модель може використовуватися для попередньої оцінки параметрів якості обслуговування абонентів транкінгових мереж стандарту TETRA і інших стандартів.

З використанням розробленої програми обчислень, можливо:1.складання таблиць (номограм); 2.розробка закінченого програмного продукту із графічним інтерфейсом користувача, які можуть використовуватися для швидкої оцінки якості обслуговування абонентів у різних сценаріях навантаження при проектуванні мереж транкінгового радіозв'язку.

ЛІТЕРАТУРА

1. Овчинников А.М., Воробьёв С.В., Сергеев С.И. Открытые стандарты цифровой транкинговой радиосвязи.Серия изданий „Связь и бизнес", М.МЦНТИ – Международный центр научной и технической информации, ООО „Мобильные коммуникации", 2000.

2. Steppler M.Mfximum number ofusers which can be served by TETRA systems//Aachen unsversity of technology proceedings.

3. http://ru.scribd.com/doc/18680861/-TETRA, Aug 17, 2009.

4. Клейнорок Л. Теория масового обслуживания. Пер. с англ./Пер. И.И. Грушко; ред. В.И. Нейман. – М.:Машиностроение, 1979.

5. Aguilar M., Barcelo F., Paradells J. Mean Waiting Time in the M/H2/s Queue: Application to Mobile Communications Systems// IMACS'97. – P. 577 – 582.

д.т.н. Сайко В.Г. (ДУТ)

СПОСІБ БАГАТОПАРАМЕТРИЧНОЇ АДАПТАЦІЇ В БЕЗДРОТОВИХ МЕРЕЖАХ FH-OFDMA

Однією з проблем розвитку сучасних бездротових систем зв'язку є відсутність сумісності між різними типами радіопристроїв передачі повідомлень і мережевої інфраструктури. Також, у зв'язку з обмеженням частотного ресурсу, розробка нових систем бездротового доступу призводить до збільшення навантаження на природний ресурс і, як наслідок, ускладнення процедури виділення частот. Тому в даний час через швидкий розвиток систем мобільного зв'язку гостро постає питання про ефективність використання частотного спектра.

Система мобільного зв'язку четвертого покоління на основі когнітивних технологій перебуває в процесі стандартизації для забезпечення ефективної організації міжмережевої взаємодії і інтегрованої служби між дротовою мережею зв'язку і бездротовою мережею зв'язку в доповнення до простої службі бездротового зв'язку, яку забезпечують системи мобільного зв'язку попереднього покоління. Відповідно, для передачі великого об'єму даних на такому ж рівні, доступному в дротовій мережі зв'язку, потрібна розробка технології для нової мережі бездротового зв'язку.

З точки зору вдосконалення методів приймання та передавання для когнітивних мереж представляє інтерес схема стрибкоподібної зміни частоти (далі називається „FH") являє собою схему зміни піднесучих, виділених конкретному терміналу абонента, і схема FH-OFDMA являє собою схему, яка комбінує схему FH і схему OFDMA. Система, що використовує схему FH- OFDMA (далі називається „система FH- OFDMA"), використовує схему FH у смугах частот з перескоком частоти піднесучих, виділених для терміналу абонента. Отже, система FH- OFDMA також розподіляє всі піднесучі, зокрема, піднесучі даних, що використовуються по всій смузі частот, таким чином, досягаючи збільшення частотного рознесення. В системі множинного доступу з ортогональним частотним поділом каналів і стрибкоподібною зміною частоти (FH-OFDMA) смуга пропускання рівномірно поділяється на ряд ортогональних піднесучих. Кожному користувачеві надається певна кількість цих піднесучих OFDMA. В FH-OFDMA користувачі також стрибкоподібно змінюють частоту (тобто, піднабір несучих OFDM, призначених користувачеві, змінюється в часі) по всій смузі пропускання. Всі користувачі в рамках одного сектора або стільники є ортогональними відносно один одного і, отже, не викликають перешкод один одному.

В останні десятиліття багато робіт з мобільних систем зв'язку присвячено релеєвським завмиранням, однак, завмирання Накагамі і методи адаптивного приймання в їхніх умовах досліджувались мало [1, 2]. В доповіді наводяться отримані аналітичні вирази ймовірності помилки від середнього ВСШ при застосуванні FH-OFDMA зв'язку в каналах з завмираннями за законом Накагамі і результати дослідження, які дозволили запропонувати новий спосіб збільшення завадостійкості радіозв'язку за технологією когнітивного радіо шляхом зниження ймовірності помилки приймання даних в каналах з завмираннями за законом Накагамі застосуванням синтезу режиму ППРЧ і OFDMA, з оптимальним вибором порогового рівня при фіксованих: потужності передавача і середнього значення ВСШ. В якості порогового рівня вибрано нормоване значення $\boldsymbol{n}$, як відношення γ_t і γ_0,

$$n = y_t / y_o$$

яке визначається з урахуванням глибини завмирань сигналу $\boldsymbol{m}$ і кількості джерел внутрішньосистемних завад $\boldsymbol{N}$. Це дозволяє визначити адаптивний режим роботи (адаптивний алгоритм) вибору тривалості та кількості стрибків.

Для реалізації алгоритму багатопараметричної адаптації, який мінімізує ймовірність помилкового приймання даних у багатопроменевих каналах з завмираннями за законом Накагамі, необхідно задати інтервал дискретизації, визначити середні часові витрати на зміну параметрів і ймовірності роботи радіолінії без порушення зв'язку на інтервалі ***To*** при різних параметрах. Вибір інтервалу ***To*** повинен проводитись з урахуванням інтервалу квазістаціонарності процесів зміни у часі параметрів сигналів і завад в багатопроменевому каналі і часу, необхідного для оцінки рівнів сигналів і завад та прийняття рішення. Часові витрати на зміну параметрів неважко визначити за відомими значеннями тривалості команд управління, часом перебудови і синхронізації для конкретного типу апаратури.

Робота радіолінії з описаним алгоритмом багатопараметричної адаптації на тривалості сеансу зв'язку здійснюється наступним чином.

На кожному інтервалі *To* проводяться вимірювання миттєвих значень амплітуди прийнятого сигналу і визначаються параметрами розподілу Накагамі . Одночасно з цим оцінюється співвідношення сигнал - шум на вході приймача і розраховується значення *Рпом*. В кінці поточного інтервалу *To* на основі розрахованих виграшів вибирається оптимальне керування, що забезпечує мінімізацію ймовірності помилкового приймання даних в каналах з завмираннями на наступному кроці. Таким чином, в залежності від обраного параметра адаптації здійснюється завчасний перехід без втрат часу на аналіз каналу, що відмовив.

Передавати дані з підвищеною швидкістю необхідно, попередньо записавши їх в буферну пам'ять. В цьому випадку сигнал буде прийматись не тільки в періоди, коли миттєве значення ВСШ перевищує рівень ***n*** , але і в періоди глибоких завмирань, істотно знижуючи завадостійкість, підвищуючи при цьому ймовірність помилки.

Вибираючи значення ***n*** під час обліку глибини завмирань сигналу ***m***, кількості джерел внутрішньосистемних завад ***N*** і розрахованої ймовірності помилки, можна здійснити передачу даних з низькою ймовірністю помилки при незначному розширенні смуги сигналу.

Побудовано імітаційну модель системи передачі даних, що функціонує за алгоритмом багатопараметричної адаптації для систем FH- OFDMA. Параметри моделі: вид модуляції QPSK, число піднесучих 512 , тривалість символу OFDMA $tc = 48$ мкс, часовий дуплекс, канал з завмираннями обвідної сигналу з розподілом Накагамі. Швидкість стрибків частоти дорівнює 100 перескок / с. Затримка сигналу ***T*** від 150 до 250 мкс. Тривалість завмирань $\tau = 0{,}4\text{-}4$ мс, тобто, виконано умову $T + tc << \tau$ і обвідна сигналу практично не піддавалася змінам за час передавання символу. Здійснено порівняння ймовірності помилки від середнього ВСШ для випадку комплексування FH- OFDMA і випадку використання OFDM. Порівняння показало, що запропонований алгоритм забезпечив суттєвий виграш у завадостійкості, а саме, при середньому значенні ВСШ 20 дБ ймовірність помилки зменшується більше, ніж в 10 разів.

ЛІТЕРАТУРА

1. Сайко В.Г. Системи бездротового цифрового радіозв'язку нового покоління: монографія. / В.Г. Сайко. – К.: ПП „Золоті ворота", 2011.– 300 с.

2. Фокин Г.А. Пути адаптации сигнала к условиям многолучевого распространения в канале широкополосного беспроводного доступа // Труды учебных заведений № 176, Санкт-Петербургский университет телекоммуникаций, 2007.

д.т.н. Сайко В.Г. (ДУТ)
к.т.н. Казіміренко В.Я. (ДУТ)

ВИКОРИСТАННЯ СИСТЕМИ ПЕРЕДАЧІ ДАНИХ ДЛЯ НАДАННЯ ПОСЛУГ ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ В СТАНДАРТІ DVB-T2

Розгортання багаточастотної мережі передбачає підвищене використання частотного ресурсу для мінімізації числа ділянок із неприйнятними умовами обслуговування (так званих тіньових або „мертвих" зон. Однак, створення умов коли в точках таких зон співпадають фази сигналів, час їх доставки та ідентичність переданих біт, що необхідне для реалізації мережного підсилення, потребує значних зусиль і не завжди можливе. І є значна імовірність створення зон із неприйнятною якістю приймання. Тобто „мертві" зони можуть залишитися хоча б на ділянках перетинання зон обслуговування сусідніми станціями.

В технічному рішенні, що розглядається в даній доповіді, покриття тіньової зони пропонується використанням технології багаточастотної мережі, де станція надання послуг еквівалентна ретрансляційній станції на вхід якої подається телевізійний контент в вигляді мультиплексів телевізійних каналів в форматі DVB-T2, які розміщуються в частотному діапазоні 470…863 МГц, а вихід в смузі на використання якої є дозвіл і яка суттєво відлаштована від смуги, що використовується в сусідній зоні обслужування (ЗО). Це дозволяє зменшити спотворення за рахунок взаємного впливу сигналів сусідніх ЗО до прийнятної величини, використовуючи, наприклад, частотну фільтрацію, а також збільшити число наданих в тіньову зону телевізійних каналів, оскільки використовується вільний частотний ресурс та прийнятна технологія передачі. При цьому слід максимізувати кількість телевізійних програм (каналів ТБ), що надаються в тіньову зону.

В такому технічному рішенні пропонується ввести до складу центральної станції по меншій мірі один передавальний ствол, в якому виконується лінійна обробка прийнятого від зовнішнього джерела інформації. До складу ствола входить приймальна антена для прийому мультиплексів DVB-T2, які розташовані в діапазоні частот 470…863МГц і яка підключена до входу ствола. До складу ствола також входять: засоби виділення прийнятних мультиплексів, введення їх в канал із загальною частотною смугою 40МГц (частотне мультиплексування), оптимальне для досягнення прийнятного рівня міжсимвольного взаємного спотворення (міжсимвольна інтерференція) сусідніми мультиплексами, засоби перетворення смуги частот в створеного каналу в частотний ресурс виходу ствола та доведення рівня сигналу до потрібного, передавальна антена.

Від абонентських станцій мережі надання доступу до послуг обміну даними запит поступає через приймальні антени і через приймальні порти поступають до блоку, де демодулюються і відновлений транспортний потік через спеціальний модуль подається в зовнішню інформаційну мережу, наприклад, мережу Інтернет. Отримана інформація від вузла провайдера даної служби маршрутизується на IP адресу абонента і через модуль комутатора комутується на фізичну адресу абонента, модулюється, проходить нелінійну та лінійну обробки і через блок введення ресурсу в виділеному йому частотному ресурсі через фідер подається на вхід передавальної антени, яка випромінює створений сигнал в зону обслуговування. Цей сигнал приймається абонентською станцією, на MAC якої він був комутований. Таким чином в зону обслуговування подається інформація телевізійного мовлення (яка може закриватися умовним доступом) і інформація, наприклад, із мережі Інтернет, яка розподіляється між абонентами на інформаційному рівні.

ЛІТЕРАТУРА

1. Интерактивная система беспроводного доступа к информационным ресурсам / [Нарытник Т.Н., Сайко В.Г., Булгач В.Л., Казимиренко В.Я.] // Зв'язок. –2011. – № 2. – С. 32 – 36.

к.т.н. Сальнікова О.Ф. (ЦНДІ ОВТ ЗСУ)

ЄДИНА АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ ЯК ОСНОВА СИСТЕМИ УПРАВЛІННЯ ОБОРОНОЮ ДЕРЖАВИ

Складність сучасної військової управлінської діяльності вимагає автоматизації управління військами (силами) на всіх рівнях та інформатизації інтелектуальної творчої діяльності посадових осіб органів управління. Передумови до можливості системної автоматизації управління Збройними Силами України (далі ЗСУ) в цілому та угрупуваннями створюють останні досягнення в області систем зв'язку і інформаційних технологій.

Для цього має бути створена глобальна інформаційно-управляюча мережа, яка забезпечує всі органи управління і безпосередньо учасників бойових дій необхідною їм інформацією в зручній для прийняття рішень формі. Крім того, в системі мають бути впроваджені комплексні математичні моделі (експертні системи), які дозволяють органам управління на основі наявної інформації „імітувати" різні варіанти дій для вибору якнайкращого та забезпечують підтримку ухвалення рішень і планування операцій. В основу такої технології має бути покладено створення імітаційно-аналітичних моделей сил і засобів збройної боротьби і геофізичних умов із застосуванням принципу об'єктно-орієнтованого аналізу складних систем. Ці моделі утворюють інформаційно-моделююче середовище для управління ЗС. За наявності інтегрованої бази даних, що містить інформацію про ЗСУ і їх угрупування, і універсального інтерфейсу можна створювати моделі будь-яких угрупувань військ (сил) протиборчих сторін в будь-якому районі України і інших районах світу, моделювати їх дії і отримувати результати прогнозу: у стратегічній ланці управління – на стратегічні дії і спеціальні операції; у оперативно-стратегічній і оперативній ланках управління – на фронтові, флотські, десантні, протидесантні, повітряні, морські операції, інші форми військах дій; у тактичній ланці – на бої, удари і бойові дії та забезпечувати управління військами (силами) в ході військових дій.

Над створенням такої системи, яка має підвищити ефективність функціонування системи управління Збройними силами України, працюють уже багато років.

Виходячи з вищенаведеного, основними задачами, які повинна забезпечити ЄАСУ є:

планування стратегічного розгортання та застосування ЗС України;

управління військами і зброєю в період підготовки до застосування та в ході застосування;

аналіз воєнно-політичної обстановки, визначення рівня загрози національній безпеці держави, планування та реалізація заходів протидії;

управління повсякденною та адміністративно-господарською діяльністю.

Приведення Збройних Сил України до рівня боєздатності, який забезпечить виконання покладених на них завдань, без розгортання ЄАСУ ЗС України сьогодні неможливе і, відповідно, потребує першочергової уваги.

ЛІТЕРАТУРА:

1. Пшеничный Г. Можем ли мы самостоятельно создать ЕАСУ? Однозначно можем и обязаны это сделать! // Defence express. – 2012. – № 4. – с. 20 – 21.

2. Михненко А. На тактическом уровне // Defence express. – 2012. – № 5. – с. 40 – 45.

3. Фролов В.С. Структурно-логічна схема Єдиної автоматизованої системи управління Збройних Сил України // Наука і оборона. – 2012. – № 1. – с. 15 – 23.

4. Пастухов О. Повна автоматизація // Атлантична панорама. – 2012. – № 2. – с. 18 – 19.

5. Постников А. Время „автоматизированных" войн // Независимое военное обозрение. – 2011. – № 1. – с. 1 – 3.

Самелюк Є.С. (ВІТІ ДУТ)

МУЛЬТИСЕРВІСНА МЕРЕЖА ЗВ'ЯЗКУ З ВИКОРИСТАННЯМ КОМУТАЦІЙНИХ ЦЕНТРІВ НА БАЗІ SOFTSWICH

Мережі зв'язку загального призначення на сьогоднішній час не в повній мірі можуть забезпечити потреби користувачів у послугах. Тому, планується перехід до мережі зв'язку, яка побудована на концепції NGN. Основою NGN є мультисервісна мережа зв'язку.

Одним з основних елементів мультисервісної мережі є вузол комутації, який може бути побудований на основі програмного комутатора (Softswich).

Програмний комутатор – це пристрій керування мережею зв'язку загального призначення, який здатний обслуговувати велику кількість абонентів і взаємодіяти з серверами додатків (платформа призначена для ефективного виконання процедур, які підтримують розробку додатків), який підтримує відкриті стандарти. Програмний комутатор є носієм інтелектуальних можливостей мережі зв'язку загального призначення та координує управління обслуговуванням викликів, сигналізацію і функціями, що забезпечують встановлення з'єднання через одну або кілька мереж.

Метою роботи є аналіз можливості застосування програмного комутатора на сучасних телекомунікаційних мережах загального призначення.

З урахуванням того, що в мережах зв'язку загального призначення передаватиметься і оброблятиметься трафік різних видів (трафік реального часу, трафік даних, відеоінформація) – мультимедійний трафік, можна виділити три основні напрями вдосконалення:

1) нові телекомунікаційні послуги з універсальним доступом з мережею загального призначення і *IP*-мереж, в контексті еволюції концепції інтелектуальної мережі і конвергенції послуг зв'язку;

2) нові підходи до забезпечення показників якості обслуговування;

3) проблема сигналізації і управління в мережі.

Аналіз застосування програмного комутатора на мережі

Проведений аналіз можливості застосування програмного комутатора показує, що його застосування на мережі загального призначення показав, що даний підхід надасть можливість доступу користувачам до більшого числа послуг,які будуть відповідати їх потребам та способу життя, а також забезпечити зручність і простоту контролю даної мережі.

Таким чином, впровадження даної технології не тільки надає змогу доступу абонентам до більшого числа послуг, але й призведе до можливості збільшення пропонованого пакету послуг та його покращення, зокрема сервісу передачі повідомлень та мобільного доступу.

ЛІТЕРАТУРА

1. Гольдштейн А.Б. Softswitch в 2004 году// Технологии и средства связи. Специальный выпуск „АТС. Коммутационное оборудование 2004". 2004. №1.

2. Б. С. Гольдштейн, А. Б. Гольдштейн. Softswitch. СПб.: БХВ – Санкт – Петербург, 2006.

к.т.н. Самойлов І.В. (ВІТІ НТУУ ДУТ)
Коротков В.С. (ВІТІ НТУУ ДУТ)

МОДЕЛЬ ДІАГНОСТИКИ КОМП'ЮТЕРНИХ МЕРЕЖ НА БАЗІ ІНТЕРВАЛЬНИХ ФУНКЦІЙ НАЛЕЖНОСТІ

На сьогодні актуальною науково-технічною проблемою є створення систем діагностування, які можуть опрацьовувати нечітку діагностичну інформацію. Сучасні комп'ютерні мережі є складними апаратно-програмними комплексами, що постійно вдосконалюються, розвиваються та модернізуються. Використання цих комплексів у провідних високотехнологічних сферах вимагає забезпечення високого рівня надійності їх функціонування. Одним з методів підвищення надійності є розроблення і впровадження ефективних систем діагностування комп'ютерних мереж. Однією з центральних задач діагностики є встановлення причин виникнення несправностей та їх усунення. Велика кількість різних факторів, вплив яких необхідно враховувати при встановленні цих причин, значно ускладнюють задачу діагностики [1]. Звичайно, кваліфіковані адміністратори мереж в змозі успішно вирішувати задачі діагностики, однак кількість таких компетентних експертів відносно мала, і їм важко передати досвід та інтуїцію молодим адміністраторам. В зв'язку з цим виникає необхідність в розробці комп'ютерних систем, які б забезпечували інтелектуальну підтримку прийняття діагностичних рішень адміністраторами середньої кваліфікації [2, 3].

До особливостей комп'ютерних мереж як об'єктів контролю та діагностування слід віднести: відсутність або надзвичайно високу вартість спеціалізованих діагностичних апаратних засобів та програм діагностування; неоднозначність діагностичної інформації; відсутність точних кількісних даних, які відображають зв'язок між зовнішніми проявами несправностей та причинами їх виникнення; залежність прояву несправностей від щільності мережного трафіка і кількості підключених абонентів; тощо. Перераховані особливості не дають можливості в повній мірі використовувати існуючі методи діагностування. Тому виникає інтерес до застосування методів та засобів штучного інтелекту [4], які дозволяють формалізовувати і використовувати доступну лінгвістичну інформацію, яка відображає розуміння експертом причинно-наслідкових зв'язків.

Одним з перспективних шляхів формалізації експертної інформації при моделюванні причинно-наслідкових зв'язків в задачах діагностики є теорія нечітких множин. Розв'язання задачі діагностики передбачає ідентифікацію залежності входи (причини) – виходи (наслідки) [5]. Особливість моделювання полягає у визначенні характеру цієї залежності в умовах невизначеності. Невизначеність виникає через те, що різні люди розуміють слова (терми) по-різному, а також через неточність вхідних даних. Оперувати даними типами невизначеності можливо засобами нечіткої логіки. Моделювання і мінімізація наслідків невизначеності здійснюється шляхом побудови нечітких систем II типу, які спроможні оперувати з усіма типами невизначеності. Для побудови таких систем використовуються функції належності II типу, серед яких найбільш поширеними є функції належності інтервального типу. Носієм моделі діагностики є експертні висловлювання типу „Причина-наслідок".

Постановка задачі. Дано: множина вхідних змінних $X = (x_1, x_2, \ldots, x_n)$; $x_i \in [\underline{x_i}, \overline{x_i}]$, $i = \overline{1, n}$; множина вихідних змінних $Y = (y_1, y_2, \ldots, y_m)$; $y_j \in [\underline{y_j}, \overline{y_j}]$, $j = \overline{1, m}$; множина причин $D = (d_1, d_2, \ldots, d_n)$, де причина d_i, $i = \overline{1, n}$, інтерпретується як нечіткий терм, що описує змінну x_i; множина наслідків $S = (s_1, s_2, \ldots, s_m)$, де наслідок s_j, $j = \overline{1, m}$, інтерпретується як нечіткий терм, що описує змінну y_j; відношення між причинами і наслідками $R \subseteq D \times S$. Задача діагностики може формулюватись у формі прямого і оберненого логічного виведення. При прямому логічному виведенні необхідно визначити

наслідки S^* для заданого вектора вхідних змінних X^*. При оберненому логічному виведенні необхідно відновити причини D^* для заданого вектора вихідних змінних Y^*. Розв'язання останньої задачі вимагає побудови моделі на базі нечітких відношень.

В загальному випадку для прийняття рішення необхідно виконати наступні дії: перетворити значення вхідних змінних в міру значимості причин; використовуючи композиційне правило виведення Заде та матрицю нечітких відношень отримати міри значимості наслідків; виконати операцію пониження типу та перетворити міри значимості наслідків у значення вихідних змінних. В результаті отримуємо модель діагностики на базі нечітких відношень, яка оперує з невизначеністю шляхом використання інтервальних функції належності нечітких термів причин і наслідків, а також використовує функції належності II типу, які дозволяють моделювати неточність вхідних даних:

$$Y = f_R^{II}(X,\ \widetilde{R},\ C_X,\ \underline{G}_{\widetilde{D}},\ \overline{G}_{\widetilde{D}},\ C_{\widetilde{D}},\ \underline{G}_{\widetilde{S}},\ \overline{G}_{\widetilde{S}},\ C_{\widetilde{S}}),$$

де $X = (x_1, x_2, \ldots, x_n)$ – вектор вхідних змінних; $\widetilde{R} = \left\{[\underline{r}_{ij}, \overline{r}_{ij}]\right\}$ – матриця інтервальних нечітких відношень II типу; $C_X = (c_1^*, c_2^*, \ldots, c_n^*)$ – вектор параметрів концентрації функцій належності, що моделюють неточність вхідних даних; $\underline{G}_{\widetilde{D}} = (\underline{g}^{\widetilde{d}_1}, \underline{g}^{\widetilde{d}_2}, \ldots, \underline{g}^{\widetilde{d}_n})$, $\overline{G}_{\widetilde{D}} = (\overline{g}^{\widetilde{d}_1}, \overline{g}^{\widetilde{d}_2}, \ldots, \overline{g}^{\widetilde{d}_n})$, $C_{\widetilde{D}} = (c^{\widetilde{d}_1}, c^{\widetilde{d}_2}, \ldots, c^{\widetilde{d}_n})$ – вектори параметрів функцій належності вхідних змінних; $\underline{G}_{\widetilde{S}} = (\underline{g}^{\widetilde{s}_1}, \underline{g}^{\widetilde{s}_2}, \ldots, \underline{g}^{\widetilde{s}_m})$, $\overline{G}_{\widetilde{S}} = (\overline{g}^{\widetilde{s}_1}, \overline{g}^{\widetilde{s}_2}, \ldots, \overline{g}^{\widetilde{s}_m})$, $C_{\widetilde{S}} = (c^{\widetilde{s}_1}, c^{\widetilde{s}_2}, \ldots, c^{\widetilde{s}_m})$ – вектори параметрів функцій належності вихідних змінних; f_R^{II} – оператор зв'язку "входи-виходи" для нечіткої системи II типу.

Таким чином для моделювання причинно-наслідкових зв'язків в умовах невизначеності використовуються інтервальні нечіткі відношення II типу. Нечіткі терми причин і наслідків формалізуються інтервальними функціями належності, в результаті чого міри значимості причин і наслідків визначаються інтервалами. Нечітка модель II типу будується на основі розширеного композиційного правила виведення Заде, з якого випливають дві системи рівнянь нечітких відношень. Ці системи пов'язують нижні (верхні) границі нечітких відношень і нижні (верхні) границі мір значимості причин і наслідків. Визначення значення вихідної змінної здійснюється шляхом операцій пониження типу і дефазифікації.

ЛІТЕРАТУРА

1. Пархоменко П.П., Согомонян Е.С. Основы технической диагностики: Оптимизация алгоритмов диагностирования, аппаратурные средства. – М.: Энергия, 1981. – 236 с.

2. Тоценко В.Г. Експертні системи діагностики і підтримки рішення. К: Наукова думка, 2004. – 124 с.

3. Герасимов Б.М., Дивизинюк М.М., Субач И.Ю. Системы поддержки принятия решений: проектирование, применение, оценка эффективности. – Севастополь: СНИЯЭиП, 2004. – 320 с.

4. Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети. – Винница: УНІВЕРСУМ-Вінниця, 1999. – 320 с.

5. Oh S. K., Pedricz W., Park H. S. Rule-based multi-FNN identification with the aid of evolutionary fuzzy granulation // Knowledge Based Systems. – 2010. – Vol. 17(1). – Pp. 1 – 13.

д.т.н. Самохвалов Ю.Я. (ВІТІ ДУТ)
Єрмоленко В.М. (ВІТІ ДУТ)
Петренко П.В. (ВІТІ ДУТ)

ЛОГІКО-ЛІНГВІСТИЧНИЙ ПІДХІД ДО ІНФОРМАЦІЙНОГО ПОШУКУ В СИСТЕМІ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ЗБРОЙНИХ СИЛ УКРАЇНИ

Інформаційний масив системи електронного документообігу Збройних сил України (СЕДО) складає понад 10 мільйонів документів, тому ефективний пошук необхідних відомостей є актуальною задачею. Досвід використання дійсної підсистеми пошуку документів (ППД), яка побудована за фактографічним принципом та орієнтована на релевантність результатів пошуку показав, що у більшості випадків вони не задовольняють інформаційну потребу користувачів. Це пов'язано з тим, що по-перше, користувач не завжди володіє точними атрибутами необхідних документів, а по-друге – не враховується семантичне наповнення документів та запитів. Аналіз класичних моделей повнотекстового пошуку, на базі яких побудовані сучасні інформаційно-пошукові системи, (Google, Yandex, Rambler, Meta),також проявив їх нездатність видавати партинентні результати інформаційній потребі користувачів. З огляду на це, для підвищення повноти та точності результатів роботи системи,пропонується використання семантичних моделей у підсистемі пошуку документів СЕДО ЗСУ. На сьогодні для проектування систем семантичного пошуку інформації використовуються 3 основних блоки: база знань, блок формалізації запитів та механізм пошуку. Для програмної реалізації цих блоків застосовують наступні моделі: фреймова модель, нейронні мережі, семантичні мережіта ін. Для кожної такої моделі, як і будь-якої класичної, документи проходять попередню індексацію. У першому випадку індекс документа представляється сукупністю взаємопов'язаних описів об'єктів та їх властивостей;у другому та третьому – орієнтованим графом, вершинами якого виступають об'єкти, а дуги задають відношення між ними. Такий підхід індексування доцільно використовувати на документах невеликого розміру, тому що пошуковий образ документа може у декілька разів перевищує об'єм оригінала. Як наслідок, представлення таким чином документів великого розміру ускладнює процес індексації, зберігання та пошуку. Для уникнення цих недоліків пропонується застосування логіко-лінгвістичного підходу до побудови системи пошуку. Однією з реалізацій такого підходу є мова логіки предикатів. Ця мова, як й інші класичні моделі, для пошуку дозволяє використовувати індекси документів у вигляді інвертованого файлу. Цей файл, як правило, містить ключові слова (терми) документа та координати їх розташування у ньому. Згідно логіки предикатів, до термів відносять не всі слова документа, а лише іменники, дієслова, прикметники та прислівники.

Для формалізації клієнтського запиту, сформованого природною мовою, використовується система лінгвістично-морфологічного аналізу, яка визначає частини речення, що присутні у ньому. На основі цієї інформації згідно правил бази знань визначається максимальна кількість фактів запиту, які можна представити предикатами. Для підвищення повноти пошуку, цей запит розширюється синонімами, відношеннями „ціле-частина", асоціаціями, логічними висновками, прописаними у інформаційно-пошуковому тезаурусі. Далі отримані предикати групуються у кон'юнктивну нормальну форму. Механізм пошуку відбувається наступним чином: із бази даних відбираються інвертовані файли документів, в яких присутні предикатні ім'я (терми) запита;далі, за координатамиих термів відшукуються абзаци, в яких вони присутні. Ці абзаци аналізуються та представляються аналогічно запиту. На наступному етапі за методом резолюцій з отриманих формул абзаців та запиту відкидаються ті предикати, які не відповідають семантиці запиту, а за тими, що лишились обчислюється ступінь відповідності документа інформаційній потребі користувача. Таким чином, побудова підсистеми пошуку документів СЕДО на базі мови логіки першого порядку дозволить відійти від релевантності та перейти до партинентності результатів пошуку, що значно підвищить його показники повноти та точності.

Самохвалов Ю.Я. (ВІТІ ДУТ)
Терещенко М.М. (ВІТІ ДУТ)

ОРГАНІЗАЦІЯ ПРИХОВАНОГО КАНАЛУ УПРАВЛІННЯ ОБ'ЄКТОМ ІНФОРМАЦІЙНОГО ДОСЛІДЖЕННЯ В ТЕХНОЛОГІЯХ МЕРЕЖЕВОЇ РОЗВІДКИ

На сьогоднішній день технології мережевої розвідки являються одним з перспективних напрямків дослідження. З розвитком систем мережевої безпеки, створення методів для непомітної роботи прихованого агента у комп'ютерних системах, а саме прихованій передачі даних, обміном управляючих сигналів, нанесення максимальних деструктивних дій та інше, потребує значного переосмислення та вдосконалення. Саме тому, виникла необхідність організації та удосконалення прихованого каналу управління об'єктом інформаційного дослідження в технологіях мережевої розвідки.

Цільовою настановою запропонованого підходу є: організація надійного каналу управління об'єктом інформаційного дослідження, а також побудова певної послідовності логічних дій для швидкого реагування на результати непередбачуваних ситуацій.

Основним елементом дослідження є прихований канал, який є комунікаційним каналом, який пересилає інформацію методом, спочатку для цього не призначеним. Сторонні спостерігачі зазвичай не можуть виявити, що крім основного каналу передачі даних є ще додатковий. Тільки відправник і одержувач знають це. Існує досить багато технологій побудови прихованого каналу. Вони ґрунтуються на маскуванні управляючих сигналів управління під стандартні системи передачі даних, такі як:

– використання протоколу *ICMP*;
– використання протоколу *DNS*;
– використання протоколу *HTTP*;
– використання *cookies* та інші.

Для реалізації даного процесу передбачається виконання наступних етапів:

1. Етап визначення меж структури комп'ютеризованої системи, яка підтверджується інформаційній атаці. Здійснюється аналіз існуючих засобів контролю та захисту інформаційних ресурсів;
2. Етап побудови прихованого каналу управління. В рамки даного етапу пропонується застосування технології побудови прихованого каналу з використанням протоколу *ICMP*. Всі вище розглянуті технології є досить ефективними, але використання протоколу *ICMP* є доцільніше, оскільки для його роботи не потрібен доступ до *Internet*, його досить легко використовувати у локальних мережах, а прості ехо-запити (*ping*) не викликають ніякої підозри.
3. Етап управління. Прихований канал поверх *ICMP* встановлює приховане з'єднання між двома комп'ютерами за допомогою ехо-запитів та ехо-відповідей протоколу *ICMP*. Дана техніка дозволяє, наприклад, повністю тунелювати *TCP* трафік через ехо-запити і відповіді (*ping*). Технічно тунелювання через прихований канал *ICMP* відбувається способом введення будь-яких необхідних даних в ехо-пакет і його пересилки на віддалений комп'ютер, віддалений комп'ютер відповідає подібним чином заносячи відповідь у інший *ICMP* пакет і відсилаючи його назад. Таким чином здійснюється передача команд до прогнозованого об'єкта управляння.

Відмінність запропонованого підходу побудови прихованого каналу управляння полягає в збільшенні ефективності його роботи за допомогою елементів програмувальної логіки, які дозволять швидко виправляти та модифікувати важливі функції, а також нададуть можливість застосування широкого діапазону різних функціональних рішень. Для певної систематизації цих дій необхідно застосувати теорію кінцевих автоматів яка використовується для контролю цифрових систем.

к.т.н. Саричев Ю.О. (ЦВСД НУОУ)
к.держ.упр. Устименко О.В. (ЦВСД НУОУ)
Кацалап В.О. (ЦВСД НУОУ)

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ У ВОЄННІЙ СФЕРІ – ТЕРМІНОСИСТЕМА ГАЛУЗІ

Важливою науковою проблемою є розробка методичного підходу до формулювання базових понять теорії національної безпеки. На жаль, незважаючи на наявність правил розроблення стандартів на терміни та визначення понять, наказ Міністра оборони України від 27.12.06 № 752 "Про затвердження Положення про стандартизацію у воєнній сфері", робота щодо створення військових термінологічних стандартів ведеться не дуже добре. Фахівці з питань національної безпеки зазначають, що на сьогодні відсутній єдиний методичний підхід щодо формування, обґрунтування та застосування категорійно-понятійного апарату. Існує нечіткість та неоднозначність визначення понять деяких термінів в офіційних документах, значна частина термінів, що вживаються в доступних виданнях, мають змістову суперечливість або однобічно відображають сутність відповідних понять та явищ. Все це стосується і термінів у сфері інформаційної безпеки. В той же час військова практика вимагає однозначного трактування термінів і понять. Отже, відсутність на сьогодні сталої термінології у цій галузі обумовлює необхідність розроблення військового стандарту з питань термінології щодо інформаційної безпеки держави у воєнній сфері, який повинен стати основою як для теоретичних досліджень, так і практичної діяльності органів державного та військового управління. В центрі воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського в поточному році завершено науково-дослідну роботу „Розробка проекту військового стандарту з питань інформаційної безпеки держави у воєнній сфері".

Загальна предметна галузь термінологічного стандарту, що досліджується – це інформаційна безпека держави у воєнній сфері, а однією із її складових є інформаційна безпека у Збройних Силах України. Для термінологічного наповнення цієї предметної галузі користувалися існуючими базовими термінами з питань інформаційної безпеки держави у воєнній сфері. Але, на жаль, офіційно прийнятого на законодавчому рівні самого визначення для поняття інформаційної безпеки держави у воєнній сфері сьогодні немає. Інформаційна безпека держави у воєнній сфері – складова інформаційної безпеки держави: стан, за якого досягнута здатність інформаційної інфраструктури воєнної сфери своєчасно сформувати та постійно підтримувати інформаційний простір воєнної сфери необхідної повноти (достатності) і захищеності для здійснення інформаційного забезпечення управління процесами військового будівництва, підготовки та застосування збройних формувань держави. Беручи до уваги постійний розвиток інформаційних систем, їх властивості та можливості створювати власні інформаційні ресурси Збройними Силами України під час підготовки до виконання завдань за призначенням, сформовано та визначено поняття інформаційної безпеки у Збройних Силах України. Під інформаційною безпекою у Збройних Силах України розуміється стан, за якого досягається здатність створити силами та засобами інформаційної інфраструктури Збройних Сил України захищений інформаційний простір, інформаційні ресурси якого забезпечують реалізацію функцій управління в ході підготовки та застосування військ (сил). Наступною складовою буде захист інформаційного середовища Збройних Сил України від деструктивного інформаційного впливу противника.

Аналіз Стратегії національної безпеки України, введеної в дію Указом Президента України № 389/2012 в частині індикаторів стану національної безпеки України, показав, що сам по собі захист в режимі очікування впливу є недієвим, тому його потрібно розглядати через складові ведення безперервного інформаційного протиборства. Під інформаційним протиборством у Збройних Силах України розуміється комплексний інформаційний вплив на систему державного та військового управління протидіючої сторони, її політичне і воєнне

керівництво, спрямований на досягнення інформаційної переваги над противником. Для ведення інформаційного протиборства та захисту інфраструктури від деструктивного інформаційного впливу в Збройних Силах України повинна бути створена система забезпечення інформаційної безпеки у Збройних Силах України. Таким чином, можна констатувати наявність в інформаційній безпеці держави у воєнній сфері декількох взаємопов'язаних інформаційних предметних галузей: інформаційної безпеки Збройних Сил України, системи забезпечення інформаційної безпеки та видів, форм, способів ведення інформаційного протиборства. Метою стандартизування термінів та визначень відповідних понять є встановлення необхідної внормованої термінології, яка задовольняє наступним вимогам: встановлює для різних предметних галузей однозначні й несуперечливі терміни для всіх сфер застосовування, зокрема, у довідковій, методичній і науковій літературі; усуває термінологічні перешкоди міжгалузевим і міждержавним науково-технічним, економічним та іншим зв'язкам; узгоджує описи об'єктів різних галузей стандартизації, у тому числі сприяє гармонізуванню національних стандартів України з міжнародними, регіональними та національними стандартами інших країн; забезпечує однозначною термінологією державні та міждержавні соціально-економічні і науково-технічні програми й законодавство України. Так, запропоновано наступні терміни та визначення понять: Кібернетичний простір (кіберпростір) - середовище, утворене організованою сукупністю інформаційних процесів управління на основі взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Інформаційна інфраструктура держави – організована сукупність носіїв даних та носіїв інформації суб'єктів інформаційної діяльності держави, що реалізовані у формі організаційно-технічних структур, з метою формування інформаційних ресурсів для забезпечення (обслуговування) інформаційних потреб особи, суспільства, держави, а також організаційних структур, які забезпечують їх функціонування згідно із чинним законодавством. При цьому організаційно-технічні структури (інформаційно-телекомунікаційні системи та мережі, інформаційні центри і пункти, засоби масової інформації тощо) здійснюють процеси створення, накопичення, зберігання, обробки і поширення інформації, а також її захисту. Інформаційна діяльність – сукупність дій, спрямованих на задоволення інформаційних потреб особи, суспільства і держави. Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації. Інформаційний ресурс – систематизовані інформація (знання), дані або інформаційні продукти, що мають цінність у певній предметній області і можуть бути використані для досягнення визначеної мети. Інформаційний продукт (продукція) - документована інформація (дані), які підготовлені і призначені для задоволення потреб користувачів. Інформаційні дії проводяться у формі інформаційних кампаній, операцій, акцій, атак, актів. Інформаційний акт – одиночна та короткочасна інформаційна дія (захід), метою якої є отримання інформації доступними засобами або захист інформаційних ресурсів на окремому об'єкті інформаційної діяльності, або інформаційний вплив на такий об'єкт чи деяку їх сукупність, або на визначене соціальне середовище. Інформаційна протидія – інформаційна дія (інформаційний захід) держави як адекватна відповідь на інформаційну діяльність, що спрямована проти неї. В цілому ж зазначений стандарт матиме понад 110 термінів та визначення понять. Військовий стандарт „Інформаційна безпека держави у воєнній сфері. Терміни та визначення" створюється на виконання Програми Міністерства оборони України з військової стандартизації на 2013 – 2015 роки. Нині він погоджується з департаментами та управліннями Міністерства оборони України та Генерального штабу Збройних Сил України, науковими та науково-дослідними установами Збройних Сил України, іншими зацікавленими підрозділами, частинами та установами. Планується, що він буде затверджений наказом начальника Центрального управління метрології і стандартизації – Головного метролога Збройних Сил України до кінця поточного року.

к.т.н. Сащук І.М. (в/ч А1906)
Бурлак Д.Ю. (в/ч А1906)

СУЧАСНІ ТЕХНОЛОГІЇ ІНТЕГРАЦІЇ ІНФОРМАЦІЙНИХ РЕСУРСІВ В СИСТЕМІ ВОЄННОЇ РОЗВІДКИ УКРАЇНИ

Система воєнної розвідки (ВР) України – це велика складна система, яка має усі системні ознаки: цілісність, наявність системного ефекту, структурність, ієрархічність, складність організації і поведінки тощо. У свою чергу, вона складається з окремих частин, кожна з яких є самостійною складною системою, спрямованою на досягнення певної мети, визначеної надсистемою (системою ВР України) [1].

Оскільки метою функціонування системи ВР України є добування, аналітична обробка та надання визначеним законом органам державної влади розвідувальної інформації, то по свої суті вона є складною інформаційною системою [2].

Активне впровадження інформаційних технологій (ІТ) у практику розвідувальної діяльності, без сумніву, значно розширили можливості розвідувальних органів щодо виконання цільових завдань. Проте суттєво спрощений доступ до різноманітної інформації через автоматизацію процесів добування, збору, обробки, зберігання та передачі даних привели до проблем, пов'язаних з необхідністю структуризації і зберігання великої її кількості, відбором у короткі терміни достовірної, повної і актуальної інформації про об'єкт (подію, явище).

Проблема, що виникає в процесі функціонування і взаємодії підсистем системи ВР при вирішенні складних багатопрофільних розвідувальних завдань полягає в розпорошеності та неповноті існуючих технологічних рішень і стандартів формування банків даних. Необхідність централізовано розв'язувати проблеми стандартизації надання інформації, розробку та узгодження протоколів взаємодії, обміну та захисту інформації на всіх етапах функціонування системи ВР на даний час залишаються невирішеним завданням.

У доповіді показано, що вирішення вище перерахованих проблем лежить у площині побудови спільного інформаційного простору, який поєднає наявні інформаційні ресурси підсистем ВР. Інтеграція даних реалізується комплексом методів, архітектурних підходів і програмних інструментів, які забезпечують узгоджений доступ і доставку даних для всієї множини процесів системи ВР.

Розглядається два аспекти зазначеної проблеми [3]. Перший полягає у тому, що необхідність інтеграції даних не є очевидною в умовах, коли кількість підсистем (організаційних структур), залучених у взаємодію, невелика або чітко визначена. При невеликій кількості взаємодіючих підсистем можна організувати взаємодію за принципом „кожний з кожним" і створити відповідні незалежні інтерфейси обміну. З іншого боку, на етапі реалізації інформаційних взаємодій, які вимагають виконання транзакцій і пов'язаного з ними інформаційного обміну між численними організаційними структурами, виникає необхідність створення певної служби інтеграції ІС різних організаційних структур між собою.

Очевидно, що виконання інтеграції за принципом „кожний з кожним і всі з усіма"приведе до квадратичного росту складності і вартості такої інтеграції. Враховуючи, що система ВР є структурованою ієрархічною складною системою, можна виокремити вертикальний та горизонтальний типи інтеграції даних. Також можливе поєднання цих двох основних типів.

Спираючись на [4] та враховуючи необхідність інтеграції інформаційних ресурсів, висунемо наступні вимоги до інформаційних інфраструктур підсистем системи ВР:

– підтримувати розширені процедури узгодження даних;

– підтримувати оперативний доступ до даних багатьох різних користувачів;

– керувати підтримкою даних, типи яких можуть значно змінитися в різних застосуваннях;

– підтримувати визначені стандартні або фактичні об'єктні моделі даних;

– забезпечувати службу виявлення (що виявляє доступні послуги та їхні характеристики);

– забезпечувати взаємне узгодження протоколів та перетворень;

– підтримувати управління даними через організаційні межі.

В загальному випадку вибір технології інтеграції даних повністю залежить від функціональних завдань, організаційної структури, рівня автономії підсистем системи ВР і потреби в аналітичних даних та форми подання вихідної розвідувальної інформації. Тому складність завдання інтеграції значно знизиться, якщо направити певні зусилля на стандартизацію опису даних та інших задіяних інформаційних ресурсів.

Короткий опис властивостей та змісту інформації будь-якого ресурсу надається його метаданими, отже обов'язковою функціональною властивістю інформаційної інфраструктури інтеграції має стати забезпечення процесів отримання (генерування), зберігання і управління метаданими ІР.

В доповіді показано, що реалізація зазначених процесів в інформаційній системі ВР можлива за рахунок впровадження інформаційно-сигнатурних технологій (ІСТ) [5]. Отже, ІСТ – це прийоми, способи та методи автоматизованого збору, обробки, накопичення, зберігання та передачі інформації про об'єкт (подію, явище) на основі виділення та аналізу його сигнатури (множини частинних сигнатур). Тут сигнатура об'єкта – сукупність характерних системних ознак (показників, параметрів, властивостей, характеристик), притаманних безпосередньо саме досліджуваному об'єкту.

Суть інформаційно-сигнатурних технологій полягає не у механічному об'єднанні всієї інформації, добутої різними засобами (у тому числі і на певний момент часу), а у виборі за короткий термін найбільш інформативних ознак, що у максимально повній мірі системно характеризують об'єкт (подію, явище).

ЛІТЕРАТУРА

1. Ільяшов О.А. Розвідка у сучасних воєнних конфліктах за досвідом іноземних країн: [Монографія] / О.А. Ільяшов, С.П. Мосов / Київ, 2011. – 280 с.

2. Закон України „Про розвідувальні органи України". Відомості Верховної Ради України (ВВР), 2001, № 19, ст.94 (зі змінами).

3. Матов О.Я. Проблеми горизонтальної інтеграції інформаційних ресурсів у багаторівневих організаційних структурах з динамічною конфігурацією / О.Я Матов, І.О. Храмова // Реєстрація, зберігання і обробка даних. – 2007. –Т. 9, № 3. – С. 88 – 97.

4. Теория информационных процессов и систем: учебник для студ. высш. учеб. заведений / [Советов Б.Я., Дубенецкий Б.Я., Цехановский В.В. и др.]; под ред. Советова Б.Я. – М.: Издательский центр "Академия", 2010. – С. 140 – 148.

5. Сащук І.М. Постановка задачі формування сигнатур об'єктів спостереження методами функціонального аналізу / І.М.Сащук // Інтелектуальна оборона: Збірка матер., стат., доп. і тез IV наук.-практ. форуму „Січневі ГІСи", (Львів, 22 – 24 січ.2013 р.) / Акад. сухоп. військ ім. гетьмана П. Сагайдачного – Л.: АСВ, 2013. С. 22 – 23.

Сидоренко В.О. (ВІТІ ДУТ)
к.т.н. Соколов В.В. (ВІТІ ДУТ)

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ГНУЧКОЇ СТРУКТУРИ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ВИКОРИСТАННЯМ ОБЄ'КТНО-РЕЛЯЦІЙНОЇ МОДЕЛІ ДАННИХ

Технології реляційних баз даних на сьогоднішній день є домінуючою. Протягом останніх років активно розвивалася технологія об'єктно – орієнтованих баз даних, спрямована почасти на подолання недоліків реляційної моделі даних. Хоча об'єктно-орієнтовані СУБД не завоювали значних успіхів на ринку, найбільш важливі їх аспекти безсумнівно знайдуть відображення в нових версій реляційних баз даних. Фундаментом технологій баз даних нового покоління стане поєднання відносин і об'єктів. Але і цей фундамент буде мати потребу в розширеннях, спрямованих на вирішення принаймні чотирьох найважливіших проблем – управління мультимедійними даними, довготривалими транзакціями, просторовими, хронологічними даними. В останні 10-20 років у цих областях проводилися інтенсивні дослідження. Проте сьогодні лише деякі промислові СУБД включають кошти для вирішення якої-небудь з цих проблем.

В доповіді представлено підхід до побудови гнучкої структури інформаційних систем, що дозволяє значно розширити область застосування таких систем в ЗСУ.

За останній часом на ринку з'явилися об'єктно-орієнтовані СУБД і супутні інструментальні засоби – частково у відповідь на очікуване зростання використання об'єктно-орієнтованих мов, а спроба подолати деякі суттєві недоліки реляційних баз даних, пов'язані з внутрішніми обмеженнями реляційної моделі. Хоча ці продукти не набули значного поширення, вони зробили внесок у наше розуміння переваг об'єктно-орієнтованого підходу до проектування баз даних. У той же час постачальники об'єктно-орієнтованих баз даних усвідомили, що основна перешкода до ринкового успіху для них – це відсутність підтримки повномасштабного не процедурної мови запитів, сумісного з ANSI SQL, і припускають доповнити свої системи такою мовою запитів. Компанія UniSQL розробила систему баз даних і засоби розробки додатків такого типу , до якого прагнуть привести свої продукти постачальники реляційних і об'єктно - орієнтованих баз даних.

Очевидно, що основу СУБД нового покоління складуть технології , що поєднують риси реляційних і об'єктно – орієнтованих баз даних. У реляційній моделі база даних являє собою централізоване сховище таблиць, що забезпечує безпечний одночасний доступ до інформації з боку багатьох користувачів. У рядках таблиць частина полів містить дані, стосовні безпосередньо до запису, а частина – посилання на записі інших таблиць. Таким чином, зв'язки між записами є невід'ємною властивістю реляційної моделі. Також у реляційній моделі досягається інформаційна й структурна незалежність. Записи не зв'язані між собою так, щоб зміна однієї з них торкнулося інших.

Реляційні бази даних страждають від розходжень у реалізації мови SQL, хоча це й не проблема реляційної моделі. Кожна реляційна СКБД реалізує якусь підмножину стандарту SQL плюс набір унікальних команд, що ускладнює завдання програмістам, які намагаються перейти від однієї СКБД до іншої. Доводиться робити нелегкий вибір між максимальною переносимістю й максимальною продуктивністю. У першому випадку потрібно дотримуватися мінімального загального набору команд, підтримуваних у кожній СКБД. У другому випадку програміст просто зосереджується на роботі в даній конкретній СКБД, використовуючи її команди і функції.

На даний час актуальною проблемою розробників являється надання користувачу інформаційної системи можливість самому будувати інформаційні об'єкти, що в свою чергу має скоротити затрати програмістів на супровід таких систем в майбутньому.

Сілко Д.О. (ВІТІ ДУТ)
к.т.н. Горбенко В.І. (ВІТІ ДУТ)

МОДЕЛЬ ГЕНЕРАТОРА НЕШТАТНИХ СИТУАЦІЙ КОМП'ЮТЕРНИХ МЕРЕЖ

Сучасні інформаційні мережі характеризуються великою складністю, неоднорідністю та територіальним розподілом. Однією з проблем сучасних інформаційних мереж є наявність великого вхідного трафіка, який найбільше навантажує комутації. Об'єм трафіка залежить від множини параметрів. В штатній ситуації трафік зазвичай знаходиться у визначеному для мережі діапазоні. Однак, виникають ситуації, коли об'єм трафіка значно зростає, що може привести до перезавантаження мережі та подальшого збою. Під нештатною ситуацією розуміється ситуація, коли за будь-яких обставин (зазвичай, невизначених) відбувається порушення нормального режиму функціонування мережі.

До нештатних ситуацій можливо віднести:

– шторм пакетів, який утворюється у випадку передавання широкомовного службового трафіка;

– широкомовний службовий трафік стека протоколів локальних мереж.

Для правильної реакції на нештатні ситуації потрібно знати, як мережа функціонує в нормальних умовах. Для визначення стану мережі необхідно знати топологію мережі, зовнішні зв'язки, конфігурацію програмного забезпечення та серверів і робочих станцій. При діагностуванні ситуації у мережі, необхідно враховувати взаємодію різних її частин в стеці протоколів *TCP/IP*. Аналіз нештатних ситуацій на реальних мережах є дуже складною задачею у зв'язку з різними типами порушення стаціонарності та малою ймовірністю їх появи. Саме тому необхідно розглядати та комбінувати різні варіанти моделювання та аналізу ситуацій в мережі за допомогою генератора нештатних ситуацій.

В доповіді розглядається модель генератора нештатних ситуацій, як сукупність проекцій рівнів моделі взаємодії відкритих систем (*OSI*):

– на канальному рівні взаємодія об'єктів з використанням апаратних адрес мережевих адаптерів *Fast Ethernet*;

– на мережевому рівні зв'язок об'єктів з використанням логічних адрес *IP*;

– на прикладному рівні аналіз нештатних ситуацій, що виявляються стандартними засобами операційної системи (*FTP*, *Telnet*, *HTTP*, *SMTP*, *SNMP*, *TFTP*).

OSI не робить відмінностей між керованими об'єктами – каналами, сегментами локальних мереж, мостами, комутаторами і маршрутизаторами, модемами і мультиплексорами, апаратним і програмним забезпеченням комп'ютерів, СКБД. Всі ці об'єкти управління входять в загальне поняття „система", і керована система взаємодіє з системою, що управляє, по відкритих протоколах *OSI*.

Для програмної реалізації моделі генератора нештатних ситуацій пропонується застосувати сокет *SOCK _ RAW*, який забезпечить доступ до усіх службових заголовків протоколів *IP*, *TCP*, *UDP*, *ICMP* та поєднає програмний генератор з мережею. Генератор нештатних ситуацій дозволить створювати пакети *IP*, *TCP* із визначеними службовими полями. Програмне забезпечення генератора нештатних ситуацій повинне містити модуль формування *Fast Ethernet* кадрів з невірними контрольними сумами *TCP*/*IP*. Для програмування була використана мову *C*, для роботи із *RAW*-сокетом застосовувалася бібліотека *WinSock* 2.2.

Таким чином, пропонується модель генератора нештатних ситуацій, яка дозволить підвищити ефективність функціонування інформаційної мережі за рахунок прогнозування нештатних ситуацій.

Сілко О.В.(ВІТІ ДУТ)
Думко Є.Ю.(ВІТІ ДУТ)

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АНАЛІЗУ ЗАХИЩЕНОСТІ МОБІЛЬНИХ ПРИСТРОЇВ НА БАЗІ ОПЕРАЦІЙНОЇ СИСТЕМИ *ANDROID*

На сьогоднішній день мобільні пристрої та планшети на базі операційної системи *Android* використовуються у силових структурах Збройних Сил України, але у вузькому колі. Проте з розвитком технологій *Android* збільшується кількість технологій та програмного забезпечення для несанкціонованого доступу до системи. Для перспективи розвитку та впровадження пристроїв *Android* важливим питанням залишається захищеність пристроїв *Android*.

Для аналізу захищеності мобільних пристроїв на базі ОС *Android* використовують різноманітні сканери для виявлення вразливостей. Найбільш ефективними з них вважають наступні: *Android Network Toolkit-Anti*, *Norton Mobile Security*, *SharesFinder*, *Lookout Mobile Security*, *Webroot SecureAnywhere Mobile*.

Повноцінний сканер вразливостей повинен складатися як мінімум з трьох головних модулів: сканера за запитом з функцією евристичного аналізу, компонента резидентного моніторингу та звіту по проведеному скануванню з можливістю швидкого реагування на знайдені помилки, вразливості чи шкідливі програмні додатки.

Android Network Toolkit-Anti – при кожному запуску відображає карту вашої мережі, пошук активних пристроїв і вразливостей, і виводить відповідну інформацію: зелений світлодіод сигналізує про активні пристрої, жовтий – про доступні порти і червоний – про знайдені вразливості. Після завершення сканування, генерує автоматичний звіт із зазначенням наявних у вразливостей і підказує як виправити кожен з них.

Norton Mobile Security. Налаштування сканування практично відсутнє. Присутня тільки можливість включити в область перевірки карту пам'яті або обмежитися вбудованою пам'яттю пристрою. Програма працює у фоновому режимі, перевіряючи додатки, що встановлюються. Для обміну статистичною інформацією і швидкого реагування на нові загрози використовується мережа Norton Comminity Watch. До неї пропонують приєднатися при першому запуску програми.

SharesFinder – утиліта сканує безпровідну мережу на наявність ресурсів з відкритим доступом. *SharesFinder* шукає і знаходить *HTTP* і *FTP* ресурси, які відразу можна переглянути. Для огляду *HTTP* ресурсів запускається браузер, а для перегляду *FTP* ресурсів необхідний сторонній *FTP* клієнт.

Lookout Mobile Security. Шукає, знаходить і видаляє шкідливі програми і віруси, блокує потенційно небезпечні веб-сторінки, які запитують паролі та інші особисті дані, дає можливість перегляду повноважень встановлених програм.

Webroot SecureAnywhere Mobile. Автоматично сканує програмні додатки та файли на наявність мобільних вірусів, шпигунських програм, троянів. Антивірусний екран блокує шкідливі додатки до їх запуску, попереджає, коли пристрій і налаштування вразливі для шкідливих атак, автоматично сканування веб-посилання і адреси, віддалено блокує мобільний телефон або планшет, якщо він втрачений або вкрадений, автоматично блокує *SMS*-спам і небажані дзвінки.

Вище перераховане програмне забезпечення не дозволяє виявити недоліки в програмному забезпеченні пристрою *Android*.

Пропонується розробити програмне забезпечення аналізу мобільних пристроїв на базі ОС *Android*, яке дозволить розширити функції існуючих програмних засобів сканування вразливостей. А саме: оцінювати захист доступу до пристрою, наявність незахищених ресурсів пристрою, не буде вимагати підключення до мережі інтернет та буде безкоштовним.

к.т.н. Слотвінська Л. І. (ВІТІ ДУТ)
к.т.н. Кузавков В. В. (ВІТІ ДУТ)

МЕТОДИКА ОЦІНКИ ЯКОСТІ ВІДБИТКІВ АНАЛОГОВОГО І ЦИФРОВОГО ДРУКУ

Однакові графічні зображення, виконані різними способами друку визначають за характерними особливостями, які можна спостерігати при значному збільшенні. Відбитки, одержані на різних видах паперу за допомогою цифрових засобів, можуть відрізнятися від ідентичних, одержаних аналоговим способом. Очевидно, відбиток, одержаний цифровим видом друку, буде в тій чи іншій мірі подібний до аналогового за графічним виконанням (розмір в тонких штрихах, чіткість штрихів, насиченість фарб).

З метою обґрунтування технологій відтворення друкованої інформації запропоновано методику визначення графічної точності передачі зображень на відбитках, одержаних на друкарських аналогових (верстат) та цифрових засобах (принтер). Суть методики полягає в одержанні відбитків з лицевого та зворотного боків різних видів паперу (кейдований, офсетний, писальний, газетний № 1) за допомогою аналогового та цифрових засобів; фотографуванні фрагменту відбитка разом з модельною фотоформою (тестовою шкалою) оснащеною лінійкою з ціною поділки 0.2 мм; аналізі відбитків за графічним виконанням. Відбитки аналогового друку одержували на малогабаритному літоофсетному верстаті з ручним приводом, призначеному для друкування невеликих тиражів в стаціонарних та польових умовах за прийнятою технологією. Відбитки цифрового друку одержували на принтерах – лазерному Canon LBP-810 та на струминному Canon PIXMA MP280 при роздільній здатності 300 dpi. Для фотографування використовували програмно-апаратний комплекс в основі якого прецизійна платформа з п’ятьма степенями свободи та точністю шкал 10 мкм.

Комплекс оснащений цифровим фотоапаратом Olympus C-765, що дозволяє моделювати репродукційну фотозйомку (регулювати відстань об’єкта зйомки до фотоапарату, розміщення фотоапарату під кутом і паралельно до площини стола на якому закріплюється відбиток). Керування фотоапаратом здійснюється за допомогою персонального комп’ютера (ПК) Asus і за програмою Cam.2Com.exe.

При проведенні фотозйомки дотримувались умов однакової освітленості відбитків. Зйомку проводили з пріоритетом видержки 1/125, діафрагма – 2.8.

Аналіз одержаних результатів здійснювали візуально та з допомогою ПК. Визначали якість передачі зображення, розмір тонких штрихів, чіткість країв штрихів, насиченість зображення фарбою, відхилення розмірів штрихів на відбитках. Встановлено, що кожен вид друку, вид паперу, лицева та зворотна сторони паперу впливають на передачу зображення. Показано характерні особливості і закономірності відтворення зображень досліджуваними видами друку. Визначено, що зображення, одержане на струминному принтері більш відповідає аналоговому відбитку плоского офсетного друку як за розмірами літер так і за розмірами штрихів та насиченістю фарби.

Методику доцільно використовувати при проведенні аналізу друкованих виробів для встановлення виду друку і в процесі відтворення відбитків.

ЛІТЕРАТУРА

1. Величко О., Сичугов О. Відтворення інформації в системі „фотоформа-друкарська форма-відбиток”. // Publishing_digital_printing. – 2004, № 3. – С.26 – 31.

2. Якуцевич С., Назар І., Лазаренко Е., Іванишин Г. Дослідження якості відбитків офсетного друку. // Друкарство. – 2005, № 6. С. 51 – 52.

3. Шашкин С. Б., Ермолаев С. А. Объективизация оценки качества изображений на твердых носителях, получаемых с помощью устройств ввода-вывода визуальной информации // Экспертная практика. 1999. № 47, с. 116 – 117.

Соколов О.В. (ВІТІ ДУТ)

АНАЛІЗ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БЕЗПРОВОДОВИХ МЕРЕЖАХ IEEE 802.11.x

Інтенсивний розвиток безпроводових мереж на базі стандарту IEEE 802.11 веде до збільшення інтересу до них з боку порушників. В стандарті безпроводових мереж 802.11 існує вбудований механізму захисту, який забезпечує конфіденційність, контроль доступу і цілісність даних, які передаються по радіоканалу. Але отримані дані підтверджують те, що у механізму захисту стандарту IEEE 802.11 є очевидні недоліки, і зловмисники з допомогою відносно простих прийомів можуть отримати доступ до конфіденціальної інформації. Ці відкриття підривають довіру як до IEEE, так і до численних постачальників безпроводових продуктів на основі стандарту 802.11.

Приведем аналіз існуючих ризиків інформаційної безпеки безпроводових телекомунікаційних систем стандарту IEEE 802.11:

Ризик перший – Шахрай (Rogue Devices, Rogues). Шахраями називаються пристрої, що мають можливість неавторизованого доступу до корпоративної мережі, часто в обхід механізмів захисту, визначених корпоративною політикою безпеки. Найчастіше це ті самі самовільно встановлені точки доступу. Статистика по всьому світу, наприклад, вказує на зловмисників, як на причину більшості зломів мереж організацій. Навіть якщо організація не використовує безпроводовий зв'язок і вважає себе в результаті такої заборони захищеною від безпроводових атак – впроваджений (навмисне чи ні) зловмисник з легкістю виправить це положення. Крім точок доступу в ролі зловмисників можуть виступити домашній роутер з Wi -Fi, програмна точка доступу Soft AP, ноутбук з одночасно включеними проводовим і безпроводним інтерфейсом, сканер, проектор і.т.д.

Ризик другий – неконтрольована область між кінцевими точками мережі. Як вже було сказано вище – безпроводові пристрої не „з'єднанні кабелем" і можуть міняти точки підключення до мережі прямо в процесі роботи. Наприклад, коли ноутбук з Windows XP або просто некоректно сконфігурований безпроводовий клієнт автоматично асоціюється і підключає користувача до найближчої безпроводової мережі. Такий механізм дозволяє зловмисникам „перемикати на себе" користувача для подальшого сканування вразливостей, фішингу або атак Man-in-The Middle. Крім того, якщо користувач одночасно підключений і до проводової мережі – він щойно став зручною точкою входу – тобто класичним зловмисником.

Ризик третій – вразливості мереж і пристроїв. Деякі мережеві пристрої, можуть бути більш вразливі, ніж інші – можуть бути неправильно сконфігуровані, використовувати слабкі ключі шифрування або методи автентифікації з відомими вразливостями. Не дивно, що в першу чергу зловмисники атакують саме їх. Звіти аналітиків стверджують, що понад 70 відсотків успішних зломів безпроводових мереж відбулися саме в результаті неправильної конфігурації точок доступу або клієнтського ПЗ.

Ризик четвертий – нові загрози і атаки. Безпроводові технології породили нові способи реалізації старих загроз, а також деякі нові, досі неможливі в проводних мережах. У всіх випадках, боротися з атакуючим стало набагато важче, тому що неможливо ні відстежити його фізичне місце розташування, ні ізолювати його від мережі.

Більшість традиційних атак починаються з розвідки, в результаті якої зловмисником визначаються подальші шляхи розвитку атаки. Для безпроводової розвідки використовуються як засоби сканування безпроводових мереж (NetStumbler, Wellenreiter, вбудований клієнт JC), так і засоби збору та аналізу пакетів, так як часто керуючі пакети WLAN незашифровані. При цьому дуже складно відрізнити станцію, що збирає інформацію, від звичайної станції, яка намагається отримати авторизований доступ до мережі або від спроби випадкової асоціації.

Багато хто намагається захистити свої мережі шляхом приховування назви мережі в маячки (Beacon), що розсилаються точками доступу, і шляхом відключення відповіді на широкомовний запит ESSID (Broadcast ESSID). Ці методи, що відносяться до класу Security through Obscurity, загальновизнано є недостатніми, тому що атакуючий все одно бачить безпроводову мережу на певному радіоканалі, і все, що йому залишається – це чекати першого авторизованого підключення до такої мережі, тому що в процесі такого підключення в ефірі передається ESSID в незашифрованому вигляді. Після чого така міра безпеки просто втрачає сенс. Деякі особливості безпроводового клієнта Windows XP SP3 ще більш погіршували ситуацію, тому що клієнт постійно розсилав ім'я такої прихованої мережі в ефір, намагаючись підключитися. В результаті, зловмисник не тільки отримував ім'я мережі, а й міг „підсадити" такого клієнта на свою точку доступу.

Ризик п'ятий – виток інформації з проводової мережі. Практично всі безпроводові мережі в якийсь момент з'єднуються з проводовими. Відповідно, будь-яка безпроводова точка доступу може бути використана як плацдарм для атаки. Але це ще не все: деякі помилки в конфігурації точок доступу в поєднанні з помилками конфігурації проводної мережі можуть відкривати шляхи для витоків інформації. Найбільш поширений приклад – точки доступу, що працюють в режимі моста (Layer 2 Bridge), підключені в плоску мережу і широкомовні пакети, що передаються в ефір з проводового сегмента, запити ARP, DHCP, фрейми STP і т.д. Деякі з цих даних можуть бути корисними для організацій атак Man- in - The- Middle, різних Poisoning і DoS атак, та й просто розвідки.

У зв'язку з цим слід очікувати велику кількість атак на них з використанням різних засобів, тому виникає проблема забезпечення інформаційної безпеки (ІБ) даних об'єктів. Ця умова визначає використання відповідних засобів і методів захисту інформації, на основі яких будується політика забезпечення ІБ. Для забезпечення безпеки інформації в стандарті 802.11 необхідно використовувати наступні заходи:

1. Виявлення наступних видів атак у безпроводових мережах:
– збір інформації про безпроводові мережі (war driving);
– виявлення несанкціонованих точок доступу і безпроводових клієнтів;
– відмова в обслуговуванні;
– обхід точки доступу;
– використання систем виявлення атак.
2. Захист інформації в безпроводових мережах за наступними напрямками:
– захист клієнтів безпроводових мереж;
– виділення безпроводовової мережі в окремий сегмент;
– використання IPSec для захисту трафіку безпроводових клієнтів;
– застосування технологій VPN для захисту безпроводових мереж.
3. Моніторинг безпроводових мереж.
4. Виконання аудиту безпеки безпровдових мереж з врахуванням специфіки аналізу захищеності безпроводових мереж і застосуванням сканерів безпеки для безпроводових мереж.

Специфіка мереж стандарту IEEE 802.11 відбивається у використовуваних підходах до аналізу ризиків. Особливістю ІБ мережі, побудованої на базі стандарту IEEE 802.11 є те, що в результаті атак, виконуваних через її вразливості, збиток завдається як ресурсам самої безпроводової мережі, так і активам організації в цілому.

Таким чином, при створенні і експлуатації захищеної безпроводової мережі необхідно здійснювати систематичний аналіз ризиків, ланцюгом якого є виявлення можливих загроз безпеки інформації, оцінка можливості їх реалізації та очікуваного збитку від такої реалізації в інтересах забезпечення захисту.

Соколов К.О. (УІТ МОУ)
к.т.н. Крижанівський О.А. (УІТ МОУ)
к.т.н. Гудима О.П. (УІТ МОУ)
Новік І.С. (УІТ МОУ)

АНАЛІЗ ВИКОРИСТАННЯ СИТУАЦІЙНИХ ЦЕНТРІВ В ДІЯЛЬНОСТІ ОРГАНІВ УПРАВЛІННЯ КРАЇН СВІТУ

В умовах стрімкого зростання інформаційних потоків і браку часу для ухвалення стратегічних рішень критично важливим стає створення для керівників різного рівня сучасного науково-технологічного середовища, що сприяє оперативному інформаційно-аналітичному забезпеченню при надзвичайних (нештатних), кризових ситуаціях та забезпечує прийняття ефективних управлінських рішень. Найважливішими елементами цього середовища є Ситуаційний (Кризовий) центр (далі – СЦ).

Великий досвід відносно створення і успішного функціонування СЦ має США, де вони розглядаються як ключовий елемент підтримки управлінських рішень на стратегічному рівні управління. Ситуаційна кімната Білого дому – це цілодобовий наглядовий і сигнальний центр, що забезпечує Президента, помічника з національної безпеки, членів Ради безпеки поточною розвідувальною і відкритою інформацією для вироблення і реалізації політики у сфері національної безпеки. Кімната існує на постійній основі, виконуючи роль розробника міжвідомчої стратегії реагування на надзвичайні ситуації, де чергують спеціально підготовлені – аналітики розвідки і фахівці з комунікацій, які ведуть безперервний моніторинг і аналіз всіх доступних інформаційних каналів.

В структурах управління Європейського Союзу (далі – ЄС) функціонує Спільний ситуаційний центр ЄС. Основними цілями та задачами цього центру є: забезпечити країни ЄС достовірною та своєчасною інформацією по питанням безпеки суспільства, оцінки ймовірних загроз; бути системою раннього попередження при загрозі терористичних актів; служити центром обміну розвідувальної інформації розвід-служб країн ЄС.

У колишньому СРСР одним з перших прообразів СЦ став оперативний штаб з ліквідації наслідків Чорнобильської катастрофи в 1986 році, на базі якого в подальшому був створений Ситуаційний Центр керівництва Міністерства з надзвичайних ситуацій.

У лютому 1996 року був введений в дію СЦ у резиденції президента Російської Федерації. Це досить складний програмно-мультимедійний комплекс, який дозволяє збирати, обробляти інформацію і представляти її президенту Російської Федерації, при цьому матеріал оперативно доповнюється новими даними, комп'ютер обробляє інформацію і відображає на екрані результати моделювання. На їх основі виробляються рішення, які доводяться до виконавців засобами того ж СЦ.

В Україні процес створення мережі СЦ, перш за все при Президентові України, міністерствах та відомствах тільки розпочинається. Його мета – вдосконалення якості державно-управлінських рішень, сприяння їх прозорості, передбачуваності, легітимності, позитивного сприйняття державної політики національної безпеки як в середині країни так і біля кордону, а також за її межами.

Завдання в частині, що стосується забезпечення національної безпеки у воєнній сфері, покладатимуться на Міністерство оборони України (далі - МО України) Тому створення СЦ МО України дозволить забезпечити якісно новий рівень управління в секторі безпеки та оборони держави.

Одним з кроків на шляху до підвищення ефективності і якості управлінських рішень у цій сфері, реагування на кризові і надзвичайні ситуацій повинна стати науково-експертна та інформаційно-аналітична підтримка управлінських процедур і процесів, що дозволить оперативно аналізувати, моделювати та прогнозувати сценарії розвитку таких ситуації і динамічно реагувати на них, виробляючи оптимально ефективні управлінські рішення.

Сорока М.В. (ЦНДІ ОВТ ЗС України)
Кадет Н.П. (НАУ)

АЛГОРИТМ ШИФРУВАННЯ ІНФОРМАЦІЇ „APR" КОМБІНОВАНИМ МЕТОДОМ НА ОСНОВІ ЗАЛИШКОВИХ ЧИСЕЛ

Сьогодні відбуваються глибинні якісні перетворення, що обумовленні потужним науково-технічним прогресом та інформаційною революцією. В результаті чого, змінюються та підвищуються вимоги до озброєння та військової техніки, збільшуються об'єми інформації, реалізуються нові більш складніші проекти. Однак, окрім безперечних переваг все це призводить до появи специфічних проблем та ризиків. Однією з таких проблем стала необхідність забезпечення ефективного захисту інформації та засобів її обробки. Доцільно відмітити, що чим сильніше проявляється інформаційна залежність, тим більші потенційні збитки від зловживань в інформаційній сфері, і тим більша потреба в захисті інформації.

Питання підвищення ефективності передачі даних постійно знаходяться в центрі уваги. Тому в даній роботі здійснюється розробка алгоритму шифрування інформації, що відповідатиме всім вимогам, які висуваються до побудови криптографічної системи захисту інформації. В даний час необхідно проводити роботу за такими важливими напрямками, як:

– побудова системи забезпечення безпеки інформаційно-телекомунікаційних систем (інформаційні фонди і телекомунікаційні інфраструктури) як об'єктів дії ризиків;

– захист інформаційних систем (інформації, інформаційної інфраструктури) від протиправних посягань, досягнення незаконної мети, забезпечення антигромадських інтересів;

– постійний моніторинг системи ризиків і погроз у сфері інформаційних відносин;

Для вирішення поставленого завдання у процесі виконання роботи було проаналізовано основні методи криптографічних перетворень, що показало основні переваги та недоліки різних шифрів [1], та проводилися дослідження вимог, що висуваються до криптографічної системи захисту інформації та на основі поставлених вимог розробляється алгоритм шифрування інформації − „APR" (algorithm of partaking with a remain) алгоритм ділення із залишком [2].

Даний алгоритм побудований на основі однієї з властивостей простих чисел, яка полягає в тому, що при діленні будь-якого цілого числа k на просте p будуть утворюватись залишки з періодом повторення не більше: p-1, де p - просте число (під цю властивість не підпадають такі прості числа: 2, 3, 5). Враховуючи вищезазначене та провівши відповідні розрахунки, прийшли до висновку, що алгоритм ділення із залишком APR дозволяє шифрувати великі об'єми інформації, при цьому не потребуючи значного об'єму ключа, оскільки навіть необ'ємний ключ дозволяє створити величезну кількість різноманітних контейнерів, кожний з яких і буде шифрувати певний символ, а незначна зміна ключа, на одне значення, призводить до абсолютно нової їхньої розстановки. Ще однією перевагою алгоритму є його адаптивність під будь-які системи криптокодування (ANSI, Unicod…).

Зауважимо, що на сучасному етапі необхідне глибоке усвідомлення на всіх рівнях державного управління тієї істини, що формування, поширення, використання і захист інформаційних ресурсів України є основою забезпечення її національних інтересів в інформаційній сфері, становлення і розвитку інформаційного простору та його інтегрування у світовий інформаційний простір.

ЛІТЕРАТУРА

1. Ленков С.В. Методы и средства защиты информации. В 2-х томах/Ленков С.В., Перегудов – Д.А., Хорошко В.А., Под ред. В.А.Хорошко. – К.: Арий, 2008. – Том II. Информационная безопасность. – 344 с., ил. с. 245 – 246.

2. Яковлев А.В., Безбогов А.А., Родин Я.Я*,* Шамкий В.Н. Криптографическая защита информации: учебное пособие. – Т.: ТГТУ, 2006. – 140 с.

Сорока Г.І. (ВІТІ ДУТ)
к.т.н. Успенський О.А.(ВІТІ ДУТ)

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ВІДДАЛЕНОГО УПРАВЛІННЯ РОБОЧИМИ СТАНЦІЯМИ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

Віддалене управління – це програмні функції операційних систем, що дозволяють отримати віддалений доступ до комп'ютера через Інтернет або ЛОМ і здійснювати управління та адміністрування віддаленого комп'ютера в реальному часі. Програми віддаленого адміністрування надають майже повний контроль над віддаленим комп'ютером: вони дають можливість дистанційно керувати робочим столом комп'ютера, можливість копіювання або видалення файлів, запуску додатків.

Велика кількість робочих станцій в сучасних підрозділах військ зв'язку призводить до ускладнення їх обслуговування та зростання обслуговуючого персоналу. Тим самим підвищуються кошти на підтримання робочих станцій у працездатності. Система віддаленого управління робочими станціями в локально обчислюваній мережі дозволяє вирішити цю проблему. Вона надає можливість адміністратору з одного робочого місця управляти декількома серверами. Це дозволяє зменшити кількість обслуговуючого персоналу та автоматизувати процеси.

Більшість сучасних програми віддаленого управління не забезпечують досить високого рівня безпеки, що недопустимо при роботі з конфіденційною інформацією. У деяких програм застосовується лише механізм аутентифікації системи *NT*, інші ненадійно шифрують мережевий трафік або не забезпечують надійного зберігання паролів.

Для усунення цих недоліків в роботі запропонована система віддаленого управління на базі операційної системи сімейсва *Windows*, яка дозволяє керувати АРМ на відстанні за допомогою використання стеку протоколів *TCP/IP*. Захист команд управління в процесі передавання їх відкритими каналами зв'язку базується на виконання таких функцій:

– автентифікація сторін, що взаємодіють;
– криптографічне закриття команд, яка передається;
– підтвердження справжності й цілісності доставленої інформації;
– захист від повтору, затримки та видалення повідомлень;
– захист від відмовлення від фактів відправлення й одержання повідомлень.

Для програмної реалізації системи розроблено два додатки: клієнтський та серверний. В клієнтській частині, створена головна форма, на якій знаходяться діалогове вікно. Команда на виконання дії передається по мережі у вигляді текстового повідомлення. Пошук потрібного серверу здійснюється в мережі за *IP*-адресою. Після встановлення з'єднання програма може взаємодіяти з сервером.

Серверна частина отримавши текстове повідомлення, розшифровує повідомлення та виконує дію відповідно до присвоєного значення цьому повідомленню.

В якості криптографічного алгоритму в системі пропонується використовувати хешування. При цьому в якості ключа використовуються не цифри, а деякий осмислений вираз, слово або послідовність символів, що називається паролем.

Робота системи забезпечується одним оператором ПЕОМ, що володіє початковим знанням про ОС *Windows XP*, а також детально ознайомлений з керівництвом користувачів до даного ПЗ.

Розроблену систему віддаленого управління доцільно використовувати в таких підрозділах ЗСУ, де використовується велика кількість серверів, які потребують постійного нагляду та адміністрування.

Стемпковська Я.А. (ВІТІ ДУТ)

АЛГОРИТМ УПРАВЛІННЯ ЗВ'ЯЗНІСТЮ НЕОДНОРІДНОЇ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ З ВИКОРИСТАННЯМ МОБІЛЬНИХ РЕТРАНСЛЯТОРІВ-МАРШРУТИЗАТОРІВ

Ефективність застосування Збройних Сил в сучасних військових конфліктах та бойових операціях залежить від своєчасної доставки інформації з поля бою (в тому числі розвідувальної інформації) для прийняття управлінських рішень посадовими особами. Забезпечення збору та передачі такої інформації можливе шляхом застосування неоднорідних безпроводових сенсорних мереж військового призначення (НБСМ ВП), які будуються за принципом Ad-Hoc. Сенсорні вузли в даних мережах розташовано випадковим чином, тому в одних місцях мережі виникають скупчення, а інших прогалини – „білі плями".

Для відновлення зв'язності між стаціонарними сенсорами в розгорнутій безпроводовій сенсорній мережі в якості таких додаткових вузлів пропонуємо використовувати мобільні роботи ретранслятори (маршрутизатори), що оснащені одним або декількома комплектами приймально-передавальної апаратури.

Однак мобільність абонентів, нестабільність каналів та маршрутів зв'язку між ними може призводити до повної або часткової втрати зв'язності мережі. Отже однією з головних задач управління такими мережами є забезпечення та підтримка зв'язності сенсорних вузлів в умовах реального часу.

Таким чином метою є розробка алгоритму управління зв'язності передачі безпроводової сенсорної мережі, яка дозволяє вирішити питання збільшення часу функціонування мережі, за рахунок знаходження та розташування мінімально необхідного набору вузлів ретрансляції (мобільних роботів-ретрансляторів).

Запропонований алгоритм дозволяє розташувати роботи ретранслятори (маршрутизатори) таким чином, щоб отримати нову структуру мережі заданої якості після попереднього ушкодження. Алгоритм управління зв'язності мережі для підвищення показників структурно-інформаційної зв'язності НБСМ ВП, який складається з адаптивних правил оптимального розміщення та переміщення множини роботів ретрансляторів (маршрутизаторів) на місцевості.

Оскільки дана задача відноситься до класу $NP-$ повних задач, тому пропонуємо:

правило, що забезпечує зв'язність НБСМ ВП;

правило, що забезпечує гарантовану якість обслуговування НБСМ ВП;

використання надлишкового апаратурного ресурсу для оптимізації заданого показника якості.

Застосування цих правил передбачає побудову та розгортання оновленої безпроводової сенсорної мережі тактичної ланки управління для забезпечення безперервної передачі інформації тобто зв'язності маршрутів передачі неоднорідної безпроводової сенсорної мережі військового призначення.

На відміну від існуючих алгоритмів запропонований відрізняється:

універсальністю (можливість вирішувати задачу для зв'язаної і незв'язаної мережі);

оперативністю (вирішуються в режимі реального часу при відхиленні від оптимуму не більше 10%);

застосування методу дозволяє збільшити пропускну здатність мережі.

Застосування бази знань, що складається зі структурних і потокових правил та способів ініціалізації дозволяє значно зменшити складність (час) пошуку квазі оптимального розміщення мобільних роботів ретрансляторів (маршрутизаторів) та збільшити ймовірність.

д.т.н. Субач І.Ю. (ВІТІ ДУТ)
Василинчик С.М. (ВІТІ ДУТ)

ПІДХІД ДО НАКОПИЧЕННЯ ДАНИХ ПРО ПАРАМЕТРИ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ МЕРЕЖІ У СХОВИЩІ ДАНИХ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ОБСЛУГОВУЮЧОГО ПЕРСОНАЛУ

Для ефективної діяльності обслуговуючого персоналу (ОП) інформаційної мережі (ІМ) потрібна системи підтримки прийняття рішень (СППР). Однією з задач СППР є оперативна та ефективна обробка великих об'ємів різнорідної інформації. Тому на даний час є актуальним питання накопичення даних про параметри функціонування ІМ, оскільки отримання їх потребує використання різних способів і методів, що не завжди відповідають вимогам ефективності та оперативності. Виникають ситуації, пов'язані з суперечливістю тих же способів, методів та механізмів.

До засобів моніторингу ІМ можна віднести системи управління мережею та засоби управління системою. Прикладами систем управління можуть служити популярні системи *HPOpenView*, *SunNetManager*, *IBMNetView*. Вони являють собою централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік у мережі. До найбільш відомих систем управління системами відносяться *LANDesk*, *IBM Tivoli*, *Microsoft Systems Management Server*, *HP OpenView*, *Novell ZENworks* і *CA Unicenter*. Вони часто виконують функції, аналогічні функціям систем управління, але стосовно інших об'єктів. У першому випадку об'єктом управління є програмне і апаратне забезпечення комп'ютерів ІМ, а у другому – комунікаційне устаткування. Але не один з виробників у повній мірі не спроможний забезпечити достатній збір даних про функціонування ІМ. Кожна із систем здатна оперувати лише певним набором параметрів, які не дають повної інформації, що у певній мірі не дозволяє ОП приймати обґрунтовані рішення за директивний час. Вирішення цієї задачі полягає у розробці та впровадженні СППР ОП, ефективність застосування якої у першу чергу залежить від якості даних, що поступають з різнорідних джерел.

У доповіді розглянуто питання підвищення ефективності роботи оператора ІМ за рахунок автоматизації процесів збору, обробки для подальшого аналізу і візуального представлення даних, що поступають з підсистеми моніторингу або інших джерел.

Аналіз показує, що для вирішення задачі збору та обробки інформації про функціонування ІМ доцільно використовувати різні системи моніторингу, використовуючи переваги кожної з них, оскільки для якісного управління ІМ сукупність даних має бути найбільш повною. За основу у виборі технології організації даних доцільно обрати Сховища Даних (СД), що являють собою інтегровані раніше роз'єднані деталізовані дані, зібрані з різних систем оперативного доступу до даних. Необхідно визначити різницю у характеристиках отриманих даних та вимоги до даних, які завантажуються у цільову базу даних (БД), вирішивши проблеми завантаження, очищення та їх узгодження. Тому СД – основа для побудови СППР ОП. І основна мета створення СД полягає в тому, щоб зробити усі значимі для управління ІМ дані доступними в стандартизованій формі, придатними для аналізу та отримання необхідних звітів. Для досягнення цього потрібно отримати дані, що відповідатимуть вимогам предметної орієнтованості, інтегрованості, прив'язки до часу та незмінності, із існуючих внутрішніх та зовнішніх, доступних для комп'ютера, джерел.

Таким чином, запропонований підхід дозволить за невеликі проміжки часу ефективно здійснювати збір даних про стан інформаційної мережі для подальшого їх аналізу та представлення у зручному вигляді.

д.т.н. Субач І.Ю. (ВІТІ ДУТ)
Васильєв О.Я. (ВІТІ ДУТ)
Осиченко О.Б.(ВІТІ ДУТ)

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМ ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК ЗА РАХУНОК ЇХ ІНТЕЛЕКТУАЛІЗАЦІЇ

Захист комп'ютерних мереж від шкідливого впливу досягається шляхом створення систем виявлення атак (СВА), які призначені для виявлення негативної активності, яка може порушити безпеку комп'ютерних мереж. Аналіз ефективності застосування методів та систем виявлення атак показує, що: більшість сучасних СВА використовують на базовому рівні ту або іншу реалізацію сигнатурного методу виявлення (порівняння шаблонів); існуючі методи виявлення атак на багато ширші, але їх використання в системах має принципові обмеження, пов'язані з вимогами верифікації, стійкості і відтворення результату, а також великим числом помилок другого роду; доступні реалізації СВА нестійкі до модифікацій атак і не можуть автоматично адаптуватися до появи нових атак.

Основними методами виявлення атак, що реалізовуються у сучасних СВА є методи виявлення аномалій і методи виявлення зловживань. Для більшості методів виявлення аномалій характерна слабка верифікація і слабка стійкість. Серед стійких і верифікованих методів, що мають при цьому низьку обчислювальну складність, можна відмітити методи розроблені на основі використання нейронних мереж та експертних систем. Головним недоліком наведених систем є те, що зараз не існує системи виявлення, яка була б адаптивна до невідомих атак. Незважаючи на наявність великого числа методів виявлення аномалій, суттєва кількість помилкових спрацьовувань, слабка стійкість і неверифікованість не дозволяє їх використовувати в системах спеціального призначення. Крім того, використання методів виявлення аномалій обмежене дослідницькими і вузькоспеціалізованими системами. Робляться спроби використати методи класифікації даних, такі як кластерний аналіз і нейронні/імунні мережі. Головний недолік цих методів, порівняно з експертними, в принциповій неможливості верифікації результату (виходу) – класи поведінки будуються на основі навчання і не представляють можливість аналітично розрахувати рівень помилок I і II роду для таких методів, а також проаналізувати коректність рішень, що приймаються. Перспективним напрямком усунення наведених недоліків, з метою підвищення адаптивності СВА щодо виявлення невідомих типів атак, є впровадження СППР, які б при низькій (лінійній) обчислювальній складності, стійкості і верифкації мали б низький рівень помилкових спрацьовувань та динамічно адаптувалися б до змін зовнішнього та внутрішнього середовища. Крім того, у теперішній час спостерігається підхід, що полягає у переході від виявлення до запобігання атакам. СВА вже включають засоби реагування на атаки, які в обов'язковому порядку включають механізми розриву з'єднань і взаємодіють із зовнішніми засобами захисту інформаційних мереж – міжмережевими екранами. Більшість методів виявлення аномалій мають високу обчислювальну складність у порівнянні з найбільш поширеним сигнатурним методом, який самостійно не забезпечує достатнього захисту систем у цілому і є достатньо формалізованим з точки зору аналізу вхідних параметрів. Для вирішення цієї задачі доцільно застосування теорії нечітких множин в якості основного методу аналізу даних, що поступають на вхід СППР, яка б при взаємодії із СВА значно збільшувала її адаптивність до невідомих типів атак і одночасно зменшувала кількість хибних спрацьовувань.

Таким чином, основними шляхами підвищення ефективності функціонування СВА є: створення СППР в якості однієї з підсистем СВА для підвищення показників адаптивності та зниження кількості хибних спрацьовувань; розробка методик формування знань у базі знань СППР, за рахунок об'єднання сигнатурного та експертного методів; подальшого донавчання БЗ за рахунок використання методів інтелектуального аналізу даних для забезпечення верифікації, стійкості та адаптивності СВА до невідомих типів атак.

д.т.н. Субач І.Ю. (ВІТІ ДУТ)
Кива В.Ю. (ВІТІ ДУТ)

ПІДСИСТЕМА ОПЕРАТИВНОГО УПРАВЛІННЯ ПАРАМЕТРАМИ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ МЕРЕЖІ ОРГАНУ ВІЙСЬКОВОГО УПРАВЛІННЯ

У теперішній час спостерігається загальна тенденція збільшення об'ємів циркулюючої інформації та мережевого трафіку в інформаційних мережах (ІМ), що призводить до погіршення якості надання послуг.

Аналіз функціонування ІМ органів військового управління (ОВУ) показує, що на даний час обслуговуючий персонал (ОП) ІМ зіштовхується з необхідністю постійного моніторингу стану ІМ. Особлива увага приділяється системам спостереження та збору статистичної інформації, які дозволяють вчасно розпізнавати та реагувати на аномалії, що відбуваються в ІМ. Система моніторингу повинна забезпечувати постійне спостереження за станом вузлів комп'ютерної мережі, виконувати перевірку доступності мережевих ресурсів і служб, стежити за роботою серверного і комунікаційного обладнання, у разі порушення нормальної роботи повідомляти обслуговуючий персонал, використовуючи різні засоби оповіщення. У своїй роботі ОП керується інформацією про стан ІМ, яка надається програмно-технічними системами моніторингу, але це приводить до додаткових витрат часу. На сьогоднішній день оператор здійснює аналіз та оцінку поточного стану ІМ шляхом вибіркової візуальної оцінки даних про параметри функціонування ІМ, користуючись існуючими програмними засобами та особистими знаннями і досвідом. Такий підхід має певні недоліки, зокрема: неможливість одночасної оцінки стану функціонування ІМ у цілому, а тільки за обраними декількома вхідними показниками; утруднення об'єктивної оцінки її стану ОП у визначенні часові нормативи в наслідок швидкоплинності змін параметрів ІМ та інше.

Усунення наведених недоліків є можливим шляхом розробки та впровадження системи підтримки прийняття рішення (СППР) ОП ІМ, однією з основних підсистем якої є підсистема оперативного аналізу даних про параметри функціонування ІМ.

Для проведення такого аналізу необхідні засоби, які б подавали і дозволяли опрацьовувати ОП дані у багатовимірному вигляді, а саме технології оперативного аналізу даних. Для оперативного аналізу даних запропоновано використання *ROLAP*-технології. Дана технологія дозволить аналізувати дані, що зберігаються в реляційній базі даних (РБД), забезпечуючи перетворення інформації в багатовимірну модель під час аналізу. У багатовимірному вигляді дані подаються ОП під час їхнього аналізу, на логічному та фізичному рівнях дані організовані у вигляді відношень реляційної моделі і зберігаються в РБД. Отже, ОП опрацьовує дані шляхом виконання операції багатовимірного аналізу, які у свою чергу, використовують засоби РБД. Виходячи з цього, пропонується реалізація підсистеми оперативного управління параметрами функціонування інформаційної мережі органу військового управління. Такий підхід до створення підсистеми оперативного аналізу дозволяє дотриматись пропозицій, сформульованих Коддом. Крім того, він забезпечує можливість реалізації технології-*ROLAP* в рамках реляційних систем керування баз даних (СКБД). Завдяки реляційним таблицям, архітектура *ROLAP* дозволяє зберігати великі обсяги даних, які будуть поступати із зовнішніх джерел. За допомогою *ROLAP* значення даних завжди будуть відповідати актуальному стану надходження цих даних із зовнішніх джерел, що є актуальним для оперативного аналізу та прийнятті рішень ОП ІМ.

Таким чином, реалізація підсистеми оперативного управління параметрами функціонування інформаційної мережі органу військового управління дасть можливість оперативно виконувати поточний аналіз ІМ за невеликі відмітки часу.

д.т.н. Субач І.Ю. (ВІТІ ДУТ)
к.т.н. Саєнко О.Г. (ВІТІ ДУТ)
Король М.А. (ВІТІ ДУТ)

МОДЕЛЬ НАДАННЯ ЗНАНЬ У БАЗІ ЗНАНЬ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ОПЕРАТОРА ІНФОРМАЦІЙНОЇ МЕРЕЖІ

На сьогодні у своїй роботі особа, що приймає рішення (ОПР) інформаційної мережі (ІМ) органу військового управління (ОВУ) аналізує поточний стан мережі шляхом вибіркового оцінюванням інформації, яка надається існуючими програмними та технічними засобами моніторингу (*HPOpenViwe*, *SunNetManager*, *IBMNetViwe*, *MRTG* тощо), а також на основі особистих знаннь і досвіду. Такий спосіб аналізу призводить до додаткових витрат часу, що у свою чергу негативно впливає на процес прийняття рішення посадовою особою, особливо в умовах суттєвого часового обмеження. Основними недоліками такого підходу є:

неможливість одночасної оцінки стану функціонування мережі в цілому, а лише за наперед обраними вхідними показниками;

утруднення об'єктивної оцінки стану ІМ обслуговуючим персоналом у встановлені часові терміни внаслідок інтенсивної зміни параметрів мережі тощо.

Дані недоліки можуть бути усунуті шляхом розробки та впровадження системи підтримки прийняття рішення (СППР) оператора ІМ.

У процесі проектування СППР на основі технологій обробки знань необхідно найбільш повно враховувати характерні особливості предметної області та забезпечувати адекватне надання знань щодо об'єкту прийняття рішень у базі знань (БЗ) СППР. Адекватність надання знань задачам, що вирішуються СППР, забезпечується правильним вибором джерел та моделі надання знань, а також відповідних методів логічного виводу.

Класичними моделями, що використовуються для надання знань у СППР є: семантичні мережі, фрейми, логічні та продукційні моделі. Також значного поширення набуло використання нейронних мереж, квантових і гібридних моделей надання знань.

Основними функціями підсистеми надання знань у СППР є: організація зберігання знань у системі; додавання нових знань і інтеграція з існуючими; вилучення застарілих знань; пошук знань; перевірка несуперечності бази знань; організація взаємодії між користувачем і базою знань.

Відповідно, для ефективного виконання наведених функцій, моделі надання знань повинні задовольняти наступним вимогам: мати прогнозовану ефективність, здатність до пояснення рішення, здатність до навчання, продуктивність, масштабованість, можливість експорту/імпорту знань, наочність. Аналіз властивостей перелічених вище моделей надання знань показує, що кожна з них лише частково відповідає заданим вимогам.

У доповіді для створення БЗ СППР оператора інформаційної мережі ОВУ, запропоновано застосування моделей надання знань, що базується на логіко-лінгвістичному підході, зокрема, що ґрунтується на теорії нечітких множин. Вона дозволяє більш ефективно вирішувати задачу розпізнавання стану ІМ ОВУ за рахунок математичної формалізації природно-мовних висловлювань у вигляді нечітких правил, що зв'язують нечіткі терми параметрів мережі та результат розпізнавання її стану.

ЛІТЕРАТУРА

1. Герасимов Б.М. Системы поддержки принятия решений: проектирование, оценка эффективности / Б.М. Герасимов, М.М. Дивизнюк, И.Ю. Субач // НАН Украины НИЦ ВС Украины „Государственный океанариум". – Севастополь: СНИИЯЭ и П, 2004. − 318 с.

2. Герасимов Б.М. Аналіз задач моніторингу інформаційних мереж та методів підвищення ефективності їх функціонування / Б.М. Герасимов, І.Ю. Субач, П.В. Хусаінов, В.О. Міщенко // Сучасні інформаційні технології у сфері безпеки та оборони, 2008. − № 3 (3), С. 24 – 27.

д.т.н. Субач І.Ю. (ВІТІ ДУТ)
к.т.н. Саєнко О.Г. (ВІТІ ДУТ)
Рубановська Н.О. (ВІТІ ДУТ)

МЕТОДИКА ФОРМУВАННЯ ПЛАНУ АНАЛІЗУ ПОВІДОМЛЕНЬ ОПЕРАТОРОМ ІНФОРМАЦІЙНОЇ МЕРЕЖІ ОРГАНУ ВІЙСЬКОВОГО УПРАВЛІННЯ

Виявлення та усунення несправностей є однією з головних функцій оператора інформаційної мережі (ІМ). В інструкціях оператора ІМ військового призначення є рекомендації по діях в найбільш типових нештатних ситуаціях. Разом з цим, якщо ситуацію не можливо віднести ні до одного з наведених типів, то заходи щодо її усунення та рішення щодо подальшого функціонування ІМ приймаються пізніше після повної обробки і аналізу інформації групою експертів (фахівців).

Досвід експлуатації ІМ показує, що вірогідність розпізнавання несправності та вироблення обґрунтованого рішення щодо подальшого функціонування ІМ черговим адміністратором на протязі короткого проміжку часу є невисокою.

Інформація щодо технічного стану ІМ та функціонування підсистем потрапляє до оператора ІМ шляхом застосування спеціального програмного забезпечення через дискретні відмітки часу. Повна оцінка інформації можлива тільки після послідовного ознайомлення з усіма елементами вихідної інформації, що в значній мірі погіршує нормативні часові показники щодо забезпечення стійкого функціонування ІМ і відновлення її основних показників у разі виникнення несправностей. Таким чином, актуальною є задача обробки усієї вхідної інформації щодо стану функціонування ІМ в реальному часі з можливістю оперативного втручання в управління мережею її оператором.

У доповіді запропоновано вирішення цієї задачі шляхом розробки та впровадження методики формування плану аналізу повідомлень оператором інформаційної мережі.

Формування плану аналізу оператором повідомлень про несправності здійснено шляхом вирішення задачі ранжування несправностей у порядку зменшення їх важливості та терміновості. Ця задача інтерпретується як задача складання розкладу. Кожна несправність $S^{(i)}$ характеризується наступними величинами: i – індекс несправності; T_i^d – директивний час аналізу повідомлення про i-у несправність; t_i – час аналізу повідомлення про i-у несправність; w_i – коефіцієнт відносної важливості i-ї несправності.

Відомо, що задачі складання оптимального розкладу не піддаються рішенню аналітичними методами та є *NP*-повними. Для їхнього вирішення застосовуються точні та наближені методи. Точні методи у наслідок їхньої великої обчислювальної складності не прийнятні для реалізації у режимі часу, близькому до реального. Тому, для вирішення задачі формування плану обробки повідомлень про несправності оператором ІМ, застосовується один з найбільш ефективних наближених методів.

Найбільш відомими алгоритмами складання розкладу у заданій постановці задачі є алгоритми Хелда-Карпа та Сахні-Горвіца. У наслідок того, що складність алгоритму Хелда-Карпа дорівнює $O\left(N \cdot 2^N\right)$ та є значно більшою ніж складність алгоритму Сахні-Горвіца – $O\left(N^2\right)$, то в основу методики формування плану покладено алгоритм Сахні-Горвіца.

Застосування даного підходу дає змогу ефективно аналізувати повідомлення про стан ІМ у директивний час, а також приймати необхідні заходи для їх усунення з метою запобігання або зменшення їхньої шкоди.

ЛІТЕРАТУРА

1. Саєнко О.Г. Модель ідентифікації стану інформаційної мережі на основі нечіткої бази знань / О.Г. Саєнко // Збірник наукових праць ВІКНУ. – № 36. – 2012. – С.131 – 136.

к.т.н. Труш О.В. (ДУТ)
Степаненко В.І. (ДУТ)
Хоменко С.Ю. (ДУТ)

ЦІЛІСНІСТЬ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Метою технічного захисту інформації є запобігання витоку технічними каналами або порушення цілісності інформації з обмеженим доступом. Аналіз наукових праць та публікацій, присвячених забезпеченню ефективного захисту інформації свідчить про те, що підвищення безпеки інформації в ІТС СП можливе лише при комплексному підході до аналізу можливих загроз й удосконалення засобів захисту від них. В даний час широко використовується узагальнена ймовірнісна модель процесу захисту інформації. У відповідності до неї обробка інформації на об'єкті O_i здійснюється в умовах впливу на інформацію різних загроз $\{З_j\}$. Для забезпечення інформаційної безпеки об'єкту СЗІ повинна здійснювати нейтралізуючий вплив на дестабілізуючі фактори та загрози.

Тому *метою* роботи є аналіз можливих загроз цілісності інформації в ІТС СП та визначення методів захисту від них. Цілісність забезпечується шляхом дотримання вимог політики безпеки по переміщенню інформації від відправника до отримувача. Під повнотою захисту при обміні, варто розуміти врахування багатьох можливих типів загроз, від яких забезпечується захист. Серед способів захисту від порушень цілісності можна виділити наступні:

– введення надмірності в саму інформацію (використання коригувальних кодів);

– введення надмірності в процес обробки інформації (використання процедури аутентифікації);

– введення системної надмірності (підвищення живучості системи).

Типовим об'єктом нападу може служити інформаційний обмін між двома користувачами системи. Тому необхідно застосовувати наступні основні методи підвищення енергетичної і структурної прихованості системи передачі:

1. робота з мінімально необхідною потужністю випромінювання, достатньою для забезпечення необхідної якості зв'язку, використання радіосистем з адаптацією за потужністю випромінювання;

2. використання оптимальних способів приймання сигналів і пристроїв захисту від навмисних завад;

3. використання складних шумоподібних сигналів з великою базою. Такі сигнали, на відміну від простих, мають більш високу завадостійкість і прихованість, а отже і ефективність при забезпеченні цілісності переданої інформації;

4. використання частотно-адаптивних ліній зв'язку.

Таким чином, проведений аналіз дозволяє зробити наступні *висновки*. В інформаційно-телекомунікаційних системах спеціального призначення основними загрозами канальній цілісності інформації є перехоплення, несанкціоноване відтворення інформації, маскування, маніпуляції даними та радіоелектронне подавлення. Для захисту від порушень цілісності інформації необхідно застосовувати введення надмірності в саму інформацію, у процес її обробки, а також введення системної надмірності. Поряд з криптографічними методами захисту інформації як один з основних напрямків забезпечення цілісності інформації в ІТС спеціального призначення заслуговує на увагу застосування методів підвищення прихованості зв'язку. Серед цих методів особливе місце займають шумоподібні сигнали, що дозволяють одночасно підвищити достовірність і прихованість передачі інформації а також підвищити рівень захищеності інформації від порушень цілісності та інших загроз.

ЛІТЕРАТУРА

1. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах".

Уманець Я.Л. (ВІТІ ДУТ)
Ошурко В.М. (ВІТІ ДУТ)

МІЖРІВНЕВИЙ ІНТЕЛЕКТУАЛЬНИЙ МЕТОД МАРШРУТИЗАЦІЇ В МОБІЛЬНИХ РАДІОМЕРЕЖАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Передача інформації та команд бойового управління між підрозділами та окремими військовослужбовцями в ході сучасних високоманеврених бойових дій вимагає застосування мереж радіозв'язку, здатних передавати різні типи інформації, а також забезпечувати самоорганізацію мобільних абонентів у мережу. Прикладом таких мереж є мобільні радіомережі (МР) класу MANET (*Mobile Ad-Hoc Networks*), які являють собою множину мобільних вузлів та базових станцій, які з'єднуються в радіомережу без завчасно розгорнутої мережевої інфраструктури [1].

Передача інформації в МР класу MANET потребує вирішення низки проблемних завдань наукового і технічного характеру, одним з найважливіших серед яких є маршрутизація потоків даних. Існуючі сьогодні протоколи та методи маршрутизації (ММ), запропоновані для використання в МР, поділяються на три основні види: табличні, зондові та гібридні. Як показали результати досліджень, табличні методи втрачають свою ефективність під час застосування в МР через необхідність розсилання значних об'ємів службової інформації. В умовах функціонування, якими характеризуються МР, найефективнішими є зондові ММ, які передбачають побудову маршрутів передачі у разі необхідності, а також відсутність маршрутних таблиць з повною інформацією про стан маршрутів у всій мережі, що значно скорочує обчислювальні ресурси вузлів, які живляться від батарей. Разом з тим, основним недоліком зондових ММ є значний час затримки передачі інформації, обумовлений необхідністю пошуку та побудови нових маршрутів, хоча це дозволяє значно скоротити об'єми службової інформації, що циркулює в МР, яка характеризується високою динамікою зміни топології. Крім того, в МР побудова маршрутів, які б забезпечували задану якість обслуговування різних типів трафіка, потребує збору та обробки інформації про стан мобільного вузла, його сусідів, а також радіоканалів, якими вони з'єднані. До такої інформації можуть відноситися наступні параметри: рівень навантаження у вузлах, ємність вузлових батарей, швидкість та напрямок переміщення вузлів, дальність радіозв'язку вузла, ширина смуги пропускання та швидкість передачі в радіоканалі, ймовірний час життя маршруту(ів) на інформаційному напрямку між вузлами.

Зважаючи на те, що, відповідно до еталонної моделі OSI, завдання маршрутизації інформаційних потоків вирішується на мережевому рівні, а зазначені вище параметри отримуються з фізичного, канального, транспортного та прикладного рівнів, то для усунення зазначених вище недоліків зондових ММ доцільно інтегрувати функції різних рівнів моделі OSI. Це дозволить ефективніше використовувати вузлові та мережеві ресурси, які витрачаються для передачі, отримання і обробки службової інформації, на основі якої приймаються рішення щодо побудови та підтримання маршрутів заданої якості.

Крім того, умови функціонування МР характеризуються невизначеністю, а множина різнорідних параметрів стану вузлів та МР унеможливлює застосування диференційних рівнянь для побудови чіткої математичної моделі взаємодії вузлів у процесі маршрутизації. У зв'язку з цим, при розробці нового зондового ММ пропонується використовувати апарат нечіткої логіки та нейронних мереж для інтелектуалізації процесу маршрутизації в МР. Застосування зазначених вище підходів дозволить побудувати маршрути заданої якості в МР класу MANET, скоротити об'єми службового трафіка та збільшити пропускну спроможність інформаційного напрямку.

ЛІТЕРАТУРА

1. Романюк В.А. Інтелектуальні мобільні радіомережі: збірник матеріалів V науково-технічної конференції [„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"] / – К.: ВІТІ НТУУ „КПІ", 2010. – С. 28 – 36.

Усік В.О. (ВІТІ ДУТ)
к.т.н. Хусаінов П.В. (ВІТІ ДУТ)

АВТОМАТИЧНА КЛАСИФІКАЦІЯ ІНЦИДЕНТІВ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Кількість інцидентів кібернетичної безпеки постійно збільшується, щодня з'являються нові загрози інформаційній безпеці, тому саме зараз особливо актуальним стало проведення детального розслідування скоєних інцидентів. Але його проведення неможливе без визначення методів, які застосовувалися під час реалізації загроз. Їх кількість постійно зростає, тому з'явилася необхідність класифікації методів їх здійснення.

Існує декілька проектів, які створили власні методи класифікації та аналізу атак на комп'ютеризовані інформаційні системи. До них можна віднести: *CAPEC (Common Attack Pattern Enumeration and Classification), Common Malware Enumeration (CME), Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration(CWE), Security database*, *The WASC (Web Application Security Consortium) Threat Classification, SANS*. Але, нажаль, жодна з існуючих класифікацій не є універсальною та існують проблеми з взаємозв'язком між даними системами. Кількість загроз що в них описані постійно зростає та на даний момент сягає вже кількох тисяч. Це призвело до збільшення проміжку часу на їх ідентифікацію та класифікацію в ході розслідування інцидентів кібернетичної безпеки та ускладнення роботи фахівців. Саме тому актуальним являється вирішення задачі автоматичної класифікації інцидентів кібернетичної безпеки для використання його в процесі розслідування. Необхідно створити систему, що дозволить оператору обравши ознаки, що притаманні тому інциденту, що розслідується з певного фіксованого переліку ознак та вказавши необхідні параметри автоматично отримати перелік загроз, що відповідають введеному запиту. Відповідність отриманих результатів введеним даним буде оцінена системою та представлена користувачу у числовому вигляді (у відсотках, %). У випадку, коли жоден з представлених у варіантів не відповідає тому інциденту, що відбувся можна буде легко додати новий тип до вже існуючої класифікації. Це значно скоротить час, що витрачається в ході розслідування, спростить роботу фахівців та дозволить більш точно визначати тип реалізованої загрози.

Вирішення даної задачі дозволить :

1) автоматизувати можливість класифікації інцидентів кібернетичної безпеки;
2) полегшити можливість класифікації раніше невідомих типів загроз;
3) швидко вносити зміни та доповнення до даної класифікації;
4) полегшити та спростити роботу користувачів.

Програмний модуль, що буде створений для вирішення цих задач повинен бути зручним у користуванні та легко доступний фахівцям у будь-який момент часу. Зважаючи на це, доцільним є створення такого ресурсу на базі сучасних *Web*-сайту, що дозволить отримати такі переваги як:

1) практичність та простота у використанні;
2) сумісність з іншими подібними системами та класифікаціями;
3) кросплатформеність (*Web*-технології підтримуються усіма існуючими платформами);
4) доступність для широкого кола користувачів не залежно від їх територіального розміщення;
5) розширення масштабу за рахунок перенесення даних сайтів з інших подібних проектів.

Для реалізації цих задач необхідно провести усестороннє дослідження та аналіз існуючих систем класифікації атак, вивчити їх структуру та основні класифікаційні ознаки, створити власний приклад такої класифікації та на основі цих даних розробити програмний модуль автоматичної класифікації інцидентів кібернетичної безпеки який можна було б застосовувати у ході проведення розслідування цих інцидентів.

к.держ.упр. Устименко О.В. (ЦВСД НУОУ)

РОЗВИТОК ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ ЯК СКЛАДОВА ПІДГОТОВКИ ТЕРИТОРІЇ ДЕРЖАВИ ДО ОБОРОНИ

Боротьба за інформаційне домінування займає все більш важливе місце в геополітичних змаганнях розвинутих країн світу. На сьогодні потенційні можливості розвитку суспільства все більш визначаються рівнем та ефективністю інформаційно-комунікаційних систем. Завдання щодо інформаційного забезпечення всіх сфер діяльності сучасного суспільства по своїй значущості вже переважає проблему індустріального розвитку [1].

Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування воєнної сили, послабити або завдати значної шкоди безпеці конкуруючої держави, яка не має дієвої системи захисту від негативних інформаційних впливів. Про це зазначено в Доктрині інформаційної безпеки України та підкреслено, що за сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки [2].

У сучасному суспільстві інформаційна безпека розглядається як самостійна складова національної безпеки держави, хоча вона пронизує всі інші сфери державної діяльності. Її забезпечення, з використанням ефективної національної інформаційної політики, значною мірою сприяє досягненню успіху у виконанні завдань в політичній, воєнно-політичній, воєнній, економічній, інформаційній, соціальній та інших сферах державної діяльності.

Розглядаючи основні заходи щодо підготовки території держави до оборони, що проводяться безпосередньо Збройними Силами України (оперативне обладнання території держави) фахівці з питань національної безпеки наголошують на важливості: будівництва та вдосконалення пунктів управління і оснащення їх засобами зв'язку та автоматизації; розвитку опорної мережі зв'язку Збройних Сил України (ЗС України) і об'єднання її із загальнодержавною (національною) мережею зв'язку [3, ст. 293].

На жаль, сучасний стан готовності території України до оборони не відповідає характеру можливих воєнних конфліктів за багатьма показниками. Міністерство оборони України не має сучасних захищених пунктів управління. Позаміські захищені пункти управління органів державної влади, захищені пункти управління ЗС України, інших складових сектора безпеки та оборони були побудовані ще за часів Радянського Союзу. На сьогодні вони морально і фізично застаріли, не обладнані сучасними засобами зв'язку. Недостатня кількість каналів зв'язку, відсутність захищених локальних обчислювальних мереж для обробки інформації з обмеженим доступом на центрах (пунктах) управління Генерального штабу ЗС України та Міністерство оборони України не дає змоги забезпечити достатню оперативність їх роботи. Інформаційна інфраструктура держави не відповідає сучасним вимогам.

Інформаційна інфраструктура держави це сукупність носіїв даних та інформації суб'єктів інформаційної діяльності держави, які реалізовані у формі організаційно-технічних засобів (інформаційних систем, центрів та пунктів, засобів масової інформації), що здійснюють створення, накопичення, зберігання, обробку і поширення інформації, засобів захисту інформації, а також організаційних структур, які забезпечують їх функціонування згідно із чинним законодавством [4].

Частину інформаційної інфраструктури держави, виведення з ладу або руйнація засобів (об'єктів) якої матиме згубні наслідки для національної безпеки, можна вважати критичною складовою інформаційної інфраструктури держави. До об'єктів критичної інформаційної інфраструктури держави можна віднести: інформаційні системи та засоби реального часу (спостереження, навігації, автоматизації управління технологічними процесами), телекомунікаційні системи, інформаційні ресурси суб'єктів сектора безпеки і оборони, національної транспортної системи, енергетичної системи, фінансової системи, оборонно-

промислового комплексу, хімічного виробництва, медицини катастроф, засобів масової інформації тощо.

Істотною проблемою забезпечення інформаційної безпеки є той факт, що матеріальну основу інформаційної інфраструктури держави складають засоби створення, збору, передачі(поширення), прийому, зберігання, пошуку, автоматизованої обробки і захисту інформації, які нині практично усі створюються на основі зарубіжних інформаційно-комунікаційних технологій. Вести мову про можливість ефективного вирішення завдань національної безпеки при їх використанні – обманювати самих себе. Ніяка сертифікація зарубіжного устаткування і програмних продуктів не дасть стовідсоткової гарантії, що в їх надрах не „зачаїлися" програмні „віруси" або „логічні бомби", які можуть бути активовані в певний час по сигналу з-за кордону.

Про реальність такої ситуації свідчать проблеми, що виникли з функціонуванням державних реєстрів інформаційної мережі Міністерства юстиції, ведення яких здійснюється державним підприємством „Інформаційний центр Міністерства юстиції України". Міністр юстиції України Олена Лукаш заявила, що за попередньою інформацією, відбувся збій програмного забезпечення, яке було розроблене ТОВ „Арт-мастер" та ТОВ „3-Т", внаслідок чого 1 жовтня було заблоковано діяльність усіх, хто користуються реєстрами, що забезпечують діяльність Державної реєстраційної служби, Державної виконавчої служби, органів юстиції і нотаріусів [5]. У Мінюсті пояснили, що детальний огляд програмного забезпечення і аналіз ситуації засвідчив, що відбулось несанкціоноване втручання в роботу комп'ютерного обладнання, автоматизованих систем та комп'ютерних мереж Міністерства юстиції, що призвело до блокування інформації і порушення встановленого порядку її маршрутизації [6].

Особливої гостроти проблема набуває у зв'язку з масовою комп'ютеризацією всіх видів діяльності людини. У військовій справі повнота та достовірність інформації все більшою мірою обумовлює оперативність прийняття рішень, структуру та якість озброєнь, оцінку рівня їх достатності, дієвість пропаганди, ефективність управління військами та зброєю, діями збройних сил та інших складових сектора безпеки та оборони і, в підсумку, визначає результат збройного протистояння. І якщо трьохденна перерва в роботі державних реєстрів інформаційної мережі Міністерства юстиції нанесла лише економічні збитки, як суб'єктам підприємницької діяльності так і державі в цілому, то аналогічна ситуація з інформаційно-обчислювальною мережею ЗС України у ході можливого конфлікту обійдеться набагато дорожче.

ЛІТЕРАТУРА

1. Устименко О. В. Інформаційна безпека як складова національної безпеки / О. В. Устименко // Дні інформаційного суспільства – 2013 : Матеріали щорічної наук.-практ. конф. за міжнар. участю, Київ, 20 – 21 травня 2013 р. / Упоряд. : М. М. Малюга; За заг. ред. д. держ. упр., проф. Н. В. Грицяк. – К. : Вид-во, 2013. – С. 76 –77.

2. Указ Президента України № 514/2009 від 08.07.2009 „Про Доктрину інформаційної безпеки України" – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2780 – 12.

3. Богданович В.Ю. Основи державного управління забезпеченням обороноздатності України: теорія і практика / В.Ю.Богданович, М.Ф.Єжеєв, І.Ю.Свида – Львів : ЛІСВ, 2008. – 300с.

4. Розробка проекту військового стандарту з питань інформаційної безпеки держави у воєнній сфері – Київ : НУОУ, 2013. – 66 с.

5. Олена Лукаш: Відбулось несанкціоноване втручання в роботу комп'ютерної мережі Міністерства юстиції – Режим доступу : http://www.minjust.gov.ua/news/44276.

6. З мережею Мін'юсту „попрацювали" хакери – Режим доступу : http://www.pravda.com.ua/news/2013/10/2/6999165/.

Фастенков М.С. (ВІТІ ДУТ)
к.т.н. Раєвський В.М. (УІТ МОУ)
к.т.н. Гурський Т.Г. (ВІТІ ДУТ)

ЗАДАЧА ВИБОРУ ДОВЖИНИ ЦИФРОВОЇ ПОСЛІДОВНОСТІ ДЛЯ ІДЕНТИФІКАЦІЇ СИГНАЛЬ-ЗАВАДОВОЇ ОБСТАНОВКИ В РАДІОКАНАЛІ

Важливою складовою системи військового зв'язку є система радіозв'язку з використанням радіозасобів різних типів, яка характеризується великою їх кількістю та щільності насичення ними. Все це призводить до утворення великої кількості завад, подібних до корисного сигналу, які зменшують, а іноді, унеможливлюють передачу інформації.

Тому постає питання розробки засобів радіозв'яку, що спроможні забезпечити передачу інформації в умовах впливу завад, подібних корисному сигналу. Для створення цих засобів використовуються переважно види кутової та амплітудної модуляції, їх різновидностей і комбінацій. Для успішного прийому взаємозаважаючих сигналів необхідними є знання наявності (відсутності) сигналу завади та знання неінформаційних параметрів корисного сигналу та завади (частоти несучого коливання, амплітуди та початкової фази сигналу).

Для оцінки неінформаційних параметрів корисного сигналу та сигналу завади, необхідно знати, які випромінювання присутні на частотах передачі двостанового сигналу за деяку кількість тактових інтервалів.

Вказана задача може бути вирішена наступним чином. Передавач абонента, що посилає виклик, перед початком передачі корисної інформації випромінює деяку апріорі відому приймальному абоненту цифрову послідовність визначеної довжини N. при практичній реалізації її можна сумістити з питанням синхронізації станцій в цілому. В точці прийому на початку сеансу зв'язку вихід демодулятора скомутований на дискретний узгоджений фільтр відповідної довжини N. Паралельно спостереження на вході демодулятора довжиною $T = \Delta t * N$ запам'ятовується. Коли відбувається спрацьовування вирішуючого пристрою на вході дискретного узгодженого фільтру (що налаштований на деякий поріг $N_{\text{пор}} < N$), виконується відновлення отриманої цифрової послідовності, і тільки потім виконується обчислення неінформаційних параметрів сигналу, якщо в каналі подібної завади немає, або обчислюються вказані параметри сигналу і подібної завади, якщо вона присутня.

Тому важливим завданням є розробка методики оцінки (розрахунку) мінімально необхідної довжини N цифрової послідоності, що застосовується для ідентифікації ситуації в каналі, при обмеженні на ймовірність виявлення корисного сигналу $P_{\text{виявл}}$ знизу та на ймовірність хибного виявлення $P_{\text{хибн виявл}}$ – зверху.

Зазначимо, що задача має суперечливу природу – збільшення ймовірності виявлення $P^*_{\text{виявл}}$ веде і до збільшення ймовірності хибного виявлення $P_{\text{хибн виявл}}$, тому вибір порогу потребує знаходження „золотої середини", коли виконуються вимоги, що визначені у методиці.

ЛІТЕРАТУРА

1. Єрохін В.Ф., Раєвський В.М. Метод синтезу оптимального розділення двостанових взаємозаважаючих сигналів частотної маніпуляції // Збірник наукових праць – К.: ВІТІ НТУУ „КПІ". – 2004. – №4. – С.38 – 47.

2. Гепко И.А. Многопользовательский прийом в CDMA: теория и методы // Зв'язок. – 2000. – №4. – С.17 – 23.

к.т.н. Федорова Н.В. (ДУТ)

МЕРЕЖІ З КОМУТАЦІЄЮ ПАКЕТІВ. СИНХРОНИЙ ETHERNET, ЯК СЕРЕДОВИЩЕ ПЕРЕДАЧІ СИНХРОНІЗАЦІ

Вступ. Майбутнє мереж електрозв'язку – це перехід від існуючого транспортного середовища SDH до технології з комутацією пакетів (IP/IPMPLS/Ethernet).

Синхронний Ethernet (SyncE) – це важливий етап розвитку технології Ethernet як доведення її до рівня, що підходить для операторів глобальних мереж, в яких необхідна синхронізація тактової частоти [1].

Планування мереж синхронізації на базі синхронного Ethernet

Механізм SyncE служить способом передавання частоти на своєму фізичному рівні так, що її можливо відстежувати від зовнішніх джерел (наприклад, від пристроїв синхронізації мережі). Тобто, канали Ethernet можливо використовувати як складові частини мережі синхронізації [4, 5]. Розвиток мереж синхронізації на базі синхронного Ethernet приносить користь операторам мереж тим, що розподілення тактової частоти відбувається без впливу варіацій затримки пакетів [2]. Однак у процесі розвитку мережі оператор буде мати справу з неоднорідним обладнанням Ethernet, в якому можуть бути, а можуть і не бути засоби синхронного Ethernet. Можливо, ***знадобиться додатковий етап планування мережі просто для того, щоб впевнитися, що до складу вибраного ланцюга синхронізації канали Ethernet побудовані на обладнанні, в якому є відповідні функції синхронного Ethernet***.

На рис.1 показані два рівня архітектури Ethernet – ETH та ETY – разом з функціями адаптації більш високого рівня у вигляді прямого та зворотного відображень каналу E1 з метою емуляції каналів на основі відносного способу відновлення тактової частоти [6]. Також на Рис.1 показано відношення до послуг емуляції каналів (circuit emulation services – CES), коли носієм послуги рівня ETY (наприклад, E1) є рівень ETH мережі [3].

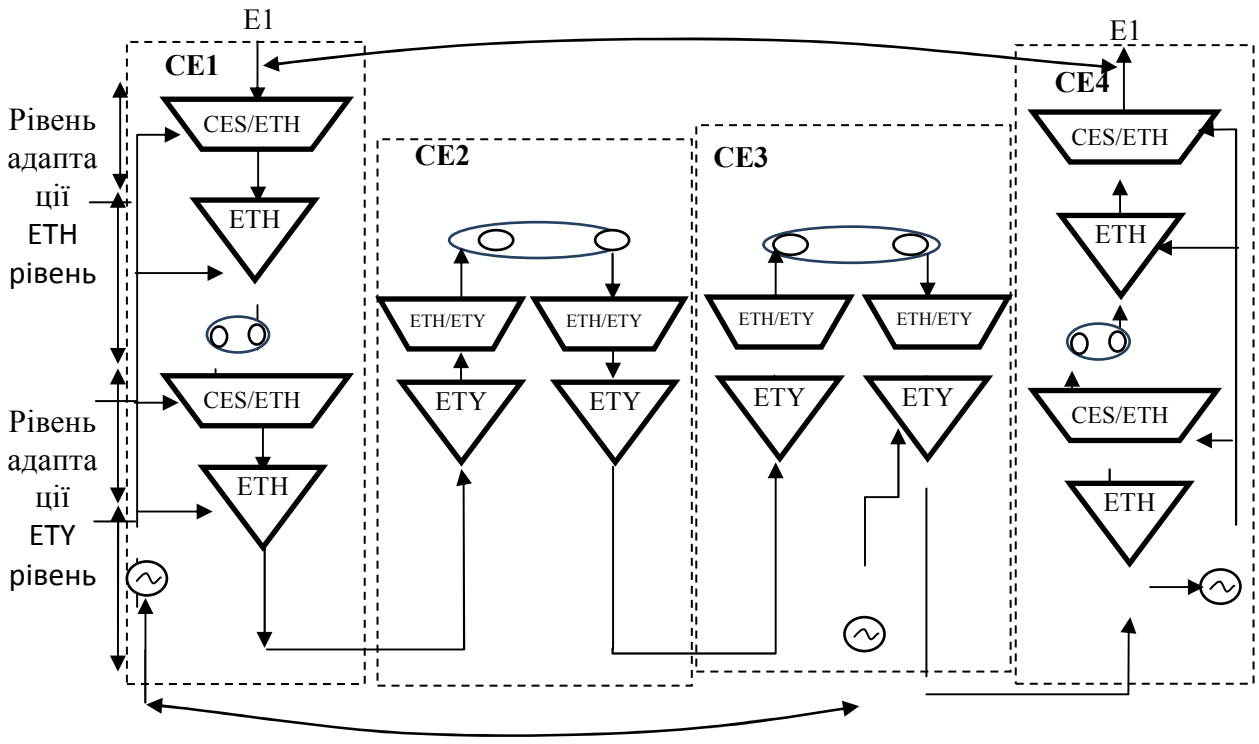


Рис.1 CES та SyncE разом з рівнями ETY та ETH

На рис. 2 представлена схема вимірювання SyncE. Наведена схема представляє собою ланцюг синхронізації з чотирьох послідовно з'єднаних комутаторів Ethernet, в якому тактовий сигнал проходив по мережі через стики 1000BASE-X та 100BASE-Tx [1].

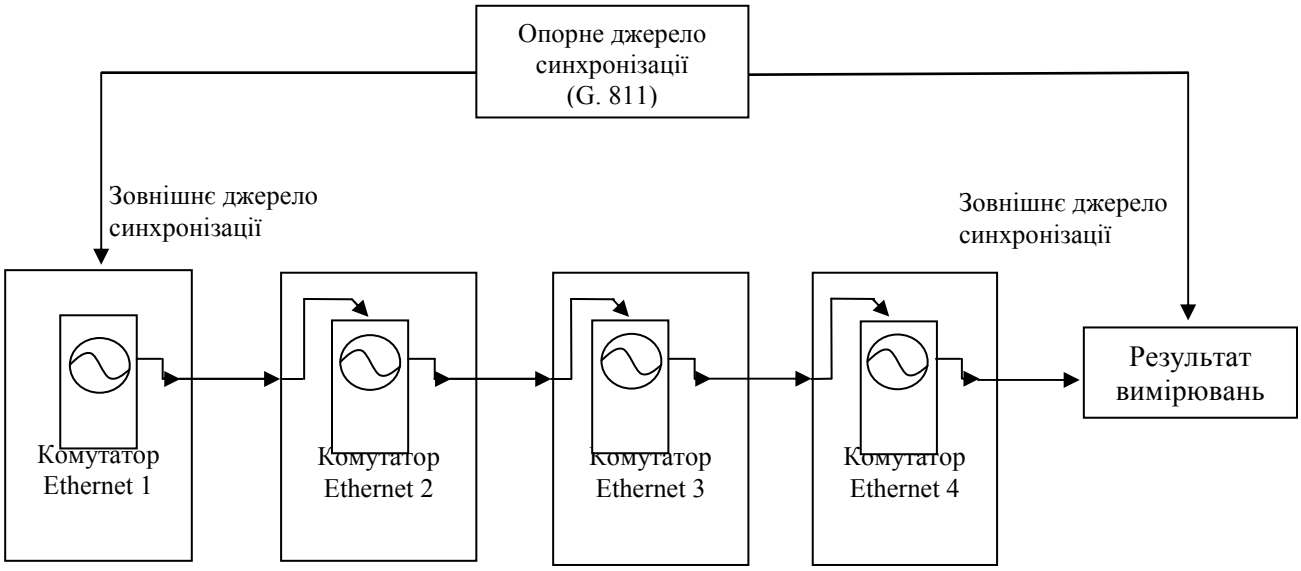


Рис. 2 Схема вимірювання SyncE

Результати проведених вимірювань наведені в [1] та говорять про високу якість передавання тактової частоти SyncE. Фазові шуми залишаються в межах декількох десятків наносекунд, що не суперечить характеристикам транспортних мереж SONET/SDH.

Висновки.

1. Архітектура Sync-E сумісна з сучасною мережею синхронізації. Таке рішення дає провайдерам електрозв'язку гнучкість в обслуговування багатьох вузлів з наперед визначеною якістю характеристик.

2. Механізм Sync-E функціонує на фізичному рівні та не залежить від навантаження мережі, що дозволяє передавати сигнал синхронізації через транзитні пристрої, але забезпечує тільки частотну синхронізацію.

3. У порівнянні з іншими способами синхронізації в IP-мережах (наприклад, протоколами NTP, PTP) SyncE є найбільш оптимальним зі сторони гарантованої якості передаваємого сигналу – в силу своєї природи та виконання на апаратному рівні для всього обладнання.

ЛІТЕРАТУРА

1. Ferrant J-L. Synchronous Ethernet: A method to transport synchronization / Jean-Loop Ferrant, Alcatel-Lucent, Mike Gilson, British Telecom, Sebastien Jobert, France Telecom, Michael Mayer and Michel Ouellette, Nortel, Laurent Montini, Cisco, Silvana Rodrigues, Zarlink, Stefano Ruffini, Ericsson // IEEE Communication Magazine. – September – 2008. – P. 126 – 134.

2. Рыжков, А.В. Способы синхронизации сетей электросвязи в условиях перезагрузки нормативной базы / А.В. Рыжков, А.В. Савчук // Электросвязь. – 2012. - №9. – С. 37 – 41.

3. IEEE 802.3-2005, „CSMA/CD Access Method and Physical Layer Specifications," 2005.

4. ITU-T Rec. G.805, „Generic functional architecture of transport networks," 2000.

5. ITU-T Rec. G.809, „Functional architecture of connectionless layer networks," 2003.

6. ITU-T Rec. G.8010, „Definitions and terminology for synchronization networks," 1996.

Фесьоха В.В. (ВІТІ ДУТ)
д.т.н. Шворов С.А. (ВІТІ ДУТ)

МЕТОДИ ОРГАНІЗАЦІЇ ФУНКЦІОНУВАННЯ АДАПТИВНИХ ТРЕНАЖЕРНИХ КОМПЛЕКСІВ ПІДГОТОВКИ ОПЕРАТОРІВ РАДІОТЕХНІЧНИХ СИСТЕМ

Як відомо, одним із напрямків підвищення рівня підготовки операторів радіотехнічних систем (РТС) є широке застосування тренажерних комплексів (ТК). Однак, існуючі ТК, як показує практика, функціонують без урахування динаміки зміни рівня підготовки та функціонального стану операторів РТС по виконанню типових навчальних завдань (НЗ). Аналіз останніх досліджень і публікацій показує, що на даний час планування тренувань, формування навчально-інформаційних моделей (НІМ) повітряної обстановки та управління процесом підготовки операторів РТС базується на інтуїції досвідченого керівника тренувань. Тому виникає необхідність в розробці методів планування, формування НІМ та управління процесом тренувань, за допомогою яких на кожному етапі навчання (з урахуванням досягнутого рівня підготовки та функціонального стану операторів РТС) забезпечується оптимальне планування та управління процесом відпрацювання НЗ різних типів.

Під ТК розуміється сукупність тренажерів операторів РТС підрозділів та частин, об'єднаних ієрархічними, системоутворюючими, інформаційними зв’язками, що забезпечують підготовку операторів та злагодження бойових обслуг КП по єдиній імітованій повітряній обстановці.

Для відпрацювання НЗ різних типів задача оптимального планування та формування НІМ може бути подана наступним чином. Необхідно сформувати таку інтенсивність імітованих тактичних ситуацій, при якій підготовка операторів до виконання НЗ зростала б до максимального рівня навченості при обмеженнях сумарного навантаження на операторів по виконанню типових операцій. Для знаходження оптимальної інтенсивності імітованих тактичних ситуацій для кожного етапу тренувань використовується модифікований метод динамічного програмування.

Перед початком тренувань оператори виконують тестові НЗ, на основі оцінки якості виконання яких визначається функціональний стан та поточний рівень підготовки операторів РТС, що необхідно для визначення прогнозованого рівня навченості наприкінці тренувань. Знаходження залежності між витратами та рівнем підготовки фахівців по виконанню типових операцій здійснюється за допомогою теоретико-експериментального методу.

У процесі тренувань, якщо рівень підготовки операторів не відповідає прогнозованому – забезпечується корегування плану інтенсивної підготовки. Із цією метою за допомогою спеціального методу управління процесом інтенсивної підготовки корегується модель імітованої обстановки, в якій для кожного етапу тренування формується мінімально необхідна кількість імітованих тактичних ситуацій, а також необхідна інтенсивність їх відтворення. При цьому мінімально необхідна кількість імітованих ситуацій визначається за допомогою метода найшвидшого спуску, що дозволяє, як показують результати імітаційного моделювання, у 1,5-2 рази скоротити часові витрати на підготовку операторів до необхідних прогнозованих рівнів навченості.

Таким чином, за допомогою розроблених методів на кожному етапі процесу підготовки операторів забезпечується адаптивне планування та відпрацювання оптимального набору НЗ з урахуванням поточного рівня навченості та функціонального стану операторів РТС й обмежень на їх навантаження. При цьому здійснюється підготовка операторів та бойових обслуг по виконанню типових навчальних завдань до максимального рівня навченості у найбільш складних умовах імітованої обстановки.

Фисюк А.О. (ВІТІ ДУТ)

МЕТОД ОБРОБКИ ШИРОКОСМУГОВИХ СИГНАЛІВ ПРИ ВПЛИВІ НЕГАУСОВСЬКИХ ЗАВАД

В сучасних системах радіозв'язку широке застосування знаходить метод багатостанційного доступу з кодовим розділенням сигналів (CDMA – Code-Division Multiple Access). В таких системах передача інформації різними абонентами здійснюється сигналами, які перекриваються за спектром і в часі, але розрізняються за формою.

Ефективність систем радіозв'язку CDMA обмежена рядом факторів, основними з яких є вплив природних та навмисних завад, нестійкість і різноманіття імовірнісних розподілів завадового комплексу, нестаціонарність каналу, випадкові флуктуації комплексних множників каналу, завмирання радіосигналів тощо.

для випадку передачі інформації по гаусівському каналу з шумами. Реальна ефективність CDMA-систем з негаусовськими каналами багато в чому визначається досяжними характеристикам завадостійкості, системної ємності та обчислювальній складності алгоритмів і пристроїв спільної обробки сигналів у складному завадовому комплексі, характерному для сучасних CDMA-систем. Дефіцит частотного, енергетичного та просторового ресурсу радіоканалів, а також особливості завадового комплексу CDMA-систем вимагають використання адекватних моделей імовірнісного опису реальних негаусівських завад, що забезпечують розробку і впровадження нових алгоритмічних і технічних рішень, спрямованих на підвищення ефективності CDMA-систем в інтересах надійної передачі інтегрального пакетного трафіка в складних і мінливих умовах інформаційної взаємодії користувачів.

Методи оптимізації CDMA-сигналів, удосконалення алгоритмів їх формування та обробки є об'єктом інтенсивних теоретичних досліджень протягом останніх років. Однак більшість відомих методів підвищення ефективності функціонування CDMA-систем одержані для випадку передачі інформації по гаусівському каналу без пам'яті. Наявність у каналі селективних завмирань і навмисних завад не дозволяє при прийнятній складності реалізації відомих алгоритмів передачі дискретних повідомлень досягти тієї ж ефективності використання реальних каналів зв'язку, що й ідеального гаусівського півнеперервного каналу. Для підвищення ефективності роботи CDMA-систем в негаусівських каналах запропонований адаптивний метод багатоабонентського розділення широкосмугових сигналів, заснований на комбінованих рішеннях паралельного відсікання негаусівських завад з інкапсульованими процедурами адаптивної обробки сигналів і поканальної демодуляції-декодування на кожній ітерації. Принцип функціонування CDMA-системи за запропонованим методом полягає в ітеративному формуванні на приймальному боці самостійних незалежних оцінок завад для кожного абонента для того, щоб відняти всі або деякі з них із прийнятого групового сигналу.

Для оцінки ефективності запропонованого методу у зазначених умовах виконане статистичне моделювання основних методів обробки сигналів в каналах з негаусовськими завадами. У процесі моделювання використовувалося квазикогерентне приймання сигналів з фазовою маніпуляцією у трипроменевому зворотному каналі з негаусовською завадою. Затримки променів уважаються відомими. Застосовувалось згорточне кодування зі швидкістю 1/2.

Проведений аналіз показує, що розроблений метод обробки сигналів забезпечує найкращі характеристики приймання в негаусовському каналі. Виграш у завадостійкості для ідентичних значень бітової помилки 10^{-3} і рівної спектральної ефективності становить 3 – 4 дБ. Запропонований метод може бути застосований в адаптивних засобах радіозв'язку при реалізації механізму захисту від природних і навмисних завад.

Фомін М.М. (ВІТІ ДУТ)
Волошенюк Є.С. (ВІТІ ДУТ)
Липовий О.І. (ВІТІ ДУТ)

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ І НАДІЙНОСТІ FSO

Атмосферні оптичні лінії зв'язку (АОЛЗ) або, в англійському варіанті, FSO (Free Space Optics) можна сміливо назвати системами нового століття! Радіочастотний діапазон, на жаль, не нескінченний, комунікації мегаполісів стають все більш складними для прокладення оптоволоконних і проводоводових ліній – людству доводиться знаходити все нові, більш довершені і зручні способи передачі інформації.

Атмосферні (бездротові, відкриті) оптичні системи передачі (АОСП) призначені для передачі цифрових потоків даних через атмосферу в інфрачервоному оптичному діапазоні довжин хвиль [1] .

Сама технологія передачі ґрунтується на передачі даних модульованим випромінюванням в інфрачервоній частині спектра через атмосферу. Оптична атмосферна система зв'язку між двома пунктами складається з двох спарених приймально-передавальних пристроїв розташованих в межах прямої видимості на обох кінцях лінії і направлених один на одного. Технологія FSO дозволяє вирішувати проблеми „останньої милі", розвивати міські мережі передачі даних і голосу, здійснювати підключення домашніх мереж або офісів до мережі Інтернет, а також організовувати резервні канали зв'язку або розширювати існуючі канали при високому ступені захищеності. Крім того, технологія використовується для комунікацій між космічними апаратами, а також є можливість її застосування і у сфері телекомунікацій спеціального призначення, в якості ліній дистанційного управління і фідерного тракту. Але, через постійне підвищення вимог до якості інформації, яка передається, необхідно звернути увагу на деякі специфічні проблеми FSO, обумовлені як апаратурою, так і особливостями АК, котрі за їх впливом на оптичний сигнал можна розділити на дві групи. Першу групу створюють процеси, що викликають енергетичне послаблення сигналу, зокрема, поглинання газами і парами складових атмосфери, поглинання і розсіювання аерозолями і опадами. Сюди ж можна віднести і світові фони, що погіршують відношення сигнал/шум на виході приймального пристрою FSO [2] .

Друга група – це процеси, пов'язані з неоднорідностями показника заломлення (турбулентністю) повітря і процеси, що створюють флуктуації амплітуди та фази оптичної хвилі.

Вирішити дані проблеми, а тим самим підвищити надійність роботи FSO систем, покликані декілька технологічних рішень, а саме:

– підвищення потужності передавача і чутливості приймача;
– зниження діаграми направленості передавальних антен;
– застосування системи автотрекінгу;
– використання резервного радіоканалу в поєднанні з оптичним каналом.

Комбінація можливостей інфрачервоних систем при роботі в умовах сильного дощу й міліметрових радіосистем в умовах сильних туманів дозволяє створювати гігабітні бездротові з'єднання крапка-крапка на дистанціях до 3 кілометрів з операторською доступністю 99,999 %. При цьому 97-99 % часу в році дані передаються через FSO-систему, стійку до радіоперешкод, а 1-3 % часу дані передаються міліметровою радіосистемою. Крім високої доступності, така комбінація дозволяє будувати систему з дублюванням каналів.

ЛІТЕРАТУРА

1. Вишневский В.М. Широкополосные беспроводные сети передачи информации / Вишневский В.М., Ляхов А.И. – М.: Техносфера, 2008.–360 с.

2. Милютин Е. Современное состояние и перспективы атмосферных оптических линий связи / Е.Милютин Сети и телекоммуникации, № 6, 2011. – с. 14 – 20.

Фомін М.М. (ВІТІ ДУТ)
Давиденко С.С. (ВІТІ ДУТ)

ПІДВИЩЕННЯ ЯКОСТІ МЕРЕЖНОГО РЕСУРСУ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ЗВ'ЯЗКУ

На сьогоднішній день розвиток галузі телекомунікацій є однією з самих стрімких у світі. На ряду зі стрімким зростанням телекомунікаційних мереж розвиваються нові IP – послуги, такі як IPTV, VoIP та інші. У зв'язку з цим за останній час значно зріс IP – трафік. Тому впровадження класів обслуговування для різних видів трафіків є необхідним завданням. Також необхідно впроваджувати систему управління трафіком, яка буде забезпечувати задані класи обслуговування для різних видів трафіку шляхом перерозподілу мережного ресурсу. Використання на транспортному рівні технології багатопротокольної комутації міток MPLS (MultiProtocol Label Switching) дозволяє забезпечити ефективну передачу трафіку з підтримкою параметрів QoS (Quality of Service). Можливості управління трафіком, спрямовані на забезпечення збалансованого використання ресурсів мережі MPLS з підтримкою QoS, реалізовуються за допомогою технологій інжинірингу трафіку Traffic Engineering (TE) за рахунок використання механізмів збалансованого завантаження ресурсів мережі, вибору оптимального маршруту проходження трафіку, використання процедур резервування і розподілу завантаження мережі, балансування трафіку і механізмів запобігання перевантажень.

Мультисервісність, що присутня у мережах, вимагає розробки науково обґрунтованих засобів досягнення необхідних показників якості обслуговування повідомлень.

Мережа MPLS умовно ділиться на дві функціонально різні області: ядро мережі і граничну область. У ядро входять пристрої, з мінімальними вимогами підтримка MPLS та участь у процесі маршрутизації трафіку (для протоколу, який комутується за допомогою MPLS). У ядрі маршрутизатори займаються тільки комутацією, а всі функції класифікації пакетів за класами FEC (Forward Error Correction – поміхостійке кодування), а також реалізацію додаткових сервісів фільтрації, маршрутизації, вирівнювання навантаження на мережу і керування трафіком беруть на себе граничні LSR.Таким чином, весь обсяг інтенсивних обчислень припадає на граничну область, а високопродуктивна комутація виконується в ядрі, що дозволяє ефективно оптимізувати конфігурацію пристроїв MPLS в залежності від їх розташування в мережі [2]. Дана особливість MPLS – відокремлення процесу комутації пакета від аналізу IP– адрес в його заголовку відкриває ряд нових можливостей. Наслідком такого підходу є те, що черговий сегмент LSP (Layered Service Provider – багаторівневий провайдер послуг) може не збігатися з черговим сегментом маршруту, який був би обраний при традиційній маршрутизації. А оскільки на встановлення відповідності пакетів певним класам FEC можуть впливати не тільки IP – адреси, а й інші параметри, то неважко реалізувати, наприклад, призначення різних LSP пакетам, які належать до різних потоків RSVP (Resource ReSer Vation Protocol – протокол резервування мережевих ресурсів) або мають різні пріоритети обслуговування. Природно, такий сценарій вдається здійснити і в звичайних маршрутизованих мережах, але рішення на базі MPLS простіше і до того ж набагато краще піддається масштабуванню.

Кожен клас FEC обробляється окремо від інших не тільки тому, що для кожного класу будується свій шлях LSP, але з причини доступу до загальних ресурсів, тобто до смуги пропускання каналу і буферного простору. Результатом є дуже висока якість обслуговування в мережах MPLS, а застосування в LSR таких механізмів управління буферизацією і черговістю, як WRED (Weighted Random Early Detection), WFQ (Weighted Fair Queing) або CBWFQ (Class Based WFQ), дає адміністратору мережі MPLS можливість ефективно контролювати розподіл ресурсів, а також ізолювати трафік окремих користувачів.

Крім того, при використанні маршруту в мережі MPLS не виникає проблем, типових для стандартної IP- маршрутизації, так як вся інформація про маршрут міститься в мітці, і пакету не потрібно нести адреси проміжних вузлів, що розширює можливості управління розподілом навантаження на мережу.

Однак на відміну від віртуального каналу фіксований шлях MPLS надається у вигляді частини інтерфейсу IP, тому для його використання не доведеться здійснювати ніяких спеціальних дій з налаштування. У кінцевому варіанті мережа на базі MPLS містить параметр, що описує, як відрізнити трафік цієї VPN [3]. Так, при вступі на IP– інтерфейс інтернет провайдера потік IP – пакетів буде аналізуватися прикордонним пристроєм MPLS, і відповідаючи критерію VPN пакети будуть направлені по шляху MPLS для подальшої обробки.

Подібна модель відкриває можливості для появи зовсім нових видів послуг, а саме: VPN з підтримкою Net Meeting від Microsoft може бути запущена на певний час на плановій основі для підтримки ряду користувачів в кількох місцях, а по настанні встановленого терміну трафік буде автоматично маршрутизироваться в MPLS VPN без втручання користувача. Шляхи MPLS будуть ліквідовані, і той же самий трафік буде оброблятися, як звичайно, наприклад – направлятися через Інтернет.

Крім цього VPN на основі MPLS може виконувати й інші завдання, зокрема цілодобово підтримувати роботу критично важливих додатків. У цьому випадку провайдер послуг визначає фіксований шлях на термін контракту з користувачем.

MPLS може залишатися в межах мережі провайдера послуг, надаючи користувачам чималі переваги, а може вийти за її межі і захопити зовнішній край локальних мереж або використовуватися при побудові корпоративних глобальних мереж. До того ж чим ближче MPLS до додатків, тим більше потенційних переваг вона здатна надати.

Безумовно, використання MPLS в корпоративних (відомчих) глобальних мережах з великим трафіком більш виправдано, ніж застосування нової архітектури в невеликих LAN, так як ізоляція трафіку в локальних мережах не є проблемою для більшості користувачів, а вимоги до захисту реалізуються на рівні додатків, так що відділення одного користувача від іншого не є складним. Проте необхідність забезпечення QoS виникає досить часто, однак при постійному зниженні цін на комутатори для локальних мереж збільшення потужності пристроїв обійдеться дешевше, ніж впровадження MPLS для управління ними.

Корисною областю застосування MPLS в локальній мережі є відділення неінформаційного трафіку від трафіку даних, оскільки аудіо-та відео інформація може передаватися комутаторами MPLS з точністю, зіставною з результатами роботи за прямим з'єднанням.

Подальша побудова моделі мережі буде залежати від вибору дисципліни обслуговування навантаження і це відкриває нові можливості по оптимізації процесу заняття мережного ресурсу та забезпечення необхідних показників якості обслуговування навантаження. Вони полягають у наданні користувачам диференційованого обслуговування, в залежності від рівня сервісу, заявленого абонентом.

ЛІТЕРАТУРА

1. Воробієнко П.П. Телекоммунікаційні та інформаційні мережі:/ П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко підруч [для вищих навчальних закладів] – К: САММІТ-КНИГА, 2010. – 640 с.

2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы/Олифер В.Г, Олифер Н.А: Учебник для вузов. 3-е изд. – СПб.: Питер, 2008. – 958.

3. Захватов М. Построение виртуальных частных сетей (VPN) на базе технологии MPLS/Захватов М.: CiscoSystems, 2007, с. 4 – 18.

Фомін М.М. (ВІТІ ДУТ)
Музиченко В.А. (ВІТІ ДУТ)
Кривенко О.В. (ВІТІ ДУТ)

АВТОРИЗАЦІЯ КОРИСТУВАЧІВ В VPN

Захист інформації в процесі її передачі по відкритих каналах заснований на використанні віртуальних захищених мереж VPN (Virtual Private Network). Віртуальною захищеною мережею VPN називають об'єднання локальних мереж і окремих комп'ютерів через відкрите зовнішнє середовище передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку циркулюючих даних.

VPN є раціональним способом організації доступу окремого комп'ютера в локальну мережу компанії. Перевагою VPN є те, що рівень безпеки і анонімності мереж VPN залежить від того, яким чином вона реалізована і налаштована. Високого рівня конфіденційності можна домогтися за допомогою спеціального програмного забезпечення та правильної його реалізації. Тонкі налаштування мереж VPN дозволяють користувачам досягти повної анонімності в віртуальному просторі.Будується VPN на основі комплексу програмно-апаратних засобів (маршрутизатори Cisco з використанням L2F (Layer 2 Forwarding), L2TP(Layer 2 Forwarding Protocol), L2TPV3 (Layer 2 Forwarding Protocol version 3) або ж на основі суто програмного рішення (Microsoft – PPTP (Point-to-Point Tunneling Protocol),Check Software Technologies – VPN-1; програмний продукт з відкритим кодом Open VPN з ліцензією GNU GPL). Незначним недоліком, які має технологія VPN, є необхідність закупівлі невеликої кількості устаткування і програмного забезпечення, а також збільшення об'ємів зовнішнього трафіку. Втім, ці витрати досить невеликі і враховуючи величезну кількість переваг VPN, вони є цілком виправдані. Захист інформації в процесі її передачі по тунелю VPN заснована на виконанні наступних функцій:

– Автентифікації взаємодіючих сторін;

– Криптографічного закриття (шифрування) переданих даних;

– Перевірки автентичності та цілісності доставленої інформації.

Серед програмних засобів авторизації оптимальним для використання є протоколи TACACS +, який використовує протокол TCP, RADIUS, DIAMETR. Для входу в систему користувач має ввести секретний ключ, стійкість якого зумовлена його довжиною, наявністю великих і малих літер, а також інших символів ASCII.

Також використовується технологія біометричної авторизації, які включають відбитки пальців, рукописну підпис, відбитки голосу і знімки сітківки ока. З точки зору безпеки деякі форми біометричної ідентифікації вразливі при атаках повторного відтворення.

Серед програмно-апаратного методів можливе використання смарт-карт і маркерів для забезпечення додаткової умови для автентифікації і авторизації користувача. Смарт-карти і маркери мають властивість безпеки, яка робить їх автоматично непрацездатними після певної кількості невдалих спроб ввести правильний PIN.Застосовуючи PIN, маркер і біометричне дослідження, корпорація могла б досягти трьохфакторної автентифікації і авторизації. Комплексний підхід до забезпечення безпеки тобто використання програмних (протоколів) і апаратних методів у поєднанні з біометрією дозволяє забезпечити систему захисту від неавторизованих користувачів, що складається з трьох рівнів.

ЛІТЕРАТУРА

1. Осовецкий Л., Оценка защищенности сетей и систем \ Шевченко В. – Экс- пресс электроника. 2002. – 452с.

2. . Девянин П.Н Теоретические основы компьютерной безопасности \ Девянин П.Н – М.: Радио и Связь – 2000 – 403с.

3. Норткатт С. Анализ типовых нарушений безопасности в сетях. \ Норткатт С. – М.: Издательский дом „Вильямс", 2001 – 386с.

Хоменко І.А. (ВІТІ ДУТ)
к.т.н. Успенський О.А. (ВІТІ ДУТ)

СИНТАКСИЧНИЙ АНАЛІЗ ТА ЗБІР ІНФОРМАЦІЙНИХ РЕСУРСІВ ДЛЯ ВИКОРИСТАННЯ В ЗАДАЧАХ УПРАВЛІННЯ

Важливим видом діяльності людини є її робота з інформацією. Вона необхідна для навчання, роботи, написання статей, рефератів, контенту для веб-сайтів. Шукаючи дані, людина неминуче стикається з проблемою їх місцезнаходження. На сьогоднішній день, найоптимальнішим варіантом знайти інформацію, є всесвітня мережа Інтернет. Але при цьому доводиться вирішувати такі завдання:

1) Великі обсяги. В епоху бурхливого розвитку цифрових технологій та жорстокої конкуренції вже всім ясно, що успішна стаття чи веб-проект немислимі без розміщення унікальної інформації на сайті. Величезний обсяг даних, який заповнюють невпинно зростаючий інформаційний простір, набагато більше перевищує можливі межі дозволеного.

2) Часте оновлення. Обслуговування величезного потоку динамічно мінливої інформації не в силах забезпечити одна людина або навіть злагоджена команда операторів. Часом інформація змінюється щохвилини і в ручному режимі оновлювати її навряд чи доцільно, що дуже сповільнює її пошук.

3) Швидкість збору. Враховуючи щорічний прогрес та щораз якісну релевантність видачі пошукових систем заданими запитами, не завжди постає можливим збір тієї інформації, що необхідна людині.

Саме тому постає питання щодо створення такого програмного модулю, що враховує ці проблеми та являється ефективним у пошуку інформаційних ресурсів. Вирішенням даної задачі займаються програми – парсери.

Парсинг – процес аналізу або розбору певного контенту на складові за допомогою роботів-парсерів (спеціальних програм або скриптів). У SEO цим контентом є html-код сторінок сайтів. Найвідоміші парсери в мережі – це пошукові роботи, які аналізують сторінки, зберігають дані аналізу у себе в базі і потім при пошуку видають релевантні та актуальні документи. Часто парсинг плутають з граббінгом. Це близькі поняття, але все ж мають різні значення. У галузі пошукової оптимізації парсинг використовується дуже часто. Всі *SEO*-інструменти щось парсингують і на основі цього надають корисні дані для аналізу. Парсинг сайтів – послідовний синтаксичний аналіз інформації, розміщеної на інтернет-сторінках. Що представляє з себе текст інтернет-сторінок? Ієрархічність набір даних, структурований за допомогою людських і комп’ютерних мов. На людській мові надана інформація, знання, заради яких, власне, люди і користуються Інтернетом. Комп'ютерні мови (*html , JavaScript , css*) визначають як інформація виглядає на моніторі.

Які ж задач допоможе вирішити програма-парсер?

У порівнянні з людиною, комп’ютерна програма-парсер:

– швидкий обхід тисячі веб-сторінок;

– акуратне відокремлення необхідної інформації ;

– безпомилковий відбір потрібного ;

– перевірка синтаксичної коректності email-адреси;

– ефективна упаковка кінцевих даних в необхідному вигляді.

Таким чином, розробка даного модулю окрім перерахованих вище можливостей дозволить користувачеві швидко та зручно виконувати пошук, збір та аналіз необхідної йому інформації.

к.т.н. Хусаінов П.В. (ВІТІ ДУТ)
Жупанов О.П. (ВІТІ ДУТ)

ВИЯВЛЕННЯ СТАТИСТИЧНИХ ПАРАМЕТРІВ МЕРЕЖЕВОГО ТРАФІКУ

Сьогодні практично всі мережеві системи захисту інформації побудовані на основі двох архітектур: сигнатурної і поведінкової. Дані архітектури мають як переваги, так і недоліки. Так системи, побудовані з використанням сигнатур, в якості індикатора визначення порушень в мережі, не можуть виявляти порушення, незакладені в данні сигнатури, а поведінкові системи характеризуються частими помилковими спрацьовуваннями. Об'єктом аналізу, незалежно від архітектури, у систем захисту даного типу є мережевий трафік, тому що інформація як службова, так і передана в мережевих пакетах є джерелом всіх мережевих взаємодій. Визначено, що інформація про мережевий трафік має статистичний характер і являє собою тимчасові послідовності. Метод статистичного аналізу мережевого трафіку широко застосовуються в якості інструменту прогнозування завантаженості каналів зв'язку, визначення втрат, якості надання послуг і т.п.

Як клас статистичний аналіз відноситься до поведінкових методів визначення порушень в мережі і заснований на зіставленні поточного стану мережевої інфраструктури з якимись визначеними заздалегідь характеристиками, характеризує штатний режим функціонування мережевої інфраструктури. Метод статистичного аналізу має різні інтерпретації, засновані на динамічних характеристиках мережевого трафіку, проте базові принципи практично у всіх ідентичні. Незаперечною перевагою використання методу статистичного аналізу є можливість визначення вперше реалізовуваних методів негативного впливу на об'єкт атаки з боку зловмисника. Однак для його успішної реалізації необхідно визначити об'єкт аналізу, мати певні характеристики, що утворюють коректну конфігурацію, мати критерії, за яким можна визначити потенційну загрозу мережевої безпеки.

Статистичний метод універсальний, оскільки для проведення аналізу є необхідним лише знання про можливі атаки і використовувані ними вразливості, і вони засновані на змінах деяких статистичних характеристик потоку пакетів. Таким чином для вирішення завдання застосування статистичного методу аналізу *TCP*/*IP* трафіку, необхідно виділити основні показники, що характеризують штатний режим функціонування мережевої інфраструктури, і здійснювати динамічний контроль над їх станом. В якості таких показників повинна використовуватися інформація, за якою можна проаналізувати історію мережевої взаємодії. До даних, які можуть бути проаналізовані відносяться поля заголовків протоколів *IP*, *TCP*, *UDP*, *ICMP* і вміст полів даних. Для скорочення часу на обробку і подальше вилучення показників для аналізу, з усієї інформації необхідно виділити тільки службові її частини. Для визначення характеристик потоку мережевого трафіку, необхідно визначити взаємодіючі логічні сутності. Під логічною сутністю можуть виступати *IP*-адреси та порти відправника і одержувача пакетів. Таким чином, метод статистичного аналізу буде застосовуватися на визначеному часовому інтервалі для мережевих пакетів, що мають однакові статистичні сутності, що дозволить більш детально проаналізувати статистику мережевих взаємодій. Також для використання в граничній методиці замість кількості отриманих або відправлених пакетів будемо фіксувати довжину пакета. Це зрозуміло стандартом формування мережевих пакетів *RFC*, де кожен нефрагментований кадр має певну постійну величину, що зумовлює використання не кількісної характеристики по числу прийнятих або відправлених пакетів, а об'ємної за кількістю інформації, обробленої мережевим інтерфейсом.

Можна зробити висновок, що штатному режиму функціонування мережі відповідає відносно сталий рівень значення математичного очікування та дисперсії проаналізованих логічних сутностей. При виникненні нештатної ситуації аналогічні оцінки за різними характеристиками змінюються значно.

Чернишук С.В. (ЖВІ ДУТ)

АЛГОРИТМ ДИНАМІЧНОГО КОНФІГУРУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ ЗАГРОЗ ЗА РЕЗУЛЬТАТАМИ МОНІТОРИНГУ ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ

Існування нового класу загроз, які прийнято називати кібернетичними, зумовлює необхідність розробки адекватних засобів протидії, здатних ідентифікувати загрозу на етапі її зародження та раннього розвитку і попередити про небезпеку. Найбільш перспективним підходом у цьому напрямку є створення систем виявлення кібернетичних загроз (СВКЗ), які, як правило, аналізують технічні показники мережного трафіку або поведінки окремого вузла мережі та в подальшому визначають рівень невідповідності результатів аналізу деякому допустимому шаблону.

Разом з тим, наведене у [1] визначення кібернетичних загроз (КЗ) свідчить про наявність ознак таких загроз не лише у комунікаційному та комп'ютерно-мережному просторі, а й у інформаційному та соціотехнічному середовищі. Виникає необхідність розширення можливостей наявних СВКЗ або розробки нових систем, які б аналізували не тільки сигнали технічних систем, а й обробляли дані, що розміщуються на відкритих інформаційних ресурсах. З цією метою у [2] запропоновано методику структурно-параметричного синтезу СВКЗ за результатами моніторингу відкритих джерел інформації (ВДІ), яка дозволяє на етапі впровадження системи оптимальним чином розподілити виділені для формування такої системи АРМ за її компонентами. При цьому критерієм оптимальності виступає рівень відповідності можливостей АРМ визначеним частковим функціям компонентів системи.

Однак, на етапі експлуатації зазначеної системи відбувається динамічна зміна навантаження на її компоненти (зростання або зниження інтенсивності інформаційних потоків, пошукових завдань тощо). Це знижує ефективність виконання системою свого призначення через невідповідність її жорсткої структури динамічному характеру вирішуваних завдань і обумовлює необхідність перерозподілу АРМ із врахуванням поточного навантаження на компоненти системи. Для цього запропоновано алгоритм динамічного конфігурування СВКЗ за результатами моніторингу ВДІ, етапами якого передбачено: формування повного переліку можливих варіантів конфігурування системи із врахуванням вихідних даних і обмежень; перерахунок для усіх варіантів конфігурування узагальненого показника відповідності кожного АРМ призначенню компоненти із врахуванням зміни навантаження на відповідну компоненту; вибір оптимального варіанту конфігурування за мінімальним значенням цільової функції ефективності функціонування усієї системи.

Таким чином, з метою забезпечення ефективного виявлення КЗ за результатами моніторингу ВДІ на етапі експлуатації відповідної системи розроблено алгоритм її конфігурування, що враховує динамічну зміну навантаження на компоненти системи та дозволяє налаштувати СВКЗ для якнайкращого виконання системою свого призначення в умовах зростання (зниження) інтенсивності вирішуваних завдань.

ЛІТЕРАТУРА

1. Даник Ю. Г. Визначення сутності та змісту кібернетичної загрози / Ю. Г. Даник, В. І. Шестаков, С. В. Чернишук // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць ЖВІ НАУ. – Житомир, 2012. – С. 4 – 14.

2. Чернышук С. В. Структурно-параметрический синтез системы обнаружения киберугроз по результатам мониторинга открытых информационных ресурсов / С. В. Чернышук, В. І. Шестаков, А. А. Писарчук „Прикладная информатика". Научно-практический журнал. – М.: Московский финансово-промышленный университет „Синергия", – 2013. – № 2 (44). – С. 57 – 67.

Чмутов О.В. (ВІТІ ДУТ)
Шкіцький В.В. (ВІТІ ДУТ)

КОМПЛЕКСНИЙ ПІДХІД ДО ОРГАНІЗАЦІЇ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ В БЕЗДРОТОВИХ МЕРЕЖАХ

Найбільш поширеними та провідними технологіями безпровідної передачі даних є технології – *LTE*, *Wi-Fi* та *Wi-Max*.*LTE (Long Termal Evolution)* та *WiMax (Worldwide Interoperability for Microwave Access)* – стандарти бездротової передачі даних четвертого покоління *(4g)*. Особливістю яких є швидкість передачі даних до 326 Мбит/с на відстані до 25 кілометрів. Слід зазначити, що дані технології є конкуруючими. *Wi-Fi (Wirelless Firedly)* – бездротова технологія передачі даних третього покоління*(3g)*,з швидкістю до 0,1 Мбит/с на відстань, до 300 метрів. Проте гострим питанням застосування та впровадження даних безпровідних мереж, єпідхід дозахисту при передачі інформації. Розглянувши вищеперераховані технології бездротової передачі даних можна зазначити, що вони використовують досить різні підходи до забезпечення безпеки.Зосередимо увагу на особливостях забезпечення захисту даних в цих технологіях. Для безпеки передачі даних в мережах *LTE* використовується протокол аутентифікації *EAP* з 128 бітними ключами і розширена ієрархія *PKI*. Передбачені і нові функціональні можливості для нових сценаріїв, що включають міжмашинну взаємодію (*M2M*) і одноразову аутентифікацію (*SSO*). Крім того, передбачений захист від несанкціонованих з'єднань поверх мультимедійної *IP* – мережі, а також потокове шифрування. Ключовим моментом в схемі є те, що псевдовипадкова послідовність ніколи не повторюється. Алгоритми що використовуються,в мережах *LTE* відпрацьовують псевдовипадкову послідовність кінцевої довжини, за допомогою можливості прив’язки сім картки до нового центру реєстрації, а також генерації послідовності на основі отриманих даних, після перереєстрації. Така технологія дозволяє змінювати ключі доступу за декілька мілісекунд без втрати швидкості та порушень роботи мережі. Основними недолікомвиділимо те, що в деяких випадках, перереєстрація та отримання нового ключа призводить до помилки реєстрації та одержання некоректних даних. В технології *Wi-Max*використовується поняття захищеного зв’язку (для даних та авторизації). По перше, для даних первинний захищений зв’язок встановлюється абонентською станцією на час процесу ініціалізації, після чого базова станція надає канал захищеного зв’язку.Динамічно захищений зв’язок встановлюється та ліквідується по мірі необхідності для сервісних потоків. По друге, для авторизації абонентська станція та базова розділяють один потік захищеного зв’язку. В цьому випадку базова станція використовує захищений канал зв’язку для авторизації та конфігурування даних. *Wi-Max* використовує алгоритм *DES*в режимі зчеплення блоку шифрів для шифрування даних, але даний алгоритм не є крипостійким.Як недолік можна виділити те, що існує можливість використання псевдо-станцій для порушення роботи мережі. В технології *Wi-Fi*застосовуються методи захисту з використанням сертифікації бездротових пристроїв на базі протоколів *WEP, WPA*та*WPA2*. Цим, в даній технології забезпечений захист від прослуховування, перехоплення та перекручення даних, з метою захисту їх від противника. Як недолік можна зазначити те, що існують досить ефективні ташвидкі методи проведення атак на дані, що передаються в мережах *Wi-Fi*. Проаналізувавши переваги і недоліки даних технологій, можна прийти до висновку, що актуальним було б використання комплексного підходу, який буде враховувати всі переваги та недоліки способів захисту конкретних технологій. Отже, необхідне застосування комплексного підходу доорганізації безпеки при передачі даних за допомогою бездротових технологій, який використовує наступні механізми: коректної прив’язки до точки доступу; отримання оригінального та неповторюваного ключа, в короткий термін з високим рівнем складності шифрування; використання захищеного зв’язку ієрархічного типу, для розмежування захищених каналів на різному рівні та використання динамічно змінюваних ключів, під час сеансу передачі даних.

к.т.н. Чумак В.К. (ВІТІ ДУТ)
Ременчук В.І. (ВІТІ ДУТ)
Волкова Ю.О. (РТФ НТУУ „КПІ”)

НАПРЯМКИ ВДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ MIMO

Для сучасних систем радіозв’язку (СРЗ) особливо актуальною задачею є підвищення пропускної здатності. Одним з напрямків підвищення швидкості передачі інформації в системах радіозв’язку є застосування технології MIMO (Multiple Input Multiple Output – багато входів – багато виходів). Але таким системам притаманні свої проблеми.

В роботі проаналізовані задачі, які виникають при обробці сигналів в системах MIMO, Та розглянуто основні шляхи вдосконалення використання технології MIMO:

Наявність перехресних завад.

В системах MIMO перехресні завади призводять до зменшення пропускної здатності. Вплив перехресних завад на пропускну здатність MIMO систем вивчено недостатньо. В зв’язку з цим, дослідження залежності пропускної здатності MIMO систем від ступеню подавлення перехресних завад, є актуальним завданням

1. Необхідність вибору методу просторово-часового кодування та кількості приймальних та передавальних антен.

Необхідно встановити оптимальний баланс між енергетичним виграшем кодування (ЕВК), відносною швидкістю кодування та складністю реалізації вибраної схеми. При виборі того, або іншого коду проводиться оцінка ЕВК. В представлених моделях використовуються схеми з видами просторово-часового кодування STC (space time coding) та блочного коду Аламоуті, однак це не виключає можливості використання інших схем кодування.

Застосування технології MIMO дозволяє значно збільшити пропускну здатність при незмінній смузі частот, що виділена для роботи системи. Пропускна здатність системи MIMO суттєво залежить від кількості передавальних і приймальних антен.

2. Наявність міжстільникових завад при застосуванні технологи MIMO в стільникових системах радіозв’язку.

MIMO приймачі, які можуть значно послабити завади від сусідніх стільників, значно поліпшують ефективність роботи багатостільникової системи. При цьому основна увага с концентрована на подавленні завад від сусідніх стільників, а не внутрішньостільникових завад. Рівень внутрішньостільникових завад в 3G з CDMA не є істотним із-за використання ортогональних кодів при передачі від базової станції (БС) до мобільної станції (МС).

Розглянемо найбільш ефективні способи обробки сигналів в приймачі, які можуть бути використані для подавлення міжстільникових завад в системах 3G з MIMO .

1. Багатокористувачеве детектування з максимальною правдоподібністю.
2. Приймач з мінімальною середньоквадратичною помилкою.
3. Сукупне кодування.
4. Схеми рознесення MIMO з замкнутим ланцюгом зворотнього зв’язку.
5. Комбінація MIMO та діаграмоутворення.

Таким чином, при передачі і обробці сигналів в системах MIMO виникає ряд задач, основними з яких є компенсація впливу завмирань та різного роду завади, які діють в радіоканалах.

Перспективним напрямком вирішення цих задач є розробка методик вибору оптимальних параметрів сигналів та способів обробки сигналів в системі MIMO в залежності від конкретного стану радіоканалу.

ЛІТЕРАТУРА

1. Слюсар В. Системы MIMO: принципы построения и обработка сигналов / В. Слюсар // Электроника: Наука, Технология, Бизнес. – 2010. – № 8. – С. 52 – 58.

Шворов А.С. (в/ч К 1410)
Фесьоха В.В. (ВІТІ ДУТ)

ПАРАМЕТРИЧНИЙ МЕТОД ОБРОБКИ ВХІДНИХ ЕЛЕКТРОННИХ ДОКУМЕНТІВ В ІНФОРМАЦІЙНО-АНАЛІТИЧНІЙ СИСТЕМІ

В умовах постійно зростаючих обсягів вхідних електронних документів (ВЕД) та жорстких часових обмеженнях щодо їх обробки в інформаційно-аналітичній системі (ІАС), виникає необхідність у визначенні важливості ВЕД з метою їх першочергової обробки. Одним із напрямків вирішення даної задачі є автоматичне визначення важливості ВЕД у сучасних ІАС за допомогою спеціального параметричного методу обробки ВЕД.

Як правило, велика кількість факторів (параметрів) та різноманітність умов, від яких залежить важливість ВЕД та проявляється його специфічність, є основною складністю у вирішенні задачі оцінки важливості ВЕД. Дану задачу можна вирішити на основі використання інтегральних методів визначення важливості ВЕД. Труднощі щодо невизначеності і багатофакторності виникають як при оцінці кожного параметра, так і при згортці сукупності оцінок усіх параметрів вхідних документів в інтегральний (узагальнений) показник важливості ВЕД. Знаходження оцінки важливості ВЕД стикається зі значними розбіжностями у формуванні й інтерпретації комплексу інформативних параметрів і способів їх обробки. Аналіз комплексу таких інформативних параметрів показує наявність великої кількості різнорідних значень, що вимірюються в порядковій шкалі, шкалах інтервалів, відношень і абсолютній шкалі. Переважна більшість існуючих методів обробки ВЕД не пристосована для врахування різнорідності (різношкальності) значень виміряних параметрів.

Для вирішення задачі оцінки важливості ВЕД проаналізовані архітектура, принципи функціонування, алгоритми навчання та можливість використання нейронних мереж. Запропоновано бальний алгоритм оцінки важливості ключових слів електронного тексту за вхідними критеріями: щільність ключового слова документа; вага ключового слова ВЕД; частота ключового слова на сторінці; частота появи ключового слова в документі; коефіцієнти, що враховують розташування ключового слова; оформлення ключового слова: стиль, розмір шрифту, жирність шрифту, редизайн документа, поправочний коефіцієнт. Наведено методичні засади побудови цільової функції оптимізаційної задачі шляхом розкриття архітектури штучної нейронної мережі та виведення її аналітичного виразу з врахуванням значень вагових коефіцієнтів синтезованої та адекватно навченої нейромережі.

При визначенні важливості ВЕД забезпечується вирішення задачі класифікації, тобто віднесення ВЕД, що характеризується набором статистичних, функціональних та технічних показників, до шкали пріоритетної обробки ВЕД на основі застосування так званого нечіткого гібридного класифікатора. Такий класифікатор є системою, що об’єднує в структурному і функціональному відношеннях принципи нейронних мережних моделей і нечітку логіку обробки даних відповідно. Поставлена задача вирішується за допомогою 4-х прошаркової нейро-нечіткої мережі. Така нейро-нечітка мережа може бути класифікована як синхронна багатопрошаркова гетерогенна мережа з локальними зв’язками, але без зворотних зв’язків. Останнє дозволяє зняти питання про динамічну врівноваженість нейромережі, що є важливою перевагою наведеної структури.

Як показує практика, запропоноване рішення для оцінки важливості ВЕД із застосуванням нечіткого гібридного класифікатора, що покладено в основу параметричного методу обробки інформації, продемонструвало науково-практичну цінність розробленого методу, застосування якого забезпечує не менше як на 10 – 15% скорочення часових витрат на обробку першочергових (найбільш важливих за шкалою пріоритету) вхідних електронних документів в ІАС.

Шевченко В.С. (ВІТІ ДУТ)
к.т.н. Голь В.Д. (ВІТІ ДУТ)

ПОРІВНЮВАЛЬНИЙ АНАЛІЗ ПЕРСПЕКТИВНОСТІ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ

З великого різноманіття існуючих стандартів бездротовової передачі даних особливе місце займають технології WiMAX та LTE, це пов'язане з їх широкими можливостями та технічними перевагами. WiMAX (Worldwide Interoperability for Microwave Access) – стандарт безпровідного зв'язку, що забезпечує широкосмуговий зв'язок на значні відстані зі швидкістю, порівняною з кабельними з'єднаннями.

LTE (Long Term Evolution) – назва мобільного протоколу передачі даних; проект 3GPP, стандарт з вдосконалення UMTS для задоволення майбутніх потреб у швидкості.

Певною мірою ці два стандарти є конкуруючими, оскільки займають майже один сегмент телекомунікаційного ринку. В цих умовах цікавим та важливим є питання аналізу перспективності поширення та застосування зазначених стандартів, отже спробуємо їх порівняти.

WiMAX підходить для вирішення наступних завдань:

– З'єднання точок доступу Wi-Fi одна з одною та іншими сегментами Інтернету.

– Забезпечення бездротового широкосмугового доступу, як альтернативи виділеним лініям і DSL.

– Надання високошвидкісних сервісів передачі даних (до 3Мбіт/с) і телекомунікаційних послуг.

– Створення точок доступу, не прив'язаних до географічного положення.

WiMAX дозволяє здійснювати доступ в Інтернет на високих швидкостях, з набагато більшим покриттям, ніж у Wi-Fi мережі. Це дозволяє використовувати технологію в якості „магістральних каналів", продовженням яких виступають традиційні DSL і виділені лінії, а також локальні мережі. В результаті подібний підхід дозволяє створювати високошвидкісні мережі в масштабах цілих міст. Багато телекомунікаційних компаній роблять великі ставки на використання WiMAX для надання послуг високошвидкісного зв'язку. По-перше, технології сімейства 802.16 дозволяють економічно більш ефективно (у порівнянні з провідниковими технологіями) не тільки надавати доступ в мережу новим клієнтам, але й розширювати спектр послуг і охоплювати нові важкодоступні території. По-друге, бездротові технології для багатьох простіші у використанні, ніж традиційні дротові канали. WiMAX і Wi-Fi мережі прості в розгортанні і по мірі необхідності легко масштабуються. Цей фактор виявляється дуже корисним, коли необхідно розгорнути велику мережу в найкоротші терміни. В сумі всі ці переваги дозволять знизити ціни на надання послуг високошвидкісного доступу в Інтернет як для бізнес-структур, так і для приватних осіб.

Для операторів зв'язку технологія LTE має наступні переваги:

– зменшення капітальних і операційних затрат і, як наслідок, підвищення доходів від надання послуг передачі даних;

– зниження сукупної вартості володіння мережею;

– розширення своїх можливостей в області конвергенції (зближення) послуг і технологій;

– можливість одночасної роботи значної кількості активних користувачів в кожній соті.

Сьогодні LTE є найбільш сучасною технологією в сегменті мобільної передачі даних, яка доповнює цілий ряд попередніх стандартів. Першим з яких був сервіс GPRS, він вперше забезпечив безперервну передачу даних, яка теоретично могла досягати 171,2 кбіт/с. Наступним кроком на етапі переходу від покоління 2G до 3G був стандарт EDGE, який дозволяв операторам мереж GSM, не вкладаючи серйозних грошей в модернізацію обладнання, в два рази збільшити швидкість передачі. Далі був стандарт IMT-2000, який

затвердив специфікації „справжнього” 3G. Технологія LTE вважається технологією четвертого покоління бездротових мереж, в якої 100% пропускної здатності використовується для послуг передачі даних, а передача голосу здійснюється у вигляді VoIP. Теоретично значення швидкості знаходиться на рівні 100 Мбіт/с, крім того технологія LTE суттєво відрізняються від класичних стандартів 3G, що дозволяє говорити про зміну поколінь – перехід до мереж, називають їх 4G.

Часто стандарт LTE вважають конкурентом WiMAX, хоча багато операторів вважають LTE більш перспективним і довготривалим стандартом із вищим потенціалом розвитку. Проте як вважають аналітики, ці стандарти будуть розвиватися паралельно.

Порівняння характеристик технологій WiMAX та LTE наведене в табл. 1.

Таблиця 1

		WiMAX	**LTE**
Максимальна швидкість передачі даних	Download	289 Мбіт/с	300 Мбіт/с
	Upload	69,1 Мбіт/с	75 Мбіт/с
Максимальне значення спектральної ефективності [біт/с/Гц]	Download	3,75	15
	Upload	2,8	3,75
Робочий діапазон		1,5-11 ГГц	700 МГц - 2,7 ГГц
Радіус дії		25-80 км	30-100 км
Кількість абонентів		приблизно 4 млн.	приблизно 30 млн.

Враховуючи всі ці аспекти, можна зробити висновок, що створена на практиці мережа LTE стане абсолютно новою в своїй сфері, буде мати велику кількість переваг перед своїми конкурентами, в неї буде перспектива стати загальновизнаною національною мережею та принести значний прибуток. Не беручи до уваги технічні характеристики даних систем, можна вважати, що для створення покриття великих територій доцільніше використовувати саме LTE, оскільки розгортання всеукраїнської мережі WiMAX є занадто дорогим. Проте, у великих містах та густозаселених регіонах мережі WiMAX можливо використовувати для доступу до мережі Інтернет.

Отже, якщо подивитися на те, що відбувається в галузі телекомунікаційних систем, можна впевнено сказати – майбутнє за LTE. Більшість найбільших мобільних операторів вибрали цей стандарт для переходу до технології наступного покоління мобільного зв’язку 4G. Хоча свого часу, коли з’явилася технологія WiMAX, багато фахівців вважали, що розвиток мобільного зв’язку може піти цим шляхом розвитку і прирівнювали WiMAX до технологій 4G. Слід зазначити, що WiMAX зароджувався як розвиток технологій бездротового фіксованого доступу, і на першому етапі відповідні стандарти регламентували тільки фіксований доступ і доступ з обмеженою мобільністю. А ось технологія LTE спочатку проектувалася як розвиток технологій мобільного зв’язку та була орієнтована на повнофункціональну підтримку мобільності. В даний час у WiMAX – рішення застосовуються переважно в якості рішень так званого бездротового DSL, його цільова спрямованість – бездротовий фіксований зв’язок, у той час як LTE, надає повнофункціональну мобільність .

ЛІТЕРАТУРА:

1. Скляр Б. Цифровий зв’язок. Теоретичні основи і практичне застосування / Пер. з англ. – М.: Видавничий дім „Вільямс”, 2003.

2. Тихвинский В.О. Сети мобильной связи LTE: технологии и архитектура. Тихвинский В.О., Терентьев С.В., Юрчук // М.: Эко-Трендз, 2010.

3. Resource allocation in multiuser multicarrier wireless systems with applications to LTE / W. Freitas, R. Lima, R. Santos, F. Cavalcanti // Optimizing wireless communication systems. – Springer, 2009.

Шевченко А. С. (ВІТІ ДУТ)
к.т.н. Кокотов О. В. (ВІТІ ДУТ)

МЕТОД ОЦІНЮВАННЯ РИЗИКІВ З УРАХУВАННЯМ ЗНИЖЕННЯ ПАРАМЕТРІВ СПЕЦІАЛЬНИХ БЕЗПРОВОДОВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ В УМОВАХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Застосування безпроводових інформаційно-телекомунікаційних систем (БІТС) спеціального призначення під час інформаційних операцій пов'язано з великою кількістю ризиків отримання збитку внаслідок реалізації атак на критичну інформацію, яка передається через радіоканали. В бойовій обстановці необхідно швидко приймати рішення та застосовувати механізми захисту інформації (МЗІ), які перекриють вразливості БІТС. Результатом застосування МЗІ може стати не лише підвищення рівня захищеності, а і зниження параметрів БІТС: перепускної здатності, швидкості передачі, дальності зв'язку, часу передачі повідомлення, що в свою чергу, в умовах бойових дій вплине на доступність інформації, а відповідно на загальний рівень ризику.

На сьогоднішній час існує велика кількість методів оцінювання ризиків, таких як: OCTAVE, CRAMM, Risk Watch, COBRA, RA2 тощо, які реалізують схожі етапи при оцінюванні ризиків, але жодний з них не враховує вплив МЗІ на зниження параметрів системи. В результаті, актуальним є розгляд впливу захисних функцій системи захисту інформації (СЗІ) БІТС, які функціонують в критичних умовах інформаційних операцій, при зміні МЗІ для забезпечення необхідного рівня захищеності інформації.

Для оцінювання загального рівня ризику пропонується застосування методу в основі якого лежить розрахунок функції ризику з врахуванням відносного зниження параметрів БІТС, внаслідок використання необхідних МЗІ:

$$R = P_{\text{зб}} \cdot Z + \sum_i L_i \,,$$

де $P_{\text{зб}}$ – імовірність отримання збитку внаслідок успішної реалізації атаки противника, Z – величина збитку від реалізованої загрози, L_i – показник обмеження i-го параметра системи в результаті застосування МЗІ, i – порядковий номер параметра БІТС.

Показник зниження параметра БІТС є відносним значенням значення параметра при застосування відповідного МЗІ до параметра БІТС без застосування МЗІ.

На основі представленого виразу оцінювання рівня ризику БІТС, з використання початкових даних інформаційного конфлікту, що представлений в роботі [1], було проведено моделювання зміни рівня ризику внаслідок зменшення швидкості передачі інформації УКХ радіостанцією при використанні завадозахищеного режиму в різних умовах завад. Результати моделювання показали, що при постійній інтенсивності атак придушення радіолінії, рівень ризику БІТС прямопропорційно змінюється відповідно до зміни параметра БІТС – швидкості передачі.

Метод оцінювання ризиків з урахуванням зниження параметрів спеціальних БІТС, дозволяє враховувати вплив зниження параметрів БІТС: перепускної здатності, швидкості передачі, дальності зв'язку, часу передачі повідомлення, внаслідок оперативної зміни МЗІ під час інформаційних операцій. Представлений метод, може застосовуватись під час проектування СЗІ для БІТС спеціального призначення та дозволить досягти рівноваги між такими показниками системи, як продуктивність та захищеність. Крім того, метод оцінювання ризиків з урахуванням зниження параметрів БІТС може бути використаний для оцінювання ефективності МЗІ.

ЛІТЕРАТУРА

1. Шевченко А. С. Модель процесу придушення радіоліній безпроводових інформаційно-телекомунікаційних систем під час інформаційної боротьби / А. С. Шевченко, О. Є. Мазулевський // Сучасний захист інформації. – 2012. – № 4. – С. 35 – 40.

Шолудько В.Г. (ВІТІ ДУТ)

НАПРЯМКИ РОЗВИТКУ ПОЛЬОВОЇ КОМПОНЕНТИ СИСТЕМИ ЗВ'ЯЗКУ ТА АВТОМАТИЗАЦІЇ ЗБРОЙНИХ СИЛ УКРАЇНИ

Система зв'язку Збройних Сил України – є важливою складовою системи управління Збройними Силами, яка забезпечує керівництво військами (силами) у мирний час та особливий період. Вона має стаціонарну (на базі стаціонарних захищених та незахищених пунктів управління) і польову (на базі рухомих, повітряних та морських пунктів управління) компоненти. Основу системи зв'язку складають інформаційно-телекомунікаційні вузли Збройних Сил, які оснащені радіо-, проводовими, тропосферними, радіорелейними та супутниковими системами.

Метою розвитку системи зв'язку ЗС України є створення в найкоротші терміни взаємопов'язаної інформаційно-телекомунікаційної інфраструктури та забезпечення відповідності вимогам управління ЗСУ в нових умовах військово-політичної обстановки у світі. Планується переоснастити на цифрові засоби стаціонарний компонент системи зв'язку та розпочати переоснащення її польового компонента, розгорнути систему захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах, створити інтегровану систему супутникового зв'язку Збройних Сил як підсистему Національної системи супутникового зв'язку України та автоматизовану систему радіозв'язку.

Отже, в якості шляхів розвитку польової компоненти системи зв'язку та автоматизації Збройних Сил України можливо визначити наступні:

впровадження єдиного типу IP засекреченого зв'язку по всім родам зв'язку;

забезпечення сумісності зі стаціонарною телекомунікаційною мережею;

використання самоналагоджувальних мереж та впровадження IP-технологій в польовій опорній мережі зв'язку Збройних Сил України в оперативній і тактичній ланках управління;

зменшення кількості апаратних зв'язку в вузлі зв'язку пунктів управління ЗС України за рахунок впровадження комплексних апаратних зв'язку;

модернізація засобів радіо, радіорелейного, тропосферного та супутникового зв'язку на лініях прямого зв'язку;

використання комплексних апаратних зв'язку доступу інформаційно-телекомунікаційних вузлів та самоналагоджувальних мереж в якості ліній прив'язки.

Основними елементами польової компоненти системи зв'язку є інформаційно-телекомунікаційні вузли рухомих пунктів управління з відповідними лініями прив'язки та польова опорна мережа зв'язку, що розгорнута проводовими, радіорелейними та тропосферними засобами.

В основу переоснащення польової компоненти системи зв'язку покладено:

поетапне переоснащення на цифрові засоби польові інформаційно-телекомунікаційні вузли рухомих пунктів управління стратегічної, оперативної та тактичної ланок;

переоснащення новітніми цифровими радіорелейними та тропосферними засобами зв'язку лінійних підрозділів зв'язку стратегічної та оперативної ланок управління;

забезпечення сумісності польової та стаціонарної компонент системи зв'язку Збройних Сил України шляхом використання ідентичних за можливостями телекомунікаційних та інформаційних систем та апаратно-програмних комплексів;

забезпечення можливості управління військами Збройних Сил України без використання стаціонарної компоненти системи зв'язку Збройних Сил України на двох оперативних напрямках;

створення технічних умов щодо спроможності польової компоненти системи зв'язку забезпечення обміну розвідувальною інформацією в оперативній та тактичній ланках управління в т.ч. з безпілотними літаючими апаратами.

В даний час можна виділити наступні основні напрямки розробок перспективних комплексів, засобів зв'язку та автоматизації управління:

розширення функціональних можливостей засобів зв'язку та автоматизації управління;

вдосконалення архітектури автоматизованої системи управління для реалізації принципів розподіленої обробки даних та її узгодження із загальною структурою управління військами;

стандартизація та уніфікація обладнання, інформаційного та програмного забезпечення;

істотне розширення спектру послуг служб зв'язку, особливо з передачі мультимедійної інформації;

використання нових способів цифрової обробки сигналів і методів завадозахищеності.

Переоснащення польової компоненти системи зв'язку передбачається здійснювати через закупівлю польових засобів зв'язку прийнятих на озброєння та переобладнанням силами ремонтних баз (майстерень) зв'язку апаратних (станцій) виробництва СРСР цифровими засобами зв'язку, які також прийнято на озброєння (постачання) або подвійного використання. На сьогоднішній день сучасні телекомунікаційні технології дозволяють командиру будь-якого рівня:

своєчасно отримати всю необхідну інформацію, в тому числі і розвідувальну, інформацію про противника, необхідну для прийняття рішення;

спільно з іншими посадовими особами штабу розробити спільне рішення;

своєчасно і достовірно видати наказ на управління підпорядкованими силами і засобами;

контролювати дії штатного складу і керувати своїми підлеглими в процесі ведення бойових дій.

Враховуючи такий підхід у польовій компоненті системи зв'язку ЗС України буде переоснащено на цифрові засоби 31 інформаційно-телекомунікаційний вузол рухомих пунктів управління, що складає від потреби: 70% – стратегічної, 20% – оперативної та 10% – тактичної ланок управління, та при цьому буде забезпечена мінімально необхідна укомплектованість лінійних частин, яка дозволить будувати переважно цифрову польову опорну мережу, можливість надання послуг цифрового зв'язку в усіх ланках управління, 100% резервування стаціонарної мережі зв'язку. Оснащення польових інформаційно-телекомунікаційних вузлів пунктів управління надасть можливість забезпечити оперативний склад усіх ланок управління якісними послугами зв'язку аналогічно з тими, які надаються на стаціонарних пунктах управління (відкриті та закриті голос, дані, відео). Це дасть можливість побудувати цифрову польову опорну мережу зв'язку в стратегічній ланці управління на двох оперативних напрямках, яка буде резервуватися стаціонарною компонентою.

Таким чином, основні напрями розвитку військової системи зв'язку, принципи оптимізації складу і оснащення військ зв'язку новими засобами, реалізація вироблених напрямів застосування передових технічних рішень і нових телекомунікаційних технологій у виробництві засобів і комплексів зв'язку дозволять керівництву ЗС України в реальному часі реагувати на зміни оперативно-стратегічної обстановки, своєчасно і з необхідною достовірністю доводити накази на застосування Збройних Сил України та забезпечити ефективне управління угрупованнями військ (сил), а також взаємодіяти з іншими військовими формуваннями держави

ЛІТЕРАТУРА

1. Стратегічний оборонний бюлетень України, 2012 року.

2. Концепція реформування і розвитку Збройних Сил України на період до 2017 року.

3. Щорічне видання "Біла книга-2012. Збройні Сили України", 2012 року.

4. Замисел переоснащення системи зв'язку Збройних Сил України цифровими засобами в період 2013 – 2017 років та шляхи його реалізації.

Шпак В.В. (ВІТІ ДУТ)
к.т.н. Хусаінов П.В. (ВІТІ ДУТ)

ЗАДАЧА АНАЛІЗУ МАСИВІВ РЕЄСТРАЦІЙНИХ ДАНИХ ПРО МЕРЕЖЕВИЙ ТРАФІК

Останнім часом спостерігається швидке впровадження сучасних інформаційних систем, які щодня генерують великі масиви даних. Такі темпи призводять до надшвидкого зростання об'ємів накопиченої інформації, що стосується інформаційних процесів, які відбуваються в системі. У зв'язку з цим, останнім часом спостерігається велике збільшення кількості кібернетичних інцидентів, що призводять до значних збитків. Тому доцільно розглянути відповідні способи та методи обробки великих об'ємів накопичених даних, з метою виявлення потенційно можливих нав'язувань кібернетичного впливу.

На сьогодні існує багато систем моніторингу комп'ютерних систем і мереж:

– PRTG (*Paessler Router Traffic Grapher*) – програмний засіб збору інформації про потоки даних та навантаження на окремі вузли мережі;

– Nagios (nagios) – програмний комплекс моніторингу, призначена для спостереження, контролю стану обчислювальних вузлів і служб, оповіщення адміністратора, якщо якісь із служб припиняють (або відновлюють) свою роботу;

– ZABBIX – система моніторингу і відстеження статусу різноманітних мережевих сервісів комп'ютерної мережі, серверів і мережевого устаткування.

Результати діяльності даних систем, як правило зберігаються у вигляді журнальних файлів великого об'єму. Для швидкої обробки та аналізу яких, доцільно використовувати кластерні системи, які є видом розподілених систем обробки диних.

Кластер – це декілька незалежних обчислювальних машин, що використовуються спільно і працюють як одна система для вирішення певних задач. Обчислювальний кластер потрібен для збільшення швидкості обрахунків за допомогою паралельних обчислень.

Однією із сфер застосування розподіленої обробки даних із використанням кластерних систем, є забезпечення кібернетичної безпеки та протидія спробам реалізації кібернетичних загроз. Кожну систему можливо представити як велику кількість об'єктів та зв'язків між ними. Якщо порівнювати стани системи в кожен момент часу, то можливо відстежити незвичний стан, що може бути причиною кібернетичних впливів. Як наслідок, виникає необхідність моніторингу та аналізу подій кібернетичної безпеки. При цьому необхідно враховувати, що дані системи накопичують великі масиви даних. Процес обробки та аналізу таких об'ємів інформації повинен відбуватися за достатньо невеликі проміжки часу, щоб отримані результати були актуальними по часу.

При цьому необхідно вирішити наступні завдання:

– розподіл задач між вузлами кластеру;

– визначення навантаження на окремих вузлах кластерної системи;

– визначення методів обробки великих масивів даних мережевого трафіку у кластерному середовищі для ефективної обробки великих масивів даних;

Отриману інформацію можливо аналізувати за допомогою кластерної технології Apache Hadoop, яка дозволяє розподілити навантаження при обробці даних з одного високо потужного обчислювального серверу по вузлам кластеру, тим самим скорочуючи час на обробку даних. Даний підхід дозволяє за відносно малий час проаналізувати великі масиви даних та отримати відповідні результати при моніторингу подій кібернетичної безпеки.

Таким чином, проаналізувавши методи забезпечення кібернетичної безпеки, планується створення програмного комплексу аналізу масивів реєстраційних даних про мережевий трафік. Задачею данного комплесу є аналіз даних отриманих при моніторингу мережевої активності та виявлення відхилень інформаційної системи від нормального стану, що може стати причиною кібернетичних інцидентів.

Штепа О.М. (ВІТІ ДУТ)
Осиченко О.Б. (ВІТІ ДУТ)

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ АТАК ЗА РАХУНОК ВПРОВАДЖЕННЯ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Проблема захисту ресурсів інформаційно-комунікаційних систем та мереж, стає ще більш актуальною у зв'язку з розвитком і поширенням глобальних обчислювальних мереж, територіально розподілених інформаційних комплексів та систем з віддаленим управлінням доступом до інформаційних ресурсів.

Вагомим аргументом для підвищення уваги до питань безпеки є бурхливий розвиток програмно-апаратних методів та засобів, здатних потай існувати в системі і здійснювати потенційні несанкціоновані дії (процеси), що перешкоджає нормальній роботі користувача та самої системи, що як наслідок безпосередньо завдає шкоди властивостям інформації (конфіденційності, доступності, цілісності).

Для своєчасного виявлення та запобігання атакам розроблено досить велику кількість програмних засобів систем виявлення атак (СВА). У загальному випадку СВА використовують три широко відомі методи для розпізнавання атак:

– сигнатурний метод, заснований на використанні шаблонів сигнатур (*pattern-based signatures*);

– сигнатурний метод, заснований на контролі частоти подій або перевищенні граничної величини;

– виявлення аномалій.

Поряд з описаними методами існує ряд інших, що в сукупності дозволяють більш точніше та ефективніше виявити будь-які втручання в комп'ютерну систему та своєчасно запобігти деструктивній дії комп'ютерної атаки. Всі методи порівнюються за наступними критеріями: 1) рівень нагляду за системою; 2) верифікованість методу; 3) адаптивність; 4) стійкість; 5) розрахункова складність.

Загальним недоліком існуючих методів розпізнавання атак є не адаптивність до виявлення модифікованих загроз, чи появі нових атак, не можливість виявлення аномалій системи для виявлення модифікованої атаки, а також низька стійкість та верифікація. Одним із найбільш перспективних шляхів, який міг би врахувати усі із перелічених критеріїв – це створення експертної системи, яка б в якості своїх підсистем описаних для функціонування системи у вигляді множини фактів та правил бази знань. На вхід експертна система отримує дані про спостереження за подіями в системі у вигляді фактів. На основі цих фактів робиться висновок про наявність чи відсутність атаки. Експертні системи вимагають постійного оновлення бази знань про атаки описами нових загроз. Головний недолік подібних систем – висока обчислювальна складність, зокрема при виявленні аномалій.

На основі аналізу літератури приходимо до висновку, що на сьогоднішній день не існує системи виявлення атак, яка б мала адаптивність до невідомих атак, а також не побудовано ефективного представлення бази знань про атаки, яке б дозволило отримувати опис можливих нових загроз на основі опису відомих атак. Для рішення даної проблеми, а саме підвищення ефективності функціонування системи виявлення атак, необхідно розробити базу знань з описами можливих атак, їх модифікацій чи можливих варіантів їх змін, яка б працювала в основі системи підтримки прийняття рішень та дозволяла передчасно, з точною ймовірністю виявляти, запобігати чи анулювати деструктивну дію комп'ютерної атаки. А з шляхом використання СППР – давала б оператору зручний інтерфейс доступу, варіанти дій та можливість оперативного реагування у разі виявлення несанкціонованого доступу, з метою запобігання порушення цілісності комп'ютерних систем чи інформації.

к.т.н. Явіся В.С. (ВІТІ ДУТ)
Вакуленко О.В. (ВІТІ ДУТ)

ОЦІНКА ШВИДКОСТІ АБОНЕНТСЬКОГО ДОСТУПУ У МЕРЕЖАХ LTE

LTE (Long Term Evolution – довгострокова еволюція) – багатообіцяюча технологія високошвидкісного мобільного доступу в Інтернет. Теоретичною швидкісною межею є 326,4 Мбіт/с у спадаючому напрямку (від базової станції до абонента) і 172,8 Мбіт/с – у висхідному (від абонента до базової станції). Американський стільниковий оператор Verizon Wireless, протестувавши реальну мережу LTE, одержав 40-50 Мбіт/с у спадаючому й 20- 25 Мбіт/с – у висхідному каналі. Російська компанія „Скартел" заявила про трохи інші результати: максимальна швидкість 20 Мбіт/с у спадаючому напрямку й 9 Мбіт/с – у висхідному [1].

Для оцінки швидкостей, які може забезпечити технологія LTE у спадаючому й висхідному каналах, важливо брати до уваги кілька важливих параметрів: метод дуплексування каналів, наявний діапазон частот, вид модуляції піднесучих, метод завадостійкого кодування даних, використання технологій MIMO (Multiple Inputmultiple Output), витрати ресурсів на управління, тривалість циклічних префіксів та ін.

Принципово новим розв'язком для радіо інтерфейсу LTE стало використання нових методів множинного доступу – OFDMA у спадаючому каналі (Orthogonal Frequency Division Multiple Access) і SC-FDMA (Single Carrier Frequency Division Multiple Access) – у висхідному. Важливо, що весь наявний спектр розбивається на ортогональні піднесучі по 15 кГц (у спадаючому каналу), кожна з яких, у свою чергу, модулюється певним видом модуляції (від QPSK до QAM64). Мінімальна смуга, що виділяється для одного абонента – 12 піднесучих. Очевидно, що використання багатопозиційних методів модуляції вимагає каналів з високим рівнем відношення сигнал/шум, погіршення ж радіо умов приведе до зниження порядку модуляції, а відповідно й швидкості передачі даних.

Таким чином, при поганих радіоумовах максимальні швидкості передачі даних у спадаючому каналі можна розділити на 3 (при QPSK одночасно передаються 2 біта інформації, при QAM64 – 6 біт). Крім порядку модуляції важливо брати до уваги й схему завадостійкого кодування. Наприклад, кодування зі швидкістю 1/2 ще у два рази знижує швидкості передачі даних.

Найважливішою особливістю мереж LTE є масштабованість займаного ними частотного спектра від 1,4 до 20 Мгц. Очевидно, що чім ширша смуга, тим більше будуть швидкості.

Мінімальною одиницею надання доступу одному користувачеві є ресурсний блок (їх кількість становить від 6 до 100 залежно від наявного спектру) – це 12 піднесучих у частотній області й один тайм-слот, або 7 OFDM-символів у часовій області тривалістю 0,5 мс. Піднесучі по краях спектра, як правило, використовуються в якості захисних інтервалів.

Немаловажним фактором при оцінці можливостей LTE є застосування технології MIMO. Існують кілька варіантів застосування MIMO. Для збільшення абонентської ємності, при цьому з різних антен передається різна інформація. У цьому випадку використання MIMO 2x2 (NMIMO = 2 – порядок MIMO) приведе до збільшення швидкості передачі даних у спадаючому каналі вдвічі. Однак реалізація такої схеми зажадає додаткові частотно-часові ресурси для передачі опорних пілот-сигналів антен.

Інформація, передана на радіо інтерфейсі, ділиться на службову інформацію, яка транслюється по різних каналах управління, і на дані користувача каналу PDSCH (Physical Downlink Shared Channel). Оскільки більшість операторів, що запустили LTE, мають спарені смуги частот для висхідного й спадаючого потоків, то розглянемо особливості саме FDD-режиму, структуру його сигналу й співвідношення між службовими ресурсами та ресурсами користувача.

Для того щоб оцінити швидкості передачі даних у спадаючому каналі, спочатку оцінимо, скільки ресурсних елементів (або OFDM-символів) передається в часовому інтервалі, що дорівнює 1 мс, залежно від наявної смуги частот.

В одному субкадрі (два тайм-слоти) на одній піднесучій передається 14 OFDM-символів. Таким чином, число OFDM-символів буде дорівнювати: 14·12=168 (12 – число, піднесучих у ресурсному блоці). Далі із загального числа символів, необхідно відняти число символів, виділених під канали управління. Коли використовується FDD-режим, 49 OFDM-символів зайняті службовою інформацією – 29% частотно-часового ресурсу [2]. У такий спосіб усього 168-49=119 символів використовуються для передачі даних користувача.

Інформаційні символи, що залишилися, необхідно домножити на кількість біт, які вони можуть містити. Число біт у символі буде визначатися способом модуляції під несучих – 2, 4 і 6 біт відповідно для QPSK, QAM16 і QAM64.

Далі необхідно врахувати вплив завадостійкого кодування. Як правило половина від отриманого числа біт піде на надмірність.

Використання MIMO збільшує швидкість у кратне число раз. Це самі основні особливості, які необхідно враховувати при оцінці швидкості.

Виконавши подібні розрахунки, нескладно одержати швидкості передачі даних у спадаючому каналі.

Для того, щоб у спадаючому каналі LTE була швидкість, зазначена в [3] – 326,4 Мбіт/с, необхідно:

– режим дуплексування: FDD;

– смуга: 20 Мгц;

– модуляція: QAM64;

– завадостійке кодування: відсутне;

– MIMO: 4x4.

Витрати ресурсів на службові канали й передачу циклічних префіксів: не враховуються (при їхньому обліку швидкість би знизилася залежно від інтенсивності навантаження на 20 – 60 Мбіт/с) [2].

Реальна швидкість доступу для мобільних абонентів у спадаючому каналі, з урахуванням складності технічної реалізації MIMO, при поганих умовах приймання (використовується QPSK) і смузі 1,4 МГц складе від 119·2:2·1000=119 кбіт/с до 357 кбіт/с залежно від числа користувачів, а при максимальній смузі частот 20 МГц і ідеальних умовах приймання (використовується QAM64) – від 119·6:2·1000=357 кбіт/с до 17,85 Мбіт/с. Швидкість доступу у висхідному каналі буде ще меншою від зазначених.

Таким чином, при впровадженні та застосуванні технології LTE, заявлена швидкість безпроводового доступу для користувачів може бути меншою, ніж та що очікується.

ЛІТЕРАТУРА

1. www.lenta.ru/news/2011/12/20/yota.

2. Дроздова В.Г., Белов М.А.Оценка пропускной способности сетей LTE. // Мобильные телекоммуникации. – 2012. – №5. – С. 20 – 22.

3. www.ru.wikipedia.org/wiki/3GPP_Long_Term_Evolution.

к.т.н. Явіся В.С. (ВІТІ ДУТ)
Вакуленко О.В. (ВІТІ ДУТ)
Радзівілов Д.Г. (ВІТІ ДУТ)

МЕТОДИКА ВИБОРУ МЕТОДА ВИСОКОШВИДКІСНОГО ДОСТУПУ ДО ВІДОМЧОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ЗА КРИТЕРІЄМ МІНІМАЛЬНОЇ ВАРТОСТІ

У сучасних системах зв'язку в наслідок розширення переліку послуг, що надаються користувачам, існує необхідність підвищення швидкості доступу до мережних ресурсів, як правило в умовах обмеженого бюджету. Запропонована методика дозволяє досягти спрощення процедури вибору метода доступу до мережі.

Визначення необхідної швидкості доступу до мережі. Мережі за пропускною спроможністю можна поділити на низькошвидкісні, середньошвидкісні та високошвидкісні. Тому для того, щоб визначитись зі швидкістю доступу до мережі треба знати пропускну спроможність транспортної мережі та вимоги користувача до мережних послуг. Методика передбачає розгалуження за швидкістю доступу на середньошвидкісні (до 100 Мбіт/с) та високошвидкісні (більше 100 Мбіт/с). Кожній гілці відповідають свої технології.

Селекція методу за швидкістю здійснюється відповідно до необхідної швидкості із загального переліку методів доступу, зведених у таблицю. Також враховується відстань між кінцевим абонентським та мережним обладнанням. На цьому етапі відбувається відбір декількох методів доступу, які задовольняють користувача за швидкістю доступу.

Вибір та розрахунок обладнання. Кожна технологія вимагає застосування різного обладнання для забезпечення доступу, тому потрібно здійснити аналіз можливого варіанту побудови мережі доступу відповідно до обраної технологій (елементи мережі доступу, кінцеве обладнання, довжина та тип кабелю, якщо він потрібен).

При виборі обладнання в загальному випадку слід враховувати такі фактори:

рівень стандартизації обладнання та його сумісність з відповідними програмними засобами та обладнанням, що використовується у мережі;

швидкість передачі інформації у мережі;

дозволені типи кабелів мережі, максимальну його довжину, захищеність від завад;

вартість та технічні характеристики обладнання.

Оцінка фінансових витрат, вона включає в себе вартість обладнання, кабелю, їх монтажу, технічного обслуговування, оренди обладнання та (або) приміщень, експлуатаційні витрати (в тому числі за користування частотним ресурсом – для безпроводових технологій). В якості кінцевого результату пропонується використовувати показник С, що являє собою вартість забезпечення швидкості доступу 1 Мбіт/с:

$$C=S/V_д$$

де S – загальна вартість організації доступу, яка отримана при оцінці фінансових витрат; Vд – швидкість доступу.

Необхідно враховувати, що кожний постачальник диктує свою ціну на обладнання, як правило у залежності від його надійності та відповідності заявленим характеристикам.

Вибір методу високошвидкісного доступу до відомчої телекомунікаційної мережі за критерієм мінімальної вартості здійснюється за показником С, що розраховується для переліку методів доступу, обраних на етапі селекції за швидкістю. В результаті обирається метод, для якого показник С приймає найменше значення.

ЛІТЕРАТУРА

1. Аджемов С.С., Урядников Ю.Ф. Технологии широкополосного доступа: динамика и перспективы развития. // Электросвязь. – 2011. – № 1. – С. 19 – 23.

2. Гольдштейн Б.С. Протоколы сети доступа. Том 2. 3-е издание – СПб.: БХВ – Санкт-Петербург, 2005. – 288 с.

к.т.н. Якорнов Є.А. (ІТС НТУУ „КПІ”)
Авдєєнко Г.Л. (ІТС НТУУ „КПІ”)
Чижевська А.В. (ІТС НТУУ „КПІ”)
Бранчук В.М. (ІТС НТУУ „КПІ”)

ПРОСТОРОВА ОБРОБКА СИГНАЛІВ ЯК ЗАСІБ ПОВТОРНОГО ВИКОРИСТАННЯ ЧАСТОТНОГО РЕСУРСУ ЛІНІЙ ЦИФРОВОГО РАДІОРЕЛЕЙНОГО ЗВ`ЯЗКУ

На сучасному етапі розвитку телекомунікаційних систем частотний ресурс ліній цифрового радіорелейного зв`язку (ЦРРЗ) у діапазонах частот до 40 ГГц майже повністю вичерпаний. Це стало стимулом для освоєння телекомунікаційними операторами світу більш високих діапазонів частот, в першу чергу – міліметрового. Необхідно відмітити, що світовий прогрес в галузі радіоелектроніки надвисоких частот, що намітився в останнє десятиліття вже дозволяє на даний час створювати лінії ЦРРЗ, що працюють на частотах 100-150 ГГц із загальною пропускною спроможністю в декілька гігабіт в секунду. Однак, по-перше, значні втрати потужності радіосигналу в гідрометеорах, що спостерігаються на трасах таких систем ЦРРЗ і які є основним обмежуючим фактором дальності їхньої дії(не більше 1..2 км), по-друге – висока на даний час вартість та недосконаліть технології виготовлення типових надвисокочастотних вузлів (гетеродини, змішувачі, фільтри, помножувачі частоти, антенно-фідерний тракт) міліметрового діапазону станцій ЦРРЗ та високі вимоги, що висуваються до вказаних вузлів (висока стабільність частоти та малий рівень фазових шумів гетеродину, великий коефіцієнт корисної дії вихідного каскаду передавача, точність виготовлення профілю антени тощо) є основними факторами, які роблять актуальною задачу пошуку нових або удосконалення відомих способів повторного використання радіочастотного ресурсу на лініях ЦРРЗ, що працюють на частотах менше 40 ГГц. При цьому бажано, щоб ці способи якомога меншою мірою вимагали модернізацію або зміну складу типового обладнання радіорелейних станцій. На думку авторів, одним із можливих способів вирішення цієї задачі є застосування на лініях ЦРРЗ просторової обробки сигналів [1]. Основна ідея цього методу полягає у використанні для розділення радіосигналів одного або декількох телекомунікаційних операторів, що одночасно використовують один й той частотний діапазон та вид поляризації, фізичного явища кривизни фазового електромагнітної хвилі [2], яке на даний час враховується в першу чергу при практичній побудові антенних решіток РЛС кругового огляду та РЛС бічного огляду поверхні Землі, що працюють в надвисокочастотному діапазоні. В доповіді наведені потенційні характеристики просторової обробки сигналів в передавальному та приймальному трактах радіорелейних станцій одноінтервальної лінії дуплексного ЦРРЗ, які теоретично показують можливість одночасної передачі та розділення радіосигналів від двох телекомунікаційних операторів, що використовують одну й ту саму смугу частот та вид поляризації з мінімальними енергетичними втратами один від одного при оптимальному виборі протяжності інтервалу лінії ЦРРЗ та міжелементній відстані в розріджених антенних решітках 1-ої та другої радіорелейних станцій лінії ЦРРЗ.

ЛІТЕРАТУРА

1. Ямпольский В.Г., Фролов О.П. Оптимизация антенных систем линий связи. М Радио и связь 1991г. 272с.

2. Кремер И.Я. Пространственно-временная обработка сигналов/И. Я. Кремер, А. И. Кремер, В. М. Петров и др.; Под ред. И. Я. Кремера. – М.: Радио и связь, 1984. – 224 с.

к.т.н. Якорнов Є.А. (ІТС НТУУ „КПІ”)
Мазуренко О.В. (ІТС НТУУ „КПІ”)

ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ БЕЗПРОВОДОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НА ОСНОВІ ТРИВИМІРНОГО ПРОСТОРОВОГО РОЗДІЛЕННЯ СИГНАЛІВ

Швидкий розвиток безпроводових телекомунікаційних систем (БПТС) у тому числі і спеціального призначення та збільшення кількості функціонуючих радіоелектронних пристроїв призвели до ускладнення сигнально-завадової обстановки та загострення проблеми завадостійкості каналів передачі даних, з якою тісно пов’язані задачі забезпечення електромагнітної сумісності, пропускної спроможності, пошуку шляхів ефективного використання радіочастотного ресурсу (РЧР). Для забезпечення безпроводового доступу до інформаційних ресурсів всім користувачам, пристроям потрібне високоефективне використання РЧР та його раціональне розподілення між ними, що поки набуло завершеності лише в часовому, частотному та кодовому вимірах. Розподіл РЧР в просторовому вимірі не набув високого розвитку і перебуває в формі його перевикористання через природнє затухання сигналу з розповсюдженням та перерозподілу у двох (кутових) вимірах тривимірного простору, проте питання підвищення його ефективності нині найбільше досліджується в напрямку засобів БПТС, зокрема технології адаптивних антенних решіток, розподілених антенних систем та MIMO систем.

Ефективним шляхом вирішення вказаної проблеми є використання методів просторово-часової обробки сигналів (ПЧОС), а особливо необхідним і ще недослідженим є її напрямок тривимірного просторового розділення сигналів, як за кутовими координатами, так і за відстанню. Це відкриває нові можливості для створення систем, що дозволятимуть значно збільшувати завадостійкість і щільність розміщення просторових каналів передачі даних в обмеженому просторі з мінімізацією затрат на побудову інфраструктури.

Тривимірне просторово розділення сигналів, що розглядається в даній доповіді базується на методах оптимальної ПЧОС, що включає як просторово-часову узгоджену фільтрацію (ПЧУФ), так і просторово-часову кореляційну обробку (ПЧКО), що є базою для алгоритмів функціонування процесорів систем дискретних випромінювачів.

Системи дискретних випромінювачів з ПЧУФ представляють собою зосереджені чи розподілені адаптивні сфокусовані антенні решітки, що функціонують лише в їх ближній та проміжній зонах випромінювання для досягнення тривимірної просторової вибірковості [1]. Системи дискретних випромінювачів з ПЧКО представляють собою розподілені антенні решітки з роздільною чи сукупною обробкою сигналів від випромінювачів, зона функціонування яких визначається виключно кореляційними властивостями каналоутворюючих ортогональних розширюючих послідовностей [2].

ЛІТЕРАТУРА

1. Oleksandr Mazurenko and Eugeniy Yakornov. Focused Arrays Beamforming. Behaviour of Electromagnetic Waves in Different Media and Structures, Ali Akdagli (Ed.), ISBN: 978 – 953 – 307 – 302 – 6, InTech, – 2011, – pp.419 – 440.

2. Мазуренко А.В., Якорнов Е.А. Методы трехмерного пространственного мультиплексирования в беспроводной связи // Матеріали 23-ої Міжнародної Кримської конференції (КрыМико 2013) „СВЧ-техника и телекоммуникационные технологии” 2013 Т.1, с.316 – 317.

Ясеновий М.С. (ВІТІ ДУТ)
к.т.н. Соколов В.В. (ВІТІ ДУТ)

РЕАЛІЗАЦІЯ НЕЗАЛЕЖНОСТІ ПРОГРАМ ВІД ЛОГІЧНОЇ СХЕМИ БАЗИ ДАНИХ

Про незалежність даних часто говорять, як про одну з основних властивостей БД. Під цим поняттям розуміється можливість зміни структури даних без зміни програм, що її використовують, а також рівень самоінтерпретованості даних. Міра незалежності даних тісно пов'язана з ступенем необхідної деталізації відомостей про організацію їх зберігання.

Для організації роботи з БД необхідно забезпечити незалежність прикладних програм від даних. Це обумовлено тим, що при зміні системи, а також з метою забезпечення ефективного обслуговування користувачів, необхідно виконувати роботи щодо зміни методів зберігання даних в БД, шляхів доступу до даних, змінювати структури і формати даних та зв'язки між ними. Якщо не застосовувати спеціальні підходи і при написанні застосувань вводити програмний опис методів доступу, засобів зберігання даних, формати даних, то при будь-якій зміні в БД для перелічених випадків буде необхідно корегувати текст програми користувача, що потребує значних витрат.

Незалежність застосувань від даних забезпечується засобами СКБД. Цей підхід базується на тому, що користувачі застосовуючи БД, не знають внутрішнє представлення даних. Розрізняють логічну і фізичну незалежність при роботі з даними. Логічна незалежність від даних означає захищеність зовнішніх схем від змін, що вносяться в концептуальну схему. Зміни концептуальної схеми БД не викликають необхідності в корегуванні існуючих зовнішніх схем для користувачів, і відповідно не викликають змін в застосуваннях, що працюють з цими схемами. Фізична незалежність від даних означає захищеність концептуальної і зовнішніх схем від змін, що вносяться у внутрішню схему. До змін внутрішньої схеми належать використання різних файлових систем або структур даних, різних пристроїв зберігання, модифікація пошукових структур тощо.

Час від часу структура бази даних може змінюватися. Але від цих змін в першу чергу не повинен страждати користувач. Припустимо, що таблиця № 1 (фізичний файл) була перетворена на дві таблиці, а потім видалена. Відзначимо, що таблиця № 1 може бути відновлена за допомогою об'єднання нових таблиць по стовпцях „Співробітник" (рис.1). Щоб приховати від користувачів зміни в структурі бази даних, можна створити курсор, який об'єднує дві нові таблиці. На жаль, стосовно курсора існує ряд обмежень на виконання деяких операторів модифікації даних. Об'єднання двох таблиць здійснюється за допомогою *SQL* запита: *create view* Таблиця № 1 *as select* ім'я, податок, дохід, адреса *from* Таблиця № 2, Таблиця № 3 *where* співробітник = співробітник.

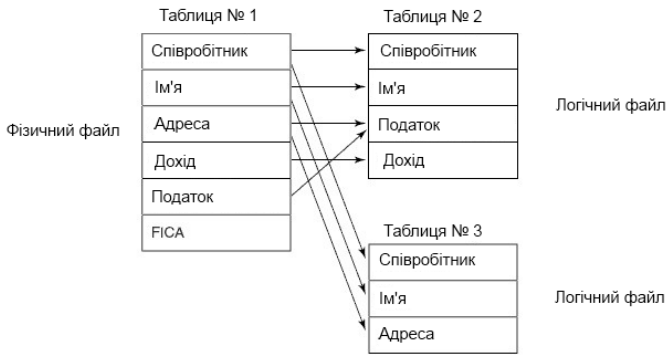


Рисунок 1. Фізична і логічна схема БД

Таким чином, незалежність даних можна визначити як імунітет програм до змін в структурах зберігання даних і в методах доступу до даних, але все ж таки треба знаходити підходи для позбавлення надмірної незалежності програмних додатків, які підключаються до локальної чи віддаленої БД.