

нарушителей и моделирования атак, их достоинства и недостатки. На основании анализа предложены усовершенствованные схемы моделирования.

Литература: 1. CERT/CC Statistics 1988-2002 – <http://www.cert.org/stats/>. 2. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. // Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. – Киев, 1999. 3. Парр Г. Л., Марков А. С. Анализ атак на автоматизированные системы на основе угроз информационной безопасности. (Балтийский государственный технический университет "ВОЕНМЕХ"). 4. Andrew P. Moore, Robert J. Ellison, Richard C. Linger. Attack Modeling for Information Security and Survivability. Technical Note CMU/SEI-2001-TN-001, 2001. 5. Joshua W. Haines, Lee M. Rossey, Richard P. Lippmann. Extending the DARPA Off-Line Intrusion Detection Evaluations. Lincoln Laboratory, Massachusetts Institute of Technology. 6. Jan Steffan, Markus Schumacher. Collaborative Attack Modeling. Department of Computer Science, Darmstadt University of Technology. 7. Nikhil Ashok Joshi. Resource/Attack Modeling and Optimal Intrusion Recovery. Master of science Thesis. University of California at Davis, 2002. 8. Wenke Lee, Wei Fan, Matthew Miller, Salvatore J. Stolfo, and Erez Zadok. Toward Cost-Sensitive Modeling for Intrusion Detection and Response. Journal of Computer Security, 2001.

УДК 33.140

КОМПЛЕКС ДЛЯ ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ДОСЛІДЖЕНЬ “АСТРА-В” – НОВА ТЕХНОЛОГІЯ ДОСЛІДЖЕНЬ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ І НАВОДІВ

Володимир Свириденко, Володимир Угрімов, Сергій Джигамон, Анатолій Передерко, Олександр Шпіта, Михайло Прокоф'єв***

*Міністерство оборони, *ПП “Бумекс”, **НДЦ “ТЕЗІС” НТУУ “КПІ”*

Анотація: Комплекс забезпечує виявлення радіосигналів, аналіз характеристик електромагнітного поля, проведення спеціальних досліджень ПЕМВН, реєстрацію, зберігання, обробку і документування одержаних результатів.

Summary: A complex provides exposure of signals radio, descriptions analysis of electromagnetic field, bowing of special SERNP researches, registration out, keeping, treatment and documenting of obtained results.

Ключові слова: Комплекс, спеціальні дослідження, пакет прикладних програм.

Вступ

Глобальна автоматизація практично всіх сфер людської діяльності привела до виникнення ряду нових проблем, однією з яких є збільшення можливості несанкціонованого витоку інформації за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН). Основними причинами цієї проблеми стали:

- різке збільшення граничної частоти задавальних генераторів і, як наслідок, виникнення можливості витоку інформації за рахунок як розширення діапазону частот, так і нових фізичних ефектів;
- поява сучасних, більш ефективних, засобів знімання інформації.

Вирішення вищезазваної проблеми в значній мірі забезпечує використання комплексу для проведення спеціальних досліджень “АСТРА-В”, в якому реалізовані нові методологія і технологія проведення досліджень ПЕМВН. Відповідно до НД ТЗИ 1.5-001-2000 комплекс відноситься до групи Г2 (аналізувальні радіовиявлювачі).

Комплекс забезпечує виявлення радіосигналів, аналіз характеристик електромагнітного поля, проведення спеціальних досліджень ПЕМВН, реєстрацію, зберігання, обробку і документування одержаних результатів.

Комплекс має такі характерні особливості:

- відкритість архітектури на рівні апаратних і програмних засобів;
- використання спеціальної методології, алгоритмів і програмних засобів обробки результатів спеціальних досліджень;
- наявність засобів автоматизації розрахунку результатів досліджень з видачею актів обстеження.

Відкритість архітектури на рівні апаратних і програмних засобів надає можливість змінювати названі засоби як на кількісному, так і на якісному рівні. Досягається це за допомогою структури програмного забезпечення, а також використання спеціальних інструментальних програмних утиліт. Ця особливість надає користувачеві можливість оперативно проводити реконфігурацію і модернізацію комплексу в залежності від конкретних задач і технічних можливостей. Спеціальна методологія, алгоритми і програмні засоби обробки результатів спеціальних досліджень надають можливість підвищити в середньому на 10% імовірність виявлення сигналу в порівнянні з аналогічними засобами. Наявність засобів автоматизації розрахунку результатів досліджень з видачею актів обстеження надає можливість підвищити в сотні разів продуктивність процесу досліджень об'єктів інформаційної діяльності (ОІД).

До складу базового комплекту комплексу входять:

- аналізатор спектру з опцією управління (HP-IV інтерфейс);
- ПЕОМ (яка має IBM-сумісний інтерфейс);
- комплект вимірювальних антен;
- додаткові пристрої (антенні підсилювачі, комутатори та ін.);
- пакет прикладних програм “Астра”.

Функціональні можливості комплексу

Автоматизація досліджень досягається шляхом використання пакету прикладних програм “Астра” (ППП “Астра”), який забезпечує:

- дистанційне управління процесом аналізу сигналів;
- перерахунок одержаних результатів згідно з калібрувальними характеристиками радіотракту;
- “вставку” даних про вимірювання в піддіапазонах спектроаналізатора в єдиний спектр радіотракту;
- відображення в зручній формі результатів вимірювання на моніторі ПЕОМ;
- масштабування відображення результатів вимірювань (відображення як частини спектру, так і всього спектру);
- зручний механізм аналізу складових спектрів;
- збереження в файл і завантаження з файлу результатів вимірювань та аналізу, а також їх друк на матеріальний носій;
- набір опцій для виявлення та аналізу побічних електромагнітних випромінювань різних об'єктів.

ППП “Астра” функціонує в середовищі ОС Windows 9X/NT і має інтуїтивно зрозумілий інтерфейс, характерний для стандартних Windows-додатків. Останні не вимагають додаткового (в області інтерфейсу) навчання оператора.

Для того, щоб оцінити гнучкість ППП “Астра”, розглянемо операції, які необхідно здійснити для виконання одного вимірювання:

- калібрування характеристик складових тракту;
- настроювання аналізатора спектру в піддіапазони, оптимізація опорного рівня, кроку шкали та ін.;
- визначення ідентифікації (імен спектрів) результатів вимірювань;
- визначення опції при вимірюванні сигналів досліджуваного ОІД.

При застосуванні ППП “Астра” описані вище умови зберігаються в файлах текстового формату (це дозволяє оператору редагувати їх будь-яким текстовим редактором в ОС Windows), створюються і редагуються утилітами з ППП “Астра”. Варіації умов задаються в вікні умов виконання вимірювань. Крім цього, для користувача, якому необхідно багато разів виконувати вимірювання в одних і тих же умовах, в ППП “Астра” є спеціальна утиліта, яка додає пункти в головне меню основного модуля програми, а при виклику його дані у вікні “Умови виконання вимірювання” встановлюються у відповідне значення (умови вимірювання по замовчуванню).

Склад пакету прикладних програм

До складу пакету прикладних програм входять наступні підпрограми:

- “Редактор пристроїв” – утиліта для візуальної побудови, редагування, збереження у файл (файл опису пристрою) і побудови з файлу інформації про пристрій, що входить до складу радіотракту ОІД;
- “Редактор трактів” – утиліта для візуальної побудови, редагування, збереження у файл (файл опису трактів) і побудови з файлів опису пристроїв файлу інформації про тракт виміру.
- “Редактор файлів управління” – утиліта для візуальної побудови, редагування, збереження у файл (файл керування аналізатором) і зчитування з файлу інформації про правила настроювання спектроаналізатора на піддіапазони, оптимізації рівня і кроку шкали в будь-якому піддіапазоні;

- “Редактор файлів сценаріїв” – утиліта для візуальної побудови, редагування, збереження у файл (файл сценаріїв виміру) і зчитування з файлу інформації про сценарії виміру;
- “Розрахунок радіуса зони R2 графічним методом” – програма для забезпечення розрахунку зони R2 графічним методом і формування вихідних документів.
- “Програма управління і аналізу” – основний модуль ППП “Астра”, що здійснює виконання вимірювання і аналіз результатів.

Опис логічної структури

Блок-схеми алгоритму функціонування утиліт “Редактор пристроїв”, “Редактор трактів”, “Редактор файлів управління”, “Редактор файлів сценаріїв” аналогічні і наведені на рис. 1.

Утиліти є сервісними і надають можливість користувачу стандартними процедурами (використовуючи технічну документацію як складову частину комплексу) підготувати його до проведення спецдосліджень, а саме – створити, змінити або зберегти файли:

- опису пристроїв, що використовуються для побудови вимірювальних трактів;
- опису вимірювальних трактів;
- управління вимірювальними приладами;
- сценарію проведення спецдосліджень.

Головне меню утиліт “Редактор пристроїв” і “Редактор трактів” містять три пункти – “Файл”, “Правка” і “?”.

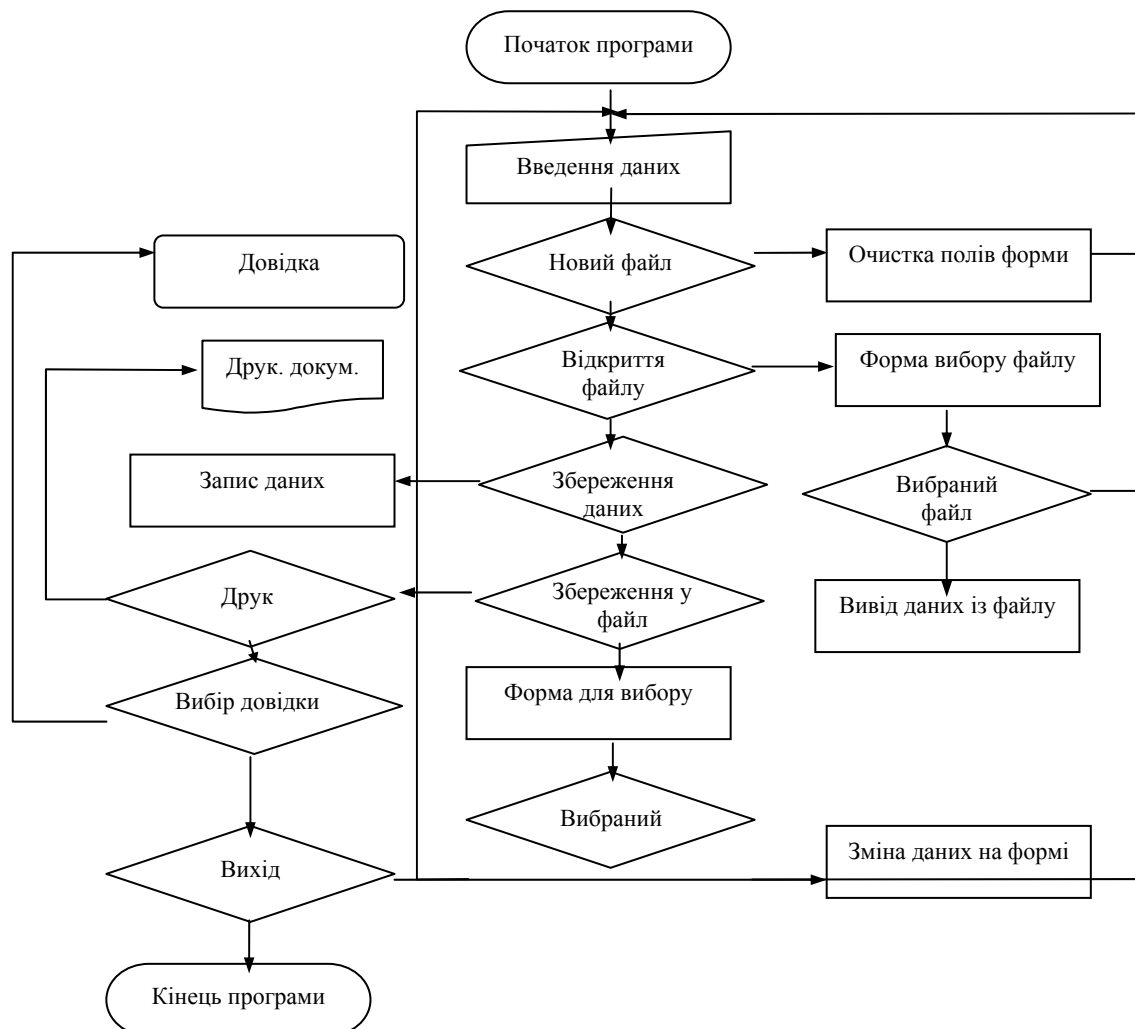


Рисунок 1 – Блок-схеми алгоритму функціонування утиліт “Редактор пристроїв”, “Редактор трактів”, “Редактор файлів управління”, “Редактор файлів сценаріїв”

Пункт меню “?” є присутнім у всіх утилітах і призначений для одержання довідки. Він містить наступні підпункти:

- “Вызов справки” – призначений для виклику довідки, причому довідка викликається згідно з активним елементом програми;
- “Содержание справки” – призначений для виклику довідки, починаючи з вікна змісту;
- “О программе ...” – виводить інформацію про утиліту (розробники, версія, номер і т. д.).

Пункт головного меню “Файл” також є присутнім у всіх утилітах і призначений для роботи з файлами, а саме для створення опису нового об’єкту (очищення всіх полів), завантаження даних з файлу інформації про об’єкт, збереження раніше завантаженого і відредагованого файлу, збереження знову створеного чи раніше завантаженого і відредагованого файлу з іншим ім’ям, для роздрукування інформації про об’єкт і завершення роботи програми.

Пункт головного меню “Правка” призначений для роботи з вибраними текстом в чарунках уведення і забезпечує вирізання вибраного і переміщення його в буфер обміну, переміщення тексту з буфера обміну в місце введення значення, скасування вибраного тексту і скасування останнього набору в поточній чарунці редакції.

Пункт головного меню утиліти “Редактор файлів управління” “Поддиапазоны” призначений для формування програми управління аналізатором спектру і забезпечує заповнення, редагування, додавання і видалення піддіапазонів.

Пункт головного меню утиліти “Редактор файлів сценаріїв” “Сценарій” призначений для формування сценарію досліджень і забезпечує створення нового сценарію виміру, зміну імені поточного сценарію виміру, видалення поточного сценарію виміру і зміну малюнка, що буде супроводжувати відповідний пункт меню в програмі управління і аналізу.

Блок-схема алгоритму функціонування програми “Програма управління і аналізу” наведена на рис. 2.

Програма забезпечує проведення вимірювань і досліджень (аналіз) технічних об’єктів. При цьому реалізуються режими:

- управління екраном монітору;
- вимірювання;
- управління спектрами в поточному екрані;
- управління видом екрану;
- сервісного налаштування;
- управління екранами багатодокументного додатку;
- доступ до довідкової системи.

В режимі управління екраном монітору програма надає можливість створювати новий екран, відкрити раніше збережені екрани, зберігати поточний екран у файл, друкувати поточний екран, завершувати роботу програми.

Програма надає можливість реалізувати режим вимірювання за раніше підготовленим сценарієм або за сценарієм, створеним в процесі вимірювань.

Програма надає можливість реалізувати процес управління спектрами в поточному екрані методом ручної і автоматичної селекції, методом верифікації, а також провести вимірювання вибраних сигналів, провести завантаження вибраного спектру в поточний екран, зберегти одержані спектри в файл.

В режимі реалізації управління видом екрану програма надає можливість змінювати вид екрану, показувати всю інформацію про спектри на екрані, встановлювати попередній вид екрану, встановлювати попередній вид екрану в смузї, встановлювати і керувати переключенням лінійної і логарифмічної шкали відображення.

В режимі сервісних налаштувань програма забезпечує загальні програмні налаштування, глобальні налаштування процесу вимірювань, зміну установки програми, запуск на виконання файлів опису пристроїв, трактів, управління вимірювальними приладами, сценаріїв проведення досліджень.

Програма управління і аналізу виконана у вигляді додатка з MDI-інтерфейсом, тобто в додатку є головне вікно і декілька дочірніх вікон, що не виходять за границі Головного вікна. Яскравий приклад MDI-дodatка – текстовий редактор Microsoft Word.

Головне вікно містить головне меню і кнопки швидкого доступу, розташовані під головним меню. Кнопки швидкого доступу дублюють найбільш вживані команди меню.

Дочірнє вікно в програмі управління «АСТРА» є засобом для відображення, редагування і аналізу спектрів. Надалі його будемо називати «Екран».

Оскільки дочірніх вікон «Екрани» в Головному вікні може бути декілька, то всі команди головного меню відносяться до активного вікна «Екран».

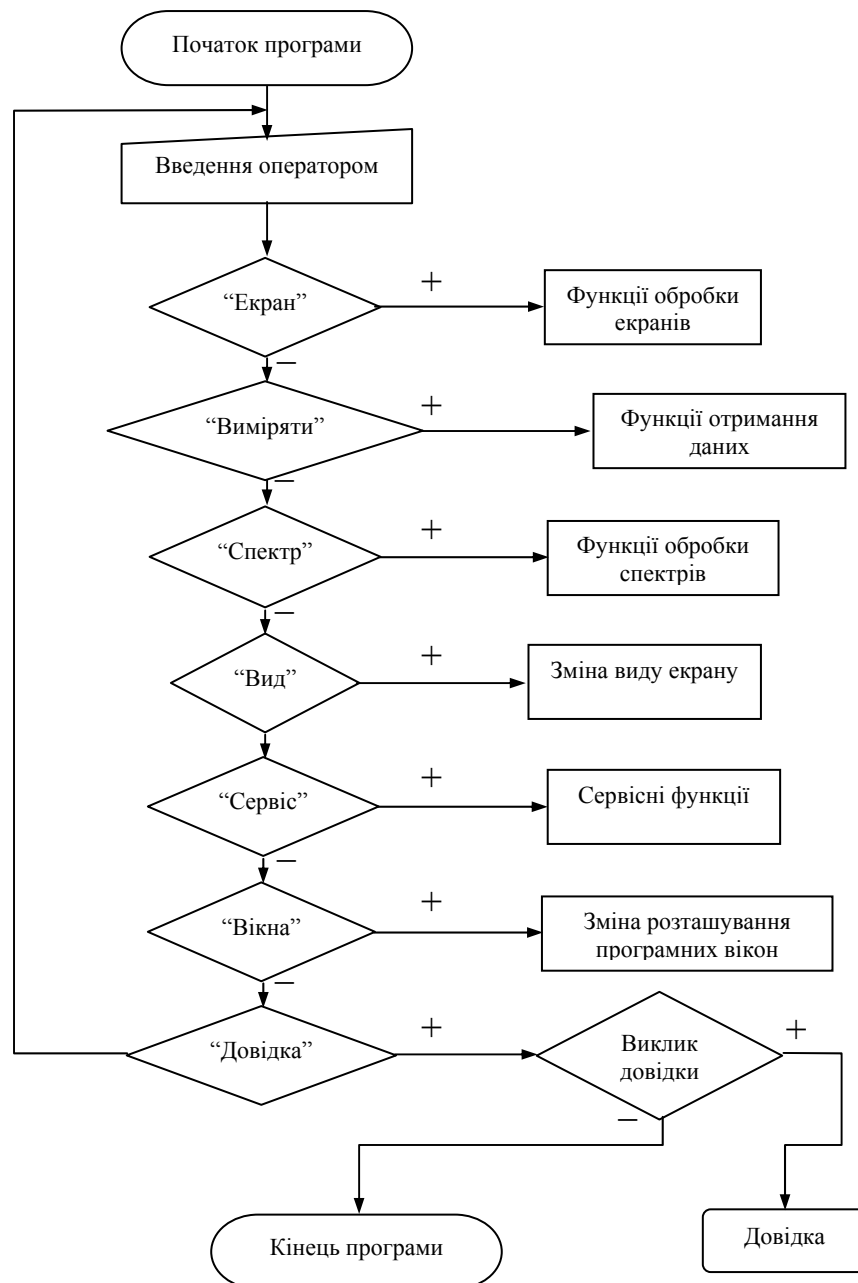


Рисунок 2 – Блок-схеми алгоритму функціонування програми “Програма управління і аналізу”

Підпрограма “Виміряти” надає можливість оператору провести процес вимірювання параметрів ІОД. При цьому вказується тип пристрою дослідження, його параметри, сценарій проведення досліджень, файли управління і опису тракту. Підпрограма реалізує також управління тестами і відображення результатів вимірювань.

Підпрограма “Спектр” призначена для відображення в графічному виді спектрів, проведення ручної селекції, відображення результатів верифікації.

У полі відображення спектрів може бути відображено до дев'яти спектрів. Кожний зі спектрів може бути двох типів:

- перший тип – результат вимірювань, тобто дані, отримані під час вимірювань зі спектроаналізатора, являють собою масив дискретних крапок, відображуваних безупинною лінією, що з'єднує крапки (нагадаємо, що відображуваний рівень може змінюватися і не збігатися з реальним; останній зберігається в пам'яті ПЕОМ відповідно до налаштувань програми, якщо на один піксель відображення приходить кілька обмірюваних крапок);

– другий тип – спектр типу складові, який складається з крапок, зазначених оператором під час проведення селекції; кожна крапка спектра такого типу відображається вертикальною лінією і відображуваний рівень не залежить від установленної смуги огляду.

Піпрограма “Вид” надає сервіс з установки наочним способом (указівкою двох крапок) необхідних смуг огляду за частотою і рівнем.

Блок-схема алгоритму функціонування програми “Розрахунок зони R2 графічним методом” наведена на рис. 3.

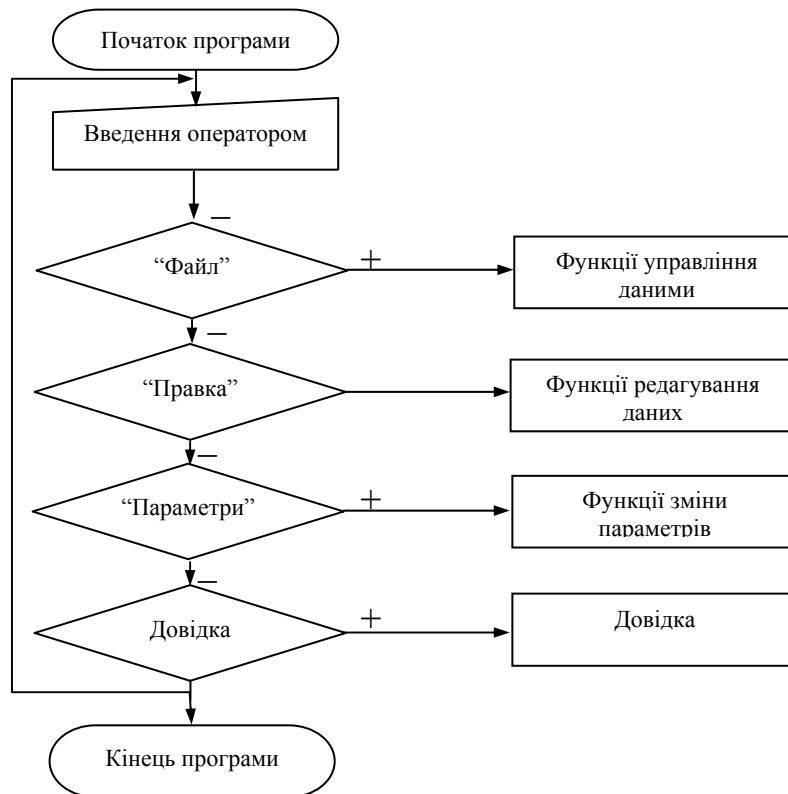


Рисунок 3 – Блок-схеми алгоритму функціонування програми “Розрахунок радіусу зони R2 графічним методом”

Програма забезпечує автоматизацію розрахунку радіусу зони R2 графічним методом та автоматичне формування звітних документів за заданими шаблонами у форматі “RTF” відповідно до вимог.

В програмі реалізовані наступні режими:

- управління даними;
- редагування даних;
- зміна параметрів;
- доступ до довідкової системи.

В режимі управління даними проводиться виклик і завантаження програми, введення вхідних даних. Структура вхідних даних може бути у форматах DOS або Windows.

Структура файлу у форматі DOS призначена для підтримки розрахунку даних, виконаних за допомогою DOS-редакторів. При цьому дані вводяться в ручному режимі.

Файл у форматі Windows забезпечує автоматичне введення і розрахунок даних, які є вихідними для комплексу “Астра”-В”.

Обидва формати мають заголовок, що описує умови, при яких проведені вимірювання та надає безпосередньо дані вимірювань.

В режимі редагування даних редагуються невірні введені дані, які зберігаються у файл і проводяться розрахунки, в результаті чого створюються текстові файли, в яких зберігаються їх результати. Ці файли мають визначену структуру, яку програма розуміє як формат “RKZ”. Структура вихідного текстового файлу визначається користувачем при установленні параметрів програми. Після цього програма за заданими шаблонами формує файли “протоколу” та “припису” в форматі “RTF” для подальшого корегування та друку зовнішніми текстовими редакторами.

В режимі зміни параметрів програма забезпечує користувачеві додатковий сервіс в його роботі. Наприклад, вибір поточного каталогу дозволяє реалізувати швидкий доступ до файлів з даними для розрахунку. Для розрахунку декількох файлів у програмі передбачено режим пакетного вводу даних.

Технічні переваги комплексу

- наявність можливості запису спектру сигналу для подальшої обробки;
- більш достовірні результати виявлення сигналів завдяки спеціальному алгоритму управління, особливо в умовах складної радіозаводної обстановки та при наявності коротких радіосигналів;
- організація конвеєрного принципу спецдосліджень шляхом розділення процесів підготовки, вимірювань і обробки результатів на програмному і апаратному рівні;
- повноцінне функціонування комплексу в багатозадачному режимі Windows, що надає можливість одночасно проводити вимірювання і підготовку звітних документів та ін.;
- можливість формування звітних документів в даних шаблонах, наприклад, “Акт інструментальної перевірки захищеності об’єкта ЭВТ” і “Предписание на эксплуатацию” (відповідно до вимог нормативних документів);
- можливість використання модифікованого комплексу для вирішення інших спеціальних задач (електромагнітна сумісність, пошук закладних пристроїв, оцінка спектру радіовипромінювань, виявлення надкоротких передач та ін.).

Організаційні переваги комплексу

- відкритість методики проведення розрахунків, наявність доступу до проміжних результатів розрахунків, можливість корегування даних;
- наявність тестового програмного забезпечення з відкритим вихідним текстом програми;
- наявність лінійного режиму вимірювань, завдяки чому збільшується точність вимірювань;
- можливість постійної модернізації програмного забезпечення відповідно до вимог замовника.

Порівняльні випробування комплексу

За базу для порівняння беремо комплекс “Навігатор” (Росія) – єдиний зарубіжний комплекс подібного класу, який використовується в Україні на даний час. Вітчизняних аналогів немає.

Порівняльні випробування вищеназаних комплексів, а також контрольні розрахунки результатів досліджень показали, що імовірність виявлення каналів витoku інформації при використанні комплексу “АСТРА” в середньому на 10% більша. Причиною цього є те, що при використанні комплексу “Навігатор” 1) рівень сигналу, який вимірюється, перевищував верхню межу аналізатора; 2) при виявленні широкопasmового сигналу можлива втрата сигналу; 3) неможливо вимірювати низькочастотні сигнали (від 10 Гц до 9 кГц); 4) мають місце недоліки в методиці верифікації та ін.

При виконанні розрахунків потенційних загроз ручним методом числові значення, одержані при дослідженні, необхідно перерахувати, користуючись графіками. Якщо значення попадає між двома лініями, оператор повинен або інтуїтивно, або інтерполяцією вибрати конкретне числове значення. В подальшому оператор повинен внести корегуючі коефіцієнти, які також визначаються з графіків. Таким чином, незалежно від кваліфікації і бажання оператора при розрахунках виникає інструментальна помилка.

Крім цього, при ручних розрахунках можуть виникати помилки, обумовлені людським фактором.

Експериментальні дослідження показали, що при ручному методі розрахунку помилка в середньому з’являється у 25% випадків.

УДК 681.325.59:519.6

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КОРРЕКТИРУЮЩИХ СВОЙСТВ ПЕРЕКЛЮЧАТЕЛЬНЫХ ФУНКЦИЙ

Оксана Тарасенко-Клятченко
НТУУ "КПИ"

Анотація: Запропоновано характеристики абсолютної та відносної автокоригуючої властивості перемикальних функцій та методика їх отримання для оцінки та порівняння ступеня розвитку автокоригувальних властивостей перемикальних функцій. Наведені приклади.