ТЕХНИЧЕСКИЕ НАУКИ

Laptiev O.A.,
PhD., senior researcher,
docent of information and cybernetic protection systems
of the State University of Telecommunications.
Kyiv, Ukraine.
ORSID - 0000-0002-4194-402X

THE ALGORITHM OF DEVELOPMENT OF MODERN COMPLEXES OF DETERMINATION, RECOGNITION AND LOCALIZATION OF THE MEANS OF ILLEGAL THE RECEIPTS OF INFORMATION

Лаптєв Олександр Анатолійович
кандидат технічних наук, СНС,
доцент кафедри
систем інформаційного та кібернетичного захисту
Державного університету телекомунікацій.
м. Київ, Україна,
ORSID - 0000-0002-4194-402X

АЛГОРИТМ РОЗРОБКИ СУЧАСНИХ КОМПЛЕКСІВ ВИЗНАЧЕННЯ,РОЗПІЗНАВАННЯ ТА ЛОКАЛІЗАЦІЇ ЗАСОБІВ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

Abstarct. The article deals with issues of leakage or loss of information, which can lead to catastrophic consequences in the object of management - transport, communications and other industries. Modern military science claims that total deprivation of communications reduces the combat capability of the army to zero. Therefore, the process of detecting, recognizing and localizing the means of silent retrieval of information in order to further block information leakage channels is considered.

The analysis of various on the principle of operation, search devices, and methods of detection, recognition and localization of the means of silent retrieval of information operating against the background of legal airwaves. The analysis makes it possible to conclude that at the present stage of society development, the process of searching for the means of silent retrieval of information goes to a qualitatively different level. Therefore, the methods of search (detection, recognition, localization), equipment and devices used to search for non-tacit information require improvement, and the problem of analyzing methods and tools for finding digital tacit information in order to identify the trend of development and development of modern requirements for them will become relevant.

Taking into account the peculiarities of modern developments of the means of silent retrieval of information, a complete methodological set of requirements is provided for the design and creation of modern automated search complexes that correspond to the process of modern automated retrieval of digital information retrieval devices that work against the background of legal airwaves in full. The algorithm and the given requirements can be used as a technical task in the design of automated software complexes of search (detection, recognition, localization) of means of silent retrieval of information, in order to identify and block channels and devices of information leakage.

Аннотация. У статті розглянуто питання витоку або втрачання інформації, що може привести до катастрофічних наслідків в об'єкті управління – транспортом, зв’язком та інших галузей промисловості. Сучасна військова наука стверджує, що повне позбавлення засобів зв'язку зводить боєздатність армії до нуля. Тому розглядається процес виявлення, розпізнавання та локалізації засобів негласного отримання інформації з метою подальшого блокування каналів витоку інформації.

Проведено аналіз різних за принципом роботи, пошукових приладів, та методів виявлення, розпізнавання та локалізації засобів негласного отримання інформації які працюють на фоні легальних сигналів радіоефіру. Аналіз дозволяє зробити висновок, що на сучасному етапі розвитку суспільства процес пошуку засобів негласного отримання інформації виходить якісно на інший рівень. Тому методи пошуку (виявлення, розпізнавання, локалізації), обладнання та пристрої , які використовуються для пошуку засобів негласного отримання інформації потребують удосконалення, а проблема аналізу методів та засобів пошуку цифрових засобів негласного отримання інформації, з метою виявлення тенденції розвитку та розробки сучасних вимог до них стане актуальною.

Враховуючи особливості сучасних розробок засобів негласного отримання інформації, надано повний методичній набір вимог, щодо проектування та створення сучасних автоматизованих пошукових комплексів, які відповідають процесу сучасного автоматизованого пошуку цифрових засобів отримання інформації які працюють на фоні легальних сигналів радіоефіру у повному обсязі. Надано алгоритм та дані вимоги можуть використовуватися, як технічне завдання при проектуванні автоматизованих програмних

комплексів пошуку (виявлення, розпізнавання ,локалізації) засобів негласного отримання інформації, з метою виявлення та блокування каналів та пристроїв витоку інформації.

Keywords: algorithm, search, radio channel, radio monitoring, automated software complex.

Ключові слова: алгоритм, пошук, радіоканал, радіомоніторинг, автоматизований програмний комплекс.

Вступ.

З підвищенням значності т цінності інформації відповідно зростає і важливість її захисту. З одного боку, інформація коштує грошей. Значить витік або втрата інформації спричинить матеріальний збиток. З іншого боку, інформація - це управління. Несанкціоноване втручання в управління може привести до катастрофічних наслідків в об'єкті управління - виробництві, транспорті та військовій справі. Наприклад, сучасна військова наука стверджує, що повне позбавлення засобів зв'язку зводить боєздатність армії до нуля.

Питання інформаційної безпеки сьогодні актуальний як ніколи раніше. Кількість використовуваної техніки продовжує зростати, отже, зростає і значущість організаційної та програмно-технічного захисту від витоку інформації.

Під витоком інформації з технічного каналу розуміється неконтрольоване поширення інформації від носія інформації, що захищається через фізичне середовище до технічного засобу, який здійснює перехоплення інформації.

Залежно від фізичної природи виникнення інформаційних сигналів, середовища їх поширення технічні канали витоку акустичної інформації можна розділити на прямі акустичні (повітряні), акустовібраційні (вібраційні), акустооптичні (лазерні), акустоелектричні (параметричні) [1]. Причому інформацію отриману з перерахованих вище каналів витоку інформації найпростіше передати по радіоканалу, в зв'язку з чим пошук радіоканалів ЗНОІ і методи нейтралізації становяться актуальними на сучасному етапе розвитку.

Аналіз літературних даних та постановка проблеми. Питанням пошуку засобів негласного отримання інформації, (ЗНОІ),присвячено значну кількість публікацій, так у [1]розглядаються питання аналізу систем радіоконтролю (радіомоніторингу) з різними технічними параметрами, які об'єднує одне - вони можуть тільки відображати і (в кращому випадку) зберігати панорами спектрів сигналів в радіоефірі. Завдання аналізу цифрових легальних каналів зв'язку вони або не вирішують взагалі, або роблять це формально - для «галочки». Причини різні - починаючи від незадовільної якості радіоприемного тракту і неможливості підключення до ПЕОМ (апарати типу Oscor Green) і закінчуючи простим нерозумінням і / або небажанням вирішувати існуючу проблему. У [3] розглядається ряд аналізаторів спектра і вимірювальних приймачів виробництва Rohde & Schwarz. Ті нечисленні засоби аналізу цифрових мереж передачі даних (Rohde & Schwarz TSMW і ПО "ROMES", різні спеціалізовані тестери цифрових засобів зв'язку, ряд інших програмних засобів цифрового аналізу сигналів) відносяться до класу "цивільних" і призначені для демодуляції широкомовних пакетів базових станцій і аналізу структури мережі . І можуть вирішувати задачу пошуку засобів негласного знімання інформації виключно з аналізу спектру радіоефіру, вони не можуть проводити аналіз цифрових сигналів, виконувати завдання локалізації засобів негласного знімання інформації.

У [4] розглядаються векторні аналізатори які використовуються для дослідження і демодуляції сигналів високошвидкісних радіоінтерфейсів і сигналів з розширенням спектру потрібні смуги паралельного аналізу порядку декількох МГц. Залежно від смуги паралельного аналізу векторні аналізатори виконують вимірювання потужності спектральних компонент з динамічним діапазоном від 60 до 90 дБ. Що випускається, зокрема, фірмою Agilent Technologies (США) блок векторної обробки 89410A серії 89400 працює з смугою паралельного аналізу при записі реалізацій в пам'ять 3 - 7 МГц і 78 кГц - при реєстрації в реальному часі. Ємність пам'яті реалізацій - до 1 млн. Відліків. Прилад експлуатується з знижувальними перетворювачами частоти 89431A або 89430 A (діапазон відповідно до 2,65 і 1,8 ГГц). Чутливість по входу - -159 дБм / Гц, рівень побічних складових - -70 дбн. Перетворювач 89411A цієї серії призначений для сполучення блоку векторної обробки з радіоприймачами і аналізаторами спектра, у яких передбачений вихід проміжної частоти 21,4 МГц. Як показано вище ці прибори призначені для спільної роботи з приймачами і аналізаторами спектра, тобто самостійно вирішить завдання пошуку і локалізації вони не можуть.

У [5] розглядається комплекс радіомоніторингу «Delta», Якій продовжує лінійку самих передових і технологічних рішень в області радіомоніторингу. Комплекс надає широкі можливості по виявленню та ідентифікації джерел сигналів, робота з ним дозволяє значно підвищити якість виконуваних завдань з виявлення незаконно діючих передавачів, контролю радіочастотного спектру і виконання інших дій, пов'язаних з дослідженням радіосигналів. Недоліком його можливо рахувати відсутність автоматичної пеленгації ЗНОІ.

З аналізу сучасної літератури можна зробити висновок, що пристроїв (приладів, програмних комплексів) для аналізу цифрових пакетів, стосовно завдань пошукового радіоконтролю зараз практично немає. Виходячи з чого задача визначення вимог до апаратури - конкретно до

апаратно програмних комплексів-здатної в повному обсязі задовольняти завданням пошуку та локалізації засобів негласного інформації -є актуальною.

Виклад основного матеріалу. Для визначення вимог до пошукових комплексам засобів негласного знімання інформації, коротко розглянемо методи приховування роботи ЗНОІ, що застосовуються при розробці таких пристроїв. Відразу відзначимо, що в даний час набагато легше зробити цифровий передавач, використовуючи сучасну елементну базу стандартних засобів зв'язку, ніж конструювати і налагоджувати «аналогову» закладку на транзисторі з позитивним зворотним зв'язком. Тому сучасні і перспективні вимоги до комплексам пошуку засобів негласного знімання інформації випливають з аналізу можливостей сучасних цифрових засобів передачі даних.

Сучасні ЗНОІ можуть використовувати такі методи приховування каналу передачі даних:

• методи накопичення інформації, і дискретної її передачі за короткі проміжки часу (до декількох Мілі секунд);

• методи накопичення інформації за досить тривалий час з наступною передачею в призначений час або при отриманні зовнішньої команди;

• періодичну або хаотичну перебудову частоти каналу випромінювання;

• використання широкосмугових сигналів, коли енергія сигналу розподілена в широкій смузі частот і сигнал не має яскраво вираженого перевищення над шумами; • реалізація шумоподібних закладок, які використовують спеціальні алгоритми кодування, що дозволяють стійка приймати інформацію при негативному відношенні сигнал / шум в точці знаходження приймача;

• вибір частоти випромінювання поряд з потужними джерелами легальних сигналів, які перевантажують прийомні тракти пошукової апаратури при недостатньому динамічному діапазоні або маскуються спектром легального сигналу при недостатньо низьких фазових шумах радіотракт пошукових комплексів;

• маскування під стандартні канали зв'язку і / або робота вузькосмугових випромінювань усередині спектра легальних широкосмугових сигналів;

• використання стандартних каналів зв'язку таких як GSM, CDMA, WiFi, BlueTooth.

Використовувані методи можуть комбінуватися один з одним. Так, наприклад, використання сигналів з над широкої смугою займаних частот може комбінуватися з методом накопичення інформації та дискретної її передачею і т.п.

Аналізуючи перераховані вище методи приховування каналу передачі даних, можна визначити вимоги до алгоритмів пошуку закладних пристроїв.

Сучасні ЗНОІ, що використовують методи накопичення інформації та дискретної її передачі, перебудови частоти випромінювання і дистанційне керування, надійно можна ідентифікувати тільки по демаскирующими ознаками в просторі амплітуда-частота-час. Які б складні алгоритми приховання каналу передачі даних не застосовувалися в закладках, вони все одно себе демаскують певної закономірністю (періодичністю) виходу в радіоефір і / або використанням обмеженого діапазону частот (обмеженого числа каналів). Ці демаскуючі ознаки ЗНОІ виявляються оператором при виконанні тимчасового аналізу радіочастотного спектру. Саме частотно-часової закономірністю закладки відрізняються від випадкових сплесків індустріального шуму в радіоефірі, який недосвідчений оператор може прийняти за закладку.

При пошуку таких ЗНОІ мова не йде про миттєве їх виявленні. Для надійного їх виявлення потрібно радіомоніторинг протягом тривалого часу: до доби або більше з подальшим аналізом всіх виміряних панорам в тимчасовій площині в поданні спектрограми («водоспаду»). Виходячи з цих міркувань, пред'являються вимоги до алгоритмів, які повинні бути реалізовані в програмному забезпеченні автоматизованого комплексу.

Відносно виявлення над широкосмугових і шум подібних закладок, зазначимо таке: метод їх виявлення заснований на тому, що в ближній зоні відношення сигнал / шум навіть у таких передавачів буде вище нуля, тому збільшення рівня шуму в окремих діапазонах частот може свідчити про роботу таких пристроїв. З цього можна сформулювати вимоги до прийомним засобам комплексів радіомоніторингу: для того, щоб відслідковувати зміну рівня шуму на тлі сильних сигналів приймальне засіб повинен мати хорошу чутливість і широкий динамічний діапазон (не менше 80-90 дБ). Теза про те, що динамічний діапазон в комплексах радіомоніторингу не так важливий, так як закладки в ближній зоні мають високу потужність сигналу і тому можна використовувати атенюатор, неприйнятний в разі пошуку над широкосмугових і шум подібних сигналів. Ситуація, коли разом із закладкою в смузі преселектора працює легальне засіб зв'язку, рівень сигналу якого перевищує рівень закладки на 70-90 дБ, в даний час не є рідкістю. Рівень 70-90 дБ - це дуже високий рівень сигналу, який здатний перевантажити багато радіоприймальні кошти. Якщо сигнал перевищує рівень динамічного діапазону приймального тракту, то на панорамі сигналів буде відображено безліч помилкових побічних і комбінаційних сигналів, які вкрай нестабільні по частоті, амплітуді і в часі. Досвід знайомства з цілою низкою представлених на ринку комплексів радіомоніторингу, при формальній відповідності параметрів їх динамічного діапазону пошуковим вимогам, виявив, що вони легко перевантажуються від працюючого неподалік

простого передавача типу «Walkie-Talkie». Природно, при наявності великої кількості помилкових сигналів говорити про якісне пошуку закладних пристроїв не доводиться.

Для пошуку «хитрих» закладок, які маскуються під спектр легальних сигналів або для пошуку вузько смугових сигналів, які вміють ховатися в спектрі легальних сигналів, комплекс радіомоніторингу повинен мати засоби детального дослідження спектрів сигналів з досягненням дозволу в одиниці Герц. Безумовно, досвід оператора і його інтуїція мають тут вирішальне значення. Проте, апаратура і програмне забезпечення комплексу повинні дозволити оператору виконувати такі завдання.

Нарешті, для ідентифікації пошуку закладних радіопристроїв, що використовують стандартні канали зв'язку, такі як DECT, GSM, CDMA, WiFi, BlueTooth, крім ідентифікації роботи цих передавачів методом аналізу відповідних частотних діапазонів, комплекс радіомоніторингу повинен мати засоби додаткового аналізу мереж, що дозволяють виявляти «чужі» MAC адреси або ідентифікувати «чужі» абонентські пристрої для тих мереж, для яких це можливо.

Необхідно констатувати, що окремих приладів аналізу цифрових пакетів, стосовно завдань пошукового радіоконтролю зараз практично немає. Першою спробою створити програмні засоби демодуляції і аналізу цифрових засобів радіозв'язку можна вважати пакет цифрової обробки сигналів в програмному забезпеченні ПО DigiScan в подальшому перетворений на ПО Delta на сьогоднішній день він дозволяє демодулировать, аналізувати, ідентифікувати і локалізувати базові станції та мобільні пристрої, що працюють в стандартах DECT, GSM, Bluetooth, Wi-Fi, TETRA, виконувати демодуляцію і відображення картинки аналогового телевізійного сигналу, в тому числі, з використанням методу інверсії синхроімпульсів, демодулировать аналогові AM і FM сигнали в смузі частот від десятків герц до декількох мегагерц.

Однак це ПО не в повному обсязі виконувало функції пошуку і локалізації (пеленгації) ЗНОІ. Тому розробники почали вдосконалювати це ПО намагаючись виконати вище викладені вимоги в повному обсязі. Результатом їх останніх розробок став комплекс «Delta X». Який наблизився до оптимального обсягу вирішуваних завдань вищевикладених вимог, але не вирішує їх в повному об’ємe. Не приділено увагу векторному аналізу і автоматичної пеленгації цифрових ЗНОІ.

Підсумовуючи вищенаведені міркування, можна сформулювати вимоги до сучасного і перспективного комплексу радіомоніторингу.

1. Сучасний комплекс радіомоніторингу повинен мати досить високоякісні тракти аналогової і цифрової обробки сигналу, щоб присутність сторонніх потужних сигналів не заважало йому виявляти над широкосмугові і шум подібні сигнали. У тактико-технічних характеристиках радіоприймальних засобів відповідність цим вимогам відбивається в таких характеристиках як чутливість і динамічний діапазон.

З розвитком технологій дані характеристики будуть поліпшуватися. За точку відліку в даний час можна прийняти характеристики сучасних вимірювальних приймачів з чутливістю - не менше -160дБт (1 Гц) і динамічним діапазоном не менше 85 дБ на частоті 1 ГГц.

2. Сучасний комплекс радіомоніторингу повинен мати досить високоякісне і багатофункціональне програмне забезпечення, яке повинно дозволяти, як мінімум, виконувати наступні функції:

• виконувати цілодобовий радіомоніторинг заданих діапазонів частот і зберігати всі результати вимірювань панорам для подальшого їх тимчасового аналізу;

• забезпечувати аналіз амплітудно-частотно-часового подання результатів радіомоніторингу в режимі реального часу і в відкладеному режимі;

• дозволяти виконувати детальний аналіз спектрів сигналів з дозволом в одиниці Герц;

• додатково досліджувати випромінювання стандартний Відкритий каналів зв’язку WiFi і BlueTooth на наявність «чужих» абонентських станцій;

• виконувати аналіз сигналів по векторній діаграмі;

• здійснювати пеленгацію невідомих джерел радіосигналів.

Крім цього, програмне забезпечення повинно підтримувати методи пошуку, що стали вже «традиційними» і широко використовуваними на практиці:

• метод рознесених антен;

• метод порівняння з еталонною панорамою;

• використання селективної лінії порога і формування переліку сигналів, які перевищили лінію порога;

• детальний аналіз характеристик спектрів прийнятих сигналів;

• автоматичний запис фонограм і низькочастотний аналіз де модульованого аудіо сигналу.

З метою порівняльного аналізу сучасного автоматизованого комплексу та комплексу якій відповідає вимогам вище, наведемо алгоритмі роботи.

Алгоритм роботи сучасного програмного комплексу та запропонованого сучасного автоматизованого комплексу наведено на Рис.1.та Рис.2.

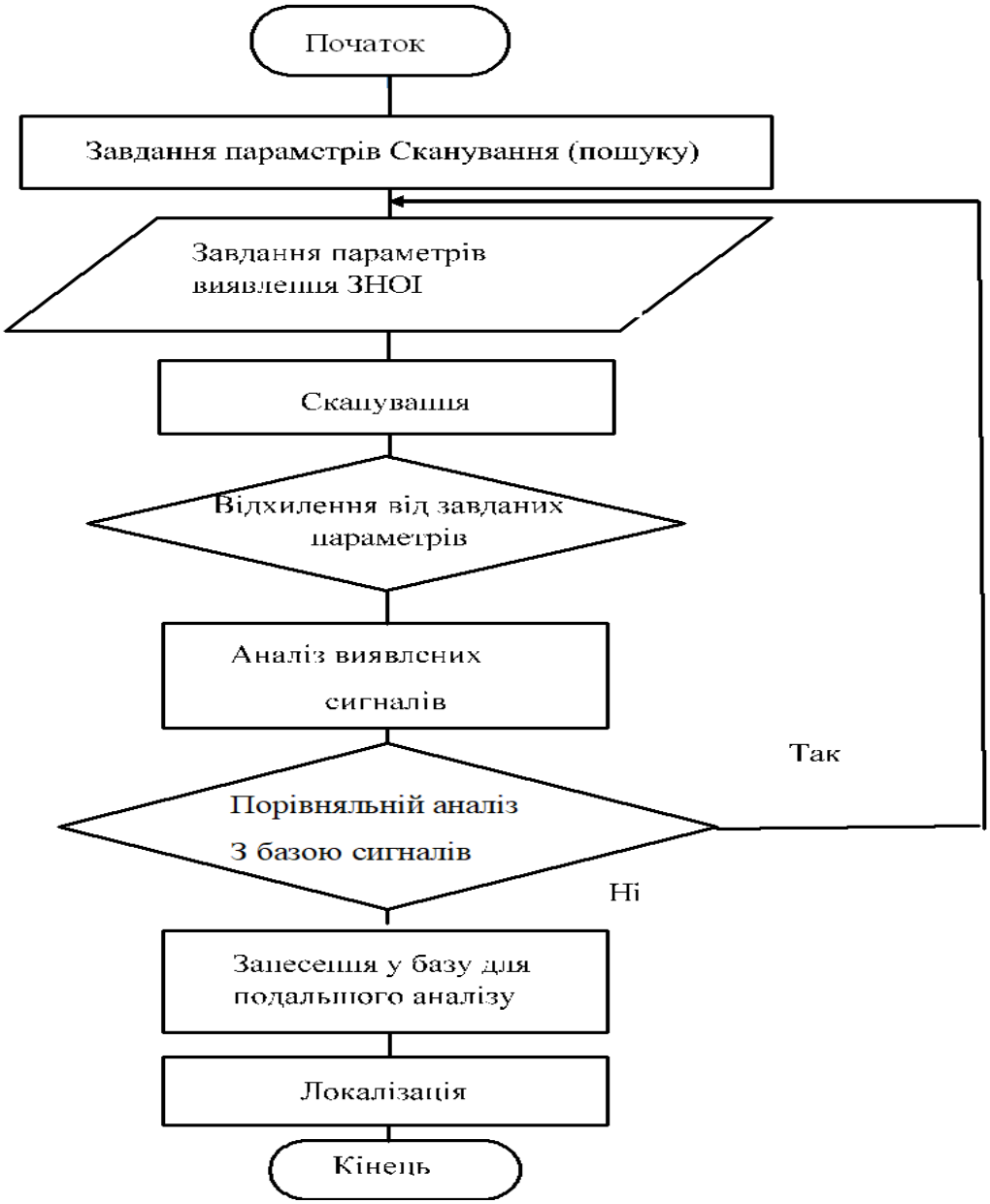

Рис.1 Алгоритм роботи сучасних автоматизованих програмних комплексів

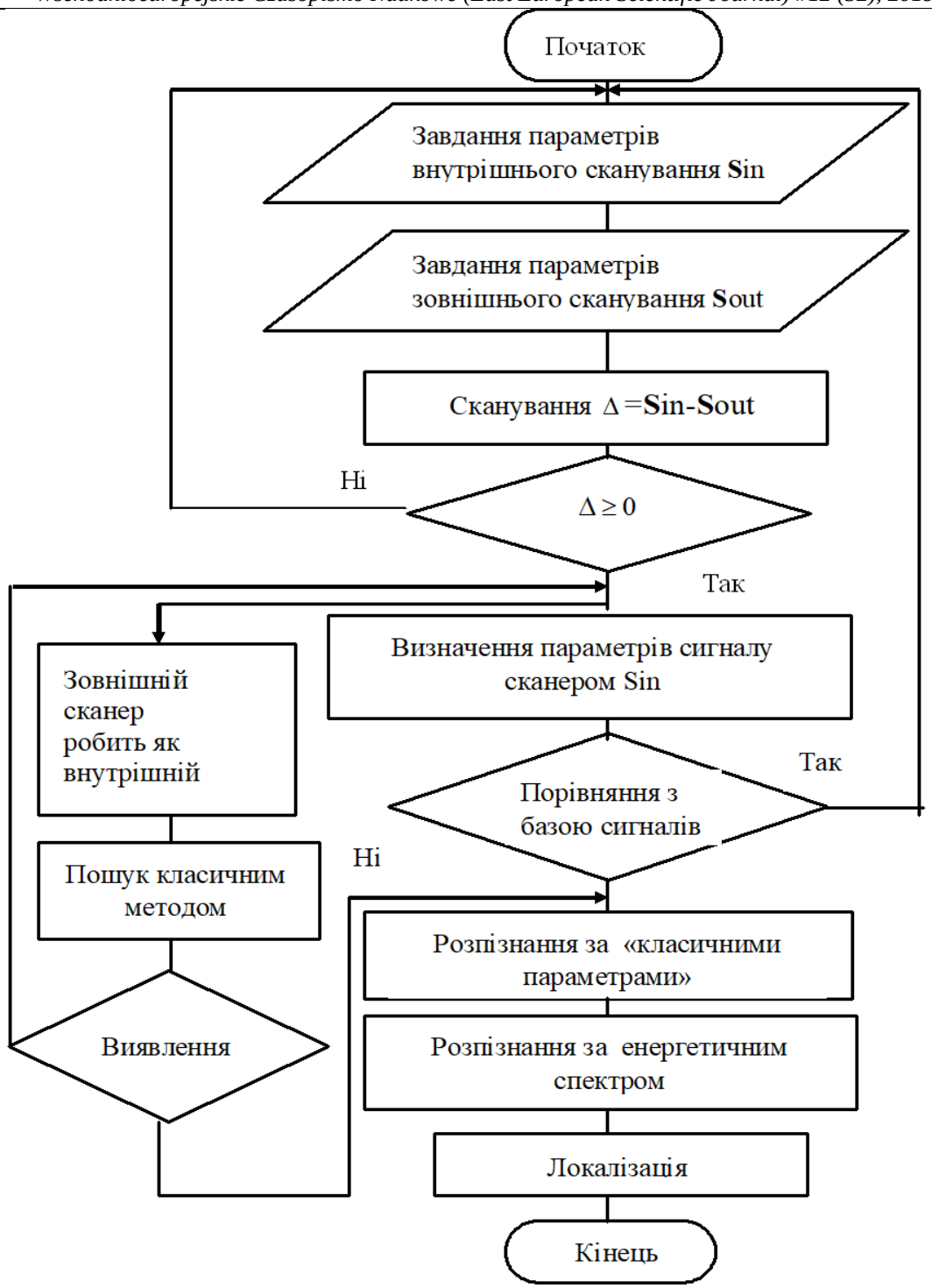

Рис.2. Алгоритм роботи нових автоматизованих програмних комплексів

З наведених алгоритмів Рис.1 та Рис.2, бачимо що запропонований комплекс використовує більш ланок визначення ЗНОІ, що свідчить про його більш надійність та більшу ймовірність визначення ЗНОІ.

Наведений на Рис.2. алгоритм, повністю відповідає вимогам сучасного комплексу пошуку та локалізації ЗНОІ.

Функціональні можливості, ергономічні характеристики і розробка програмного забезпечення всіх комплексів є найбільш актуальними на сьогоднішній день, так як, безумовно, пошук сучасних ЗНОІ - це інтелектуальна боротьба розробника таких засобів і оператора, що виконує пошук закладок. Програмне забезпечення - це інструмент по шукача, і від того, наскільки воно функціонально і зручно, в чималому ступені визначає результат робіт.

Висновки:

1. Проведено аналіз приладів і програмних комплексів пошуку засобів негласного отримання інформації, який показав відсутність автоматизованих програмних комплексів які дозволяють вирішувати завдання автоматизованого пошуку цифрових ЗНОІ.

2.Враховую особливості сучасних розробок засобів негласного отримання інформації, надано повний набір вимог для проектування та створення сучасних автоматизованих пошукових комплексів які відповідають процесу сучасного автоматизованого пошуку цифрових ЗНОІ в повному обсязі. Дані вимоги можуть використовуватися як технічне завдання при проектуванні автоматизованих програмних комплексів пошуку цифрових ЗНОІ.

3.Порівняльний аналіз наведених алгоритмів роботи автоматизованих комплексів, довело обмеженість існуючих комплексів та показав перевагу запропонованого комплексу пошуку та локалізації ЗНОІ у методології виявлення та локалізації сучасних ЗНОІ.

Література:

1. Захист інформації. Технічний захист інформації .Терміни та визначення (ДСТУ 3396.2-97) .– [Дійсний від 01.01.1998]. – (Державний Стандарт України).

2. А.В.Кривцун Использование новых возможностей комплекса радиомониторинга и цифрового анализа сигналов «Кассандра-М» для обнаружения современных специальных технических средств с передачей информации по радиоканалу [Электронный ресурс] /А.В. Кривцун А.В.Захаров режим доступа: http://www.inspectorsoft.ru/article.php?id=388 (24.05.2019)

3. Цифровой пеленгатор "Rohde & Schwarz DDF0xE"/Техника для спец служб,бюро научно-технической информации, основано в 1999 году. [Электронный ресурс] режим доступа:http://www.bnti.ru/des.asp?itm=4446&tbl=04.01.01.01.01. (24.05.2019)

4.Ананский Е.В.что такое радиозакладки и как их обнаружить? (часть2)/журнал «служба безопасности» [Электронный ресурс] режим доступ: http://www.kvirin.com/articles/267/

5. Лаптєв О.А. Грозовський Р.І. Аналіз та тенденції розвитку засобів пошуку цифрових радіозакладок //Сучасні інформаційні технології у сфері безпеки та оборони: науковий журнал, К.: УНО України імені Івана Черняховського, (2)35,2019, С 35-41.

6. Лаптєв О. А., Федоренко Р. М., Берестов Д. С. Удосконалення методики пошуку цифрових радіозакладок в діапазоні Wi-Fi //, Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського, №2(66),2019., С102-107.

7. Лаптєв О.А., Половінкін І.М, Мусієнко А.П., Клюковський Д.В. Використання метода Проні для аналізу випадкових сигналів радіомоніторингу //East European Scientific Journal, Poland, № 9 (49), 2019 part 3, P.41-46.

8. Laptiev Oleksandr, ShuklinGerman, Savchenko Vitalii, Barabash Oleg, MusienkoAndrii and Haidur Halyna, The Method of Hidden Transmitters Detection based on the Differential Transformation Model// International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 8 No. 6 (November - December 2019) Scopus Indexed - ISSN 2278 – 3091

Volkov A.N.
PhD, associate professor,
National University «Odessa Maritime Academy»

REFLECTION OF VIRTUAL REGION OF TARGET IN THE CASE OF SUPERIORITY OF ITS SPEED ABOVE SPEED OF SHIP

Волков Александр Николаевич
кандидат технических наук, доцент кафедры Судовождение,
Национальный университет "Одесская морская академия"

ОТОБРАЖЕНИЕ ВИРТУАЛЬНОЙ ОБЛАСТИ ЦЕЛИ В СЛУЧАЕ ПРЕВОСХОДСТВА ЕЕ СКОРОСТИ НАД СКОРОСТЬЮ СУДНА

Summary. The features of reflection of virtual region of target are considered, when its speed more of speed of ship. Procedure of reflection of virtual region is resulted on an electronic card and it is shown that in the situation of superiority of speed of target above speed of ship a virtual region consists of two regions, a form and location of which depend on mutual position of ship and target, and also parameters of their motion. The examples of reflection of virtual region on an electronic chart for different situations of dangerous rapprochement are resulted.

Аннотация. Рассмотрены особенности отображения виртуальной области цели, когда ее скорость больше скорости судна. Приведена процедура отображения виртуальной области на электронной карте и показано, что в ситуации превосходства скорости цели над скоростью судна виртуальная область состоит из двух подобластей, форма и расположение которых зависят от взаимной позиции судна и цели, а также параметров их движения. Приведены примеры отображения виртуальной области на электронной карте для разных ситуаций опасного сближения.

Key words: safety of navigation, preventing of collision of vessels, virtual region, features of reflection of virtual region.