ISSN 2311-7249 (Print)
ISSN 2410-7336 (Online)

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ БЕЗПЕКИ ТА ОБОРОНИ

№ 2(29)
2017

Науковий журнал

Засновник і видавець

Національний університет оборони України
імені Івана Черняховського
Журнал заснований у 2008 році

Адреса редакції

Національний університет оборони України
імені Івана Черняховського
Інститут інформаційних технологій

Повітрофлотський проспект, 28,
Київ, 03049
sitnuou@ukr.net
http://www.sit.nuou.org.ua

телефон: (044)-271-07-31, (098)-273-48-62
факс: (044)-271-07-31

Журнал зареєстровано в Державній реєстраційній службі України
(свідоцтво КВ №20490-10290ПР)

Журнал видається
українською, російською та англійською мовами

Журнал виходить 3 рази на рік

Наказом Міністерства освіти і науки України
від 29 грудня 2014 р. №1528 журнал включено до
Переліку наукових фахових видань України
в галузях "технічні науки" та "військові науки"

Рекомендовано до друку Вченою радою Національного університету оборони України імені Івана Черняховського (протокол № 12 від 31 серпня 2017 р.)

При використанні матеріалів посилання на журнал
"Сучасні інформаційні технології
у сфері безпеки та оборони" обов'язкове

Редакція може не поділяти точку зору авторів
Відповідальність за зміст поданих матеріалів
несуть автори

Журнал індексується у наукометричних базах:
Citefactor, Google Academy, Index Copernicus, The Journal Impact Factor. Directory of Research Journals Indexing (DRJI)

Журнал представлений у базах даних:
Bielefeld Academic Search Engine (BASE), Directory of Open Access Journals (DOAJ), Research Bible, WorldCat.

Журнал внесений до каталогів бібліотек:
Vernadsky National Library of Ukraine.

В номері:

MODERN INFORMATION TECHNOLOGIES IN THE SPHERE OF SECURITY AND DEFENCE

ISSN 2311-7249 (Print)
ISSN 2410-7336 (Online)

№ 2(29) 2017

Scientific journal

Founder and Publisher

National Defence University of Ukraine
named after Ivan Cherniakhovsky
The journal was founded in 2008

Address:

National Defence University of Ukraine
named after Ivan Cherniakhovsky,
Information Technology Institute

Povitroflotskiy ave. 28, Kyiv, 03049
sitnuou@ukr.net
http://www.sit.nuou.org.ua

Telephone: (044)-271-07-31, (098)-273-48-62
Fax: (044)-271-07-31

The journal is registered
in the State Registration Service of Ukraine
(certificate КВ №20490-10290ПР)

The journal is published
in Russian, Ukrainian and English

The journal is published thrice a year

According to the Document of the Ministry of Education and Science of Ukraine
issued on December 29, 2014 (№ 1528) the journal was included into the Ukrainian list of specialized scientific publications in engineering sciences and military sciences

Recommended to publication by the Scientific Council of the National Defence University of Ukraine named after Ivan Cherniakhovsky (Protocol No. 12, 31 August 2017)

The journal is indexed in the scientometric bases:
Citefactor, Google Academy, Index Copernicus, The Journal Impact Factor. Directory of Research Journals Indexing (DRJI)

The journal is presented in the databases:
Bielefeld Academic Search Engine (BASE), Directory of Open Access Journals (DOAJ), Research Bible, WorldCat.
The journal is added to the libraries:
Vernadsky National Library of Ukraine.

Contents:

УДК 355.45

Віктор Євгенович Бобильов *(канд. військ. наук, с.н.с.)*
Сергій Миколайович Кононенко
Анатолій Анатолійович Кравчук

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХОДІВ ОПЕРАТИВНОЇ ТА БОЙОВОЇ ПІДГОТОВКИ ВІЙСЬК (СИЛ) ЗБРОЙНИХ СИЛ УКРАЇНИ ЗА РАХУНОК ВИКОРИСТАННЯ НОВИХ ВИСОКОТЕХНОЛОГІЧНИХ МЕТОДІВ ЇЇ ПРОВЕДЕННЯ

Пошук шляхів шляхів підвищення ефективності заходів оперативної та бойової підготовки військ (сил) є завжди актуальним. Форми та способи ведення сучасних операцій та бойових дій постійно змінюються і потребують зовсім інших підходів для підготовки військових формувань, щоб реалізувати їх. Гібрідність сучасних війн, зразки озброєння на нових фізічних поинципах, високоточна зброя та широке застосування інформаційних технологій привели до значних змін до вимог боездатності та бойової готовності частин та підрозділів Збройних Сил України. Тому втілення нових високотехнологічних методів у підготовку військ (сил) нададуть реальну допомогу командувачам та командирам всіх рівнів військового управління у формуванні у підлеглих теоретичних знань та тверді практичні навички підготовки та проведення сучасного бою. Одним із перспективних таких шляхів є втілення у заходи оперативної та бойової підготовки військ комп'ютерних програм або засобів імітаційного моделювання бойових дій (у подальшому – імітаційне моделювання). Воно широко використовується у практиці підготовки армій провідних країн світу. На думку авторів вони також мають стати двигуном подальшого прогресу оперативної та бойової підготовки у Збройних Силах України. У статті описуються переваги використання імітаційного моделювання у ході заходів оперативної та бойової підготовки військ (сил).

Ключові слова: *оперативна та бойова підготовка, імітаційне моделювання, органи військового управління, прийняття рішень.*

Вступ

У зв'язку з агресивними діями Російської Федерації по відношенню до України та їх непередбаченного зростання перед Збройними Силами України (ЗСУ), як николи, стоїть завдання по відстоюванні незалежності України та її територіальної цілістності.

Тому важливе значення має пошук нових форм та методів ведення операцій (бойових дій), особливо в умовах ведення гібридної війни.

Одним з основних шляхів їх вироблення та підвищення боєздатності і бойової готовності частин та підрозділів ЗСУ стає удосконалення їх бойової та оперативної підготовки (ОБП) .

Найважливішою вимогою до ефективності проведення ОБП є використання тренажерів як для одиночної підготовки військовослужбовців, так і для підготовки та злагодження підрозділів, частин та органів військового управління оперативних угруповань військ (сил)[1, 4].

Постановка проблеми. Усі тренажери можна поділити на три основних види [1]:

реальні – реальні зразки озброєння та військової техніки у реальних умовах обстановки (польове заняття, навчання із проведенням бойових стрільб, навчально-бойові заняття) для підготовки військовослужбовців;

віртуальні – віртуальні зразки озброєння і військової техніки або їх компоненти (наприклад, кабіна водія або механіка-водія) у віртуальних умовах обстановки для підготовки військовослужбовців;

конструктивні (військові ігри) – комп'ютерні програми (програми імітаційного моделювання (ІМ)), які оперують віртуальними військовослужбовцями, що використовують віртуальні зразки військової техніки та озброєння і проводять бойові дії у віртуальних умовах обстановки.

На даний час дуже важливого значення набирає підготовка органів військового управління прийняттю рішень та управлінню військами в умовах ведення гібрідної війни та невизначенності більшості зовнішніх та внутрішніх факторів, що впливають на хід військових операцій (бойових дій).

Тому на перший план виходять нові високотехнолгічні методи, що використовуються для підготовки органів військового управління всіх рівнів. До них, якраз, і відносяться конструктивні тренажери (військові ігри). Основою таких тренажерних комплексів є програми імітаційного моделювання, що заснованні на використанні методу імітаційного моделювання [7].

Аналіз остатніх досліджень і публікацій.

Метод імітаційного моделювання – це метод військово-теоретичного або військово- технічного дослідження об'єкта (явища, процесу, системи) шляхом створення та вивчення його аналога (моделі) здатного заміщувати досліджуваний об'єкт у процесі дослідження з метою отримання інформації про реальну систему [3, 5].

Імітаційне моделювання являє собою процес конструювання моделі, що імітує складну реальну систему, таку як ЗСУ, та постановки експерименту на цій моделі з метою або зрозуміти поведінку системи (ЗСУ), або оцінити (в рамках відповідних обмежень) різні стратегії (способи дій), що забезпечують функціонування даної системи. Імітаційне моделювання, є методом дослідження спрямованим на опис поведінки системи; висунення припущень і гіпотез, які можуть пояснити поведінку системи; використання цих гіпотез для передбачення майбутньої її поведінки. Цей метод моделювання є одним з найдієвіших інструментів дослідження складних систем, управління якими пов'язане з прийняттям рішень в умовах невизначеності. При імітаційному моделюванні процеси функціонування системи-оригіналу підмінюються процесами, імітованими іншою системою (моделлю), але з дотриманням основних правил (режимів, алгоритмів) функціонування оригіналу [3].

У даний час існує багато типів моделювання, включаючи ті, які використовувалися роками, але використання комп'ютерного імітаційного моделювання відкриває нові горизонти. Комп'ютерне ІМ використовується в усьому світі військовими, у виробництві, у сфері освіти, а також в якості технологічного засобу, що покращує проведення підготовки, аналізу та вирішення питань, пов'язаних з розробкою та закупівлею нового обладнання, наприклад для ЗСУ.

Що ж дає використання ІМ для Збройних Сил України розглянемо нижче.

Метою статті є визначення шляхів підвищення ефективності заходів оперативної та бойової підготовки військ (сил).

Виклад основного матеріалу дослідження.

Характерними можливостями програм імітаційного моделювання є наступні [6].

ІМ – це спроба відобразити, або змоделювати реальний світ. Звісно, не увесь світ, а певні його аспекти.

ІМ може використовуватись для відігравання військових операцій (бою), в основному для проведення військових навчань різного рівня, а також може використовуватись і для їх аналізу.

ІМ – імітує дії окремих військовослужбовців (людей) або їх груп, які впливають на ефективність військових операцій (бойових дій), з врахуванням людського фактору, що базується на фізіології людини; елементи навколишнього середовища, а також погодні умови та інші фізичні явища

За допомогою ІМ можна зрозуміти ціну поразки або перемоги, при чому витрати на проведення підготовки нього, "розіграш" завдань та перегляд штабних процедур з офіцерами штабу будуть меншими ніж за умови проведення навчань без використання ІМ.

Також можна проводити з командирами та офіцерами штабів навчання за сценарієм "а що, як...", тобто відповідно до дій, які їм доведеться виконувати у реальній операції (бою).

ІМ дає можливість створювати різноманітні сценарії, які не можуть бути відтворені при проведенні реального навчання.

ІМ дозволяє розіграти дії за умов, в яких ви будете виконувати завдання перед відправкою на місце виконання цих дій.

Шляхом поєднання різноманітних засобів ІМ, можна відійти від методів підготовки, коли керівник наказує тому, хто навчається, що йому необхідно робити, що, в свою чергу, сприяє обміну ідеями між різними типами військових, цивільних та навчальних установ та закладів [7].

Під час розіграшу різноманітних навчальних сценаріїв відбувається збір даних про хід навчання. Після завершення навчання результати аналізу їх проведення з відповідними висновками можуть надаватись командирам та офіцерам штабів для удосконалення своїх фахових знань та практичних навичок.

ІМ – це економічний засіб проведення заходів оперативної підготовки з великою кількістю військовослужбовців одночасно. При цьому підготовка може проводитись в різних регіонах країни, без необхідності витрачати кошти на дорогу.

ІМ дозволяє не витрачатись на здійснення сухопутних та повітряних перміщень, що неможливо при проведенні реального навчання.

Аналітики використовують ІМ, як допоміжний засіб у визначенні правильного сполучення сил для забезпечення національних військових цілей.

Виходячі з наведенних характеристик імітаційного моделювання в Україні визначено три сфери для застосування ІМ. Серед них:

Бойова підготовка окремих солдат та офіцерів або невеликих підрозділів. Збройні Сили України будуть продовжувати застосовувати традиційну індивідуальну підготовку навичкам у бою, але також будуть використовувати технології ІМ наскільки це можливо [2].

Аналіз планів військових операції бойових дій). Аналіз планів операцій базується на традиційному вивченні місцевості, а також дружніх сил та сил противника. За допомогою комп'ютерних технологій ІМ можливо проводити більш систематичний та детальний аналіз можливих планів операцій, а також визначити найшвидший, найбезпечніший та найбільш ефективний варіант плану операції в умовах, що склалися [5].

Також слід звернути увагу на операції з підтримки миру, так як ІМ дозволяє підготуватися до участі у таких операціях у складі коаліційних

сил ООН, в рамках програми Партнерство заради миру, які використовують тренажери ІМ на міжнародному рівні для підготовки до такого типу операцій.

Крім того, ІМ дозволяє відпрацювати практичні навички роботи в штабах. Також воно в змозі повністю відтворити процеси технічного забезпечення та ремонту. Існує можливість відображення місцезнаходження припасів та найкращого шляху їх доставки у пункт призначення. ІМ здатне відобразити місцевість, противника, цивільне населення та навіть повсякденні дії, тобто пересування військ противника і інше відображаються у змінах на екрані [6].

Офіцери мають можливість відпрацювання штабних процедур без розгортання сил. При правильному застосуванні ІМ офіцери штабу не помітять різниці між реальним навчанням і навчанням з застосуванням ІМ.

Окремі солдати, екіпажі та невеликі підрозділи можуть відпрацьовувати різноманітні навички, або поведінку у небезпечних умовах операції (бойових дій), до остаточного їх опанування.

Можна побачити позитивні вплив на вартість навчання зі зростанням рівня використання ІМ, що є дуже важливим в умовах недостатнього фінансування ЗСУ.

Таким чином, ІМ має дуже широкий спектр характеристик, що дозволяє зробити його найкращим вибором для подальшого удосконалення заходів з ОБП військ (сил).

Висновки й перспективи подальших досліджень

Спираючись на міркування, що наведенні вище можна зробити деяки висновки.

По-перше, використання ІМ приведе до покращення боєздатності та бойової готовності військ (сил) ЗСУ.

По-друге, дозволить покращіти та вдосконалити технологічний потенціал ЗС України.

А також, використання ІМ дозволить створити єдину та досконалу технологічну інфраструктуру, яка буде відповідати вимогам підготовки ЗСУ як на оперативно-тактичному так і нас стратегічному рівні, що надасть можливість вдосконалювати теоретичні та практичні навички як командирів та офіцерів органів військового управління різного рівня, так і окремих солдат та невеликих підрозділів (невеликі підрозділи можуть відпрацьовувати певні навички або проводити підготовку до виконання небезпечних завдань до досягнення необхідного рівня майстерності).

Література

1. Імітаційне моделювання у практиці підготовки військ : навч. посіб. / колектив авторів; за заг. ред. О. Ю. Пермякова. – К. : НУОУ ім. Івана Черняховського, 2015. – 120 с.
2. Методика підготовки і проведення командно-штабних навчань за допомогою комп'ютерів з використанням технологій імітаційного моделювання. – Київ: НУОУ, 2011, - 59 с.
3. Основи імітаційного моделювання. Навчальний посібник. - Київ: НАОУ, 2005, - 26 с.
4. Перспективи застосування інформаційних технологій в збройній боротьбі. Аналітичний матеріал каф. інформатизації штабів. НАОУ. – Київ: 2003, -20 с.
5. Шеннон Р. Имитационное моделирование систем: искусство и наука. М., изд. "Мир", 1978, 418 с.
6. Joint Conflict & Tactical Simulation (JCATS 13.0). Довідник (скорочене видання). – Об'єднане командування США, об'єднаний військовий центр (Суффолк, США).
7. Engineering principles of Combat Modeling ahd Distributed Simulation? First Edition. Edited by Andreas Tolk. John Wiley & Sons, Inc. Published 2012.

Повышение эфективности мероприятий оперативной и боевой подготовки войск (сил) Вооруженных Сил Украины за счет использования высокотехнологичных методов ее проведения

Виктор Евгеньевич Бобылёв *(канд. воен. наук, с.н.с.)*
Сергей Николаевич Кононенко
Анатолий Анатольевич Кравчук

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Поиск путей путей повышения эфективности мераприятий оперативной и боевой подготовки войск (сил) является всегда актуальным. Формы и способы ведения современных операций и боевых действий постоянно меняются и требуют совершенно других подходов для подготовки воинских формирований, чтобы реализовать их. Гибриднисть современных войн, образцы вооружения на новых физических поинципах, високоточное оружие и широкое применение информационных технологий привели к значительным изменениям к требованиям боеспособности и боевой готовности частей и

подразделений Вооруженных Сил Украины. Поэтому внедрение новых высокотехнологичных методов в подготовку войск (сил) предоставит реальную помощь командующему и командирам всех уровней военного управления в формировании у подчиненных теоретических знаний и твердых практические навыков подготовки ведения современного боя. Одним из таких перспективных путей является внедрение в мероприятия оперативной и боевой подготовки войск компьютерных программ или средств имитационного моделирования боевых действий (дальше - имитационное моделирование). Оно широко применяется в практике подготовки армий ведущих стран мира. По мнению авторов они так же могут стать двигателем дальнейшего прогресса оперативной и боевой подготовки в Вооруженных Силах Украины. В статье описываются преимущества использования имитационного моделирования в ходе мероприятий оперативной и боевой подготовки войск (сил).

***Ключевые слова**: оперативная и боевая подготовка, имитационное моделирование, органы военного управления, принятия решений.*

Increasing the effectiveness of the operational and combat training of troops (forces) of the Armed Forces of Ukraine due to the use of new high-tech methods for its implementation.

***Viktor Y. Bobylov** (Candidate of Military Sciences, Senior Research Fellow)*
Serhii M. Kononenko
Anatolii A. Kravchuk

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

Finding ways to improve the effectiveness of operational and combat training of troops (forces) is always relevant. The forms and methods of conducting modern operations and battle are constantly changing and require quite different approaches for the training of military formations to implement them. The gibberish nature of modern wars, patterns of weapons on new physical features, high-precision weapons and the widespread use of information technology have brought about significant changes to the requirements of combat capability and combat readiness of troops and units of the Armed Forces of Ukraine. Therefore, the implementation of new high-tech methods in the training of troops (forces) will provide real help to the commanders and agency of all levels of military management in shaping the subordinate theoretical knowledge and solid practical skills in preparing and conducting a modern battle. One of the most promising ways of this is the implementation of computer programs or means of simulation of combat operations (hereinafter - simulation) in the operational and combat training of troops. It is widely used in the practice of preparing the armies of the leading countries of the world. According to the authors, they should also become the engine for further progress of operational and combat training in the Armed Forces of Ukraine. The article describes the advantages of using simulation for operational and combat training of troops (forces).

***Key words**: operational and combat training, simulation, military management agency, decision making.*

References

1. Simulation in the training of troops: teach. manual / Collective of authors; Per community Ed. O.Yu. Permyakov. - K.: Ivan Chernyakhovsky NDUU, 2015. 120p.
2. Method of training and conducting command post exercises using computers and simulation techniques. -Kyiv: NDUU, 2011, -59p.
3. Fundamentals of simulation. Tutorial. - Kyiv: NDAU, 2005, 26p.
4. Prospects for the use of information technology in armed struggle. Analytical material Departmet of staffs informatization. NDAU - Kyiv: 2003, -20 p.
5. Shannon R. Simulation systems: art and science. M., ed. "Mir", 1978, 418 p.
6. Joint Conflict & Tactical Simulation (JCATS 13.0). Directory (short edition). - United Allied Command, United Military Center (Suffolk, USA).
7. Engineering principles of Combat Modeling ahd Distributed Simulation? First edition Edited by Andreas Tolk. John Wiley & Sons, Inc. Published in 2012.

УДК [623.611:621.396]:519.876.5

Анатолій Петрович Волобуєв
Дмитро Анатолійович Бухал

Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ВИЯВЛЕННЯ СИСТЕМОЮ РАДІОРОЗВІДКИ ПРОТИВНИКА СИСТЕМИ РАДІОЗВ'ЯЗКУ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ, ЯКА ЗАСТОСОВУЄ ШУМОПОДІБНІ СИГНАЛИ З ДИСКРЕТНОЮ ЧАСТОТНОЮ МОДУЛЯЦІЄЮ ПСЕВДОВИПАДКОВОЮ ПОСЛІДОВНІСТЮ

У статті запропоновано метод математичного моделювання виявлення системою радіорозвідки систем радіозв'язку військового призначення, які застосовують шумоподібні сигнали з дискретною частотною модуляцією псевдовипадковою послідовністю. Зазначена задача математичного моделювання вирішується в інтересах оцінювання рівня радіомаскування систем радіозв'язку військового призначення відносно до систем радіорозвідки нового покоління провідних країн світу, яким притаманні суттєво ширші розвідувальні спроможності. Застосовуючи апарат тензорного числення для моделювання, вдалося покласти в основу оцінювання рівня радіомаскування підходи, притаманні електродинаміці, і забезпечити прийнятну адекватність моделі виявлення. Крім того, наряду з радіостанціями, які застосовують шумоподібні сигнали дискретною частотною модуляцією псевдовипадковою послідовністю, під час моделювання розглянуто розгортання хибних радіомереж в інтересах забезпечення необхідного рівня радіомаскування системи радіозв'язку військового призначення.

Ключові слова: *система радіорозвідки, система радіозв'язку військового призначення, математичне моделювання, електромагнітне поле, рівень радіомаскування, шумоподібні сигнали.*

Вступ

Постановка проблеми. Стрімкий розвиток систем радіорозвідки в збройних силах розвинутих у воєнному відношенні країн світу і появу систем радіорозвідки нового покоління [1-2] та відставання України у питаннях створення сучасних розвідзахищених систем радіозв'язку військового призначення, викликав невідповідність між наявними спроможностями систем радіозв'язку військового призначення щодо боротьби з системами радіорозвідки та спроможностями, які потрібні для боротьби з системами радіорозвідки нового покоління. Тобто не забезпечується необхідний рівень радіомаскування систем радіозв'язку військового призначення. Надання рекомендацій стосовно боротьби систем радіозв'язку військового призначення з системами радіорозвідки з метою забезпечення необхідного рівня радіомаскування є завданням теорії радіомаскування систем радіозв'язку військового призначення. Означена мета досягається розв'язанням низки часткових завдань, одним з яких є оцінювання рівня радіомаскування системи радіозв'язку військового призначення, що вимагає застосування відповідного методичного апарату.

Аналіз останніх досліджень і публікацій. Дослідження, пов'язані з розробляннням методичного апарату оцінювання рівня радіомаскування систем (засобів) радіозв'язку військового призначення, в різні часи проводилися такими науковцями як Палій А.І., Сіфоров В.І, Ізюмов Н.М., Вартанесян В.А., Цветнов В.В., Демін В.П., Купріянов А.І., Макаренко С.І., Каневський З.М., Літвіненко В.П., Макаров Г.В. та іншими [3-11]. У відомих публікаціях даних авторів пропонується оцінювання рівня радіомаскування системи (засобу) радіозв'язку військового призначення здійснювати за більш ніж двадцятьма ймовірнісними показниками, такими як ймовірність виявлення засобу радіозв'язку за заданий час; математичне очікування часу виявлення засобу радіозв'язку із заданими параметрами; ймовірність пелентування засобу радіозв'язку із заданими параметрами тощо. До появи систем радіорозвідки нового покоління застосування даних показників можна вважати обґрунтованим, тому що приймання радіосигналів систем радіозв'язку військового призначення можливе лише на фоні завад, в умовах змін параметрів операційного району, як середовища розповсюдження електромагнітних хвиль та дії інших непередбачуваних факторів. Тому виявлення радіосигналів систем радіозв'язку військового призначення є випадковим, помилки визначення параметрів радіосигналів – випадкові, а висновки та рішення, які радіорозвідка приймає на основі результатів приймання та обробляння радіосигналу, можуть бути помилковими. Але ймовірнісним показникам притаманний суттєвий недолік, а саме, перевірка адекватності аналітичних співвідношень для таких показників вимагає суттєвих обсягів статистичного матеріалу, що далеко не завжди можливо, а системи радіорозвідки нового покоління набули спроможностей щодо викриття засобів радіозв'язку майже миттєво з ймовірністю близькою до одиниці за умови їх розвідувальної доступності [1].

Отже, авторами за допомогою різноманітних методів математичного моделювання отримані відповідні аналітичні співвідношення для зазначених

показників. Детальний аналіз даних співвідношень дозволяє зробити висновок, що математичні моделі систем радіорозвідки противника, які використовувалися авторами під час отримання аналітичних співвідношень для показників рівня радіомаскування систем (засобів) радіозв'язку військового призначення, не відповідають системам радіорозвідки нового покоління. Зокрема, не враховується той факт, що всі види сучасних засобів радіорозвідки, а саме космічні, стратосферні, повітряні, наземні та морські, працюють як єдина система радіорозвідки, що дозволяє забезпечити безпрецедентну розвідувальну доступність систем радіозв'язку військового призначення. Зазначеним системам притаманний також високий рівень автоматизації, використання сучасної високопродуктивної розвідувальної радіоелектронної апаратури (підвищеної чутливості) та програмного забезпечення. Системи радіорозвідки нового покоління набули спроможності щодо виявлення і перехоплення складних (шумоподібних) радіосигналів (зокрема радіосигналів із дискретною частотною модуляцією (ДЧМ) псевдовипадковою послідовністю (ПВП)), сигналів малої тривалості та сигналів які передаються за протоколами маршрутизації пакетів. Реалізовано метод однопозиційного виявлення місцеположення. До того ж, у відомих аналітичних співвідношеннях для показників рівня радіомаскування не враховуються координати місцеположення засобів радіозв'язку військового призначення та засобів радіорозвідки противника (як відомі так і передбачувані), наявність хибних радіомереж.

Таким чином, оцінювання рівня радіомаскування систем радіозв'язку військового призначення за допомогою відомих аналітичних співвідношень для показників рівня радіомаскування, особливо в умовах високої динаміки обстановки на полі бою та застосування систем радіорозвідки нового покоління, не дозволить отримати коректні оцінки. Насамперед через відсутність у складі відомого методичного апарату оцінювання рівня радіомаскування систем радіозв'язку військового призначення методів математичного і математичних моделей, спроможних відобразити та врахувати розвідувальні спроможності систем радіорозвідки нового покоління, що обумовлює потребу у розроблянні подібних методів і моделей.

Мета статті полягає в розроблянні методу математичного моделювання виявлення системи радіозв'язку військового призначення системою радіорозвідки противника, який враховує наявність хибних радіомереж, координати місцеположення засобів радіозв'язку військового призначення та засобів радіорозвідки противника (як відомі так і передбачувані), спроможність систем радіорозвідки нового покоління виявляти шумоподібні сигнали з ДЧМ ПВП і може бути використаним для вирішення завдання оцінювання рівня радіомаскування системи радіозв'язку військового призначення під час забезпечення необхідного рівня радіомаскування.

Методи дослідження

У ході дослідження були застосовані основні положення математичного апарата тензорного числення на основі теорії електродинаміки та теорії зв'язку.

Виклад основного матеріалу дослідження

Будемо вважати, що система радіорозвідки нового покоління розгорнута на Q засобах радіорозвідки, а система радіозв'язку військового призначення розгортається на M радіостанціях, що застосовують сигнали з ДЧМ ПВП. Крім того, додатково розгортаються хибні радіомережі на $M_{хиб}$ хибних радіостанціях. Всі види засобів радіорозвідки, а саме космічні, стратосферні, повітряні, наземні та морські, працюють як єдина система, що обумовлює необхідність оцінювання розвідувальних доступностей радіостанцій для всіх засобів радіорозвідки, спираючись на координати місць їх розміщення, відомі від своєї розвідки або передбачувані нею.

В основу методу математичного моделювання покладене положення електродинаміки [12], згідно з яким електромагнітне поле в будь-якій точці простору подається антисиметричним 4-тензором 2 рангу, так званим тензором поля:

$$\mathbf{F}=\begin{pmatrix} 0 & \left(\frac{\partial}{\partial t}A_1-\frac{\partial}{\partial x}A_0\right) & \left(\frac{\partial}{\partial t}A_2-\frac{\partial}{\partial y}A_0\right) & \left(\frac{\partial}{\partial t}A_3-\frac{\partial}{\partial z}A_0\right) \\ -\left(\frac{\partial}{\partial t}A_1-\frac{\partial}{\partial x}A_0\right) & 0 & -\left(\frac{\partial}{\partial y}A_1-\frac{\partial}{\partial x}A_2\right) & \left(\frac{\partial}{\partial x}A_3-\frac{\partial}{\partial z}A_1\right) \\ -\left(\frac{\partial}{\partial t}A_2-\frac{\partial}{\partial y}A_0\right) & \left(\frac{\partial}{\partial y}A_1-\frac{\partial}{\partial x}A_2\right) & 0 & -\left(\frac{\partial}{\partial z}A_2-\frac{\partial}{\partial y}A_3\right) \\ -\left(\frac{\partial}{\partial t}A_3-\frac{\partial}{\partial z}A_0\right) & -\left(\frac{\partial}{\partial x}A_3-\frac{\partial}{\partial z}A_1\right) & \left(\frac{\partial}{\partial z}A_2-\frac{\partial}{\partial y}A_3\right) & 0 \end{pmatrix}, \quad (1)$$

де $(A_0, A_1, A_2, A_3) = \mathbf{A}$ - потенціал електромагнітного поля, створеного радіостанцією.

Сигнали з ДЧМ ПВП утворюються в результаті стрибкоподібної зміни несучої частоти за законом деякої періодичної числової послідовності при незмінних амплітуді та кроці квантування за частотою і часом. Вираз, що описує один період $[0,T]$ сигналу з ДЧМ ПВП та відсутністю стрибків фази в моменти переключення частоти можна подати у вигляді [13,14]:

$$J(t)=Jd(t)\sum_{k=1}^{K}u\left(t-(k-1)t_u\right)\exp\left\{i2\pi\left(f_0+(N_k-D)\Delta f\right)t+\gamma_0\right\},\quad 0\le t\le Kt_u, \quad (2)$$

де J - амплітуда сигналу ($J=\sqrt{2P}$, P – потужність сигналу);

$$d(t)=\begin{cases}1 & при\ 0\le t\le T_b;\\ 0 & при\ t\notin[0,T_b]\end{cases}$$

T_b - тривалість передавання одного біта інформації;

K - кількість елементів кодової послідовності на тривалість біта інформації ($K=T_b/t_u$);

t_u – тривалість елементу кодової послідовності;

$u\left(t-(k-1)t_u\right)=\begin{cases}1 & при\ (k-1)t_u\le t\le kt_u,\\ 0 & при\ t<(k-1)t_u,\ t>kt_u\end{cases}$ - функція одиничного стрибка;

$f_0=sf_t$ (для цілих чисел s) - несуча частота;

f_t – тактова частота вироблення сигналу генератором тактової частоти;

$\Delta f=cf_t$ – дискрет частоти (для цілих чисел c);

$N_k\in\overline{1,K}$; $N_s=N_g$ *при* $s=g$ - числова послідовність;

$D=(K+1)/2$;

γ_0 - початкова фаза сигналу ($\gamma_0\in[0,2\pi]$).

Спираючись на [12-15], складові потенціалу електромагнітного поля в реальних (або передбачуваних) місцях знаходження засобів радіорозвідки противника для радіостанцій з антенною решіткою, що застосовують складні (шумоподібні) сигнали з ДЧМ ПВП можна подати таким чином:

$$(A_1)_{mq}=\frac{\mu L_{mq}}{4\pi}\sum_{n=0}^{N-1}\sum_{k=1}^{K}j_{m_{n_x}}u\left(t-(k-1)t_u\right)\exp\left\{i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)t+\gamma_{0_{m_{n_x}}}\right\}\times$$
$$\times\frac{\exp\left(-i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)\sqrt{\varepsilon\mu}\sqrt{\left(x_{зp_q}-x_{m_n}\right)^2+\left(y_{зp_q}-y_{m_n}\right)^2+\left(z_{зp_q}-z_{m_n}\right)^2}\right)}{\sqrt{\left(x_{зp_q}-x_{m_n}\right)^2+\left(y_{зp_q}-y_{m_n}\right)^2+\left(z_{зp_q}-z_{m_n}\right)^2}},\qquad(3)$$

$$(A_2)_{mq}=\frac{\mu L_{mq}}{4\pi}\sum_{n=0}^{N-1}\sum_{k=1}^{K}j_{m_{n_y}}u\left(t-(k-1)t_u\right)\exp\left\{i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)t+\gamma_{0_{m_{n_y}}}\right\}\times$$
$$\times\frac{\exp\left(-i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)\sqrt{\varepsilon\mu}\sqrt{\left(x_{зp_q}-x_{m_n}\right)^2+\left(y_{зp_q}-y_{m_n}\right)^2+\left(z_{зp_q}-z_{m_n}\right)^2}\right)}{\sqrt{\left(x_{зp_q}-x_{m_n}\right)^2+\left(y_{зp_q}-y_{m_n}\right)^2+\left(z_{зp_q}-z_{m_n}\right)^2}},\qquad(4)$$

$$(A_3)_{mq}=\frac{\mu L_{mq}}{4\pi}\sum_{n=0}^{N-1}\sum_{k=1}^{K}j_{m_{n_z}}u\left(t-(k-1)t_u\right)\exp\left\{i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)t+\gamma_{0_{m_{n_z}}}\right\}\times$$
$$\times\frac{\exp\left(-i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)\sqrt{\varepsilon\mu}\sqrt{\left(x_{зp_q}-x_{m_n}\right)^2+\left(y_{зp_q}-y_{m_n}\right)^2+\left(z_{зp_q}-z_{m_n}\right)^2}\right)}{\sqrt{\left(x_{зp_q}-x_{m_n}\right)^2+\left(y_{зp_q}-y_{m_n}\right)^2+\left(z_{зp_q}-z_{m_n}\right)^2}},\qquad(5)$$

$$(A_0)_{mq}=\frac{\frac{\partial}{\partial x_{зp_q}}(A_1)_{mq}+\frac{\partial}{\partial y_{зp_q}}(A_2)_{mq}+\frac{\partial}{\partial z_{зp_q}}(A_3)_{mq}}{-i2\pi\varepsilon\mu\sum_{k=1}^{K}\left\{f_{0_m}+(N_k-D)\Delta f_m\right\}}.\qquad(6)$$

де $\left((A_0)_{mq},(A_1)_{mq},(A_2)_{mq},(A_3)_{mq}\right)=\mathbf{A}_{mq}$ – потенціал електромагнітного поля, створеного m-ю радіостанцією в реальному (або передбачуваному) місті знаходження q-го засобу радіорозвідки;

μ – абсолютна магнітна проникність операційного району, як середовища розповсюдження електромагнітних хвиль, Гн/м (якщо антена радіостанції знаходиться у повітрі $\mu=4\pi\times10^{-7}$ Гн/м);

N – кількість випромінювачів в антенній решітці радіостанції;

L_{mq} – функція ослаблення електромагнітної хвилі в напрямку від m–ї радіостанції на q–й засіб радіорозвідки;

$\left(j_{m_{n_x}},j_{m_{n_y}},j_{m_{n_z}}\right)$ – проекції вектору амплітуди щільності електричного струму в n–му випромінювачеві антенної решітки m–ї радіостанції;

$i=\sqrt{-1}$;

f_{0_m} – несуча частота випромінювання m–ї радіостанції (ГГц);

$\left(\gamma_{0_{m_{n_x}}},\gamma_{0_{m_{n_y}}},\gamma_{0_{m_{n_z}}}\right)$ – проекції вектору початкових фаз щільності електричного струму в n–му випромінювачеві антенної решітки m–ї радіостанції;

ε – абсолютна діелектрична проникність операційного району, як середовища розповсюдження електромагнітних хвиль, ф/м (якщо антена радіостанції знаходиться у повітрі $\varepsilon=\frac{10^{-9}}{36\pi}$ ф/м);

$\left(x_{m_n}, y_{m_n}, z_{m_n}\right)$ – координати n–го випромінювача антенної решітки m–ї радіостанції;

$\left(x_{зp_q}, y_{зp_q}, z_{зp_q}\right)$ – реальні (або передбачувані) координати q–го засобу радіорозвідки.

Умови ведення радіорозвідки зазвичай такі, що засобам радіорозвідки достеменно невідомо, з яким сигналом вони будуть мати справу. Тому єдиною ознакою наявності сигналу на вході приймача засобу радіорозвідки може служити те, в якій ступені потужність цього коливання перевищує потужність власних шумів приймача. Судити про рівень потужності прийнятого коливання можна по її оцінці, сформованій за деякий час спостереження T.

Для вирішення подібних задач застосовується, як відомо [13,14,16], приймач, оптимальний для виявлення невідомого сигналу лише по оцінці потужності (енергії) процесу, що спостерігається. Цей приймач фільтрує вхідне коливання у визначеній полосі частот, детектує квадратичним детектором та інтегрує за час спостереження T. Нормований до T результат інтегрування – є оцінкою потужності вхідного коливання. Вона порівнюється в компараторі з наперед обраним порогом. Якщо поріг перевищено, то приймається рішення про наявність на вході приймача засобу радіорозвідки корисного сигналу. Таким чином, можна ввести коефіцієнт електромагнітної доступності m–ї радіостанції для q–го засобу радіорозвідки:

$$Э_{mq} = \frac{\int_0^T P_{mq}(t)}{P_{пор_q} T}, \qquad (7)$$

де $P_{mq}(t)$ – миттєва потужність електромагнітного поля, яке створює m–а радіостанція в місці знаходження q–го засобу радіорозвідки;

$P_{пор_q}$ – поріг для q–го засобу радіорозвідки.

Як відомо з [12]

$$P_{mq}(t) = \frac{E_{mq}^2(t) + H_{mq}^2(t)}{4\pi}, \qquad (8)$$

де $E(t), H(t)$ – відповідно миттєві напруженості електричного та магнітного полів.

При чому

$$E_{mq}^2(t) = E_{mq_x}^2(t) + E_{mq_y}^2(t) + E_{mq_z}^2(t), \qquad (9)$$

$$H_{mq}^2(t) = H_{mq_x}^2(t) + H_{mq_y}^2(t) + H_{mq_z}^2(t), \qquad (10)$$

де $\left(E_{mq_x}(t), E_{mq_y}(t), E_{mq_z}(t)\right)$,

$\left(H_{mq_x}(t), H_{mq_y}(t), H_{mq_z}(t)\right)$ – відповідно проекції миттєвих напруженостей електричного та магнітного полів в обраній системі координат.

Зазначені проекції є компонентами тензору електромагнітного поля (1), що дозволяє подати коефіцієнт електромагнітної доступності m–ї радіостанції для q–го засобу радіорозвідки так:

$$Э_{mq} = \frac{\int_0^T \left(F_{mq_{01}}^2(t) + F_{mq_{02}}^2(t) + F_{mq_{03}}^2(t) + F_{mq_{32}}^2(t) + F_{mq_{13}}^2(t) + F_{mq_{21}}^2(t)\right)}{4\pi P_{пор_q} T}, \qquad (11)$$

або через потенціал електромагнітного поля

$$Э_{mq} = \frac{1}{4\pi P_{пор_q} T} \int_0^T \left[\left(\frac{\partial}{\partial t}(A_1)_{mq} - \frac{\partial}{\partial x_{зp_q}}(A_0)_{mq}\right)^2 + \left(\frac{\partial}{\partial t}(A_2)_{mq} - \frac{\partial}{\partial y_{зp_q}}(A_0)_{mq}\right)^2 + \right.$$
$$+ \left(\frac{\partial}{\partial t}(A_3)_{mq} - \frac{\partial}{\partial z_{зp_q}}(A_0)_{mq}\right)^2 + \left(\frac{\partial}{\partial t}(A_2)_{mq} - \frac{\partial}{\partial y_{зp_q}}(A_3)_{mq}\right)^2 +$$
$$\left. + \left(\frac{\partial}{\partial x_{зp_q}}(A_3)_{mq} - \frac{\partial}{\partial z_{зp_q}}(A_1)_{mq}\right)^2 + \left(\frac{\partial}{\partial y_{зp_q}}(A_1)_{mq} - \frac{\partial}{\partial x_{зp_q}}(A_2)_{mq}\right)^2 \right] dt. \qquad (12)$$

Враховуючи (2–6), складові коефіцієнту електромагнітної доступності m–ї радіостанції для q–го засобу радіорозвідки матимуть такий вигляд (наприклад для $F_{mq_{01}}(t) = \frac{\partial}{\partial t}(A_1)_{mq} - \frac{\partial}{\partial x_{зp_q}}(A_0)_{mq}$, решта складових розраховується аналогічно):

$$\frac{\partial}{\partial t}(A_1)_{mq} = \frac{m L_{mq}}{4\pi} \sum_{n=0}^{N-1} \sum_{k=1}^{K} \exp\left\{i2\pi\left[\left(f_{0_m} + (N_k - D)\Delta f_m\right)t + \gamma_{0_{m_{n_x}}} u\left(t - (k-1)t_u\right)\left(f_{0_m} + (N_k - D)\Delta f_m\right)\right]\right\} \times$$
$$\times \frac{\exp\left(-i2\pi\left(f_{0_m} + (N_k - D)\Delta f_m\right)\sqrt{\varepsilon_m}\sqrt{\left(x_{зp_q} - x_{m_n}\right)^2 + \left(y_{зp_q} - y_{m_n}\right)^2 + \left(z_{зp_q} - z_{m_n}\right)^2}\right)}{\sqrt{\left(x_{зp_q} - x_{m_n}\right)^2 + \left(y_{зp_q} - y_{m_n}\right)^2 + \left(z_{зp_q} - z_{m_n}\right)^2}}, \qquad (13)$$

$$\frac{\partial}{\partial x_{зp_q}}(A_0)_{mq} = \frac{1}{-i2\pi f_{0_m} \varepsilon_m} \frac{\partial}{\partial x_{зp_q}}\left(\frac{\partial}{\partial x_{зp_q}}(A_1)_{mq} + \frac{\partial}{\partial y_{зp_q}}(A_2)_{mq} + \frac{\partial}{\partial z_{зp_q}}(A_3)_{mq}\right), \qquad (14)$$

де $\frac{\partial}{\partial x_{зр_q}}\left(\frac{\partial}{\partial x_{зр_q}}(A_1)_{mq}\right) = \frac{m\lambda_{mq}}{4\pi}\sum_{n=0}^{N-1}\sum_{k=1}^{K} j_{m_{n_x}}\left[t-(k-1)t_u\right]\cdot \exp\left\{i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)t+\gamma_{0_{m_{n_x}}}\right\}\cdot$

$$\cdot \exp\left(-i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)\sqrt{\varepsilon\mu}\sqrt{\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2}\right)\cdot$$

$$\cdot\left[\frac{3\left(x_{зр_q}-x_{m_n}\right)^2}{\left[\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2\right]^{\frac{5}{2}}}-\frac{1-4\pi^2\left(f_{0_m}+(N_k-D)\Delta f_m\right)^2\varepsilon\mu\left(x_{зр_q}-x_{m_n}\right)^2}{\left[\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2\right]^{\frac{3}{2}}}+\right.$$

$$\left.+\frac{i6\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)\sqrt{\varepsilon\mu}\left(x_{зр_q}-x_{m_n}\right)^2}{\left[\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2\right]^2}-\frac{i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)\sqrt{\varepsilon\mu}}{\left[\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2\right]^{\frac{1}{2}}}\right\}, \quad (15)$$

$$\frac{\partial}{\partial x_{зр_q}}\left(\frac{\partial}{\partial y_{зр_q}}(A_2)_{mq}\right) = \frac{m\lambda_{mq}}{4\pi}\sum_{n=0}^{N-1}\sum_{k=1}^{K} j_{m_{n_y}}\left[t-(k-1)t_u\right]\cdot \exp\left\{i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)t+\gamma_{0_{m_{n_y}}}\right\}\cdot$$

$$\cdot \exp\left(-i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)\sqrt{\varepsilon\mu}\sqrt{\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2}\right)\cdot$$

$$\cdot\left[\frac{3\left(x_{зр_q}-x_{m_n}\right)\left(y_{зр_q}-y_{m_n}\right)}{\left[\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2\right]^{\frac{5}{2}}}-\frac{4\pi^2\left(f_{0_m}+(N_k-D)\Delta f_m\right)^2\varepsilon\mu\left(x_{зр_q}-x_{m_n}\right)\left(y_{зр_q}-y_{m_n}\right)}{\left[\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2\right]^{\frac{3}{2}}}+\right.$$

$$\left.+\frac{i6\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)\sqrt{\varepsilon\mu}\left(x_{зр_q}-x_{m_n}\right)\left(y_{зр_q}-y_{m_n}\right)}{\left[\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2\right]^2}\right\}, \quad (16)$$

$$\frac{\partial}{\partial x_{зр_q}}\left(\frac{\partial}{\partial z_{зр_q}}(A_3)_{mq}\right) = \frac{m\lambda_{mq}}{4\pi}\sum_{n=0}^{N-1}\sum_{k=1}^{K} j_{m_{n_z}}\left[t-(k-1)t_u\right]\cdot \exp\left\{i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)t+\gamma_{0_{m_{n_z}}}\right\}\cdot$$

$$\cdot \exp\left(-i2\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)\sqrt{\varepsilon\mu}\sqrt{\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2}\right)\cdot$$

$$\cdot\left[\frac{3\left(x_{зр_q}-x_{m_n}\right)\left(z_{зр_q}-z_{m_n}\right)}{\left[\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2\right]^{\frac{5}{2}}}-\frac{4\pi^2\left(f_{0_m}+(N_k-D)\Delta f_m\right)^2\varepsilon\mu\left(x_{зр_q}-x_{m_n}\right)\left(z_{зр_q}-z_{m_n}\right)}{\left[\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2\right]^{\frac{3}{2}}}+\right.$$

$$\left.+\frac{i6\pi\left(f_{0_m}+(N_k-D)\Delta f_m\right)\sqrt{\varepsilon\mu}\left(x_{зр_q}-x_{m_n}\right)\left(z_{зр_q}-z_{m_n}\right)}{\left[\left(x_{зр_q}-x_{m_n}\right)^2+\left(y_{зр_q}-y_{m_n}\right)^2+\left(z_{зр_q}-z_{m_n}\right)^2\right]^2}\right\}. \quad (17)$$

Для радіостанцій, які застосовують сигнали з ДЧМ ПВП доцільно прийняти такий критерій замаскованості:

$$\begin{cases} Э_{mq} < 1 \\ t_m / t_{зр_q} < 1 \\ f_{m_{дчм}} / f_{пор_{q_{дчм}}} < 1 \end{cases}, \quad (18)$$

де t_m – тривалість роботи на передачу m–ї радіостанції; $t_{зр_q}$ – час реакції q–го засобу радіорозвідки; $f_{m_{дчм}}$ – тактова частота ПВП, яка модулює частоту сигналу m–ї радіостанції; $f_{пор_{q_{дчм}}}$ – порогове значення тактової частоти ПВП, яка модулює частоту сигналу радіостанції, вище якого q–й засіб радіорозвідки не спроможний виявляти роботу радіостанцій, що працюють в режимі ДЧМ ПВП.

Якщо умови (18) не виконуються одночасно для трьох різних засобів радіорозвідки, то радіостанція вважається незамаскованою, що пов'язано з потребою у трьох пеленгах на радіостанцію для визначення її

місцеположення системою радіорозвідки. В окремих випадках, зокрема для КХ радіостанцій та наявності в системі радіорозвідки противника засобів радіорозвідки, спроможних реалізовувати метод однопозиційного визначення місцеположення, достатньо невиконання умов (18) для одного засобу радіорозвідки.

Таким чином, застосовуючи запропонований критерій (18) можна оцінити кількість замаскованих радіостанцій в системі радіозв'язку військового призначення $M_{зм}$. При цьому рівень радіомаскування системи радіозв'язку військового призначення для системи радіорозвідки противника пропонується оцінювати за показником розвідувальної доступності, а саме:

$$R = \frac{M_{зм} + M_{хиб}}{M} 100\%, \qquad (19)$$

де $M_{хиб}$ – кількість хибних радіостанцій, які розгортаються з метою радіомаскування поза межами загальної кількості радіостанцій в системі радіозв'язку M.

Висновки й перспективи подальших досліджень

Запропонований метод математичного моделювання дозволяє оцінити рівень радіомаскування систем радіозв'язку військового призначення, які застосовують шумоподібні сигнали з ДЧМ ПВП, з урахуванням розвідувальних спроможностей систем радіорозвідки нового покоління, координат місцеположення засобів радіозв'язку військового призначення та засобів радіорозвідки противника (як відомих так і передбачуваних), параметрів шумоподібних сигналів з ДЧМ ПВП та наявності хибних радіомереж. В майбутніх роботах доцільно зосередити зусилля на проблемах математичного моделювання виявлення системами радіорозвідки нового покоління систем радіозв'язку військового призначення, що застосовують інші види шумоподібних сигналів.

Література

1. Меньшаков, Ю. К. Виды и средства иностранных технических разведок: учебное пособие [Текст] / под ред. М. П. Сычева. – М.:Изд–во МГТУ им. Н.Э.Баумана, 2009. – 656 с. **2.** Оружие и технологии России: энциклопедия. XXI век в 13 т. [Текст] / под ред. зам. Пред. Прав–ва РФ – Министра обороны РФ С. Иванова. – М.: Изд. дом «Оружие и технологи», 2006. – Т. XIII: Системы управления, связи и радиоэлектронной борьбы. – 695 с. **3. Цветнов, В. В.** Радиоэлектронная борьба: радиомаскировка и помехозащита [Текст] / В. В. Цветнов, В. П. Демин, А. И. Куприянов. – М.: Изд–во МАИ, 1999. – 240 с. **4. Макаренко, С. И.** Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты [Текст] : монография / С. И. Макаренко, М. С. Иванов, С. А. Попов. – СПб.: Свое изд–во, 2013. – 166 с. **5. Палий, А. И.** Радиоэлектронная борьба (средства и способы подавления и защиты радиоэлектронных систем) [Текст] / А. И. Палий. – М.: Воениздат, 1981. – 320 с. **6. Цветнов, В. В.** Радиоэлектронная борьба: радиоразведка и радиопротиводействие [Текст] / В. В. Цветнов, В. П. Демин, А. И. Куприянов. – М.: Изд–во МАИ, 1998. – 248 с. **7. Вартанесян, В. А.** Радиоэлектронная разведка [Текст] / В. А. Вартанесян. – М.: Воениздат, 1975. – 255 с. **8. Вартанесян, В. А.** Радиопеленгация [Текст] / В. А. Вартанесян, Э. Ш. Гойхман, М. И. Рогаткин. – М.: Воениздат, 1966. – 248 с. **9. Куприянов, А. И.** Теоретические основы радиоэлектронной борьбы [Текст] / А. И. Куприянов, А. В. Сахаров. – М.: Вузовская книга, 2007. – 356 с. **10.** Основы радиопротиводействия [Текст] : учебник для слушателей ВВНЗ СВ. – М.: Воен. акад. им. М. В. Фрунзе, 1962. – 268 с. **11. Каневский, З. М.** Теория скрытности. Часть 1. Основы теории скрытности: Учеб. пособие. [Текст] / З. М. Каневский, В.П.Литвиненко, Г.В. Макаров – Воронеж: Воронеж. гос. техн. ун–т, 2003. – 92 с. **12. Ландау, Л.Д.** Краткий курс теоретической физики в 3 кн. Кн.1: Механика. Электродинамика [Текст] / Л.Д.Ландау, Е.М.Лифшиц. – М.: Наука: Глав. ред. физ.–мат. лит., 1969. – 271 с. **13. Тузов, Г. И.** Помехозащищенность радиосистем со сложными сигналами [Текст] / Г.И. Тузов, В.А. Сивов, В.И. Прытков и др. под ред. Г.И.Тузова – М.: Радио и связь, 1985. – 264 с. **14. Борисов, В. И.** Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью [Текст] / В.И. Борисов, В.М. Зинчук, А.Е.Лимарев, Н.П.Мухин, Г.С.Нахмансон под ред. В.И.Борисова – М.: Радио и связь, 2003. – 640 с. **15. Зелкин, Е. Г.** Методы синтеза антенн: Фазированные антенные решетки и антенны с непрерывным раскрывом [Текст] / Е. Г. Зелкин, В. Г. Соколов. – М.: Сов. радио, 1980. – 296 с. **16. Варакин, Л.Е.** Системы связи с шумоподобными сигналами [Текст] / Л.Е.Варакин. – М.: Радио и связь, 1985. – 384 с.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ОБНАРУЖЕНИЯ СИСТЕМОЙ РАДИОРАЗВЕДКИ ПРОТИВНИКА СИСТЕМЫ РАДИОСВЯЗИ ВОЕННОГО НАЗНАЧЕНИЯ, ИСПОЛЬЗУЮЩЕЙ ШУМОПОДОБНЫЕ СИГНАЛЫ С ДИСКРЕТНОЙ ЧАСТОТНОЙ МОДУЛЯЦИЕЙ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТЬЮ

Анатолий Петрович Волобуев
Дмитрий Анатольевич Бухал

Центральный научно–исследовательский институт Вооруженных Сил Украины

В статье предложен метод математического моделирования выявления системой радиоразведки систем радиосвязи военного назначения, которые функционируют с использованием шумоподобных сигналов с дискретной частотной модуляцией псевдослучайной последовательностью. Предложенная задача математического моделирования решается в интересах оценивания уровня радиомаскировки систем радиосвязи военного назначения относительно систем радиоразведки нового поколения ведущих стран мира, которым присущи более широкие разведывательные возможности. За счёт использования аппарата тензорного исчисления в интересах моделирования, удалось положить в основу оценивания уровня радиомаскировки подходи, которые свойственны электродинамике, и обеспечить приемлемую адекватность предложенной модели. Кроме этого, наряду с радиостанциями,

которые используют шумоподобные сигналы дискретной частотной модуляции псевдослучайной последовательностью, во время моделирования рассмотрено разворачивание ложных радиосетей для обеспечения необходимого уровня радиомаскировки системы радиосвязи военного назначения.

Ключевые слова: *система радиоразведки, система радиосвязи военного назначения, математическое моделирование, электромагнитное поле, уровень радиомаскировки, шумоподобные сигналы.*

MATHEMATICAL MODELING OF THE DETECTION BY THE RADIO RECONNAISSANCE SYSTEM OF ENEMY OF MILITARY RADIO COMMUNICATION SYSTEM THAT USES NOISE−TYPE SIGNALS WITH DISCRETE FREQUENCY MODULATION BY A PSEUDO−RANDOM SEQUENCE

Anatolii P. Volobuiev
Dmytro A. Bukhal
Central Scientific Research Institute of UA Forces

The article proposes a method for mathematical modeling of the detection by the radio reconnaissance system military radio communication systems that using noise−type signals with discrete frequency modulation by a pseudo−random sequence. The proposed problem of mathematical modeling is solved in the interest of estimating the level of radiomasking of military radio communication systems concerning the new generation of radio reconnaissance systems of the leading countries of the world, which have broader reconnaissance capabilities. Due to using of the apparatus of tensor calculus in the interests of modeling, it was possible to base the estimation of the level of radiomasking approaches, which are typical for electrodynamics, and to provide with acceptable adequacy of the proposed model. In addition, together with stations that use noise−like signals of discrete frequency modulation with a pseudo−random sequence, the deployment of false radio networks is considered during simulation to provide the required level of radio masking of the military radio communication system.

Key words: *radio reconnaissance system, military radio communication system, mathematical modeling, electromagnetic field, level of radiomasking, noise−type signals.*

References

1. Menshakov, Yu. K. Types and means of foreign technical intelligence: textbook [Text] / ed. M.P. Sychev. − Moscow: Izd−vo MSTU them. N.E. Bauman, 2009. − 656 p.

2. Weapons and technologies of Russia: encyclopedia. XXI century in 13 toms. [Text] / Ed. Minister of Defense of the Russian Federation S. Ivanov. − Moscow: Izd. House "Arms and Technologists", 2006. − T. XIII: Control systems, communications and electronic warfare. − 695 p.

3. Tsvetnov, V. V. Radio−electronic warfare: radio−masking and noise protection [Text] / V.V. Tsvetnov, V.P. Demin, A.I. Kupriyanov. − Moscow: Izd−vo MAI, 1999. − 240 p.

4. Makarenko, S. I. Interference immunity of communication systems with pseudo−random working frequency tuning [Text]: monograph / S.I. Makarenko, M.S. Ivanov, S.A. Popov. – S.Pb.: The publishing house, 2013. − 166 p.

5. Paliy, **A. I.** Radio−electronic warfare (means and methods of suppression and protection of radio electronic systems) [Text] / A.I Paliy. − Moscow: Military Publishing, 1981. − 320 p.

6. Tsvetnov, V. V. Radio−electronic warfare: radio reconnaissance and radio counteraction [Text] / V.V. Tsvetnov, V.P. Demin, A.I. Kupriyanov. − Moscow: Izd−vo MAI, 1998. − 248 p.

7. Vartanesyan, V. A. Radio−electronic reconnaissance [Text] / V.A. Vartanesyan. − Moscow: Military Publishing, 1975. − 255 p.

8. Vartanesyan, V. A. Radio direction−finding [Text] / V.A. Vartanesyan, E.Sh. Goichmann, M.I. Rogatkin. − Moscow: Military Publishing, 1966. − 248 p.

9. Kupriyanov, A. I. Theoretical foundations of electronic warfare [Text] / A.I. Kupriyanov, A.V. Sakharov. − Moscow: The University Book, 2007. − 356 p.

10. Fundamentals of radiocountermeasures [Text]: textbook for students military academies. − Moscow: Mil. Acad. them. M.V. Frunze, 1962. − 268 p.

11. Kanevsky, Z. M. The theory of security. Part 1. Fundamentals of the theory of security: tutorial. [Text] / Z.M. Kanevsky, V.P. Litvinenko, G.V. Makarov − Voronezh: Voronezh. State. Tech. Univ., 2003. − 92 p.

12. Landau, L. D. A short course of theoretical physics in 3 books. Book 1: Mechanics. Electrodynamics [Text] / L.D. Landau, E.M. Lifshits. − Moscow: Science: Head. Ed. fiz.−mat. lit., 1969. − 271 p.

13. Tuzov, G. I. Noise immunity of radio systems with complex signals [Text] / G.I. Tuzov, V.A. Sivov, V.I. Prytkov etc, Ed. G.I. Tuzov − Moscow: Radio and Communication, 1985. − 264 p.

14. Borisov, V. I. Interference immunity of radio communication systems with spreading of the signal spectrum by modulation of a pseudo−random carrier by sequence [Text] / V.I. Borisov, V.M. Zinchuk, A.E. Limarev, N.P. Mukhin, G.S. Nakhmanson, ed. V.I. Borissov − Moscow: Radio and Communication, 2003. − 640 p.

15. Zelkin, E.G. Methods for the synthesis of antennas: Phased antenna arrays and antennas with a continuous opening [Text] / E.G. Zelkin, V.G. Sokolov. − Moscow: Sov. radio, 1980. − 296 p.

16. Varakin, L.E. Communication systems with noise−type signals [Text] / L.E.Varakin. – Moscow: Radio and Communication, 1985. − 384 p.

УДК 623

Даник Юрій Григорович *(д-р техн. наук, професор, начальник інституту)*[1]
Дупелич Сергій Олексійович *(викладач кафедри)*[2]

[1]***Національний університет оборони України імені Івана Черняховського, Київ, Україна***
[2]***Житомирський військовий інститут імені С П Корольова, Житомир, Україна***

СТРАТЕГІЧНІ АСПЕКТИ БОРОТЬБИ З РОБОТОТЕХНІЧНИМИ КОМПЛЕКСАМИ

У статті розглянуто стратегічні аспекти боротьби з робототехнічними комплексами. Запропоновано перспективну модель боротьби з робототехнічними засобами робототехнічних комплексів та сформульовано перспективні шляхи розвитку систем боротьби з робототехнічними комплексами і напрями їх бойового застосування. Встановлено, що в процесі функціонування таких систем необхідно здійснювати безперервний аналіз співвідношення часу видачі розвідувальної та бойової інформації з урахуванням як великої кількості різноманітних робототехнічних засобів робототехнічних комплексів противника, так і різнотипних засобів, які входять до складу зазначених систем. На основі проведеного аналізу принципів функціонування системи боротьби з наземними, повітряними (БПЛА), надводними та підводними робототехнічними комплексами противника визначено відповідні організаційно-технічні заходи та обґрунтовано перспективні напрями щодо розробки вітчизняної системи боротьби з робототехнічними комплексами противника. Запропоновано загальну багатомірну модель циклів Бойда.

Ключові слова: *безпілотні літальні апарати та безпілотні авіаційні комплекси (БПЛА та БАК), бойове застосування робототехнічних комплексів (БАК тощо), протидія робототехнічним комплексам (БАК тощо) та засобам (БПЛА тощо), виявлення робототехнічних комплексів (засобів).*

Вступ

Постановка проблеми. В сучасних війнах та військових конфліктах значно зросли важливість та масштаби застосування робототехнічних комплексів. Робототехнічні комплекси (РТК) є сукупністю:

апаратних засобів (наземних, повітряних, надводних та підводних тощо робототехнічних засобів (РТЗ));

програмно-алгоритмічних комплексів;

систем управління, що забезпечують комплексну (дистанційну, автономну або змішану) автоматизацію виконання задач.

Такі комплекси вже стали обов'язковою складовою озброєння армій провідних країн світу [1–3]. Аналіз їх застосування в останніх збройних конфліктах [4], в тому числі і під час проведення антитерористичної операції на території Донецької та Луганської областей свідчить про значне зростання їхньої ролі під час виконання різноманітних завдань.

Зважаючи на це, крім розвитку форм і способів застосування власних РТК (безпілотних літальних апаратів (БПЛА) тощо) постає питання ефективної протидії аналогічним системам (засобам) противника. Тому в провідних країнах світу проводяться інтенсивні дослідження в цій сфері. Розроблені інноваційні та існуючі організаційні заходи, системи (комплекси) дозволяють в певному сенсі вирішувати зазначені питання, але необхідний рівень ефективності, як в організаційному, так і технічному плані, і досі не забезпечений. В Україні також проводяться заходи щодо дослідження і розробки засад та комплексів (засобів) боротьби із РТК та РТЗ РТК [4–7].

Таким чином, проблема боротьби з РТК противника є надзвичайно актуальною і вимагає якомога швидшого вирішення, для чого необхідне комплексне залучення причетного до цієї сфери наявного наукового та технічного потенціалу держави.

Вказану проблему доцільно вирішувати шляхом створення спеціалізованих систем боротьби з РТК та РТЗ РТК противника для забезпечення їх своєчасного виявлення, ідентифікації та протидії.

Аналіз останніх досліджень і публікацій. До цього часу опубліковано багато робіт вітчизняних та зарубіжних фахівців, присвячених питанням боротьби з РТК [5, 8–11].

В організаційних заходах пріоритетними є підходи щодо створення єдиних засад боротьби з РТК (тих типів і класів, з якими неможливо або неефективно боротися існуючими засобами) та систем для їх реалізації із органів управління та відповідно оснащених підрозділів, які мають у своєму складі специфічні технічні засоби для вирішення зазначених задач. При цьому, розробляються і впроваджуються концепції, стратегії, засади, форми, способи, методи, тактика бойового застосування тощо.

Характерною рисою підходів, які розглядаються, є комплексність використання засобів виявлення, видачі цілевказівок, наведення та ураження, що функціонують на різних фізичних

принципах. Системність при цьому забезпечується шляхом об'єднання інформаційних потоків та сумісної обробки даних. Самі засоби доцільно розміщувати із забезпеченням раціонального просторового розташування в межах визначеного району відповідальності комплексу, що, як показали дослідження, сприяє підвищенню ефективності його застосування та живучості.

Однак з урахуванням недостатньої кількості діючих засобів протидії РТК противника з одного боку та їх недостатньою ефективністю і малими ресурсними можливостями з іншого, проблема боротьби з РТК противника досі залишається невирішеною.

Враховуючи це **метою статті** є висвітлення концептуальних напрямів щодо комплексного вирішення проблеми розробки комплексів боротьби з РТК противника та формування засад їх бойового застосування.

Виклад основного матеріалу дослідження

Стратегічні аспекти боротьби з РТК визначаються і залежать від наступних факторів:

інтенсивного розвитку та розширення спектру типів, класів, масштабів, варіантів і можливостей, а також наслідків застосування РТК;

розширення можливостей геоінформаційного та навігаційного забезпечення та всебічної інформаційної підтримки застосування РТК;

розвитку та впровадження групового і комплексного застосування РТК та РТЗ РТК;

зниження помітності та ускладнення своєчасного виявлення РТЗ РТК в різних частотних діапазонах;

ускладнення радіоелектронної обстановки в сучасних воєнних конфліктах;

комплексного застосування інноваційних комплексів (засобів) технічних видів розвідки та радіоелектронної боротьби (РЕБ), комплексів оперативного управління силами і засобами;

високої динаміки, маневреності сучасних бойових дій, їх швидкоплинності, вибірковості і можливості забезпечення високого ступеню ураження об'єктів, зростання швидкості маневру військами (силами) і вогнем, застосування різних мобільних угруповань військ (сил), з одного боку, а з іншого можливості ведення позиційної війни зі створенням ешелонованої оборони;

складності досягнення балансу між потрібним і наявним часом повного циклу «виявлення-ураження (зриву виконання завдання)» РТК (РТЗ);

наявності і відповідності вітчизняному і світовому досвіду, стану розвитку техніки і воєнного мистецтва, концепцій, стратегій, засад, форм, способів, методів, моделей, тактики бойового застосування комплексів боротьби з РТК (РТЗ);

наявності відповідних висококваліфікованих фахівців та інтегрованого навчально-наукового, дослідно-випробувального комплексу, в якому на єдиній базі здійснюють освітню і наукову діяльність за високотехнологічними напрямами.

РТК широко використовуються в інтересах ведення розвідки, вогневої підтримки військ (сил), охорони і оборони важливих об'єктів, доставки вантажів, встановлення різноманітних засобів і пристроїв, а також виконання спеціальних завдань та інших дій у важкодоступних або небезпечних для людини місцях. Ефективність застосування РТК визначається співвідношенням між важливістю і обсягами завдань, які можуть бути вирішеними за їх допомогою та вартістю їх розроблення, виробництва й експлуатації.

Разом з цим своєчасність вжиття заходів протидії РТК противника вимагає достатньої ефективності застосування залучених для виконання цього завдання сил і засобів, а головним напрямом для вирішення зазначених завдань може бути розробка комплексів боротьби з наземними, повітряними, надводними та підводними РТК (РТЗ) противника. Базова функціональність таких комплексів досягається шляхом реалізації у їх структурі опорних принципів, згідно яким реалізується повний цикл протидії від виявлення до потрібного впливу, а однією із умов її ефективного функціонування є потреба створення єдиної системи управління.

РТК може бути знешкодженим шляхом ураження (вогневого, радіоелектронного тощо) його комплексу управління чи РТЗ РТК, які входять до складу РТК. Не менш ефективним шляхом є взяття під контроль комплексу (засобів) управління ними з використанням засобів кібернетичного впливу.

Традиційно вважається, що боротьба з РТЗ РТК противника передбачає поетапне вирішення завдань та здійснення процедур їх виявлення (В), захоплення на супроводження та супроводження (С), ідентифікацію (І), видачу цілевказівок та ураження (У) (рис. 1).

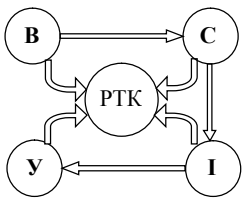


Рис. 1. Існуюча модель ведення боротьби з РТЗ РТК противника

Але застосування традиційних підходів призводить або до несвоєчасного виявлення РТЗ РТК противника, або ж до неможливості їх ураження за допомогою існуючих засобів. Крім цього, така модель боротьби має принциповий недолік, який полягає у відсутності можливості

запобігання діям РТЗ РТК противника без їх фізичного знищення або знешкодження.

Для усунення зазначених недоліків пропонується розглядати процес боротьби з РТЗ РТК противника як єдину систему, додатковими процедурами якої є прогнозування дій (ПД) РТК та комплексна протидія (КПР) ним.

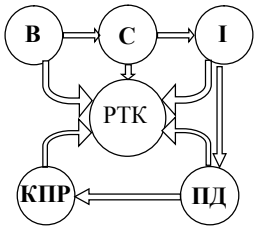


Рис. 2. Перспективна модель ведення боротьби з РТЗ РТК противника

Виявлення факту застосування противником РТЗ РТК є важливим завданням як для збереження прихованості і раптовості дій військ (сил), так і забезпечення їхньої живучості. Однак застосування існуючих засобів для виявлення сучасних РТЗ РТК, які мають малі розміри, виготовляються з композитних матеріалів та можуть діяти в різних умовах обстановки, виявилось проблематичним. З урахуванням зазначеного, підсистема виявлення РТЗ РТК противника повинна являти собою сукупність різнотипних технічних засобів розвідки об'єднаних єдиною системою управління, а запорукою її якісного функціонування є забезпечення принципів формування правил вибору тих засобів, які для заданих умов обстановки забезпечать максимальне значення імовірності правильного виявлення РТЗ РТК противника.

Отже, найбільш дієвим підходом для вирішення завдання виявлення РТЗ РТК противника є застосування комплексних систем, до складу яких можуть входити: комплекси засобів радіолокації (оснащені засобами пасивної радіолокації, засобами активної радіолокації і засобами державної системи радіолокаційного розпізнавання); комплекси засобів виявлення супутніх слідів (оснащені ультрафіолетовими приймачами і лазерами); комплекси засобів акустичної розвідки (оснащені засобами виявлення у звуковому діапазоні хвиль і засобами виявлення в ультразвуковому діапазоні хвиль); комплекси засобів оптикоелектронної розвідки (оснащені засобами виявлення у видимому діапазоні хвиль, засобами виявлення (ЗВ) в інфрачервоному діапазоні хвиль і засобами виявлення в ультрафіолетовому діапазоні хвиль) [5].

В результаті здійснення першої процедури буде сформована множина параметрів $W = \{C_1, C_2, ... C_I, \}$, у якій кожен з елементів C_i, $i = \overline{1, I}$ характеризує сукупність сигнатур виявленого і-м ЗВ об'єкту та місце його знаходження.

Захоплення на супровід РТЗ РТК здійснюється з метою отримання додаткових вимірювань параметрів W, які дозволяють уточнювати значення елементів C_i до необхідного для переходу в режим супроводження рівня. Проте сучасні РТЗ РТК характеризуються широкими можливостями щодо зміни швидкості свого руху та маневреності, а за групового застосування – специфічністю побудови бойових порядків та тактики дій. Саме тому виконання завдання супроводження РТЗ РТК противника пов'язано зі значними труднощами. Для його вирішення до складу систем боротьби з РТЗ РТК противника необхідно включати програмно-апаратні засоби з адаптивними алгоритмами попередження зриву супроводу маневруючих та групових цілей.

Задача та процедура ідентифікації виявлених об'єктів є одними з ключових під час виконання заходів боротьби з РТЗ РТК противника. У даному випадку вони полягають у визначенні належності виявлених сигнатур до певного класу за виміряними значеннями їх параметрів. Постійно зростаюча кількість РТЗ РТК, збільшення варіантів режимів їх роботи призводить до ускладнення процесу розпізнавання. Існуючі ж алгоритми ідентифікації [12,13] є недостатньо ефективними та не завжди забезпечують однозначне віднесення виявлених засобів до конкретних РТЗ РТК противника. Тому виникає необхідність у розробці нових алгоритмів, які б забезпечили усунення неоднозначності у результатах розпізнавання та підвищили б імовірність правильної ідентифікації.

Результатом виконання третьої процедури буде сформована множина $O = \{Z_1, Z_2, ... Z_K, \}$, у якій містяться елементи Z_k, $k = \overline{1, K}$, що характеризують сукупність ознак належності виявленого об'єкту певному k-му класу РТЗ РТК.

Прогнозування дій РТЗ РТК полягає у визначенні можливих напрямів їх руху та режимів роботи бортового обладнання з метою визначення шляхів щодо подальшого їх знешкодження або введення противника в оману.

Комплексна протидія РТЗ РТК противника планується та організовується після отримання інформації про їх особливості, прогнозування їх дій та оцінки небезпеки, яку вони представляють. Комплекс протидії може включати:

повне або часткове (до достатнього для зриву виконання противником завдань рівня) радіоелектронне подавлення системи управління або радіоелектронного обладнання РТЗ;

створення умов для отримання РТЗ противника інформації, яка забезпечує введення його в оману;

втручання в роботу бортової навігаційної системи РТЗ шляхом підміни сигналів космічних або інших навігаційних систем (спуфінг);

перехоплення керування РТЗ РТК та спрямування його в зону досяжності для безпечного захоплення;

кінетичне ураження РТЗ РТК противника на основі комплексного застосування систем зенітного та зенітного ракетного прикриття, систем винищувального авіаційного прикриття тощо [14].

Перспективним підходом є застосування зброї на нових фізичних принципах (лазерна, пучкова, електромагнітна зброя тощо) [15]. Дієвим способом протидії повітряним робототехнічним комплексам (безпілотним авіаційним комплексам (БАК) та БПЛА) є застосування спеціальних БПЛА винищувачів-перехоплювачів, які оснащені засобами ураження у вигляді будь-яких екранів (сітка з вічком, меншим за габарити цілі, троси з важками, відстань між якими менша за габарити цілі, система нитей тощо), які закріплені на БПЛА вільно чи у спеціальних контейнерах, або у вигляді викидних сіток у піропатронах [16], а також застосування переносних засобів ураження, бойова частина яких оснащена системою об'ємного вибуху тощо [6].

Крім зазначеного, до складу системи боротьби з наземними, повітряними, надводними та підводними РТК противника повинні входити система управління, а також комплекс засобів автоматизації (рис. 3).

Рис. 3. Склад комплексу боротьби з РТЗ РТК противника (варіант)

Комплекси боротьби з наземними, повітряними, надводними та підводними РТК противника повинна забезпечувати виконання таких основних завдань:

1. Виявлення і захоплення на супровід відповідних (наземних, повітряних, надводних або підводних) РТЗ РТК противника у контрольованій зоні за допомогою наявних засобів.

2. Розпізнавання типів РТЗ РТК противника.

3. Визначення найбільш імовірних напрямків, маршрутів руху та тактики дій РТЗ РТК противника.

4. Здійснення автоматизованого управління засобами виявлення та протидії РТЗ РТК в режимі часу, близькому до реального.

5. Автоматизоване здійснення обробки та комплексування розвідувальних даних, формування сигнатур об'єктів.

6. Визначення просторових координат РТЗ РТК противника.

7. Визначення засобів та порядку дій щодо протидії РТЗ РТК противника

8. Здійснення видачі цілевказівок засобам протидії.

9. Організація виконання спеціальних заходів боротьби з РТК противника.

Застосування системи боротьби з РТЗ РТК противника в першу чергу передбачає їх виявлення будь-яким із ЗВ, що включені до складу системи, на заданому рубежі виявлення (рис. 4). Потрібні рубежі видачі розвідувальної інформації (ВРІ) та видачі бойової інформації (ВБІ), її точність і дискретність повинні забезпечувати своєчасне приведення сил і засобів протидії (ЗПд) РТЗ РТК в необхідний ступінь бойової готовності і виконання ними цільових завдань.

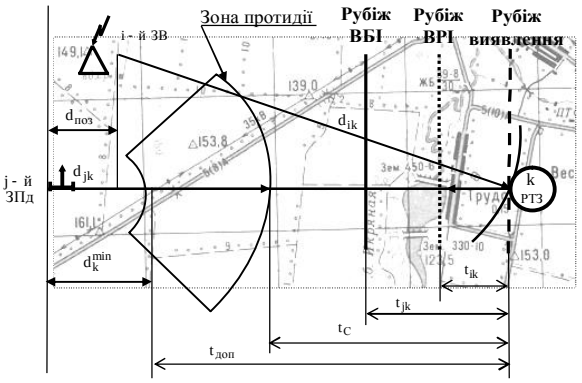


Рис. 4. До визначення часових параметрів системи боротьби з РТК противника

При цьому час, який витрачено на виявлення і протидію РТЗ РТК t_C повинен бути меншим за допустимий час $t_{доп}$, який характеризує початок виконання завдань відповідним РТЗ РТК на дальності d_k^{min}:

$$t_C < t_{доп}. \qquad (1)$$

Розрахункові рубежі ВРІ та ВБІ для кожного РТЗ РТК визначаються часом його виявлення та отримання даних, максимальним запізнюванням інформації в системі опрацювання і передачі даних, а також часом приведення відповідних ЗПд у готовність №1 з урахуванням їх дислокації та максимальної реалізації їх можливостей щодо протидії РТЗ РТК [14].

Потрібний рубіж ВРІ $d_{ВРІ}$ розраховується за формулою:

$$d_{ВРІ} = d_{jk} + V_k\left(t_{СУ} + t_{БГ} + t_{роб} + t_{пд} + t_{затр}\right). \qquad (2)$$

де d_{jk} –відстань до дальньої межі зони протидії j-го ЗПд k-го РТЗ РТК;

V_k – швидкість k-го РТЗ РТК

$t_{СУ}$ – робітний час системи управління;

$t_{БГ}$ – встановлений строк переходу у готовність № 1

$t_{роб}$ – робітний час ЗПд;

$t_{пд}$ – час, який витрачається на протидію РТЗ;

$t_{затр}$ – час затримки інформації.

Потрібний рубіж ВБІ $d_{ВБІ}$ розраховується за формулою:

$$d_{ВБІ} = d_д + V_{РТЗ}\left(t_{СУ} + t_{роб} + t_{пд} + t_{затр}\right). \qquad (3)$$

Значення термінів часу для проведення окремих операцій можуть визначатися нормативними документами і тактико-технічними характеристиками елементів системи боротьби з РТК противника.

Час ВРІ t_{ik} для кожного ЗВ визначається з урахуванням відстані від нього до рубежу виявлення d_{ik}:

$$t_{ik} = \frac{d_{ik} - d_{ВРІ}}{V_k}, \qquad (4)$$

Час ВБІ t_{jk} визначається часом руху РТЗ РТК від моменту його виявлення i-м ЗВ на відстані до дальньої межі зони протидії d_{jk} j-го ЗПд, $j = \overline{1, J}$ – кількість ЗПд з урахуванням $t_{роб}$ та $t_{пд}$:

$$t_{jk} = \frac{d_{ik} \pm d_{поз} - d_{jk}}{V_k} + t_{роб} + t_{пд}, \qquad (5)$$

де $d_{поз}$ –відстань від точки розміщення i-го ЗВ до місця знаходження j-го ЗПд.

Таким чином, розрахунок визначених часових параметрів вимагає великої кількості вихідних даних, а результат залежатиме від характеристик засобів системи боротьби з РТК, від параметрів РТЗ РТК противника, а також можливостей ЗВ щодо їх виявлення, при цьому забезпечення виконання умови (1) є необхідним для досягнення заданої якості виконання цільових завдань системи боротьби з РТК противника.

Взагалі весь процес боротьби з РТК противника з відповідним ступенем узагальнення та абстрагування може бути розглянутий в рамках теорії Дж. Бойда [17]. Універсальний цикл діяльності, за Бойдом, передбачає послідовне виконання таких процедур, як спостереження, орієнтування, рішення та дія (СОРД) (рис. 4).

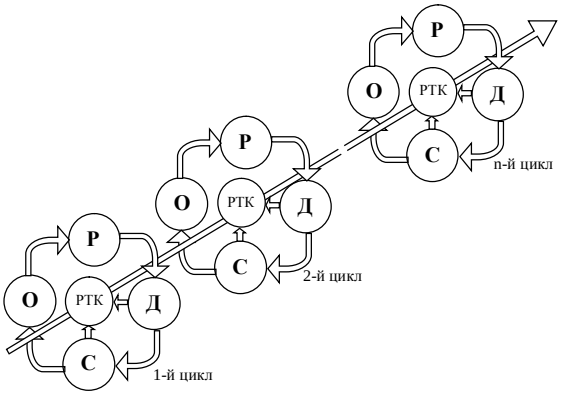


Рис. 5. Схема багатократного спірального повторення циклу СОРД

Перша процедура – спостереження – це процес організації та ведення розвідки противника у районі відповідальності, виявлення, захоплення на супроводження та супроводження РТЗ РТК. Орієнтування включає здійснення передбачення можливих задач РТЗ РТК, прогнозування їх дій та оцінки небезпеки яку вони представляють, визначення потреби у дорозвідці, вибір відповідних засобів протидії. Рішення включає визначення варіантів на які саме РТЗ РТК, у якому порядку, де, чим і коли впливати з прогнозною, на основі аналізу сукупності відповідних показників, оцінкою ефективності впливу та вибору із засобів впливу таких, застосування яких є найбільш раціональним. Дія включає видачу цілевказівок визначеним рішенням засобам впливу на РТЗ РТК, здійснення впливу та оцінку його результатів.

Характерною рисою циклів СОРД в класичній постановці є їх одномірність. Тобто, досягнення поставленої мети, за Бойдом, повинно вирішуватись циклічно, але цикли при цьому не перетинаються, а продовжуються послідовно. Слід зазначити, що внутрішні, паралельні, паралельно-послідовні взаємопов'язані та незалежні цикли і такі, що виникають за умови певних дій або є безумовною необхідністю для вирішення інших взаємопов'язаних задач, які мають місце в багатьох практичних задачах і приводять до багатомірності в рамках теорії Бойда, до цього часу не досліджувалися. Тому в процесі досліджень ці питання отримали свій розвиток в рамках вирішення проблеми боротьби з РТК та РТЗ РТК. Так, передчасний початок наступного циклу (до закінчення дії) призводить або до подавлення циклів СОРД, або ж до виникнення об'єктів з нескінченним циклом [17]. В той же час системи боротьби з РТК противника, як було зазначено, оснащуються різнотипним ЗВ. Це призводить до того, що кожен i-й ЗВ розпочинає виконання цільових завдань у різні моменти часу, а отже для кожного ЗВ існує свій власний цикл СОРД. Крім того, для забезпечення протидії РТЗ РТК можуть бути задіяними J ЗПд. Оскільки кожен j-й ЗПд має свої часові нормативи бойової роботи, то, відповідно, для нього має місце власний цикл СОРД. Зазначені фактори призводять до того, що процес функціонування системи боротьби з наземними, повітряними, надводними та підводними РТК противника характеризується багатомірністю (рис. 6).

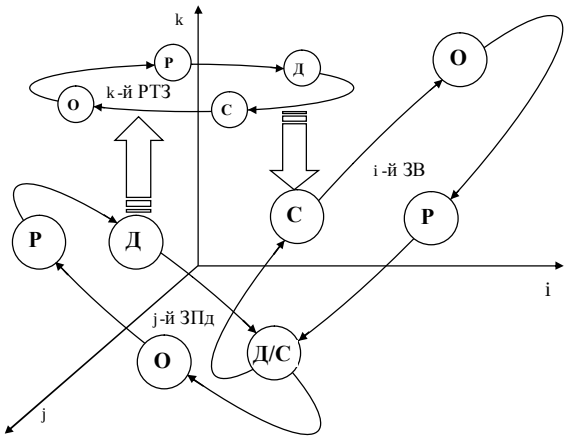


Рис. 6. Модифікований цикл СОРД

Отже, для забезпечення якісного функціонування системи боротьби з РТК противника необхідний постійний аналіз часових параметрів ВРІ та ВБІ в залежності від класу РТК, типу ЗВ і ЗПд, що будуть застосовуватися. Це забезпечується шляхом оперативного управління підсистемою виявлення РТЗ РТК – визначенням необхідних для виконання задачі типів ЗВ, їх раціонального розміщення на місцевості та структурно-елементного розподілу за складовими підсистеми протидії.

Загальна постановка задачі прийняття рішення щодо визначення необхідної для певної ситуації структури підсистеми виявлення може бути сформульована за допомогою моделі, яка включає три складові: модель підсистеми виявлення, її оцінку та прийняття рішення.

Модель підсистеми виявлення S можна представити у вигляді наступної сукупності множин і операторів [18]:

$$S = \langle A, U, L, B, T, X, Y \rangle, \qquad (6)$$

де A – множина умов її функціонування;

U – множина допустимих управлінь;

L – множина можливих технічних рішень (альтернатив структури і параметрів підсистеми виявлення);

B – множина поточних інформаційних характеристик підсистеми виявлення;

T – множина часових станів;

X – множина можливих станів підсистеми виявлення в процесі її функціонування;

Y – множина виходів підсистеми виявлення.

Зазначені множини пов'язані в межах моделі системи наступними операторами:

$$f : A \times X \times T \to Y, \qquad (7)$$

де $f(a,x,t) \in Y$ – поточний вихід системи $y \in Y$ у залежності від її станів $x \in X$ та умов функціонування $a \in A$ в момент часу $t \in T$;

$$h : A \times B \times T \to U, \qquad (8)$$

де $h(a,b,t) \in U$ – реалізоване управління системою $u \in U$, яке визначається наявною інформацією $b \in B$ щодо умов функціонування $a \in A$ в момент часу $t \in T$;

$$g : L \times U \times T \to X, \qquad (9)$$

де $g(v,u,t) \in X$ – оператор, який визначає стан системи за прийнятої структури $l \in L$ в залежності від реалізованого управління системою $u \in U$ в момент часу $t \in T$.

Модель оцінювання системи E може бути представлена набором:

$$E = \langle A, Y, L, P \rangle, \qquad (10)$$

де P – множина значень показників якості функціонування підсистеми виявлення.

Оператор показників якості задається відображенням:

$$p: A \times L \times Y \to P, \qquad (11)$$

де $p(a,l,y) \in P$ характеризує ефективність функціонування підсистеми виявлення в залежності від умов $a \in A$, прийнятої структури $l \in L$ і виходів підсистеми виявлення $y \in Y$ у вигляді сукупності часткових показників якості системи $p \in P$.

Модель вибору Q визначається у вигляді сукупності множин, які представляють собою введене на множині альтернатив відношення переваг:

$$Q = \langle A, P, H, R \rangle, \qquad (12)$$

де H – формалізоване представлення вимог до підсистеми виявлення, а оператор: $q: A \times P \times H \to R$ – відображення наборів часткових показників якості в лінійну впорядковану шкалу переваг R, наприклад, у відрізок $R = [0,1]$.

Модель прийняття рішення D щодо підсистеми виявлення може бути представлена сукупністю розглянутих моделей:

$$D = \langle S, E, Q \rangle. \qquad (13)$$

Якщо відмітити найбільш суттєві для прийняття рішення компоненти стосовно структури підсистеми виявлення, то модель (13) можна записати у вигляді:

$$D = \langle A, L, P, H, p, q \rangle, \qquad (14)$$

яка містить розглянуті у (6)–(12) компоненти.

Формалізація методів прийняття рішення зводиться до оптимізації визначених параметрів, які характеризують необхідну структуру підсистеми виявлення, за деякою цільовою функцією, яка виступає в ролі узагальненого показника якості за наявності обмежень, що визначають область допустимих рішень. Це полягає в реалізації функцій, за яких приймається такий варіант підсистеми виявлення з усіх можливих, за якого забезпечується збереження (покращення) визначеного функціоналу Y_C – ефективності її функціонування.

Відомо [7], що ефективність застосування систем виявлення в загальному випадку оцінюється такими групами показників: імовірнісними, просторовими та часовими. Наприклад, для систем виявлення БПЛА основними показниками якості, які характеризують ефективність її застосування для різних умов оперативної обстановки, можуть бути:

з імовірнісних показників - умовні імовірності правильного виявлення та розпізнавання БПЛА;

з просторових показників - реалізовані зони виявлення БПЛА залежно від параметрів ЗВ системи з урахуванням впливів активних та пасивних завад;

з часових показників - оперативність видачі розвідувальної інформації.

Умовна імовірність правильного виявлення БПЛА $P_в\left(\overrightarrow{n_x}\right)$ визначає встановлення факту його наявності у відповідному районі простору в процесі прийому й обробки сигналів і перешкод за допомогою $\overrightarrow{n_x}$-ї комбінації пасивних та активних ЗВ [19]. Умовна імовірність правильної ідентифікації БПЛА $P_р\left(\overrightarrow{n_x}\right)$ полягає у визначенні його типу та належності і здійснюється шляхом аналізу даних щодо його параметрів руху і поведінки в польоті, місця і часу запуску та інших даних, отриманих від $\overrightarrow{n_x}$-ї комбінації пасивних та активних ЗВ. За отриманих значень імовірностей правильного виявлення та розпізнавання та заданих значень імовірностей хибної тривоги виявлення $F_в^{пор} = \text{const}$ і хибної тривоги розпізнавання $F_р^{пор} = \text{const}$ за критерієм Неймана-Пірсона приймається рішення щодо наявності БПЛА у заданому районі.

З урахуванням зазначеного, якість застосування підсистеми виявлення визначається використанням такої комбінації ЗВ, за якої буде забезпечено виявлення та ідентифікацію БПЛА з показниками, не гірше заданих:

$$\left\{P_в\left(\overrightarrow{n_x}\right) \geq P_{в0}; P_р\left(\overrightarrow{n_x}\right) \geq P_{р0}\right\}, \qquad (15)$$

де $\overrightarrow{n_x}$ – вектор, який відображає склад підсистеми виявлення;

$x = \overline{1, X}$ – кількість комбінацій пасивних та активних ЗВ;

$P_{в0}$ – порогове значення показника якості виявлення;

$P_{в0}$ – порогове значення показника якості розпізнавання.

Реалізована зона виявлення БПЛА в заданому районі $\bigcup_{m=1}^{M} \bigcup_{i=1}^{I} \left(Q_{iz}^{R}(j_h, l_h)\right)$ означує частину району з урахуванням впливів активних та пасивних завад, у межах якої реалізуються можливості ЗВ щодо виявлення БПЛА з імовірністю, не нижче заданої [20]. Якість застосування підсистеми виявлення буде визначатися розміром m-кратного покриття заданого району $W(j_h, l_h) = \text{const}$ реалізованими зонами виявлення ЗВ, включених до складу системи, при цьому:

$$\sum_{m=1}^{M}\sum_{i=1}^{I}\left(Q_{iz}^{R}(j_h, l_h)\right) \geq Q_0, \qquad (16)$$

де Q_0 – площа необхідної зони виявлення;

$m = \overline{1, M}$ – кількість типів ЗВ;

$h = \overline{1, H}$ – кількість точок району розвідки, в яких можуть бути розміщені ЗВ.

Показник оперативності видачі розвідувальної інформації підсистеми виявлення $t_{ijk}^{оп}$ полягає в її здатності вирішувати цільові завдання в режимі часу, який забезпечує швидке реагування на зміну обстановки та своєчасну протидію БПЛА противника [21]. Якість застосування підсистеми виявлення визначається умовою забезпечення допустимого значення показника оперативності видачі розвідувальної інформації $t_{допk}^{оп}$:

$$t_{ijk}^{оп} \leq t_{допk}^{оп}, \qquad (17)$$

Оскільки система призначена для забезпечення своєчасного виявлення БПЛА, то ефективність її застосування визначається за наступного розподілу часткових критеріїв з урахуванням умов (15)–(17):

$$Y_C = \begin{cases} \left\{P_в\left(\overrightarrow{n_x}\right) \to \max; P_p\left(\overrightarrow{n_x}\right) \to \max\right\}, \\ \sum_{m=1}^{m}\sum_{i=1}^{I}\left(Q_{iz}(j_h, l_h)\right) \to \max, \\ t_C \to \min. \end{cases} \qquad (18)$$

Запропонований у [19–21] розв'язок задачі у вигляді (18) забезпечує вирішення завдання прийняття рішення щодо ефективності застосування визначеного варіанту підсистеми виявлення БПЛА в залежності від визначених умов і обмежень. Розроблені методики вибору ЗВ, їх розміщення на місцевості та структурно-елементного розподілу за елементами системи протидії дозволяють визначати раціональний склад підсистеми виявлення та формувати правила переваги застосування певного ЗВ залежно від умов обстановки, отримувати квазіоптимальні координати розміщення ЗВ та визначати матрицю оптимального структурно-елементного розподілу ЗВ за елементами системи протидії.

Висновки й перспективи подальших досліджень

Таким чином, в процесі досліджень було встановлено, що якісне вирішення завдання боротьби з РТК противника вимагає комплексного підходу з залученням доступних сил та засобів і ефективне управління ними в процесі вирішення цільових завдань. На основі аналізу світових тенденцій щодо стратегій, засад, форм, способів, методів, тактики бойового застосування систем контролю навколишнього простору визначені стратегічні аспекти боротьби з РТК та запропонована структура і окреслено основні завдання перспективних комплексів боротьби з РТЗ РТК противника.

На прикладі вирішення задач боротьби з РТК та РТЗ РТК розглянутий загальний багатомірний випадок застосування теорії Бойда.

Практична реалізація запропонованих підходів та отриманих рішень забезпечує можливість створення раціональної структури системи боротьби з РТК, що дозволить своєчасно виявляти та протидіяти РТЗ противника. Ефективне вирішення завдання протидії РТК також вимагає проведення відповідних організаційно-технічних заходів та постійного науково-технічного супроводження вітчизняної системи боротьби з РТК противника шляхом:

1. Формування єдиних поглядів відповідних державних органів щодо розвитку систем боротьби з РТК противника та внесення необхідних змін і доповнень до основних керівних документів у сфері національної безпеки і оборони України.
2. Розроблення та прийняття Концепції створення системи боротьби з РТК противника.
3. Розроблення стандартів України щодо систем боротьби з РТК противника, сумісних зі стандартами НАТО.
4. Визначення єдиних підходів до класифікації та затвердження номенклатур засобів військового призначення перспективної системи боротьби з РТК противника.
5. Уніфікації складових елементів перспективної системи боротьби з РТК противника.
6. Формування кооперації науково-дослідних установ і підприємств-виробників різних міністерств і відомств та ефективної координації їх діяльності в сфері боротьби з РТК противника.
7. Організація підготовки фахівців за напрямами боротьби з РТК противника.

Література

1. Современные военные роботы – боевые системы будущего [Електронний ресурс] // Militaryarms.ru . – Режим доступу : https://militaryarms.ru/voennaya-texnika/boevye-mashiny/voennye-boevye-roboty. **2.** В ходе СКШУ «Центр-2015» впервые применяется робототехника инженерных войск [Електронний ресурс] // Министерство обороны Российской Федерации. – Режим доступу : http://function.mil.ru/news_page/country/more.htm?id=12056386@egNews. **3.** Unmanned Warrior 2016 Technology Fact Sheets [Електронний ресурс] // The Office of Naval Research (ONR) . – Режим доступу : https://www.onr.navy.mil/en/Media-Center/unmanned-

warrior. **4. Даник Ю. Г.** Безпілотна авіація в сучасній збройній боротьбі : монографія / Ю. Г. Даник, В. Г. Радецький, І. С. Руснак. – К. : НАОУ, 2008. – 224 с. **5.** Патент UA104494 U. Система виявлення, розпізнавання, супроводження повітряних та наземних цілей / Даник Ю. Г., Дупелич С. О.; власники патенту Даник Ю. Г., Дупелич С. О.; заявл. 25.05.15; опубл. 10.02.16, Бюл. № 3. – 6 с. : іл. **6.** Патент UA104662 U. Переносний засіб ураження повітряних малорозмірних цілей / Даник Ю. Г., Дупелич С. О.; власники патенту Даник Ю. Г., Дупелич С. О.; заявл. 10.08.15; опубл. 10.02.16, Бюл. № 3. – 4 с. : іл. **7. Даник Ю. Г.** Теорія і техніка протидії безпілотним засобам повітряного нападу. Кн. 1. Безпілотні засоби повітряного нападу. Застосування та перспективи розвитку. Виявлення малопомітних засобів повітряного нападу / Ю. Г. Даник, В. І. Карпенко, Г. А. Дробаха, Р. Е. Пащенко // Монографія. Х. : Міністерство оборони України, ХВУ, 2002. – 220 с. **8. Moses A.** Radar-based detection and identification for miniature air vehicles / A. Moses, M. J. Rutherford, K. P. Valavanis // IEEE International Conference on Control Applications. – Denver, CO, USA. September 28–30, 2011. – P. 933–940. **9. Saravanakumar A.** Exploitation of Acoustic signature of low flying Aircraft using Acoustic Vector sensor / A. Saravanakumar, K. Senthilkumar // Defence Science Journal. – March 2014. – Vol. 64, No. 2. – P. 95–98. **10.** Detecting, Tracking and Indentifying Airborne Threats with Netted Sensor Fence / W. Shi, G. Arabadjis, B. Bishop, P. Hill // Sensor Fusion – Foundation and Applications. – Rijeka, Croatia : InTech Europe, 2001. – P. 139–158. **11.** Основи побудови безпілотних роботизованих систем спеціального призначення : навч. посіб. / Ю. Г. Даник, П. П. Топольницький, І. В. Пулеко та ін. – Житомир : ЖВІ, 2016. – 292 с. **12. Саврасов Ю. С.** Алгоритмы и программы в радиолокации / Ю. С. Саврасов. – М. : Радио и связь, 1985. – 216 с., ил. **13. Петраш С. В.** Алгоритм розпізнавання джерел радіовипромінювання для засобів радіомоніторингу / С. В. Петраш, О. Р. Черняк, С. О. Дупелич, С. В. Тимчук // Системи управління, навігації та зв'язку. – К. : ЦНДІНУ, 2012. – Вип. 1(21). – Т. 2. – С. 52-56. **14.** Довідник з протиповітряної оборони / А. Я. Торопчин, І. О. Романенко, Ю. Г. Даник та ін. – К. : МО України, Х. :ХВУ, 2003. – 368 с. **15.** Наприкінці цього літа у морської піхоти США з'явиться перша лазерна зброя підтримки [Електронний ресурс] // Надзвичайне. – Режим доступу : http://www.надзвичайне.com.ua/uncategorized/Naprik-nc-c-ogo-l-ta-u-mors-ko-p-hoti-SShA-z-yavit-sya-persha-lazerna-zbroya-p-dtrimki. **16.** Патент UA 105778 U. Спосіб бойового застосування безпілотних літальних апаратів для ураження малорозмірних повітряних цілей / Даник Ю. Г., Дупелич С. О.; власники патенту Даник Ю. Г., Дупелич С. О.; заявл. 10.08.15; опубл. 11.04.16, Бюл. № 7. – 4 с. : іл. **17. Буренок В. М.** Развитие военных технологий XXI века: проблемы, планирование, реализация / В. М. Буренок, А. А. Ивлев, В. Ю. Корчак. – Тверь : Изд-во ООО «КУПОЛ», 2009. – 624 с., іл. **18. Карминский А. М.** Автоматизированное проектирование и синтез радиосистем / А. М. Карминский, И. М. Коган // Итоги науки и техники. Серия радиотехника. – 1987. – №37. – С. 91-144. **19. Korobiichuk I.** The Selection Methods for Multisensor System Elements of Drone Detection / I. Korobiichuk, M. Nowicki, Y. Danyk and other. – Recent Advances in Systems, Control and Information Technology. – Springer International Publishing AG, 2017. – P. 20–26. **20. Журавський Ю. В.** Методика оптимізації розміщення елементів багатопозиційної мультисенсорної системи виявлення безпілотних літальних апаратів / Ю. В. Журавський, С. О. Дупелич // Труди університету : зб. наук. праць. – К. : НАОУ, 2016. – № 1(140). – С. 148–156. **21. Дупелич С. О.** Удосконалена методика визначення зв'язків між елементами багатопозиційної мультисенсорної системи / С. О. Дупелич // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. – Житомир : ЖВІ, 2016. – Вип. 13. – С. 41–50.

СТРАТЕГИЧЕСКИЕ АСПЕКТЫ БОРЬБЫ С РОБОТОТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ

Даник Юрий Григорьевич *(д-р техн. наук, профессор, начальник института)*[1]
Дупелич Сергей Алексеевич *(преподаватель кафедры)*[2]

[1]*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*
[2]*Житомирский военный институт имени С П Королева, Житомир, Украина*

В статье рассмотрены стратегические аспекты борьбы с робототехническими комплексами. Предложена перспективная модель борьбы с робототехническими средствами робототехнических комплексов и сформулированы перспективные пути развития систем борьбы с робототехническими комплексами и направления их боевого применения. Обнаружено, что в процессе функционирования таких систем необходимо осуществлять непрерывный анализ соотношения времени выдачи разведывательной и боевой информации с учетом как большого количества разнообразных робототехнических средств робототехнических комплексов противника, так и разнотипных средств, которые входят в состав указанных систем. На основании проведенного анализа принципов функционирования системы борьбы с наземными, воздушными (БПЛА), надводными и подводными робототехническими комплексами противника определены соответствующие организационно-технические меры и обоснованно перспективные направления относительно разработки отечественной системы борьбы с робототехническими комплексами противника. Предложено общую многомерную модель циклов Бойда.

Ключевые слова: *беспилотные летательные аппараты и беспилотные авиационные комплексы (БПЛА и БАК), боевое применение робототехнических комплексов (БАК), противодействие робототехническим комплексам (БАК) и средствам (БПЛА), обнаружение робототехнических комплексов (средств).*

STRATEGIC ASPECTS OF FIGHT AGAINST ROBOT SYSTEMS

Yuriy H. Danyk *(Doctor of Technical Sciences, Professor, chief of a Institute)*[1]
Sergiy O. Dupelich *(teacher of a Department)*[2]

[1]*National University of defense of Ukraine named after I. Cherhjahovskogo, Kyiv, Ukraine*
[2]*Zhytomyr military Institute named after S. Korolyov, Zhytomyr, Ukraine*

Strategic aspects of fight AGAINST robot systems are considered. The perspective model of struggle with robot means of robot systems was offered. Perspective ways of development of systems of struggle with robot systems and directions of their fighting use are formulated. It is revealed that in the course of functioning of such systems it is necessary to carry out the continuous analysis of a parity of time of delivery of the intelligence information and battle information. It is thus necessary to take into account considerable quantity of robot systems and means, which are a part of the specified systems. The main organizational-technical tasks were defined on the basis of the spent analysis of principles of functioning of system of struggle with robot systems of land, air (UAV), surface and underwater. Perspective directions concerning Ukrainian system of struggle with robot systems are grounded. It is offered the general multidimensional model of cycles of Boyd.

Keywords: *unmanned aerial vehicles and unmanned aerial systems (UAV and UAS), fighting application robot systems (UAS), counteraction robot systems (UAS) and means (UAV), detection robot systems (means).*

References

1. "Modern soldiery robots are the battle systems of the future" [*"Sovremennyie voennyie robotyi – boevyie sistemyi buduschego"*], available at: https://militaryarms.ru/voennaya-texnika/boevye-mashiny/voennye-boevye-roboty. **2.** "During manoeuvres "Center-2015" robotics of engineering troops is first used " [*"V hode SKShU «Tsentr-2015» vpervyie primenyaetsya robototehnika inzhenernyih voysk"*], available at: http://function.mil.ru/news_page/country/more.htm?id=12056386@egNews. **3.** "Unmanned Warrior 2016 Technology Fact Sheets", available at: https://www.onr.navy.mil/en/Media-Center/unmanned-warrior. **4. Danyk Yu. H.**, Radetskyi V. H., Rusnak I. S., (2008) A unmanned aviation is in the modern armed fight : monograph. [*Bezpilotna aviatsiia v suchasnii zbroinii borotbi : monohrafiia*], NUDU, Kiev, 224 p.

5. Danyk Yu. H., Dupelych S. O. (2016), Patent of UA104494 U. System of exposure, recognition, accompaniment of air and surface aims. [*Systema vyiavlennia, rozpiznavannia, suprovodzhennia povitrianykh ta nazemnykh tsilei*], Kiev, 6 p. **6. Danyk Yu. H.,** Dupelych S. O. (2016), Patent of UA104662 U. Portable decimator of air littlesize aims. [*Perenosnyi zasib urazhennia povitrianykh malorozmirnykh tsilei*], Kiev, 4 p. **7. Danyk Yu. H.**, Karpenko V. I., Drobakha H. A., Pashchenko R. E. (2002), Theory and technique of counteraction to unmanned facilities of air attack. B. 1. Pilotless facilities of air attack. Application and prospects of development. Exposure of barely visible facilities of air attack. [*Teoriia i tekhnika protydii bezpilotnym zasobam povitrianoho napadu. Kn. 1. Bezpilotni zasoby povitrianoho napadu. Zastosuvannia ta perspektyvy rozvytku. Vyiavlennia malopomitnykh zasobiv povitrianoho napadu*], KhMU, Kharkov, 220 p. **8. Moses A.,** Rutherford M. J., Valavanis K. P. (2011), Radar-based detection and identification for miniature air vehicles, IEEE International Conference on Control Applications, pp. 933–940. **9. Saravanakumar A.,** Senthilkumar K. (2014), Exploitation of Acoustic signature of low flying Aircraft using Acoustic Vector sensor, Defence Science Journal, Vol. 64, No. 2, pp. 95–98. **10. Shi W.**, Arabadjis G., Bishop B., Hill P. (2001) Detecting, Tracking and Indentifying Airborne Threats with Netted Sensor Fence, Foundation and Applications, pp. 139–158.**11. Danyk Yu. H.,** Topolnytskyi P. P., Puleko I. V. and other (2016), Bases of construction of the pilotless robot systems of the special setting : train aid. [*Osnovy pobudovy bezpilotnykh robotyzovanykh system spetsialnoho pryznachennia : navch. posib.*], ZVI, Zhitomir, 292 p. **12. Savrasov Yu. S.** (1985), Algorithms and programs are in a radio-location. [*Algoritmyi i programmyi v radiolokatsii*], Radio i svyaz, Moskow, 216 p. **13. Petrash S. V.,** Cherniak O. P., Dupelych S. O., Tymchuk S. V. (2012), An algorithm of recognition of sources of radio of radiation is for facilities of monitoring radio. [*Alhorytm rozpiznavannia dzherel radiovyprominiuvannia dlia zasobiv radiomonitorynhu*], Systemy upravlinnia, navihatsii ta zviazku, No. (1) 21, pp. 52–56. **14. Toropchyn A. Ya.**, Romanenko I. O., Danyk Yu. H. (2003), A reference book is from air defense. [*Dovidnyk z protypovitrianoi oborony*], MO Ukrainy, Kiev, KhMU, Kharkov, 368 p. **15.** "At the end of this summer the first laser weapon of support will appear at the marines of the USA" [*"Naprykintsi tsoho lita u morskoi pikhoty SShA ziavytsia persha lazerna zbroia pidtrymky"*], available at:: http://www.надзвичайне.com.ua/uncategorized/Naprik-nc-c-ogo-l-ta-u-mors-ko-p-hoti-SShA-z-yavit-sya-persha-lazerna-zbroya-p-dtrimki.

16. Danyk Yu. H., Dupelych S. O. (2016), Patent of UA105778 U. A method of battle application of pilotless aircrafts is for the defeat of littlesize air aims. [*Sposib boiovoho zastosuvannia bezpilotnykh litalnykh aparativ dlia urazhennia malorozmirnykh povitrianykh tsilei*], Kiev, 4 p. **17. Burenok V. M.**, Ivlev A. A., Korchak V. Yu. (2009), Development of soldiery technologies of XXI century : problems, planning, realization. [*Razvitie voennyih tehnologiy HHI veka: problemyi, planirovanie, realizatsiya*], Tver : Izd-vo OOO «KUPOL», 624 p. **18. Karminskiy A. M.**, Kogan I. M. (1987), Automated planning and synthesis of radio of the systems. [*Avtomatizirovannoe proektirovanie i sintez radiosistem*], Itogi nauki i tehniki. Seriya radiotehnika, No. 37, pp. 91–144. **19. Korobiichuk I.**, Nowicki M., Danyk Yu. and other. (2017), The Selection Methods for Multisensor System Elements of Drone Detection Recent Advances in Systems, Control and Information Technology. – Springer International Publishing AG, pp. 20–26. **20. Zhuravskyi Yu. V.**, Dupelych S. O. (2017), Methodology of optimization of placing of elements of the multiposition multisensory system of exposure of uunmanned aerial vehicles [*Metodyka optymizatsii rozmishchennia elementiv bahatopozytsiinoi multysensornoi systemy vyiavlennia bezpilotnykh litalnykh aparativ*], Trudy universytetu, No. (1) 140, pp. 148–156. **21. Dupelych S. O.** (2016), Improved method of determination of connections between elements of multiposition multisensor system. [*Udoskonalena metodyka vyznachennia zviazkiv mizh elementamy bahatopozytsiinoi multysensornoi systemy*], Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system : zb. nauk. prats., No. 13, pp. 41–50.

УДК 621.391

Николай Васильевич Захарченко *(доктор технических наук, профессор)*
Александр Вячеславович Кочетков *(кандидат технических наук)*
Евгений Александрович Севастеев
Антон Сергеевич Криль

Одесская национальная академия связи им. А.С. Попова, Одесса, Украина

ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ СКРЫТНОСТИ ПЕРЕДАЧИ НЕРАВНОВЕРОЯТНОГО АЛФАВИТА ПРИ ТАЙМЕРНОМ КОДИРОВАНИИ

Для повышения информационной скрытности передачи неравновероятного алфавита при таймерном кодировании предложен метод вторичного кодирования передаваемого неравновероятного первичного алфавита с целью обеспечения равновероятной передачи символа в канале с точностью до одного процента. Определено количество различных кодовых комбинаций («банк» кодовых слов символа) обеспечивающих равновероятную передачу кодовых слов. Для уменьшения времени передачи предложено использование таймерных сигналов, определена оптимальная длительность таймерного кодового слова. Показано, что именно равновероятность появления символов на приеме не позволяет различать их статистическим анализом и делает такие сообщения трудно дешифрируемыми.

Ключевые слова: *информация, энтропия, информационная емкость найквистового элемента, интервал реализаций, таймерные сигналы, момент модуляции.*

Введение

При расшифровке полученного при несанкционированном доступе к передаваемому сообщению чаще всего используется статистический метод распознавания передаваемого символа, основанный на вероятностях использования отдельных символов в первичном тексте. Таким образом, статистический метод распознавания обеспечивает расшифровку полученного при несанкционированном доступе сообщения – шифрограммы.

Постановка проблемы. В работе предлагается метод кодирования неравновероятного первичного алфавита в кодовое множество с максимальной энтропией, обеспечивающего равновероятную передачу в канале.

Анализ последних исследований и публикаций. На современном этапе в Украине, как и во всем мире, основными проблемами развития телекоммуникаций является повышение скорости передачи информации и сохранение высокой верности приема информации. Решение данных задач достижимо посредством повышения эффективности системы передачи [1] и применения помехоустойчивого кодирования.[2] Одним из методов повышения эффективности системы передачи является использование многоуровневых сигналов [3]. Использование многоуровневых таймерных сигналов позволяет в системах цифровой связи значительно повысить скорость передачи информации [6].

Повышение верности приема информации достигается за счет применения помехоустойчивого кодирования в системе передачи информации [4].

Таким образом, использование этих двух методов позволяет строить более эффективные системы связи.

Цель статьи. Для повышения эффективности системы связи предложено использование таймерных сигналов для увеличения скорости передачи и метода кодирования неравновероятного первичного алфавита в кодовое множество с максимальной энтропией, для повышения информационной скрытности передаваемого сообщения.

Методы исследования

В ходе исследования использовались следующие методы: анализ теоретических источников по проблемам применения статистического декодирования шифрограммы, изучение и анализ информационных параметров позиционных и таймерных кодов, теорем кодирования информации, на основе энтропийного подхода.

Изложение основного материала исследования

Количество информации $I(x_i)$,содержащейся в событии x_i происходящем с вероятностью $P(x_i)$ определяется [1, 5]:

$$I(x_i) = \log_2 \frac{1}{P(x_i)}. \qquad (1)$$

Для полного ансамбля событий:

$$X = \begin{pmatrix} x_1; & x_2; & x_3; \ldots x_n \\ P(x_1); P(x_2); P(x_3); \ldots P(x_n); \end{pmatrix}$$

среднее значение $\bar{I}(x)$ информации по всему ансамблю событий [2]:

$$\bar{I}(x) = M[I(x_i)] = H, \quad (2)$$

называется энтропией сообщения (H) и измеряется в двоичных единицах на сообщение:

$$H = -\sum_{i=1}^{n} P(x_i) \log_2 [P(x_i)]. \quad (3)$$

Воспользуемся основным свойством энтропии [3]: при заданном числе "n" символов энтропия максимальна и равна:

$$H(x) = \log_2 n, \quad (4)$$

лишь тогда, когда

$$P(x_1) = P(x_2) = \ldots = P(x_n) = 1/n. \quad (5)$$

Для примера возьмем алфавит русского языка. В таблице 1 приведены n = 32 символа русского языка (x_i) (в том числе и символ (пр) – пробел), вероятности их появления $P(x_i)\%$ (в процентах) [6], и вероятности появления $P(x_i)\%$ округленные до ближайшего целого большего значения в процентах $E^+[P(x_i)\%]$.

С целью обеспечения в канале равновероятной передачи всех символов с точностью до одного процента предлагается для каждого подлежащего передаче символа x_i выделить количество различных кодовых комбинаций равное числу $E^+[P(x_i)\%]$.

Общее число различных комбинаций для алфавита русского языка $\sum E^+[P(x_i)\%] = 116$ кодовых слов. Превышение общего числа комбинаций больше 100% является следствием округления вероятностей $P(x_i)$ до ближайшего большего целого числа процентов (табл. 1).

Все комбинации, относящиеся к конкретному символу x_i зациклены и передаются по очереди при появлении данного символа в передаваемом тексте.

Таким образом, для возможности обеспечения равновероятной передачи по каналу различных кодовых конструкций, передатчик должен содержать для каждого символа x_i "банки" различных кодовых слов в количестве $E^+[P(x_i)\%]$.

Для алфавита русского языка таких "банков" будет 32 (по количеству передаваемых символов) с общей памятью 116 кодовых слов.

Таблица 1

Вероятностные параметры символов русского языка

№ п/п	1	2	3	4	5	6	7	8	9	10	11
x_i	пр	А	Б	В	Г	Д	Е,Ё	Ж	З	И	Й
$P(x_i)\%$	17,5	6,2	1,4	3,8	1,3	2,5	7,2	0,7	1,6	6,2	1
$E^+[P(x_i)\%]$	18	7	2	4	2	3	8	1	2	7	1
№ п/п	12	13	14	15	16	17	18	19	20	21	22
x_i	К	Л	М	Н	О	П	Р	С	Т	У	Ф
$P(x_i)\%$	2,8	3,5	2,6	5,3	9	2,3	4	4,5	5,3	2,1	0,2
$E^+[P(x_i)\%]$	3	4	3	6	9	3	4	5	6	3	1
№ п/п	23	24	25	26	27	28	29	30	31	32	
x_i	Х	Ц	Ч	Ш	Щ	Ь,Ъ	Ы	Э	Ю	Я	
$P(x_i)\%$	0,9	0,4	1,2	0,6	0,3	1,4	1,6	0,3	0,6	1,8	
$E^+[P(x_i)\%]$	1	1	2	1	1	2	2	1	1	2	
$\sum_{i=1}^{n} E^+[P(x_i)\%] = 116$											

С целью экономии времени передачи воспользуемся таймерными сигналами [1]. Принцип построения таймерных сигнальных конструкций (ТСК) представлен на рис. 1, и заключается в следующем. Сигнальный алфавит бинарных ТСК формируется на интервале времени $(T_{ck} = m t_0)$, t_0 – величина найквистового элемента (обратная полосе пропускания канала), при базовом элементе отсчета длительностей Δ

($D = t_0/S$, S Î 1; 2; 3; ... k – целые числа.

Таким образом, на интервале $(T_{ck} = m t_0)$ расположено $n = mS$ точек отрезков Δ. Из всего множества 2^n возможных на интервале T_{ck} сигналов разрешенными считаются только те, в которых соседние значащие моменты модуляции (ЗММ) отстоят друг от друга на время, не меньшее чем $SD = t_0$. Это условие обеспечивает минимум межсимвольных искажений. Каждый ЗММ может занимать на оси времени позиции, расположенные на расстоянии $kD³ t_0$ друг от друга, причем Δ определяется как минимальное расстояние между соседними положениями одного ЗММ в разных конструкциях. Информация о передаваемом сообщении, переносимая ТСК, содержится в номере временной позиции, занимаемой ЗММ, причем первый информационный ЗММ может появиться не раньше, чем через SD позиций от момента начала сигнала (нулевой позиции).

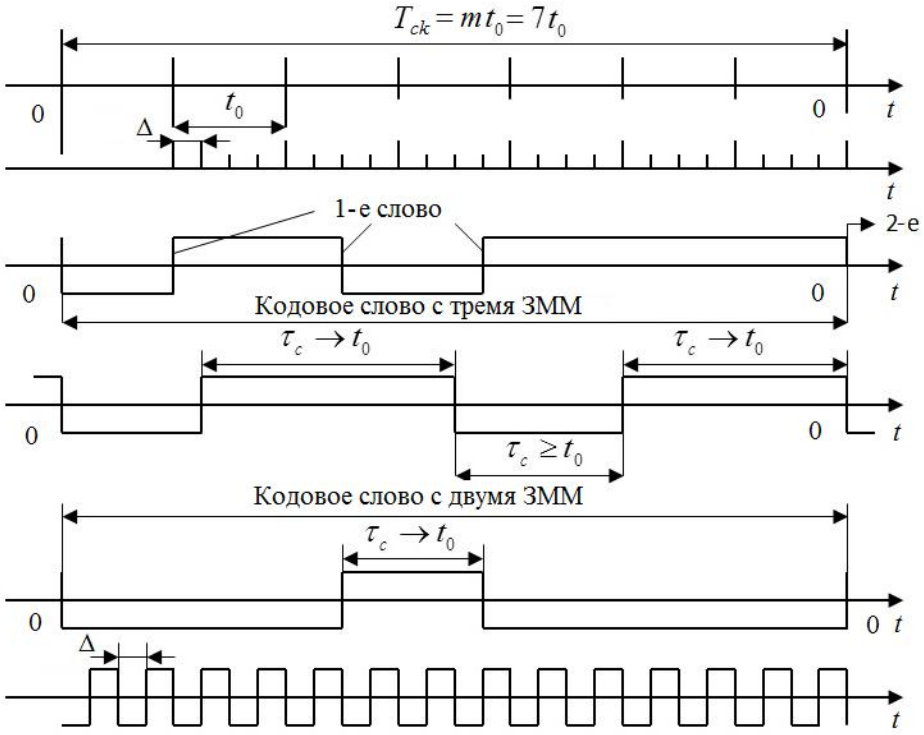


Рис. 1. Формирование сигнального алфавита бинарных ТСК на интервале времени $T_{ck} = mt_0$ при базовом элементе D

Так как величина $D < t_0$, то увеличение пропускной способности возможно, если число реализаций сигнала N_p на интервале (mt_0) не меньше чем 2^m. Можно показать, что при заданном $S = t_0/D$ на интервале m единичных элементов мощность сигнального алфавита бинарных ТСК определяется как [4]

$$N_p(i = \text{const}) = C^i_{mS-i(S-1)},$$

$$N_p(i = \text{var}) = \sum_{i=1}^{m} C^i_{mS-i(S-1)}, \qquad (6)$$

$$C^i_m = \frac{m!}{i!(m-i)!}, \qquad (7)$$

где i – число ЗММ в сигнальной кодовой конструкции. Среди разрешенных сигналов могут быть реализации с одним ЗММ, двумя, тремя и т. д. С максимальным числом моментов модуляции m возможна только одна реализация.

Для примера в табл. 2 приведено количество реализаций ТСК $T_{ck} = mt_0S$ и сигналов простого двоичного кода $N_p = 2^m$.

Таблица 2

Количество реализаций ТСК и среднее значение ЗММ для величин: i=3, $T_c = mt_0 \times S$; $N_p = 2^m$

m / S	m = 4, $N_p = 16$	m = 5, $N_p = 32$	m = 6, $N_p = 64$	m = 7, $N_p = 128$	m = 8, $N_p = 256$	m = 9, $N_p = 512$
2	10	35	84	165	286	455

3	20	84	220	455	816	1330
4	35	165	455	969	1771	2925
5	56	286	816	1771	3276	5456
6	84	455	1330	2925	5456	9139
7	120	680	2024	4495	8436	14190
8	165	969	2925	6545	12341	20825

Как видно из табл. 2, на одном и том же интервале T_{ck} можно образовать большее количество ТСК, чем сигналов простого двоичного кода $N_p = 2^m$.

Следовательно, скорость передачи, т. е. количество передаваемой информации на интервале T_{ck} увеличивается. Так как минимальное расстояние между ЗММ двух ближайших кодовых слов равно $D < t_0$, а прием значащих моментов воспроизведения (ЗМВ) осуществляется методом анализа в отдельных зонах D [1] то, естественно, вероятность ошибочного приема такого сигнала выше, чем элемента при разрядно-цифровом коде.

Из приведенной выше информации о методе формирования ТСК на m-элементном интервале времени T_{ck} следует, что за счет значения $D(S)$ одно и то же число реализаций можно получить на различных интервалах времени.

Для примера на рис. 2 представлены зависимости длительности сигнальной конструкции при заданной мощности кодового множества и параметра S. Из этих зависимостей следует, что при $S \geq 2$ для получения $N_p = 2^m$ можно затратить время $t_c < mt_0$. При этом это неравенство тем сильнее, чем больше значение S.

Пусть множество 116 кодовых слов представляет кодовые конструкции с тремя информационными отрезками x_1, x_2, x_3 [4]. Для возможности оценки принадлежности к передаваемому множеству потребуем, чтобы координаты x_1, x_2, x_3 удовлетворяли условию [1]:

$$x_1 + 2x_2 + 3x_3 = 0 \,(\mathrm{mod}\, 7) \qquad (8)$$

Тогда мощность множества M из которого можно выбрать 116 кодовых слов удовлетворяющих условию (8) должна быть [4] $M \geq 116 \times 7 = 812$ к.с. Каждое из этих 812 кодовых слов должно иметь энтропию равную $\log_2 812 = 9{,}65$ двоичных единиц.

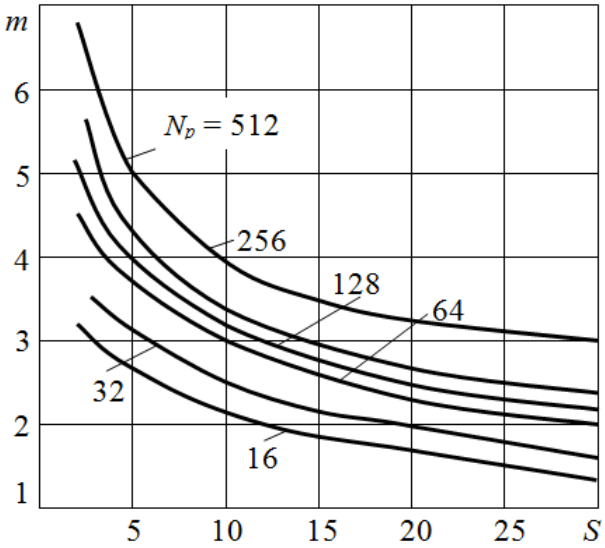


Рис. 2. – Зависимости длительности сигнальной конструкции при заданной мощности кодового множества и параметра S

Выбрав реализации кодовых слов удовлетворяющих условию (8) на интервале $T_p = 5t_0$, мы синтезируем кодовые конструкции с максимальной энтропией [2, 4]:

$$H = \log_2 N_p \qquad (9)$$

и максимальной информационной емкостью $I_н$ найквистового элемента (t_0):

$$I_н = \frac{H}{m} = \frac{\log_2 N_p}{m}, \qquad (10)$$

В таблице 3 приведены значения энтропии как функции: $H = f(m, S)$ (в числителе) и информационной емкости найквистового элемента (в знаменателе) для $m \in [4, 10]$, при $S \in [2, 12]$.

Таблица 3

Энтропия и информационная емкость найквистового элемента

S \ m	4	5	6	7	8	9	10
2	3,322/0,83	5,129/1,026	6,392/1,065	7,366/1,052	8,16/1,02	8,830/0,98	9,41/0,941
3	4,321/1,08	6,392/1,279	7,781/1,297	8,830/1,261	9,672/1,209	10,377/1,153	10,982/1,098
4	5,129/1,282	7,366/1,473	8,830/1,472	9,920/1,417	10,79/1,349	11,514/1,279	12,134/1,213
5	5,807/1,452	8,160/1,632	9,672/1,612	14,790/1,541	11,673/1,459	12,414/1,379	13,042/1,304
6	6,392/1,598	8,830/1,766	10,377/1,730	11,514/1,645	12,414/1,552	13,159/1,462	13,793/1,379
7	6,907/1,727	9,409/1,882	10,383/1,831	12,134/1,733	13,042/1,630	13,793/1,533	14,432/1,443

8	7,366/1,842	9,920/1,984	11,514/1,919	12,677/1,811	13,591/1,699	14,346/1,594	14,989/1,499
9	7,781/1,945	10,377/2,076	11,987/1,999	13,158/1,880	14,078/1,760	14,837/1,649	15,482/1,548
10	8,160/2,040	10,790/2,158	12,414/2,069	13,591/1,942	14,516/1,815	15,277/1,697	15,923/1,592
11	2,127	2,233	2,134	1,998	1,864	1,742	1,632
12	2,208	2,303	2,193	2,051	1,910	1,783	1,669

Из таблицы 3 следует:

1. С увеличением m при $S = \text{const}$ энтропия реализаций также увеличивается.

2. Информационная емкость одного найквистового элемента максимальна на интервале реализации $T_p = 5t_0$ (для $S > 3$); $I_н(m=4) < I_н(m=5) > I_н(m=5)$.

В качестве оптимальной длительности кодовых слов следует выбирать $T_p = 5t_0$, что соответствует максимальной информационной емкости найквистового элемента.

При передаче по каналам с гауссовским шумом следует учитывать, что вероятность ошибочного приема таймерной сигнальной кодовой конструкции – ТСК ($P_о$) определяется величиной зоны Δ, среднеквадратическим отклонением значащего момента восстановления (σ), которая, в свою очередь зависит от соотношения сигнал/шум, а также средним числом переходов в слове [1] ($\bar{i}$).

$$P_о = 1 - [\Phi(\Delta/2\sigma)]^{\bar{i}}, \quad (11)$$

где: Φ(x) – интеграл вероятностей:

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{\frac{-t^2}{2}} dt. \quad (12)$$

Учитывая, что с увеличением S растет не только число реализаций N_p, но и вероятность ошибочного приема их $(P_о)$, то для каждого канала есть свое значение Δ_0, при котором реализуется максимальная пропускная способность системы. При этом каждая из реализаций сигнала на интервале $(T_{ck} = m t_0)$ представляет собой одну из реализаций многопозиционного во времени сигнала. Тогда значение пропускной способности:

$$C_m = \frac{1}{m}(\log_2 N_p - H_{пот}). \quad (13)$$

Здесь $H_{пот}$ определяет потери в канале из-за неопределенности в принятии кодовой сигнальной конструкции:

$$H_{пот} = -\left[P_п \log_2 P_п + (1 - p_п)\log_2 \frac{1 - P_п}{N - 1}\right], \quad (14)$$

где $P_п$ - вероятность правильного приема сигнальной конструкции с i – перехода:

$$P_п = 2[\Phi(\Delta/2\sigma)]^{\bar{i}}. \quad (15)$$

На рис. 3 приведены зависимости пропускной способности каналов с разным уровнем флуктуационных шумов (задано $h = (u_с/u_ш)$ как функции S (кривые 1, 2, 3 для h = 7,5 и m = 8, 6, 5 соответственно, кривые 4, 5, 6 для h = 5,5 и m = 8, 6, 5 в соответствии).

Из рисунка 3 следует, что для каждого значения h является величина зоны, при которой C_m будет максимальной. На практике оптимальное значение определяется среднеквадратичным отклонением смещения фронта сигнала на выходе канала (σ_k), $\Delta_{опт}$ = (3,8 ... 5,5); σ_k = 3,8 ... 4,5/h.

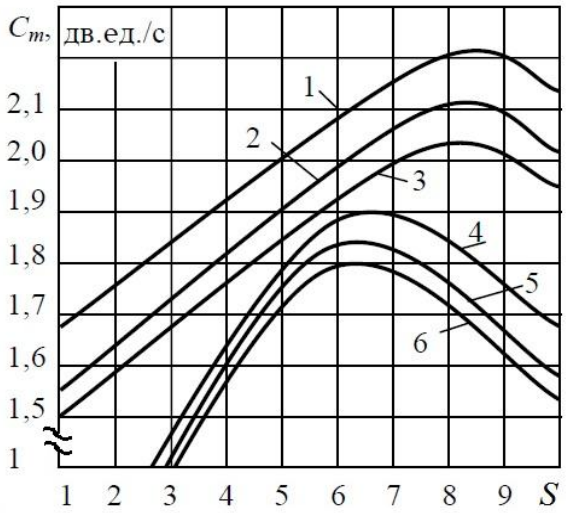


Рис. 3. Зависимости пропускной способности канала $C_i = f(S)$ при h = const, m = const

Выводы и перспективы дальнейших исследований

Анализ таблиц 1-3 показывает:

1. С увеличением интервала реализации "m" ($T_{ck} = m t_0$) при $S = \text{const}$ число возможных сигнальных конструкций растет (табл. 1). Информационная емкость одного кодового слова ($\log_2 N_p$) также растет с увеличением интервала реализации "m" (табл. 3).

2. Информационная емкость одного найквистового элемента при увеличении m вначале растет (до $m \le 5$), а при $m > 5$ начинает снижаться. Для каждого "m" информационная емкость с ростом "S" увеличивается.

Как показано выше, ограничением для "S" является вероятность смещения одного момента модуляции на величину $[P(q = 1\Delta)] < P_3$.

Выбор параметра "S" целесообразно ограничивать значением $S = 8$, так как при $S > 8$ увеличивается вероятность ошибочного приема одного момента модуляции даже в "хорошем" состоянии канала. Связано это с тем, что при $S > 8$ растет значение информационной емкости одного кодового слова ($\log_2 N_p$), но еще быстрее растут потери за счет увеличения вероятности ошибки на $q = 1D$.

Именно равновероятность появления символов на приеме не позволяет различать их статистическим анализом и делает такие сообщения трудно дешифрируемыми.

Литература

1. Эффективные системы передачи информации / Н.В. Захарченко, Е.М. Рудый, А.А. Вараксин, М.А. Мамедов, М.М.Гаджиев; под ред. Н.В. Захарченко. – Баку: ЭЛМ. – 2007. – 568 с.

2. Захарченко М. В. Системи передавання даних Том 1. Завадостійке кодування / М. В. Захарченко – Одеса.: Фенікс 2009. – 447 с.

3. Захарченко М. В. Порівняння ансамблів кодових множин, синтезованих на основі декількох модулів з ансамблями, реалізованими на основі таймерних сигнальних конструкцій / М. В. Захарченко, С. М. Горохов, О. В. Кочетков, В. В. Гордейчук, Е. Б. Шамшидін // Системи обробки інформації. – 2017. – № 1. – С. 18-21.

4. Захарченко М. В. та ін. Математичні основи оптимізації телекомунікаційних систем: підручник. За заг. ред. Захарченко М.В. - Одеса: ОНАЗ ім. О.С.Попова, 2010.– 240 с.

5. Фельдбаум А.А и др. Теоретические основы связи и управления. М.: Физматгиз – 1963. – 932 с.

6. Захарченко Н.В. Эффективность двухсимвольных ансамблей в симплексных системах на базе корректирующих таймерных сигнальных конструкций / Н.В. Захарченко, В.Й. Кильдишев, Д.В. Голев, А.В. Толкачев // Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». – 2017. – № 1. – С. 215-218.

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ СКРИТНОСТІ ПЕРЕДАЧІ НЕРІВНОЙМОВІРНОГО АЛФАВІТУ ПРИ ТАЙМЕРНОМУ КОДУВАННІ

***Микола Васильович Захарченко** (д-р техн. наук, професор, професор кафедри)[1]*
***Олександр Вячеславович Кочетков** (канд. техн. наук, ст. викладач кафедри)[1]*
***Євген Олександрович Севастєєв** (ст. викладач, аспірант кафедри)[1]*
***Антон Сергійович Кріль** (аспірант кафедри)[1]*

[1]Одеська національна академія зв'язку ім. О.С. Попова, Одеса, Україна

Для підвищення інформаційної скритності передачі нерівноймовірноного алфавіту при таймерному кодуванні запропонований метод вторинного кодування нерівноймовірного первинного алфавіту що передається з метою забезпечення рівноймовірної передачі символу в каналі з точністю до одного відсотка. Визначено кількість різних кодових комбінацій («банк» кодових слів символу) що забезпечують рівноймовірну передачу кодових слів. Для зменшення часу передачі запропоновано використання таймерних сигналів, визначена оптимальна тривалість таймерного кодового слова. Показано, що саме рівноймовірна поява символів на прийомі не дозволяє розрізняти їх статистичним аналізом і робить такі повідомлення складними для розшифрування.

***Ключові слова:** інформація, ентропія, інформаційна ємність найквістового елемента, інтервал реалізацій, таймерні сигнали, момент модуляції*

TO INCREASE THE INFORMATION SECRECY TRANSMISSION NONEQUIPROBABILITY ALPHABET FOR TIMER CODING

***Nikolay V. Zakharchenko** (Doctor of Technical Sciences, Professor, Professor of a Department)[1]*
***Aleksandr V. Kochetkov** (Candidate of Technical Sciences, Senior Lecturer of a Department)[1]*
***Yevgeniy A. Sevasteev** (Graduate student, Senior Lecturer of a Department)[1]*
***Anton S. Kril** (Graduate student of a Department)[1]*

[1]A.S. Popov Odessa national academy of telecommunications, Odessa, Ukraine

To increase the information concealment of the transmission of the uneven-probability alphabet in timed encoding, a method is proposed for secondary coding of the transmitted non-equal probability primary alphabet in order to ensure equiprobable transmission of the symbol in the channel with an accuracy of one percent. The number of different code combinations ("bank" of the code words of the symbol) is determined to ensure equiprobable transmission of codewords. To reduce the transmission time, the use of timer signals is suggested, the optimal length of the timer codeword is determined. It is shown that it is the equiprobability of the appearance of symbols at the reception that makes it impossible to distinguish them by statistical analysis and makes such messages difficult to decipher.

***Key words:** Information, entropy, information capacity naykvist element, implementations interval, timer signals, time modulation.*

References

1. Effective information transfer systems / N.V. Zakharchenko, E.M. Rudy, A.A. Varaksin, M.A. Mamedov, M.M. Hajiyev; Ed. N.V. Zakharchenko. - Baku: ELM. - 2007. - 568 p. **2. Zakharchenko M.V** Data transmission systems Volume 1. Noise-proof encoding / MV Zakharchenko - Odessa: Phoenix 2009. - 447 p. **3. Zakharchenko M.V** Comparison of ensembles of code sets synthesized on the basis of several modules with ensembles implemented on the basis of timer signal constructions / M.V Zakharchenko, S.M. Gorokhov, O.V. Kochetkov, V.V. Gordeichuk, E.B. Shamshidin // Systems of information processing. - 2017. - No. 1. - P. 18-21. **4. Zakharchenko M.V** and others. Mathematical bases of optimization of telecommunication systems: a textbook. For zag Ed. Zakharchenko MV - Odessa: ONAT them. O.Popova, 2010.- 240 p. **5. Feldbaum A.A**. et al. Theoretical Foundations of Communication and Management. Moscow: Fizmatgiz - 1963. - 932 p. **6. Zakharchenko N.V** Efficiency of two-character ensembles in simplex systems based on corrective timed signal constructions / N.V. Zakharchenko, V.Y. Kildishev, D.V. Golev, A.V. Tolkachev International scientific and technical journal "Measuring and computing engineering in technological processes".. - 2017. - No. 1. - P. 215-218.

УДК 629.5

Олександр Олегович Каніфольський *(канд. техн. наук, доцент)*[1]
Миколай Миколайович Конотопець *(канд. техн. наук, доцент)*[2]

[1]***Одеський національний морський університет, Одеса, Україна***
[2] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

РОЗВ'ЯЗАННЯ ЗАДАЧІ ПОПОВНЕННЯ МАЛОТОННАЖНОГО ФЛОТУ З УРАХУВАННЯМ ОБМЕЖЕНЬ ПО ПОГОДНИМ УМОВАМ

Метод рішення задачі поповнення флоту, що базується на порівнянні кінетичної енергії малого судна і енергії хвилі запропонований в даній статті. Увагу акцентовано на суднах і катерах перехідного режиму руху. Хвилювання інтенсивністю чотири бали вибрано для дослідження і максимальна довжина суден, кораблів та катерів, перехідного режиму ефективних для цих умов представлена на графіку. Вимоги різних класифікаційних товариств до характеристик хвиль різних районів плавання приведені до спільного знаменника. Метод прогнозу зниження швидкості судна на хвилюванні різної інтенсивності розроблений і перевірений розрахунками. Рівняння прирощення опору води руху судна і прирощення енергії руху представлені в диференціальній формі. Порівняльний аналіз даних про втрати швидкості судном на хвилюванні різної інтенсивності, який базується на дослідженнях різних авторів, наведено в табличній формі.

Ключові слова: *задача поповнення малотоннажного флоту; розміри малих суден обмеженого району плавання; зниження швидкості судна на хвилюванні.*

Вступ

Постановка проблеми. При проектуванні суден і кораблів може виникнути ряд проблем, пов'язаних з призначенням складу флоту. Ці питання належать до вирішення зовнішньої задачі проектування. До області цієї задачі теорії проектування зазвичай відносять: розробку способів оптимізації флоту; задачу поповнення флоту; встановлення загальних вимог до суден. Надалі ця інформація використовується для визначення характеристик суден, які будуть вказуватися в завданнях на проектування, для вирішення внутрішньої задачі проектування, пов'язаної з конкретним судном. Одним з питань, при розробці технічного завдання на проектування, є район і дальність плавання судна, його автономність. Виникає необхідність: оцінити швидкість судна і її зниження, пов'язане з характеристиками хвилювання в регіоні; визначити граничні розміри судна і його швидкість, при яких судно зможе використовуватися, при передбачуваних характеристиках хвиль. Існує і ряд інших завдань стосовно співвідношення і обмеження головних розмірів судна. Особливо ці питання актуальні для малих швидкісних суден і кораблів, так як їх ефективна експлуатація пов'язана зі збереженням заданої швидкості і виконанням покладених на них завдань.

Аналіз останніх досліджень і публікацій. Деякі дослідження присвячені питанням зниження швидкості судна, при русі на хвилюванні. В одній з таких робіт розглядається втрата швидкості на зустрічному регулярному хвилюванні моделей пасажирських суден прибережного плавання [2]. Але як зазначено в цьому ж джерелі «… отсутствуют надежные данные по потере скорости судов рассматриваемого назначения в различных штормовых условиях». Дані випробувань говорять про можливе падіння швидкості, в перехідному режимі руху, число Фруда по довжині 0.45, в середньому близько 20%, в залежності від характеристик хвилювання.

В іншому джерелі [3] наведені формули для оцінки втрати швидкості швидкісного судна на хвилюванні, прискорення при вертикальній хитавиці і амплітуди поздовжньої хитавиці $dv = a_1 v h_в^{3/2}$, $\ddot{z} = a_2 g h_в^{3/2}$, $y = a_3 h_в$, в залежності від висоти хвилі $h_в$. До складу цих рівнянь входять коефіцієнти a_1, a_2 і, a_3, що залежать від проектних параметрів. Далі проводиться аналіз залежності $dv = a_1 v h_в^{3/2}$ на основі діаграми упор - опір. Зроблено висновок, що при середніх вимогах до мореплавства (2-3 бали хвилювання), відношення $\frac{dv}{v} = 0{,}1 \pm 0{,}02$. При 4 -5 балах хвилювання, $\frac{dv}{v} = 0{,}17 \pm 0{,}05$. Експлуатація швидкохідного судна при більшому хвилюванні не передбачена, що пов'язано з нормативами комфортності і безпеки. Це підтверджується даними [2].

Ці методи можуть використовуватись для попередньої оцінки втрати швидкості на хвилюванні, але не дають відповідь на наступне питання. Яке саме за мінімальним розміром судно може бути використано, при даних параметрах хвиль? Як приклад: чи можна виходити в море на малому моторному човні типу «Ока – 4», при висоті хвилі один метр? Завод-виготовлювач дозволяє експлуатацію цього човна при висоті, що дорівнює 0.7 м.

Деякі класифікаційні суспільства, крім обмеження району плавання, вводять поняття розрахункової граничної висоти хвилі, з якої швидкісне судно може зустрітися в рейсі [6].

Правила [4] вводять обмеження району плавання для суден довжиною менше 24 м незалежно від забезпечення нормованих морехідних якостей. Обмеження району плавання малого судна ґрунтується на досвіді плавання однотипних суден з урахуванням гідрометеорологічних умов. Вводяться поняття: обмеження по району плавання і обмеження через погодні умови. В основному хвилювання, при якому дозволена експлуатація малого судна через погодні умови, обмежена шістьма балами. Для пасажирських суден - чотири бали. Висота хвилі 3,5 м відповідає хвилюванню 5 балів та характерна для району плавання R3-RSN (III ЗП). Це за визначенням [5] - змішане (річка-море) плавання на хвилюванні з висотою хвилі 3% - ної забезпеченості 3,5 м, з урахуванням конкретних обмежень по району та умовам плавання, обумовлених режимами басейнів, з встановленням при цьому максимально допустимого віддалення від місця притулку, яке не має перевищувати 50 миль.

Мета статті. Мета даної статті - розробка методу для визначення параметрів малого швидкохідного судна, в залежності від конкретного хвильового регіону і прогнозування зниження швидкості, при русі на зустрічному хвилюванні.

Виклад основного матеріалу дослідження

В основу запропонованого методу покладено порівняння кінетичної енергії судна і повної енергії хвилі. Залежно від того яка з енергій має більше значення буде зроблений висновок про прийнятність параметрів судна (водотоннажності, довжини, швидкості) для експлуатації в районі з даними параметрами хвиль.

Енергія $E_{в1} = \frac{\rho g h_в^2 L_в}{8}$ - енергія на одиницю ширини поверхні хвилі, висотою $h_в$ і довжиною $L_в$. Тоді енергія хвилі діючої на всю ширину судна B буде описана формулою

$$E_в = \frac{\rho g h_в^2 L_в}{8} B .$$

Кінетична енергія судна, з урахуванням приєднаної маси води, як $E_c = \frac{1{,}1mv^2}{2} = \frac{1{,}1\rho c_b LBdv^2}{2}$. Представляючи питому енергію хвилі у вигляді $E = \frac{1{,}1\rho g h_в^2 L_в}{8}\frac{B}{d}$, отримуємо значення E, що характерне для суден з різними значеннями відносної ширини $\frac{B}{d}$.

Нерівність, в якому порівнюються питома кінетична енергія судна і питома енергія хвилі, з урахуванням відносної ширини $\frac{B}{d}$ буде виглядати

$$\frac{1{,}1\rho c_b LBdv^2}{2d} \le \frac{\rho g h_в^2 L_в}{8}\frac{B}{d} .$$

Для забезпечення прийнятних морехідних якостей судна або корабля існують оптимальні значення відносної довжини $\frac{L}{B}$ і коефіцієнта загальної повноти c_b. Після підстановки значень $\frac{L}{B}$ = 6 і c_b = 0,5, середніх значень прийнятних для плавзасобів перехідного режиму руху, можна отримати вираз для розрахунку довжини судна $L \le \sqrt{\frac{1{,}36 g h_в^2 L_в}{v^2 c_B}\frac{B}{d}}$ [1].

Графіки, що допомагають визначити допустимі розміри судна для району плавання R3-RSN ($h_{3\%}$ = 3,5 м, $L_в$ = 70 м) наведені в [1]. Нижче буде зроблений розрахунок для деяких інших районів плавання, що визначаються різними класифікаційними товариствами.

Спільні правила товариств GL, BV і RINA [6] визначають наступні райони плавання (мова оригіналу), табл. 1.

З'явилася необхідність провести порівняльний аналіз різних вимог класифікаційних товариств, що безперечно допоможе проектувальнику при створенні проекту швидкісного судна чи корабля.

Таблиця 1

Райони плавання і висоти хвиль

Район плавання	Висота хвилі $h_{1/3}$	Висота хвилі $h_{3\%}$
"Open-sea service"	$h_{1/3} \ge 4$ м	$h_{3\%} > 5{,}3$ м
"Restricted open-sea service"	2,5 м $\le h_{1/3} <$ 4 м	3,3 м $\le h_{3\%} <$ 5,3 м
"Moderate environment service"	0,5 м $< h_{1/3} <$ 2,5 м	0,7 м $< h_{3\%} <$ 3,3 м
"Smooth sea service"	$h_{1/3} \le$ 0,5 м	$h_{3\%} \le$ 0,7 м

У Правилах [6] використовується термін висота «значних» хвиль (середня висота найбільшої третини хвиль) $h_{1/3}$. Формула, що зв'язує це поняття і висоту хвилі 3% - ної забезпеченості має вигляд $h_{3\%} = 1{,}33h_{1/3}$. Середнє значення висоти хвилі $h_{3\%}$ для району "Moderate environment service" дорівнює 2 м, що відповідає інтенсивності 4 бали.

Правила [4] вводять обмеження через погодні

умови: «Непассажирским судам длиной менее 15 м разрешается выход и нахождение в море при интенсивности волнения не более четырех баллов…Пассажирским судам … длиной от 20 до 24 м - не более четырех баллов…»

Нижче, на рисунку 1, наведено розрахунок визначення малого судна для району плавання з хвилюванням 4 бали, висота хвилі $h_{3\%}$ = 2 м, довжина хвилі $L_в$ = 40 м.

У даній роботі розглядаються швидкохідні судна і кораблі перехідного режиму, з відносними швидкостями 1,18 < Fr_V < 3, що відповідає числам Фруда по довжині від 0,45 до 0,98 (цей діапазон показаний двома горизонтальними лініями, рис. 1).

На цьому ж рисунку нанесені точки характерні

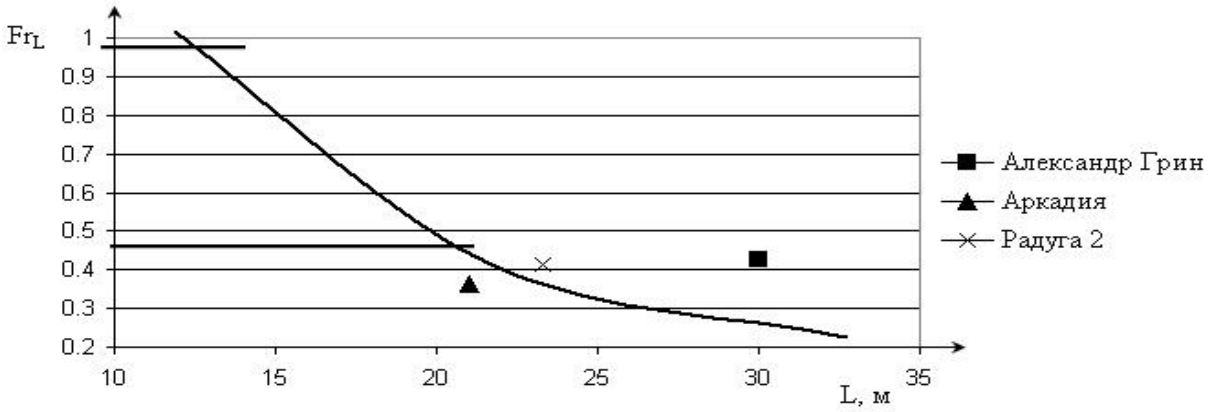


Рис. 1. Мінімальна довжина суден і кораблів, хвилювання 4 бали

для деяких пасажирських суден прибережного плавання.

Відповідно до графіка, при Fr_L = 0,45, мінімальна довжина судна близько 22 м. При Fr_V = 3, допустима довжина малого судна 13 м.

Довжина судна «Александр Грин» більше, ніж отримано за розрахунком. Максимальне значення висоти хвилі, яке прийнятне для цього судна за правилами GL $h_{1/3}$ = 2,2 м або $h_{3\%}$ = 2,9 м.

З метою прогнозування зниження швидкості судна на хвилюванні, з урахуванням енергії хвилі, опір води при русі судна можна представити у вигляді [3]

$$R = av^2W \qquad (1)$$

де a - коефіцієнт що враховує щільність води, поправки; W - площа змоченої поверхні судна.

Приріст опору визначається шляхом диференціювання рівняння (1).

$$dR = 2aWdv \qquad (2)$$

Рівняння балансу потужності з урахуванням (1)

$$dRv = 2Rdv \qquad (3)$$

Співвідношення прирощення швидкості і опору

$$\frac{dv}{v} = \frac{dR}{2R} \qquad (4)$$

На одиничній ділянці переміщення ds , можна записати рівняння для прирощення енергії

$$\frac{dv}{v} = \frac{dRds}{2Rds} = 0{,}5\frac{dE}{E} \qquad (5)$$

Також можна записати враховуючи енергію хвилі та кінетичну енергію судна

$$\frac{dv}{v} = 0{,}5\frac{dE}{E} = 0{,}5\frac{E_в}{E_c} \qquad (6)$$

В літературі [2] наведені дані про втрати швидкості, в перехідному режимі руху, на зустрічному хвилюванні моделі судна «Александр Грин» при буксируванні постійним вантажем, рисунки 2 та 3. Співвідношення довжини хвилі і довжини судна $\frac{L_в}{L}$ = 0.85 і 1 (26 м і 30 м відповідно), висота хвилі $h_{3\%}$ = 1.3 м і 1.5 м ($\frac{L_в}{h_{3\%}}$ = 20). На цих же рисунках, представлений розрахунок передбачуваної втрати швидкості за формулою (5).

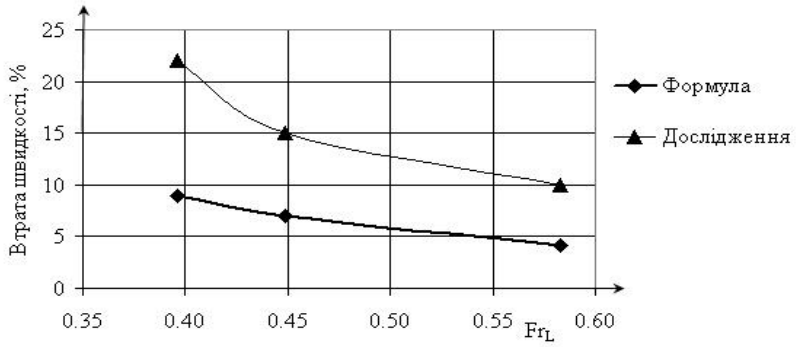


Рис. 2. Втрата швидкості на хвилюванні $\frac{L_в}{L}$ = 1, $\frac{L_в}{h_{3\%}}$ = 20

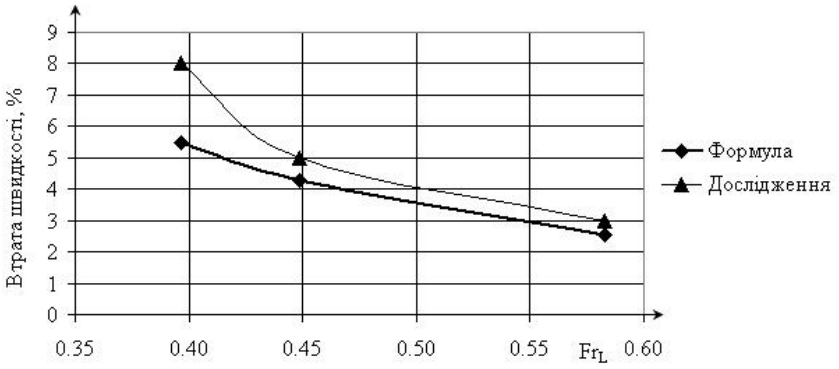


Рис. 3. Втрата швидкості на хвилюванні $\frac{L_в}{L}$ = 0.85, $\frac{L_в}{h_{3\%}}$ = 20

Аналізуючи рисунки, можна відзначити, що при однаковій довжині хвилі і судна (рис.2), передбачувана розрахункова втрата швидкості за формулою (5) менше, ніж отримана при випробуваннях. Це пов'язано з тим, що при числах Fr_L = 0,4, настає перехідний режим руху, виникає ходова хвиля з довжиною, яка дорівнює довжині судна, що супроводжується інтерференцією хвиль. За умови рівності довжин хвилі і судна користуватися формулою (5) потрібно з обережністю.

При відмінності довжин хвилі і судна формула (5) дає досить точні результати, рис. 3.

У таблиці 2 представлені дані про падіння швидкості на хвилюванні отримані з різних джерел.

Таблиця 2

Зниження швидкості судна на хвилюванні

Хвилі	Втрата швидкості, %		
	Дані [3]	«Александр Грин», [2]	«Александр Грин», формула (5), $\frac{L_в}{h_в}$=15
2-3 бали	8-12 %	8 %	5 %
4 – 5 балів	12-22 %	22 %	16 %

Висновки.

У статті запропоновано методи вирішення завдання поповнення флоту, в залежності від обмежень через погодні умови і пов'язаної з нею задачі прогнозування зниження швидкості судна на хвилюванні.

Користуючись запропонованими в статті рекомендаціями і даними про хвилювання в регіоні, можна визначити головні розміри суден, кораблів і катерів флоту, які можуть бути використані з максимальною віддачею.

Прогноз зниження швидкості судна на хвилюванні різної інтенсивності надзвичайно важливий при експлуатації суден спеціального призначення, а також для ефективного виконання завдань військовими катерами.

Розв'язання обох завдань, в представленому вигляді, запропоновано вперше.

Література

1. Канифольский А.О. Термин «быстроходное малое судно прибрежного плавания» // Зб. наук. праць ОНМУ. - Одеса: ОНМУ, 2010. - №29. – С. 17-25. **2. Леви Б.З.** Пассажирские суда прибрежного плавания. - Л.: Судостроение, 1975. - 320 с. **3. Царев Б.А.** Оптимизационное проектирование скоростных судов. - Л.: ЛКИ, 1988. - 103 с. **4. Регистр судоходства Украины.** Правила освидетельствования судов. - К.: Регистр судоходства Украины, 2005. – 573 с. **5. Российский Морской Регистр Судоходства.** Циркулярное письмо главного управления РМРС № 007-2.1-253ц, 2007. – 7с. **6. Germanischer Lloyd.** Rules for Classification and Construction. Chapter 5. High Speed Craft. - Humburg: Gebrüder Braasch, 1996. – 272р.

РЕШЕНИЕ ЗАДАЧИ ПОПОЛНЕНИЯ МАЛОТОННАЖНОГО ФЛОТА С УЧЕТОМ ОГРАНИЧЕНИЙ ПО ПОГОДНЫМ УСЛОВИЯМ

Александр Олегович Канифольский *(канд. техн. наук, доцент, доцент кафедры)*[1]
Николай Николаевич Конотопец *(канд. техн. наук, доцент, профессор кафедры)*[2]

[1]*Одесский национальный морской университет, Одесса, Украина*
[2]*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

Метод решения задачи пополнения флота, основанный на сравнении кинетической энергии малого судна и энергии волны предложен в данной статье. Внимание акцентировано на судах и катерах переходного режима движения. Волнение интенсивностью четыре балла выбрано для исследования и максимальная длина судов, кораблей и катеров, переходного режима эффективных для этих условий представлена на графике. Требования различных классификационных обществ к характеристикам морского волнения приведены к общему знаменателю. Метод прогноза снижения скорости судна на волнении разработан и проверен расчетами. Уравнения приращения сопротивления воды движению судна и приращения энергии представлены в дифференциальной форме. Сравнительный анализ данных о потере скорости судном на волнении различной интенсивности, который базируется на исследованиях разных авторов, приведен в табличной форме.

Ключевые слова: *задача пополнения малотоннажного флота; размеры малых судов ограниченного района плавання; снижение скорости судна на волнении.*

SOLUTION OF THE PROBLEM OF COMPLETING A SMALL FLEET WITH RESPECT TO WEATHER CONDITIONS

Oleksandr O. Kanifolskyi *(Ph.D., Docent, Docent of chair Theory and Designing of Ship of Odessa National Maritime University)*[1]
Mykola M. Konotopets *(Ph.D., Docent, Professor of a Departmentt)*[2]

[1]*Odessa National Maritime University, Odessa, Ukraine*
[2]*National Defense University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

The method of solving the task of replenishing the fleet, based on a comparison of the kinetic energy of a small vessel and the wave energy, is proposed in this article. Attention is focused on the vessels and boats of transitional mode. A wave with a characteristic of four points is selected for the study and the maximum length of ships and boats of the transitional mode that are effective for these conditions is shown on the graph. The requirements of different classification societies to the characteristics of seawaves are reduced to a common denominator. The method of foreknowing the reduction of the speed of the vessel on waves of varying intensity was developed and tested by calculations. The equations of increment of water resistance and energy increment are presented in differential form. Comparative analysis of data on the loss of speed of the vessel on waves of different intensity, which is based on the studies of different authors, is given in tabular form.

Keywords: *the task of replenishing of the small tonnage fleet; dimensions of the small vessels in a limited area of navigation; reduction of the speed in rough sea.*

References

1. Kanifolskyi O.O. The term “speed small craft of restricted open sea navigation” / O.O. Kanifolskyi // Scientific papers ONMU. - Odessa, 2010.- №29. – P. 17-25. **2. Levi B.Z.** “Passenger ships of coastal navigation”, Shipbuilding, 1975.- 320 p. **3. Tsarev B.A.** “Optimal design of high-speed vessels”, LSI, 1988. – 103 p. **4. Register of Shipping of Ukraine**. Rules for the survey of ships. - K.: Register of Shipping of Ukraine, 2005. – 573 p. **5. Russian Maritime Register of Shipping.** Circular letter of the General Directorate RMRS № 007-2.1-253c. New symbols for the classification of ships and floating structures in the Rules, 2007. – 7p. **6. Germanischer Lloyd.** Rules for Classification and Construction. Chapter 5. High Speed Craft. - Humburg: Gebrüder Braasch, 1996. - 272p.

УДК 355.6

В'ячеслав Леонідович Козачук *(кандидат технічних наук, старший науковий співробітник)*
Василь Петрович Харченко *(кандидат військових наук, старший науковий співробітник)*

Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

МЕТОДИЧНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ПАРАМЕТРІВ ПРОЦЕСУ МОНІТОРИНГУ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ ПІД ЧАС ЕКСПЛУАТАЦІЇ

У нинішній час моніторинг як метод дослідження застосовують у багатьох галузях економіки. Але як і всякий процес моніторинг повинен мати певні параметри. Одним з найважливіших слід вважати такий параметр, як дискретність спостереження та/або фіксації значень характеристик та показників, що характеризують технічний стан об'єкту, за яким ведеться спостереження. Існуючі методи визначення дискретності мають вагомі недоліки, що суттєво обмежують сферу застосування, тому виникає необхідність розробки нового методичного підходу розрахунку цього параметра моніторингу. Вирішення такого завдання стає можливим за умови застосування теореми Котельникова, відомої також як теорема дискретності. Відповідно до цієї теореми спочатку розраховується спектр функції, яка описує процес зміни значень показника, за яким здійснюється моніторинг, визначається верхня частота спектру та розраховується дискретність спостереження. Визначаються умови корегування отриманої моделі в умовах нестаціонарності розглядуваного процесу.

Ключові слова: *моніторинг, теорема Котельникова, дискретність, спостереження, технічний стан, апроксимація.*

Вступ

Постановка проблеми в загальному вигляді. Поняття **"**моніторинг" міцно увійшло в практику не лише науково-дослідних робіт, але й багатьох галузей економіки. Однак загальноприйнятого розуміння сенсу та наповнення поняття "моніторинг" як процесу, як певної сукупності операцій у часі досі не існує. Так, прийняті в ряді джерел формулювання поняття "моніторинг" іноді суттєво відрізняються. Найчастіше поняття "моніторинг" трактують таким чином: "…комплекс заходів, які забезпечують регулярне (постійне) спостереження за технічним станом … з метою попередження негативних явищ, що впливають на цілісність і надійність об'єктів спостереження", а також: "…система планових, безперервних або періодичних спостережень і контролю, яка проводиться за спеціально розробленою програмою для визначення змін у технічному стані об'єктів та оцінки їх з метою недопущення граничних значень контрольованих параметрів" [1, 2]. Тобто, як витікає з наведеної дефініції, моніторинг є процес, який протікає у часі. І якщо це процес, то він має бути описаний низкою параметрів, що повинні піддаватися вимірюванню. Одним з найважливіших слід вважати такий параметр моніторингу, як дискретність спостереження та/або фіксації значень характеристик та показників технічного стану об'єкту, за яким ведеться спостереження.

Аналіз останніх досліджень і публікацій. Аналіз відкритих джерел, присвячених розглядуваному питанню, свідчить про те, що і раніше проводилися дослідження щодо визначення параметрів моніторингу складних організаційно-технічних об'єктів (СОТО). Так, у роботі [3] розглядались питання дискретності фіксації значень параметрів процесу, що спостерігається. Визначити періодичність контролю параметрів процесу пропонувалось на основі положень теорії апроксимації, виходячи із припустимої точності подання розглянутого процесу. Апроксимуючий степеневий багаточлен $F_и(t)$, що проходить через усі дискретні значення функції x(t) повинен задовольняти таким умовам:

$$\begin{cases} F(t_1)=a_0+a_1t_1+...+a_nt_1^n=x_1 \\ F(t_2)=a_0+a_1t_2+...+a_nt_2^n=x_2 \\ ..... \\ F(t_n)=a_0+a_1t_n+...+a_nt_n^n=x_n \end{cases}$$

Рішення наведеної системи рівнянь має вигляд інтерполяційного полінома Лагранжа:

$$F(t_n)=\sum_{k=0}^{n} x \frac{\prod_{i=0,i\neq k}^{n}(t-t_i)}{\prod_{i=0,i\neq k}^{n}(t_k-t_i)}.$$

Погрішність апроксимації розраховується так

$$\Delta\psi=\frac{M_n}{n!}\left|\prod_{i=0}^{n}(t-t_i)\right|,$$

де M_n — максимальне значення модуля n-ої похідної функції в інтервалі апроксимації.

При першому ступені апроксимуючого багаточлена прогнозні значення інтервалів часу

між моментами контролю параметрів визначається з рівняння:

$$|\Delta\psi_{max}| = M_1 \Delta t_1,$$

звідки

$$\Delta t_1 = |\Delta\psi_{max}| / M_1 .$$

Якщо апроксимувати багаточленом другого ступеня, то

$$\Delta t_2 = \sqrt{\frac{8|\Delta\psi_{max}|}{M_2}} .$$

При апроксимації багаточленами третього ступеня інтервал між вимірюваннями має бути таким:

$$\Delta t_3 = \sqrt{\frac{16|\Delta\psi_{max}|}{M_3}} .$$

Якщо погрішність $\Delta\psi_{max}$ £ 2%, то різниця між інтервалами квантування Δt_1, Δt_2, …, Δt_n незначна.

Для використання методу апроксимації з метою визначення періодичності контролю показників необхідні дані про швидкість зміни кожного параметра та припустимої погрішності його апроксимації степеневим багаточленом. Для одержання такої інформації потрібно зібрати й обробити значну кількість даних, що досить трудомістко й займає багато часу (цей фактор був майже головним у ті часи), тому в практиці розглянутий метод застосування не знайшов. Також слід відмітити, що моделювання процесу, що спостерігається, лише багаточленами, на наш погляд, є помилковим шляхом, тому що реальні процеси зміни, наприклад, технічних параметрів СОТО, можуть мати майже будь-який вигляд.

Відсутність науково обґрунтованого методичного підходу до встановлення частоти вимірів параметрів (дискретності вимірів) приводить або до втрати інформації через великі інтервали квантування часу, внаслідок чого можливі ускладнення та навіть аварії при експлуатації СОТО, або до додаткових трудових витрат при надмірно великій частоті контролю й підвищенню загальної вартості контролю. Виходячи з наведеного, можна зробити висновок про необхідність розроблення методичного апарату, який дозволяв би без зайвого суб'єктивізму визначити та обґрунтувати припустимі інтервали квантування часу дискретного контролю параметрів при здійсненні моніторингу.

Тому **метою статті** є розгляд порядку визначення інтервалів квантування часу в процесі моніторингу технічного стану озброєння та військової техніки (ОВТ).

Виклад основного матеріалу дослідження

Однією з головних цілей моніторингу технічного стану (ТС) ОВТ як об'єкту моніторингу є виявлення динаміки зміни значень параметрів ОВТ (у загальному випадку під технічним станом об'єкту моніторингу розуміють сукупність якостей, що змінюються у процесі виробництва, випробувань та експлуатації, які характеризують його функціональну пристосованість в певних умовах використання [4]). Як правило, ТС визначається шляхом оцінювання показників ТС, серед яких слід виділити, у першу чергу, вимірювані показники та розраховані показники. Вимірювані показники ТС — це показники, які можна представити у вигляді значень вимірюваних параметрів (характеристик) об'єкту моніторингу. Розраховані показники — це показники якостей об'єкту моніторингу, які обчислюють за різноманітними алгоритмами на основі значень вимірюваних показників. Основним способом виявлення (оцінювання) ТС є збирання, обробка та аналіз отриманої внаслідок вимірювання та обчислення інформації про ТС. Збір інформації про ТС — це процес отримання та відповідного розподілу усіх значень вимірюваних показників. Обробка інформації про ТС — це процес отримання оцінок значень вимірюваних показників на основі зібраних даних, які характеризують певним показником ступеню довіри до цих оцінок. Метою аналізу інформації про ТС є отримання узагальнених оцінок сукупності показників ТС, значення яких у явному вигляді вказують або ступінь працездатності об'єкту моніторингу, або — разом з оцінками ступеню довіри до отриманих результатів — місце та вид виниклої відмови.

Внаслідок моніторингу формується деяка наявність накопичених даних про технічний стан систем та підсистем зразків ОВТ, яка дозволяє спрогнозувати працездатність (непрацездатність) ОВТ та попередити появу відмов та аварійних ситуацій. У процесі моніторингу технічного стану ОВТ як діагностична інформація можуть бути використані: результати інспекційного контролю, дані, отримані вимірюванням параметрів, які характеризують поточний технічний стан ОВТ, попередні дані контролю, а також інша подібна інформація. Для здійснення моніторингу потрібна система пристроїв, яка має такі технічні засоби: сукупність вимірювачів (датчиків температури, тиску, корозії, току, деформацій, витоків тощо), які розташовані на контрольованих елементах та зв'язані з пунктом контролю за допомогою дротового або бездротового з'єднання; сервер для збору, обробки та зберігання отриманої інформації та пристрій для відображення результатів моніторингу. Таким чином, з технічної точки зору, практична реалізація системи моніторингу технічного стану ОВТ проблем не викликає.

Але разом з тим залишається не вирішеним питання визначення дискретності фіксації значень

параметрів ОВТ, що спостерігаються, тобто мова йде про визначення параметрів процесу моніторингу, зокрема інтервалів квантування часу Δt_i (рис. 1).

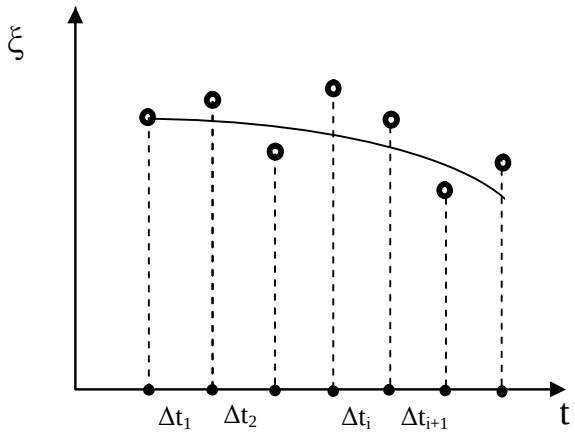


Рис.1. Порядок визначення дискретності фіксації значень параметрів ОВТ

Вирішення цього завдання стає можливим за умови застосування теореми Котельникова, формулювання якої таке: будь-яку безперервну функцію зі спектром, що обмежений смугою частот від нуля до Fв, можна однозначно визначити послідовністю її миттєвих значень, які отримані через інтервали $T_д \le 1/2\ Fв$ з формули:

$$x(t)=\sum_{t=-\infty}^{\infty} x(iT_Д)\frac{\sin 2\pi F_в(t-iT_Д)}{2\pi F_в(t-iT_Д)}$$

Теорему Котельникова також можна використовувати й для випадкових сигналів. У цьому випадку вона формулюється таким чином: для випадкового процесу з односторонньою спектральною щільністю, яка відповідає умові $G_x(f)=0$ при $f > F_в$ ряд приймає вигляд

$$\sum_{t=-\infty}^{\infty} X(iT_Д)\frac{\sin 2\pi F_в(t-iT_Д)}{2\pi F_в(t-iT_Д)},$$

де $X(iT_д)$ — випадкові величини, що є значеннями випадкового процесу, які отримані через інтервали часу $T_д=1/2Fв$ [5].

Наведемо приклад розрахунку часу дискретизації. Для цього приймемо, що процес зміни контрольованого параметра описується експоненційною функцією — $x(t) = \exp(-\beta t)$.

Спектр експоненційної функції є рівним:

$$X(\omega)=\int_{-\infty}^{\infty} x(t)e^{-i\omega t}dt=-\frac{1}{\beta+\omega}e^{-t(\beta+i\omega)}\Big|_0^{\infty}=$$

$$=-\frac{1}{\beta+i\omega}(0-1)=\frac{1}{\beta+i\omega},$$

де ω — частота спектру.

Таким чином, спектральна функція є величиною комплексною. Її модуль визначається так:

$$|X(\omega)|=\frac{1}{\sqrt{\beta^2+\omega^2}}=\frac{1/\beta}{\sqrt{1+\left(\frac{\omega}{\beta}\right)^2}}.$$

Якщо позначити $T=\frac{1}{\beta}$, то $x(t) = \exp(-t/T)$ та $|X(\omega)|=\frac{T}{\sqrt{1+(\omega T)^2}}$.

Необхідно відмітити, якщо $\omega \to \infty$, то $|X(\omega)| \to 0$. Таким чином, необхідно визначити верхню границю — $\omega_{гр}$. Якщо $\omega=\frac{1}{T}$, то $|X(\omega)|=\frac{T}{\sqrt{2}}$ а при $\omega=\frac{2}{T}$, $|X(\omega)| \approx 0{,}45T$ (рис.2).

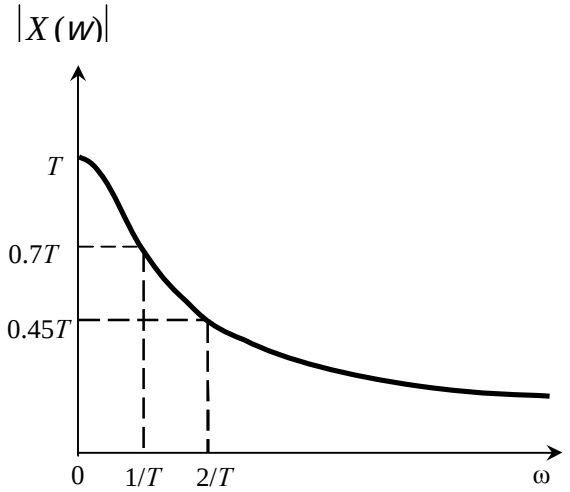


Рис.2. Модуль спектра експоненційної функції

Таким чином, якщо обрати значення модуля $|X(\omega)| \approx 0{,}45T$, то $\omega_{гр} = Fв=\frac{2}{T}$. Звідси

$T_д = 1/2Fв = T/4$, а так як $T=\frac{1}{\beta}$, то $T_д = 1/4\beta$.

Крім того, приймається гіпотеза, що процес зміни значень параметра ОВТ ξ(t), що спостерігається, є стаціонарним. У цьому випадку значення дискретності часу фіксації значень процесу зміни параметрів ОВТ визначається, виходячи з передбачуваної моделі процесу змін значень параметру ξ(t) (як правило, як модель такого процесу вибирається часовий ряд [6]. Для формування моделі відповідно з результатами моніторингу процесу змін значень параметру ξ(t) будується апроксимуюча функція. Отримання такої функції в аналітичному вигляді дає можливість розрахувати її, після чого, виходячи із значень верхньої граничної

частоти спектра апроксимуючої функції, згідно з теоремою Котельникова, розраховується значення дискретності часу фіксації значень параметрів Δt. Слід відмітити, що при виконанні умови стаціонарності (квазістаціонарності) процесу на інтервалі спостереження значення Δt = const.

Однак реальні процеси зміни значень параметрів ОВТ найчастіше не є стаціонарними і в цьому випадку може знадобитися корекція як моделі, так відповідно й значення дискретності часу фіксації. Для цього в кожній точці фіксації t_i (t_i Î T, T — інтервал моніторингу параметра ξ(t)) значень параметра ξ(t) здійснюється розрахунок $\frac{d\xi}{dt}$. Якщо $\left|\frac{d\xi}{dt}\right|$; 0, то модель процесу зміни значень параметра, що контролюється, не корегується, та відповідно на інтервалі спостереження значення Δt=const. Якщо після чергового шагу контролю, який здійснений в точці t_j, виконується умова $\left|\frac{d\xi}{dt}\right|$? 0, то знов виконується розрахунок спектру функції, її верхньої частоти та відповідно розраховується дискретність інтервалу спостереження Δt_{i+1}. Таким чином здійснюється корегування дискретності спостереження.

Після корегування моделі при наступному вимірюванні перевіряється стаціонарність процесу зміни значень параметра ξ(t) — розраховується друга похідна функції — моделі процесу змін значень параметрів — $\xi\text{¢¢}(t)$. Якщо виконується умова $\xi\text{¢¢}(t) = 0$, то модель не корегується, якщо $\left|\xi\text{¢¢}(t)\right|$? 0, то необхідно знову формувати модель процесу змін значень ξ(t).

Висновки й перспективи подальших досліджень

Запропоновано методичний підхід до визначення параметрів процесу моніторингу технічного стану озброєння та військової техніки під час експлуатації, в основу якого покладено суто математичний розрахунок дискретності спостереження процесу зміни значень параметрів технічного стану озброєння та військової техніки як складних організаційно-технічних об'єктів, деградація яких відбувається з плином часу.

Запропонований методичний підхід також передбачає створення можливості корегування виду або типу функцій, які описують процеси зміни значень параметрів та характеристик технічного стану. Корегування є можливим та доцільним у випадку нестаціонарності процесу, що спостерігається.

Перспективами подальших досліджень може бути пошук інших підходів до визначення параметрів процесу моніторингу технічного стану озброєння та військової техніки під час експлуатації. В першу чергу, це стосується подальшого удосконалення раніше розробленого методичного апарату вибору оптимальної (або раціональної) сукупності діагностичних параметрів та характеристик, які з достатнім ступенем вірогідності описують технічний стан озброєння та військової техніки.

Література

1 ДСТУ «Науково-технічний моніторинг об'єктів будівництва» (проект).

2 ДБН В.1.3-2:2010 «Геодезичні роботи у будівництві» / Київ, Мінрегіонбуд. 2010. – 55 с.

3 Булатов А.И. Контроль процессов бурения нефтяных и газовых скважин / Булатов А.И., Демихов В.И., Макаренко П.П. – М.: «Недра», 1998. – 345 с.

4 Зеленцов В.А. Методология создания и применения интеллектуальных информационных технологий наземно-космического мониторинга сложных объектов / В.А. Зеленцов, А.П. Ковалев, М.Ю. Охтилев, Б.В. Соколов, Р.М. Юсупов / Труды СПИИРАН. 2013. Вып. 5(28). – С. 7–81.

5 Радиотехнические системы передачи информации / Под ред. В.В. Калмыкова. – М.: Радио и связь, 1990. – 304 с.

6 Венгринович В.Л. Мониторинг технического состояния. Анализ рисков в технических системах / Неразрушающий контроль и диагностика № 2, 2014. – С.3–25.

МЕТОДИЧЕСКИЙ ПОДХОД К ОПРЕДЕЛЕНИЮ ПАРАМЕТРОВ ПРОЦЕССА МОНИТОРИНГА ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ ВО ВРЕМЯ ЭКСПЛУАТАЦИИ

Вячеслав Леонидович Козачук *(канд. техн. наук, с.н.с.)*
Василий Петрович Харченко *(канд. воен. наук, с.н.с.)*
Центральный научно-исследовательский институт Вооруженных Сил Украины, Киев, Украина

В нынешнее время мониторинг как исследовательский прием применяют во многих областях экономики. Но как и всякий процесс мониторинг должен иметь определенные параметры. В первую очередь это касается такого параметра, как дискретность наблюдения или фиксации значений

характеристик и параметров, которые характеризуют состояние объекта, за которым ведется наблюдение. Существующие методы определения дискретности имеют весомые недостатки, которые существенно ограничивают сферу применения, поэтому возникает необходимость разработки нового методического подхода расчета этого параметра мониторинга. Решение такой задачи становится возможным при условии применения теоремы Котельникова, известной также как теорема дискретности. Согласно этой теореме сперва рассчитывается спектр функции, которая описывает процесс изменения значений параметра сигнала, за которым осуществляется мониторинг, определяется верхняя частота спектра и рассчитывается дискретность наблюдения. Затем определяются условия коррекции полученной модели в условиях не стационарности наблюдаемого процесса.

Ключевые слова: *мониторинг, теорема Котельникова, дискретность, наблюдение, техническое состояние, аппроксимация.*

METHODICAL APPROACH TO DETERMINING PARAMETERS OF THE PROCESS OF MONITORING THE TECHNICAL CONDITION OF WEAPONS AND MILITARY EQUIPMENT AT OPERATION

Vyacheslav L. Kozachuk *(Candidate of Technical Sciences, Senior Research Fellow)*
Vasyl P. Kharchenko *(Candidate of Military Sciences, Senior Research Fellow)*
The Central Research Institute of the Armed Forces of Ukraine, Kiev, Ukraine

The monitoring is used as a method of research in many areas of the economy. But like every process, the monitoring ought to have certain parameters. First of all, this concerns such a parameter as the discreteness of observation or fixation of values of characteristics and parameters that characterize the state of the object, which is being monitored. Existing methods for determining discreteness have significant drawbacks, which substantially limit the scope of application, so it becomes necessary to develop a new methodological approach to calculating this monitoring parameter. The solution of such problem becomes possible with condition of applying the Kotelnikov's theorem, also known as the theorem of discreteness. According to this theorem, the function spectrum is first calculated that describes the process of changing the values of the signal parameter, which is monitored, the upper frequency of the spectrum is determined, and the discreteness of the observation is calculated. Then the conditions for correcting the obtained model are determined in conditions of non-stationarity of the observed process.

Keywords*: monitoring, Kotelnikov's theorem, technical condition, discreteness, observation, approximation.*

References

1 DSTU "Scientific and technical monitoring of construction projects" (project).

2 DBN V.1.3-2: 2010 "Geodetic works in construction" / Kyiv, Minregionstroy. 2010. - 55 p.

3 Bulatov A.I. Control of drilling processes of oil and gas wells / Bulatov A.I., Demikhov V.I., Makarenko P.P. - M .: "Nedra", 1998. - 345 p.

4 Zelentsov V.A. Methodology of creation and application of intelligent information technologies for ground-space monitoring of complex objects / V.A. Zelentsov, A.P. Kovalev, M.Yu. Okhtilev, B.V. Sokolov, R.M. Yusupov / Proceedings of SPIIRAS. 2013. Vol. 5 (28). - p. 7-81.

5 Radiotechnical systems of information transmission, Ed. V.V. Kalmykov. - M .: Radio and Communication, 1990. - 304 p.

6 Vengrinovich V.L. Monitoring of technical condition. Risk analysis in technical systems / Nondestructive testing and diagnostics № 2, 2014. - p.3-25

UDK 355.45

Serhii Anatoliyovych Mykus *(Candidate of Military Sciences, associated professor)*

National Defence University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine

THE STRATEGY OF BUILDING FUNCTIONALLY STABLE INFORMATION-TELECOMMUNICATION SYSTEMS

The article introduces the notion of "functionally stable information-telecommunication system", gives grounds for the need to implement this property into all modern information and telecommunications systems. The strategy and theoretical basis of scientific-methodical apparatus for providing information and telecommunications systems with functional stability properties have been described.

Keywords: *functional stability, information and telecommunication system, reliability, strategy.*

Introduction

The industry associated with information technology is now becoming ever more relevant. It should be emphasized that the study of the existing science-based approaches to the increase of the effectiveness of complex technical systems, including telecommunication ones, brought us to the conclusion on the formation of a new priority approach associated with provision of a system with a functional stability [1-9]. Implementation of a functional stability is achieved by the use of different types of redundancy (instrumental, time, information, functional, capacity, etc.) in a complex technical system, through resource leveling to compensate the consequences of emergency situations. It is fundamental that at the design stage additional redundancy must not be implemented, and compensation of the consequences of emergency situations will be carried through leveling of the existing resources. The problem is to identify such redundancy and to form the signals of recovering control at the required moment aimed at its leveling. This is the main difference between the problem of ensuring a functional stability and the problem of design of structurally redundant systems.

Target Setting. The known properties of complex technical systems, such as stability, reliability, survivability, fault-tolerance characterize functioning of systems under the influence of failures and damage. But they do not allow full description of the functioning processes in the conditions of significant damage, the impact of failures flows, possible terrorist influences, as well as errors of operators and other internal and external destabilizing influences. Therefore, it is advisable to provide the information and telecommunications systems with such property of complex technical systems as a functional stability [1].

Analysis of latst research and publications. Many scientific works have described a functional stability [2], and one of them [3] - the property of functional stability and its general idea for complex technical systems. Our study introduces the notion of a functional stability of a dynamical system as "properties of the system that represent its ability to perform at least a set minimum of its functions in case of a failure in the information, computing and power components of the system, as well as the influences of external factors stipulated by the operating conditions". We propose main stages of the procedure to provide the system with this property, namely: detection and recognition of an emergency situation, with the subsequent compensation of the consequences due to implementation of recovering control. The problem of a functional stability of on-board information and control complex of an aircraft has been considered in more details.

At present, in spite of the available meaningful scientific results of the theory of functional stability, mathematical models of complex systems researched by them fail to adequately describe the functioning of all the existing systems. Therefore, it is relevant to summarize the theory of functional stability of complex technical systems and develop it for specific systems, namely, - for information and telecommunication systems. Analysis of the known scientific provisions of the existing theory of functional stability determines the fact of absence of direct publications concerning the solution of the problem of design of functionally stable information and telecommunications systems.

The paper [4] was the first to define and prove the general difference between a stability of functioning and a functional stability: a stability of functioning characterizes the behavior of the coordinates of an unexcited and excited operation of the system, while a functional stability describes the deviation of the main functions of the coordinates at an unexcited and excited operation. Distributed information system is mathematically described by a random graph, which peaks are connected by a triangle principle. In other words, in case of any emergency situations, the information from each node must reach (albeit not by the shortest path) each node in the system. Our research has offered a necessary and sufficient condition for the functional stability of distributed information systems of special purpose, that means all the switching nodes must be operational and the alternative routes of transmission of information between nodes must be available. We have also proposed a framework of categories and concepts connected with a functional stability, which is a set of mathematical models,

signs, indicators, criteria, stock and areas of a functional stability. The methods to define graph connectedness to be able to calculate indicators of a functional stability of distributed information systems have been generalized and further developed. The sets of methods for the synthesis of a structure of functionally stable distributed information systems have been developed, which include the method of solution of a specific problem and the method of solution of a general problem of synthesis. The technique for identification of emergency situations in functionally stable distributed information systems has been improved, which is based on the principles of the so-called stray diagnostic kernel and does not require additional hardware redundancy to solve the problems of identification.

Kravchenko Yu.V. [2] gave a formalized definition to a functional stability of a pseudo-satellite radionavigation system. Unlike for a distributed information system, the so-called "star" is assumed to be a model for connections between the elements of a pseudo-satellite radionavigation system, and loaded orgraphs - its mathematical model. The problem of synthesis of the system structure was solved on the basis of the theory of matroids, gradient algorithms and the method of sequential increase of the rank of a k-uniform matroid developed by the author. The concept of formation of the structure of pseudo-satellite radionavigation system was offered, which is different from existing approaches to the design of multiway radio-navigation systems due to availability of functional stability through the use of structural redundancy and formation of recovering control in order to compensate the consequences of emergency situations (in case of failures, faults, destructions, combat and other damages of pseudo-satellites) to enable the system to perform the functions of navigation. The implementation of the concept allows to synthesize the system structure taking into account a possible loss of its components, as well as to reduce the number of pseudo-satellites 2-4 times with equal values of the indicator of a functional stability. A framework of categories and concepts of functional stability of the structure of the a pseudo-satellite radionavigation system (a sign, an indicator, a criterion, a boundary, and an area of a functional stability) has been further developed and can be applied to any multiway radio-navigation systems, allowing it to formalize in the mathematical way the objective function and limitations in the problem of the structure optimization, as well as quantitatively and qualitatively evaluate the property of a functional stability of the structures of pseudo-satellite systems. A model for the synthesis of a structure of a pseudo-satellite radionavigation system was developed, which is different from the existing approaches to the synthesis of structures of multiway radionavigation systems due to availability of a functional stability; application of the proposed method of sequential increase of the rank of a k-uniform matroid. The method of determining the value of the indicator of a functional stability of the structure of a pseudo-satellite radionavigation system was developed for the first time, which fully takes into account both the accuracy of the solution of a navigation task by consumers, and a structural redundancy of a pseudo-satellite system, as well as the ability to control a structural redundancy of the system to compensate the consequences of failures, faults, destruction, combat and other damage to pseudo-satellites. Application of these methods allows to have a quantitative evaluation of a functional stability of any structures of multiway radio-navigation systems in the analysis of the existing and the synthesis of advanced systems [5].

A considerable contribution in the development of the theory of a functional stability was made by Professor Nedelko S.M. [6]. Namely, his works gave a further development to the classic concept of ensuring a functional stability of complex technical systems, which is characterized by a new strategy to ensure a functional stability of automated air traffic control systems in the context of itemization of the stage of "compensation" through substages: identifying existing resources (redundancy areas), formation of the procedure of optimum (suboptimum) usage of redundancy and estimation of the system condition after leveling of the resources. Professor Obidin D.M. in his works [7] further developed the existing concept of a functional stability of complex technical systems, which differs from existing approaches by the proposed strategy and the principles of ensuring the functional stability properties for intelligence systems of automatic aircraft flight control in the context of the development of the phase of "recognition" of a classical theory through implementation of the verification of the decentralized unclear database to determine the authenticity of the data elements, and the stage of "compensation" where during the formation of recovering control a subjective character of the data is taken into account through the indicators of reliability of the database elements to compensate the consequences of emergency situations during the aircraft flight.

So, to develop and implement information technologies in the society we must consider the general problem of raising the efficiency of information and telecommunication systems, for which the problem of ensuring a functional stability for the system is a specific one.

The aim of the article is to present the strategy and theoretical background of the methodological framework to ensure functional stability for information and telecommunication systems.

Presentation of the main research material

Functional stability of an information and telecommunication system is its property to be in an operational condition, that is, to carry out at least the required minimum of its functions within a given time interval or its lifelength under the condition of failure of its components in case of external and internal factors due to redistribution of different types of redundancy.

Analysis of requirements to the design of a functionally stable system discovered a conflicting situation, which represents the worsening conflict between the following requirements:

between the requirement to increase the efficiency, that entails additional expenses, and the requirement to reduce the costs while designing and upgrading;

between the requirement to reduce the time on upgrades, which reduces the efficiency of the system, and the requirement to increase the efficiency.

This controversial situation makes the basis for the actual new scientific problem connected with ensuring the properties of a functional stability of information and telecommunications systems. It is possible to solve this scientific problem through the use of the theory of ensuring a functional stability of information and telecommunications systems proposed by the authors of this article. This theory includes a set of logically related conceptual, theoretical and technological bases. The conceptual basis describes a system of views or, in other words, a basic leading idea – the concept of ensuring functional stability properties. The strategy of ensuring the properties of a functional stability is substantiated and developed. A scientific hypothesis that this property will be ensured at the expense of intellectualization of the stages of a "classic" strategy is suggested.

This idea is comprehensively studied in the theoretical basis using new scientific approaches, methods, techniques, algorithms and mathematical models. As a result scientific-methodical apparatus for the analysis and synthesis of a functionally stable information and telecommunications system has been developed. A systematic approach, the theory of artificial intelligence, universal algebra, fuzzy logic and a theory of emergent field make the theoretical basis of the study.

The concepts and theoretical bases of the so-called FS-systems and E-field have been introduced and developed.

FS-system refers to a system of algebra, that represents the grid on which the specified additional binary relation that has some rule-oriented-logical properties was set. The grids in the context of this definition are considered in their broad sense, with their type being specified in particular models. The concept of FS-system is an abstract description of a set-theoretical model of a rule-oriented structure. This generalization is achieved using mathematical grids as the basis for an algebraic system. A binary relation is set on the grid that contains the semantics of a rule-based-logical conclusion.

E-field or an emergent field is a mathematical formalization of the system effect or emergence – one of the important properties of a complex system. Rules of the so-called operations of "emergence addition" and "emergence multiplication" are substantiated and presented. The authenticity of this theoretical result is confirmed by the fact that it was received on the basis of one of the laws of dialectics – the law of transition of quantity into quality.

Conclusions and perspective for future research

Thus, it is expected that the design of functionally stable information and telecommunications systems will enable us to successfully solve many problems of the design and development of new generations of data systems, because these systems allow: significant expansion of the range of application conditions; ensuring a comprehensive optimization of performance of tasks assigned to the functions system; increase in the efficiency of the systems as a whole; significant reduction of time and financial costs connected with development and adoption of individual designs of hardware and software.

References

1. Yu.V. Kravchenko, S.A. Mykus, «The Current State and the Future Development of the Modern Theory of Functional Stability», in Proc. of the G.E. Pukhov Inst. of Modeling Problems in Energy Eng., vol. 68, pp.60-68, Sep. 2013. **2. N.P. Buslenko**, V.V. Kalashnikov, I.N. Kovalenko, Lectures on the Theory of Complex Syst., Moscow, USSR: Soviet radio, 1973. **3. V. Mashkov**, J. Barilla, P. Simr, «Applying Petri Nets to Modeling of Many-Core Processor Self-Testing when Tests are Performed Randomly», J. Electron. Testing: Theory and Applicat. (JETTA), vol. 29, pp. 25–34, Feb. 2013. **4. O.V. Barabash**, Construction of a Functionally Stable Distributed Inform. Syst., Kiev, Ukraine: National University of Defense of Ukraine, 2004. **5. Yu.V. Kravchenko**, «The Method of Consecutive Increase of the Rank of k-homogeneous Matroid for the Synthesis of the Structure of a Pseudo-satellite Radio-navigation Systems», Modern Inform. Technologies in the Sphere of Security and Defense, no. 2(2), pp. 19-22, Aug. 2008. **6. S.M. Nedilko,** The Basic Concepts of the Theory of Functional Stability Automated Air Traffic Manage. Syst., Kirovohrad, Ukraine: State Flight Academy of Ukraine, 2011. **7. D.M. Obidin**, O.V. Barabash, «The Signs and Criteria of Functional Stability for Intellectual Aircraft Automatic Control System», Syst. of Weapons and Military Equipment: Scientific J., no. 1 (29), pp. 133-136, Mar. 2012. **8.Yu.V. Kravchenko**, O.A. Leshchenko, S.A. Mykus, «Functional Stability of Information and Telecommunication Systems», East European Scientific J., no.2(6), pp.47-52, Feb. 2016. **9. Yu. Kravchenko**, V. Vialkova, «The problem of providing Functional Stability Properties of Information Security Systems», in Proc. of the XIIIth Int. Conference «Modern Problems of Radio Eng., Telecommun., and Comput. Sci.» (TCSET'2016), 2016, pp. 526-530.

СТРАТЕГИЯ ПОСТРОЕНИЯ ФУНКЦИОНАЛЬНО УСТОЙЧИВЫХ ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННЫХ СИСТЕМ

***Сергей Анатольевич Мыкусь** (канд. воен. наук, доц.)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье уделено внимание научной проблеме обеспечения свойства функциональной устойчивости информационно-телекоммуникационным системам. Решение данной научной проблемы возможно путем использования предложенной автором статьи теории обеспечения функциональной устойчивости информационно-телекоммуникационным системам. Данная теория включают совокупность логически связанных между собой концептуальных, теоретических и технологических основ. В концептуальных основах сосредоточена основная руководящая идея - концепция обеспечения свойства функциональной устойчивости. Излагается стратегия обеспечения свойства функциональной устойчивости. Выдвигается научная гипотеза о том, что данное свойство будет обеспечено за счет интеллектуализации этапов «классической» стратегии. В теоретических основах данная идея всесторонне исследуется на основе новых научных подходов, методов, методик, алгоритмов и математических моделей. В результате разработан научно-методический аппарат анализу и синтеза функционально устойчивой информационно-телекоммуникационной системы. Теоретической основою является системный подход, теория искусственного интеллекта, универсальная алгебра, нечеткая логика и теория эмерджентных полей. Введены понятия и разработаны теоретические основы так называемых FS - систем и E - поля.

***Ключевые слова:** функциональная устойчивость, информационно-телекоммуникационная система, надежность, стратегия.*

СТРАТЕГІЯ ПОБУДОВИ ФУНКЦІОНАЛЬНО СТІЙКІЙКИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Сергій Анатолійович Микусь (канд. військ. наук, доц.)

Національний університет оборони України імені Івана Черняховського, Київ, Україна

У статті приділена увага науковій проблемі забезпечення властивості функціональної стійкості інформаційно-телекомунікаційним системам. Вирішення даної наукової проблеми можливо шляхом використання запропонованої автором статті теорії забезпечення функціональної стійкості інформаційно-телекомунікаційним системам. Дана теорія включає сукупність логічно зв'язаних між собою концептуальних, теоретичних і технологічних основ. У концептуальних основах зосереджена основна керівна ідея - концепція забезпечення властивості функціональної стійкості. Викладається стратегія забезпечення властивості функціональної стійкості. Висувається наукова гіпотеза про те, що дана властивість буде забезпечена за рахунок інтелектуалізації етапів «класичної» стратегії. У теоретичних основах дана ідея всебічно досліджується на основі нових наукових підходів, методів, методик, алгоритмів і математичних моделей. У результаті розроблений науково-методичний апарат аналізу й синтезу функціонально стійкої інформаційно-телекомунікаційної системи. Теоретичною основою є системний підхід, теорія штучного інтелекту, універсальна алгебра, нечітка логіка й теорія емерджентних полів. Уведені поняття й розроблені теоретичні основи так званих FS - систем і E - поля.

***Ключові слова:** функціональна стійкість, інформаційно-телекомунікаційна система, надійність, стратегія.*

Література

1. Кравченко Ю.В. Сучасний стан та шляхи розвитку теорії функціональної стійкості / Ю.В. Кравченко, С.А. Микусь // Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – К.: ІПМЕ, 2013. – Вип. 68.– С. 60–68. **2. Бусленко Н.П.** Лекции по теории сложных систем / Н.П. Бусленко, В.В. Калашников, И.Н. Коваленко. – М.: Сов. радио, 1973. – 440 с. **3. Артюшин Л.М.** Оптимизация цифровых автоматических систем, устойчивых к отказам / Л.М. Артюшин, О.А. Машков. – К.: КВВАИУ, 1991. – 89 с. **4. Барабаш О.В.** Построение функционально устойчивых распределенных информационных систем / О.В. Барабаш. – К.: НАОУ, 2004. – 226 с. **5. Кравченко Ю.В.** Применение метода последовательного увеличения ранга k-однородного матроида в задаче синтеза структуры псевдоспутниковой радионавигационной системы / Ю.В. Кравченко // Сучасні інформаційні технології у сфері безпеки та оборони. – К.: 2008. – №2(2). – С. 19 – 22. **6. Неділько С.М.** Основи теорії функціональної стійкості автоматизованої системи управління повітряним рухом / С.М. Неділько. – Кіровоград: ДЛАУ, 2011. – 220 с. **7. Обідін Д.М.** Ознаки та критерії функціональної стійкості інтелектуалізованої системи автоматичного управління польотом літака. / Д.М. Обідін, О.В. Барабаш // Системи озброєння і військова техніка: Науковий журнал. – Х.: ХУПС, 2012. – № 1 (29). – С. 133 – 136. **8. Кравченко Ю.В.** Функціональна стійкість інформаційно-телекомунікаційних систем. / Ю.В. Кравченко, О.А. Лещенко, С.А. Микусь // Східно Європейський науковий журнал, 2016. – № 2(6). – С. 47-52. **9. Кравченко Ю.В.** Проблема забезпечення властивості функціональної стійкості системам захисту інформації./ Ю. Кравченко, В. Віалкова // XIII Міжнародна конференція «Сучасні проблеми радіотехніки, телекомунікаційних і комп'ютерних наук» (TCSET'2016), 2016, С. 526-530.

УДК 681.51:623.592

***Андрей Станиславович Могилатенко*[1]**
***Юрий Александрович Данилов*[2]**
Максим Анатольевич Павленко *(доктор технических наук, доцент)*[3]

[1]***Воинская часть А0593, Никополь, Украина***
[2]***Командование Воздушных Сил Вооруженных Сил Украины, Винница, Украина***
[3]***Харьковский национальный университет Воздушных Сил имени Ивана Кожедуба, Харьков, Украина***

РАЗРАБОТКА МЕТОДА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ ПОТОКОМ СООБЩЕНИЙ О ВОЗДУШНЫХ ОБЪЕКТАХ ОТ ИСТОЧНИКОВ РАДИОЛОКАЦИОННОЙ ИНФОРМАЦИИ В АСУ РЕГИОНАЛЬНЫХ ЦЕНТРОВ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ

Использование адаптивного подхода к управлению информационным потоком сообщений о ВО от источников РЛИ предусматривает решение следующих задач адаптации: задача распознавания ситуаций применения методов сжатия и выдачи сообщений о ВО для информационного потока РЛИ; задача распределения методов сжатия и выдачи РЛИ по сообщениям о ВО в общем информационном потоке; задача непосредственного изменения структуры сообщений о ВО. Для решения задачи изменения структуры сообщений о воздушном потоке необходимо разработать протокол формирования и обработки сообщений о ВО с переменной структурой. При этом решающие правила должны разрабатываться с использованием интеллектуальных информационных технологий.

Ключевые слова: *метод, управление, сжатие*

Разработка протокола формирования и обработки адаптивной структуры сообщений о ВО

Для возможности использования предложенных методов в рамках базового протокола обмена радиолокационной информацией (РЛИ) в формате ASTERIX необходимо разработать правила формирования и обработки адаптивных сообщений о воздушном объекте (ВО) для каждого метода сжатия РЛИ.

Сжатие информации о качественных признаках. В поле спецификации формата ASTERIX необходимо зарезервировать место под определение наличия или присутствия всех сформированных признаковых групп в сообщении о ВО. Если какая-то группа признаков не изменилась и была исключена из сообщения о ВО, то соответствующее значение бита полевой ссылки этой группы устанавливается в нуль, иначе - в единицу.

На приемной стороне (в комплексе средств автоматизации (КСА) потребителей РЛИ) анализируется поле спецификации и выявляется наличие или присутствие в принятом сообщении о ВО всех оговоренных групп признаковой информации. При отсутствии какой-либо признаковой группы считается, что она не изменилась предыдущего сообщения по данному ВО и восстанавливается по предыдущим значениям.

Сжатие информации о скорости ВО. Аналогично, как в методе сжатия признаковой информации, в поле спецификации указывается наличие или присутствие составляющих скорости полета ВО.

На приемной стороне (в КСА потребителей РЛИ) анализируется поле спецификации, и при наличии координатной информации анализируется первичный байт составного координатного информационного элемента. При выявлении признака метода коррекции моделируемых трасс ВО производится коррекция соответствующих значений координат относительно экстраполированных значений предыдущего сообщения по данному ВО.

Переменная дискретность выдачи РЛИ. На приемной стороне (в КСА потребителей РЛИ) используется экстраполяция координат для обновления РЛИ по невыданным сообщениям о ВО.

Группирование ВО. Используется протокол, аналогичный как в существующих КСА центров управления воздушным движением для группирования ВО.

Селекция ВО. Снимается ВО с выдачи, если по ней потребитель получает РЛИ от других источников. На приемной стороне, в случае не обновления РЛИ по одному ВО в течении нескольких циклов выдачи, считается что источник снял данный ВО с выдачи.

Разработанный протокол формирования и обработки сообщений о ВО, позволяющий учитывать применение разработанных методов сжатия РЛИ, требует незначительного усовершенствования формата ASTERIX для представления модифицированных признаковых и координатных информационных элементов. Эффективность реали-

зации разработанных методов будет зависеть от способа формализации решаемых задач адаптивного формирования и выдачи сообщений о ВО.

Разработка метода представления знаний о задачах адаптивного формирования и выдачи сообщений о ВО

Использование продукционной модели представления знаний для формализации решающих правил обладает определенными преимуществами [1]. Продукции являются одними из наиболее популярных средств представления знаний в интеллектуальных системах [2]. Продукции, с одной стороны, близки к логическим моделям, что позволяет организовать на них эффективные процедуры вывода, а с другой стороны, более наглядно отражают знания, чем классические логические модели. В них отсутствуют жесткие ограничения, характерные для логических исчислений, что дает возможность изменять интерпретацию элементов продукции. Вместе с тем, продукционным моделям свойственны определенные недостатки:

- процесс вывода имеет низкую эффективность, так как при большом числе продукций значительная часть времени затрачивается на непроизводительную проверку условий применения правил;
- проверка непротиворечивости системы продукций становится весьма сложной из-за недетерминированности выбора выполняемой продукции;
- при задании модели предметной области в виде совокупности продукций нельзя быть уверенным в ее полноте ввиду отсутствия строгой теории продукционных систем.

Содержательная постановка задачи. Необходимо разработать метод представления знаний о задачах адаптивного формирования и выдачи сообщений о ВО на основе продукционной модели знаний, обеспечивающий полное и непротиворечивое представление знаний, а также оперативный и вывод на этих знаниях.

Решение задачи. При организации вывода в системе продукций возникает необходимость выбора той продукции, которая в данной ситуации должна быть активизирована. При централизованном управлении выполнением продукций решение о выборе продукции вырабатывает специальная система управления, а при децентрализованном определяется сложившейся ситуацией. Рассмотрим основные стратегии управления выполнением продукций [2].

Принцип «стопки книг». Он основан на идее, что наиболее часто используемая продукция является наиболее важной. Продукции как бы образуют «стопку», в которой порядок определяется накопленной частотой использования продукций. Вместе с тем, использование данного принципа для потока сообщений о ВО не обладающими свойствами стационарности изменения информационных элементов, не приведет к формированию устойчивой «стопки». В этом случае, процесс выбора продукций будет неэффективен, так как связан с частыми процедурами сортировки продукций по частоте их исполнения.

Принцип наиболее длинного условия. Он заключается в выборе той продукции, у которой стало истинным наиболее «длинное» условие выполнимости ядра. Этот принцип основан на том соображении, что частные правила, относящиеся к узкому классу ситуаций, важнее общих правил, относящихся к широкому классу ситуаций, так как первые учитывают больше информации о ситуации, чем вторые. Недостатком данного принципа является необходимость заранее упорядочить условия по вхождению друг в друга по отношению «частное-общее», поэтому его целесообразно применять лишь в тех случаях, когда знания хорошо структурированы привязкой к типовым ситуациям, на которых задано отношение типа «частное-общее».

Принцип «классной доски». При реализации данного принципа, выделяется специальное рабочее поле памяти - аналог классной доски, на которой мелом пишут объявления и стирают их при необходимости тряпкой. На этой «доске» параллельно выполняющиеся процессы находят информацию, инициирующую их запуск, на нее же они и выносят информацию о своей работе, которая может оказаться полезной для других процессов. Недостатком данного принципа является необходимость разработки специальных методов защиты от «порчи знаний» работающими продукциями.

Принцип приоритетного выбора. Он связан с введением статических или динамических приоритетов на продукции. Статические приоритеты могут формироваться априори на основании сведений о важности продукционных правил. Динамические приоритеты вырабатываются в процессе функционирования системы. Ограничением применения данного принципа при формировании и выдаче сообщений о ВО, является невозможность получения устойчивых приоритетов продукционных правил, так они напрямую зависят от изменений информационных элементов в сообщениях о ВО не обладающих стационарным характером.

Управление по именам. В этом случае задаются для имен продукции, входящих в некоторую систему, некоторой формальной грамматикой или другой процедурой, обеспечивающей сужение фронта выбора продукций. Однако при модификации системы продукций за счет введения новых правил, возникает необходимость согласования их имен с принятой формальной грамматикой в системе продукций и разработки специальных методов проверки корректности активизации данных правил.

Принцип метапродукций. Он основан на идее ввода в систему продукций специальных метапродукций, задачей которых является организация управления в системе продукций при возможности неоднозначного выбора продукции. Данный принцип наиболее полно удовлетворяет разработанной системе продукций, так как выполнение очередной продукции зависит от условия выполнения преды-

дущей.

В этом случае такой порядок управления выводом в системе продукций удобно представить в виде функциональной сети, представляющей собой ориентированный граф, в котором вершинам будут соответствовать отдельные продукционные правила, а дугам отношения следования, определяющие порядок выполнения продукций. В этом случае, для представления метапродукций необходимо использовать специальные вершины-разветвители, в которых будет определяться маршрут активизации продукций на функциональной сети.

Используя объединение принципа метапродукций для управления выводом в системе продукций и функциональной сети разработана интегрированная модель представления знаний о задачах адаптивного формирования и выдачи сообщений о ВО, представленная на рис.1. Штриховыми линиями выделены подсети, соответствующие сферам знаний: Si - сфера, которая описывает правила определения базовой совокупности методов сжатия и выдачи сообщений, S2 - сфера, которая описывает правила применения методов сжатия и выдачи РЛИ к сообщениям о ВО. Данные подсети функционируют асинхронно: подсеть S1 активизируется раз в 10 с, что соответствует циклу обновления РЛИ, и результатом ее вывода является активизация одного из отношений U1-D3, U2-D2, U3-D1, U3-P9, которое остается активным до следующего цикла активизации подсети S1. Подсеть S2 активизируется при формировании каждого сообщения о ВО для выдачи потребителю. На рис.1 используются следующие обозначения:

△ - вершины начальных условий, которые содержат множество Ni исходных данных для решающих правил определения базовой совокупности методов сжатия и выдачи сообщений о ВО и применения этих методов к сообщениям о ВО;

(Pi) - функциональная вершина соответствующая решающему правилу с именем Pi;

▽ - вершина-разветвитель, активизироваться может только один из выходов, согласно заданным условиям, которые описаны метапродукциями Ui;

(Ц) - целевая вершина, соответствующая результату управления информационным потоком сообщений о ВО: применение к отдельному сообщению о ВО метода сжатия или выдачи РЛИ для согласования производительности источника РЛИ с пропускной способностью канала ПД;

(Di) - вершина-ключ, работающая по логике элемента ИЛИ: если активизирован хотя бы один вход, то активизируется выход.

Обеспечить оперативный вывод на знаниях в такой модели в реальном масштабе времени удается за счет априорного ограничения набора продукций для их исполнения после выполнения очередной продукции. Такие ограничения описаны в вершинах-разветвителях и получены исходя из логики решения задач адаптивного формирования и выдачи сообщений о ВО. Условие в вершине U1 позволяет выбрать продукцию P2 для последующего исполнения если оцененное значение пропускной способности канала передачи данных (ПД) относительно сообщений о ВО, меньше производительности источника РЛИ при использовании полного формата сообщений, иначе рассогласования нет и решать задачу назначения методов сжатия и выдачи РЛИ каждому ВО нет необходимости, что соответствует цели управления информационным потоком сообщений о ВО. Данное условие соответствует метапродукции:

$$(Ul); M(C^{пер}, G^{полн}) \Rightarrow P2, \text{ иначе Ц.} \quad (1)$$

Условие в вершине U2 позволяет выбрать продукцию P4 для последующего исполнения если количество устраняемой избыточности в потоке РЛИ при использовании метода сжатия информации о скорости полета ВО, больше необходимого объема уменьшения количества информации в потоке РЛИ, иначе необходимо выполнить продукцию P3. Данное условие соответствует следующей метапродукции:

$$(U2); MR(D_p \cdot T, W_V \cdot m_v) \Rightarrow P4, \text{ иначе P3.} \quad (2)$$

Условие в вершине U3 позволяет выбрать продукцию P6 для последующего исполнения если количество устраняемой избыточности в потоке РЛИ при использовании метода сжатия координатной информации в сообщениях о ВО, больше необходимого объема уменьшения количества информации в потоке РЛИ, иначе необходимо выполнить продукцию P9. Данное условие соответствует следующей метапродукции:

$$(U3); MR(D_y, W_{xy} \cdot m_{xy}) \Rightarrow P6, \text{ иначе P9} \quad (3)$$

Условие в вершине U4 позволяет выбрать продукцию P10 для последующего исполнения, если метод переменной дискретности выдачи РЛИ не может быть применен к данному сообщению о ВО, иначе к этому сообщению не применяется больше никакой метод, так как оно исключено из выдачи потребителю на данном цикле обновления РЛИ, что соответствует целевой вершине. Данное условие соответствует следующей метапродукции:

$$(U4); \overline{P}(pd, j, h) \Rightarrow P10, \text{ иначе Ц} \quad (4)$$

Условие в вершине U5 позволяет выбрать продукцию P11 для последующего исполнения, если метод группирования ВО не может быть применен к данному сообщению о ВО, иначе к этому сообщению не применяется больше никакой метод, что соответствует целевой вершине. Данное условие соответствует следующей метапродукции:

$$(U5); \overline{P}(gr, j, h) \Rightarrow P11, \text{ иначе Ц} \quad (5)$$

Условие в вершине U6 позволяет выбрать продукцию P6 для последующего исполнения если

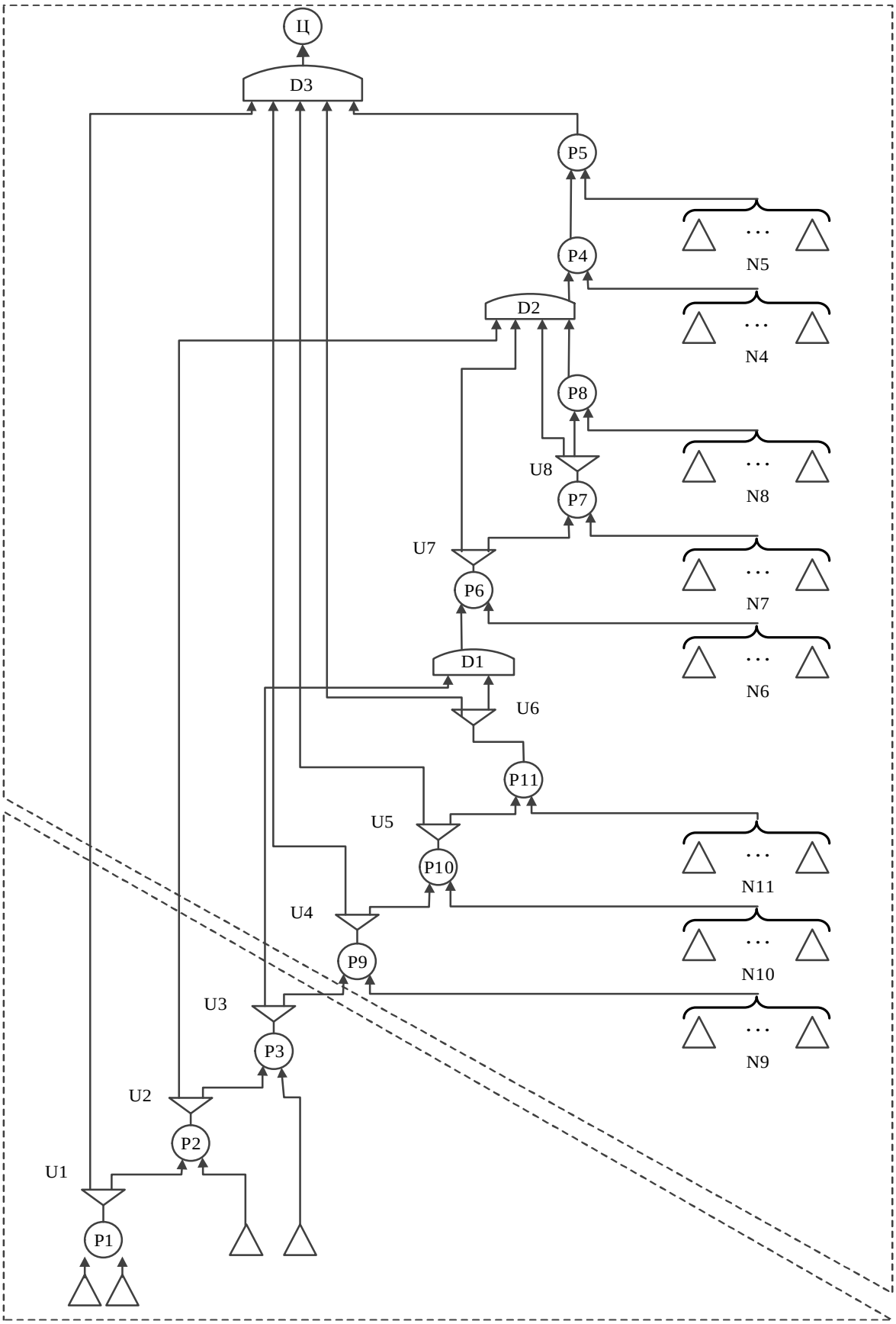


Рис. 1. Интегрированная модель представления знаний о задачах адаптивного формирования и выдачи сообщений о ВО

метод селекции ВО не может быть применен к данному сообщению о ВО, иначе к этому сообщению не применяется больше никакой метод, что соответствует целевой вершине. Данное условие соответствует следующей метапродукции:

$$(U6); \overline{P}(s, j, h) \Rightarrow P6, \text{ иначе Ц} \quad (6)$$

Условие в вершине U7 позволяет выбрать продукцию Р4 для сжатия информации о скорости ВО если метод переноса системы координат применен к сообщению о ВО, иначе продукцию Р7 для оценки возможности применения метода относительного кодирования координат в сообщении. Данное условие соответствует следующей метапродукции:

$$(U7); P(psk, j, h) \Rightarrow P4, \text{ иначе P7} \quad (7)$$

Условие в вершине U8 позволяет выбрать продукцию Р4 для сжатия информации о скорости во если метод относительного кодирования координат применен к сообщению о во, иначе продукцию Р8 для оценки возможности применения метода коррекции моделируемых трасс для сжатия координатной информации. Данное условие соответствует следующей метапродукции:

$$(U8); P(ok, j, h) \Rightarrow P4, \text{ иначе P8} \quad (8)$$

Рассмотрим состав начальных условий Ni для решающих правил определения базовой совокупности методов сжатия и выдачи сообщений о ВО и применения этих методов к сообщениям о ВО:

$N1 = \{\hat{C}^{пер}, G^{полн}\}$ - соответственно значения пропускной способности канала ПД относительно сообщений о ВО и производительности источника РЛИ при использовании полного формата сообщений;

$N2 = \{D_p, W_v, m_v\}$ - соответственно величина рассогласования между производительностью источника РЛИ и пропускной способностью канала ПД; количество устраняемой избыточности в сообщении о ВО при использовании метода сжатия информации о скорости полета ВО; количество ВО, к которым может быть применен метод сжатия информации о скорости полета во в сообщении, из числа выдаваемых данному потребителю;

$N3 = \{D_v, W_{xy}, m_{xy}\}$ - соответственно количество неустраняемого рассогласования производительности источника с пропускной способностью канала ПД в результате применения метода сжатия информации о скорости полета ВО; количество устраняемой избыточности в сообщении о ВО при использовании методов сжатия координатной информации в сообщении ВО; количество ВО, к которым может быть применен метод сжатия координатной информации в сообщении, из числа выдаваемых данному потребителю;

$N4 = \{pr_1, ..., \delta r_{\hat{e}}, PERV(j, h)\}$ - множество значений k групп качественных признаков в сообщении о ВО; признак новизны ВО для потребителя;

$$N5 = \{PERV(j, h), P(gr, j, h - l), P(s, j, h - l), P(pd, j, h - l), EX(j, h - l)\}$$

-соответственно признаки новизны ВО для потребителя; группирования ВО, селекции ВО, переменной дискретности выдачи или выдачи экстраполированных данных в предыдущем цикле обновления РЛИ;

$$N6 = \{WG(j, h), x_j, y_j, h_j, x_z, y_z, h_z, D_{max}\}$$

- соответственно признак вхождения j-го ВО в состав первичной группы; координаты j-го ВО и головного z-го ВО; максимальное расстояние, у которого размер кода не превышает одного байта;

$$N7 = \{V_{j,h}, V_{max}, PERV(j, h), P(gr, j, h - l), P(s, j, h - l), P(pd, j, h - 1)\}$$

-соответственно значения скорости j-го ВО; максимальная скорость полета ВО, при которой приращение координат за период обновления РЛИ не превысит значения, имеющего однобайтовый размер кода; признаки новизны j-го ВО для потребителя, а также значения признаков группирования ВО, селекции ВО, переменной дискретности выдачи в предыдущем цикле обновления РЛИ;

$$N8 = \{MAN(j, Q, h), MAN(j, V, h), MAN(j, H, h), PERV(j, h), P(gr, j, h - l), P(s, j, h - l), P(pd, j, h - l)\}$$

- соответственно значения признаков маневра j-го ВО по курсу, скорости и высоте, признака новизны ВО для потребителя, а также значения признаков группирования ВО, селекции ВО, переменной дискретности выдачи в предыдущем цикле обновления РЛИ;

$$N9 = \{s^{ý(h)}_{j(xy)}, s^{äîï(h)}_{j(xy)}, s^{ý(h)}_{j(h)}, s^{äîï(h)}_{j(h)}, PERV(j, h), rang(j), K_{pot}\}$$

- соответственно с.к.о. экстраполяции координат и высоты j-го ВО и допустимые значения с.к.о. координат и высоты j-го ВО; значение признака новизны j-го ВО для потребителя; значение ранга j-го ВО и достаточное количество сообщений о ВО, к которым необходимо применить методы выдачи с потерей качества РЛИ;

$N10 = \{WG(j, h)\}$ - значение признака вхождения j-го ВО в первичную группу;

$N11 = \{WG(j, h), DUB(j)\}$ - соответственно значение признака вхождения j-го ВО в первичную группу и признака получения потребителем информации по j-тому ВО от других источников.

Разработанная интегрированная модель представления знаний о задачах адаптивного формирования и выдачи сообщений о ВО позволяет оценить непротиворечивость и полноту представления знаний. Так в ряде работ показано, что для сетевых моделей представления знаний имеется возможность выявления некорректностей знаний, используя информацию о структуре графа модели. [3,5,6].

	N1	N2	N3	N4	N5	N6	N7	N8	N9	N10	N11	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	U1	U2	U3	U4	U5	U6	U7	U8	D1	D2	D3	Ц
N1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N3	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
N11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
P1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
P2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
P3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
P4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
P6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
P7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
P8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
P9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
P10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
U1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
U2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
U3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
U4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0
U5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0
U6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
U7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
U8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
D1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
D2	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
D3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Ц	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Рис.2. Матрица смежности графа интегрированной модели представления знаний

Анализ полноты графа предусматривает проверку возможности достижения конечной (целевой) вершины при любом логически истинном наборе начальных условий. Для каждой вершины графа необходимо определить множество вершин, которые являются достижимыми, и необходимые условия для ее достижения и следствий (целей, для которых данная вершина является одним из условий достижения). Несоблюдение перечисленных требований приводит к появлению вершин, неопределенных по условию достижения:

- «изолированные» вершины - при отсутствии необходимых и достаточных условий их достижения;

- «тупиковые» вершины - при отсутствии следствий достижения цели;

- «висящие» вершины - при отсутствии и условий и следствий достижения вершин.

Некорректность такого типа позволяет выявить матрица смежности анализируемого графа сетевой модели, представленная на рис.2. При этом используют следующие правила анализа вершин:

1. если все элементы строки и столбца, которые соответствуют анализируемой вершине, имеют значение 0, то такая вершина является «изолированной»;

2. если все элементы строки, которые соответствуют анализируемой вершине, имеют значение 0, то такая вершина является «тупиковой»;

3. если все элементы столбца, которые соответствуют анализируемой вершине, имеют значение 0, то такая вершина является «висящей».

Представленные правила анализа графа сетевой модели для определения ее полноты обусловлены свойствами матрицы смежности. Следует отметить, что анализ целевых и начальных вершин графа должен быть направлен только на выявление «изолированных» вершин. Оценка полноты интегрированной модели (рис.1) на основе указан-

ных правил анализа ее матрицы смежности (рис.2) позволяет сделать вывод о корректности графа разработанной модели с точки зрения полноты.

Проведем оценку непротиворечивости графа разработанной сетевой модели. В работах [3] показано, что из свойств отношений между вершинами сетевой модели следует, что наличие контуров на графе модели свидетельствует о противоречивости этих отношений при рассмотрении порядка достижения целевых вершин. Под контуром понимается путь на графе, начальная вершина которого совпадает с конечной.

Важным этапом в устранении данного вида противоречий является их локализация, которая представляет собой выявление и выделение множества противоречивых элементов знаний.

Существует ряд методов поиска контуров на ориентированном графе [4, 5]. Вместе с тем, в работе [7] доказано, что достаточным условием отсутствия контуров в сетевом представлении знаний является отсутствие дуг на графе, исходящих из вершин с большим уровнем иерархии и входящих в вершины с меньшим уровнем иерархии. Уровень иерархии вершины при этом определяется ее максимальным рангом в графе, т.е. максимальным количеством дуг на пути от начальных вершин до этой вершины. Тогда для графа на рис.1 можно определить уровни иерархии (УИ) вершин, представленные в таблице 1.

Таблица 1

Уровни иерархии вершин графа разработанной сетевой модели

Индекс вершины	N1-N9	P1	P2	P3	P4	P5	P6	P7	P8	P9	D1	D2	Ц
Уровень иерархии	0	1	2	3	4	5	6	8	9	11	7	10	12

Таким образом, используя матрицу смежности (рис.2) и информацию о уровнях иерархии вершин (табл.1) можно определить отсутствие контуров на графе сетевой модели (рис.2), что обеспечивает непротиворечивость графа этой модели представления знаний. Проверку графа сетевой модели на полноту и непротиворечивость необходимо проводить не только на этапе создания сетевой модели, но и после каждой ее корректировки.

Таким образом, формализация процесса адаптивного управления с помощью комбинированного представления знаний моделями продукций и функциональной сети позволяет производить оперативную модификацию разработанного метода путем добавления/исключения или изменения методов адаптивного управления и взаимосвязей между ними.

Выводы

1. Разработанный протокол формирования и обработки адаптивной структуры сообщений о воздушных объектах, позволяющий учитывать применение разработанных методов сжатия радиолокационной информации, позволяет усовершенствовать формат ASTERIX для представления модифицированных признаковых и координатных информационных элементов. Для этого в поле спецификации необходимо предусмотреть полевые ссылки на сформированные признаковые группы и ввести в состав первичной части составного поля координатного информационного элемента признаки применения методов сжатия координатной информации.

2. Для описания решающих правил целесообразно использовалась интегрированное представление знаний с помощью объединения моделей продукций и функциональной сети, что позволяет производить оценку полноты и непротиворечивости представления знаний из анализа графа сети и производить оперативную модификацию разработанного метода формирования и выдачи сообщений о воздушных объектах от источников радиолокационной информации в региональном центре управления воздушным движением.

Литература

1. Поспелов Д.А. Ситуационное управление. Теория и практика. - М.: Наука, 1986. - 288 с. **2.** Искусственный интеллект. - В 3-х кн. Кн. 2. Модели и методы: Справочник / Под ред: Д.А. Поспелова. - М.: Радио и связь, 1990. - 304 с. **3. Герасимов Б.М.** и др. Человеко-машинные системы принятия решений с элементами искусственного интеллекта.- К.: Наукова думка, 1993.- 184 с. **4. Гладун Р.П.** Планирование решений. - К.: Наукова думка,1997. -232 с. **5. Двухглавов Д.Э**. Методики контроля корректности формализованных описаний задач принятия решений в открытых экспертных системах: Дис. ... канд. Техн. наук: 20.02.12. - Харьков: ХВУ, 1999. - 216 с. **6. Карпов С.И.** Методики синтеза вариантов решений в открытой экспертной системе: Дис. ... канд. Техн. наук: 20.02.12. - Харьков: ХВУ, 1999. - 203 с. **7. Низиенко Б.И.** Разработка методов и средств формализации, пополнения и контроля корректности знаний для открытой экспертной системы реального времени командного пункта: Дис. ... канд. Техн. наук: 20.02.12. - Х.: ХВУ, 1995. - 204 с.

РОЗРОБКА МЕТОДУ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ ПОТОКОМ ПОВІДОМЛЕНЬ ПРО ПОВІТРЯНІ ОБ'ЄКТИ ВІД ДЖЕРЕЛ РАДІОЛОКАЦІЙНОЇ ІНФОРМАЦІЇ В АСУ РЕГІОНАЛЬНИХ ЦЕНТРІВ УПРАВЛІННЯ ПОВІТРЯНИМ РУХОМ

***Андрій Станіславович Могілатенко*[1]**
***Юрій Олександрович Данилов*[2]**
***Максим Анатолійович Павленко* (д-р техн. наук, доцент)[3]**

[1]*Військова частина А0593, Нікополь, Україна*
[2]*Командування Повітряних Сил Збройних Сил України, Вінниця, Україна*
[3]*Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна*

Використання адаптивного підходу до управління інформаційним потоком повідомлень про повітряні об'єкти від джерел радіолокаційної інформації передбачає вирішення наступних завдань адаптації: завдання розпізнавання ситуацій застосування методів стиснення і видачі повідомлень про повітряні об'єкти для інформаційного потоку радіолокаційної інформації; задача розподілу методів стиснення і видачі радіолокаційної інформації за повідомленнями про повітряні об'єкти в загальному інформаційному потоці; задача безпосередньої зміни структури повідомлень про повітряні об'єкти. Для вирішення завдання зміни структури повідомлень про повітряний потік необхідно розробити протокол формування та обробки повідомлень про повітряні об'єкти зі змінною структурою. При цьому вирішальні правила повинні розроблятися з використанням інтелектуальних інформаційних технологій.

Ключові слова: *метод, управління, стиснення*

DEVELOPMENT OF THE METHOD OF MANAGEMENT OF THE INFORMATION FLOW OF MESSAGES ABOUT AIR OBJECTS FROM SOURCES OF RADAR INFORMATION IN AUTOMATED CONTROL SYSTEMS OF REGIONAL AIR TRAFFIC CONTROL CENTERS

***Andrey S. Mohilatenko*[1]**
***Yuriy A. Danilov*[2]**
***Maksim A. Pavlenko* (Doctor of Technical Sciences, Associate Professor)[3]**

[1]*Military unit A0593, Nikopol, Ukraine*
[2]*Command of the Air Forces of the Armed Forces of Ukraine, Vinnytsia, Ukraine*
[3]*Kharkiv national University of Air Force named after Ivan Kozhedub, Kharkiv, Ukraine*

The use of an adaptive approach to managing the information flow of messages about an airborne object from sources of radar information provides for the solution of the following adaptation tasks: the task of recognizing the situations of applying compression methods and issuing messages about an air object for the information stream of radar information; The task of distributing methods for compressing and issuing radar information from reports on an airborne object in the general information flow; The task of directly changing the structure of messages about an air facility. To solve the problem of changing the structure of messages about the air flow, it is necessary to develop a protocol for the formation and processing of messages about an air object with a variable structure. At the same time, decisive rules should be developed using intelligent information technologies.

Keywords: *method, control, compression*

References

1. Pospelov D.A. Situational management. Theory and practice. [*Situatsionnoye upravleniye. Teoriya i praktika*]. - Moscow: Nauka, 1986. - 288 p. **2.** Artificial intelligence. - In 3 books. Book 2. Models and methods: Handbook [*Modeli i metody. Spravochnik*] / Ed .: D.A. Pospelov. - Moscow .: Radio and Communication, 1990. - 304 p. **3. Gerasimov B.M.** and others. Man-machine decision-making systems with elements of artificial intelligence. [*Chelove-komashinnyye sistemy prinyatiya resheniy s elementami iskustvennogo intellekta*] - K .: Naukova Dumka,, 1993.- 184 p. **4. Gladun R.P.** Planning solutions. [*Planirovaniye resheniy*] - Kiev .: Naukova Dumka, 1997. -232 p. **5. Dvuhglavov D.E.** Methods for controlling the correctness of formalized descriptions of decision-making tasks in open expert systems [*Metodiki kontrolya korrektnosti formal-izovannykh opisaniy zadach prinyatiya resheniy v otkrytykh ekspertnykh sistemakh*]: Dis. ... Cand. Techn. Sciences: 20.02.12. - Kharkiv: KMU, 1999. - 216 p. **6. Karpov S.I.** Methods of synthesis of solutions in an open expert system [*Metodiki sinteza variantov resheniy v otkrytykh ekspertnykh sistemakh*]: Dis. ... Cand. Techn. Sciences: 20.02.12. - Kharkiv: KMU, 1999. - 203 p. **7. Nizienko B.I.** Development of methods and means of formalization, replenishment and control of the correctness of knowledge for an open expert system of real-time command posts [*Raz-rabotka metodov I sredstv formalizatsii, popolneniya i kontrolya korrektnosti znaniy dlya otkrytoy ekspertnoy sistemy real'nogo vremeni komandnogo punkta*]: Dis. ... Cand. Techn. Sciences: 20.02.12. - Kharkiv. .: KMU, 1995. - 204 p.

УДК 335.45

Мурасов Рустам Камілович *(канд. техн. наук)*
Кононенко Сергій Миколайович
Мельник Ярослав В'ячеславович

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ЗАСТОСУВАННЯ ТЕОРІЇ ПЕРКОЛЯЦІЇ ДЛЯ ОЦІНЮВАННЯ СТІЙКОСТІ ГЕТЕРОГЕННИХ МЕРЕЖ В УМОВАХ КІБЕРАТАК

В сучасних умовах функціонування гетерогенних мереж, виникає необхідність в оцінюванні їх надійності та оптимізації. Оскільки на даний час зростання перепускної спроможності мереж вже досягло ліміту, розглядається можливість підвищення стійкості мереж шляхом оптимізації їх структури. У роботі розглянуто застосування теорії перколяції для оцінювання стійкості гетерогенних мереж. В роботах інших авторів вже розглядається успішне застосування теорії перколяції в областях фізики, хімії. Оскільки сучасні гетерогенні мережі не структуровані та не мають однорідної структури та варіантів з'єднання то теорія перколяції дозволяє описати цю мережу. Також буде знайдений «перколяційний поріг» - мінімальну кількість з'єднань та вузлів при якої мережа зберігає здатність функціонувати. При визначенні значення «коефіцієнт надійності гетерогенної мережі» можливо буде моделювати та будувати різні варіанти мереж в залежності від його значення. Це дозволяє оцінювати стійкість мережі на етапі проектування та оптимізувати існуючі до заданого рівня. Дозволить виявити слабкі місця для потенційних DDoS атак.

Ключові слова: *перколяція; гетерогенні мережі; кіберебезпека; стійкість комп'ютерної мережі; DDoS атаки .*

Вступ

В умовах сучасної гібридної війни, бойові дії перемістились і у інформаційній простір, оскільки вже 90% інформаційного простору знаходиться у кіберпросторі. Тому частіше об'єктами атак стають сервера, сайти. На всіх рівнях від програмного до технічного постійно ведеться пошук рішення задачі по підвищенню стійкості гетерогенних мереж. На даний час най поширеним способом кібератак є DDoS атаки тому виникає завдання створення ефективної протидії та забезпечення стабільної роботи мережі в умовах кебернебезпеки.

Постановка проблеми. В рамках даної статті розглядається можливість та ефективність застосування теорії перколяції для визначення стійкості гетерогенної мережі та її оптимізації

Аналіз останніх досліджень і публікацій. Задачі забезпечення стійкості мереж вже розглядались у роботах [1, 2, 3], але вони мали вузькоспеціалізовані напрямки і не можуть бути застосовані як методи для більшості гетерогенних мереж.

Метою статті є дослідження які проводилося в рамках НДР шифр "Стійкість ГМ". У ході дослідження використовувалися такі методи: теорія перколяції, теорія графів, теорія математичного аналізу, теорія складних систем, теорія інформаційних систем.

Виклад основного матеріалу дослідження

Перколяція це наука про впорядковані структури об'єктів в невпорядкованих середах. Це надає широкі можливості по дослідженню та створенню нових форм та методів побудови комп'ютерних мереж в структурі глобальної мережі.

Наприклад впорядкована структура – це визначені вузли та з'єднання проміж ними в мережі Інтернет які забезпечують функціонування деякої електронної системи, як варіант для проведення розподілених командно-штабних навчань з використанням засобів імітаційного моделювання.

Надійність гетерогенної мережі – це здатність мережі виконувати свої функції при деструктивній дії на неї. Ці дії можуть бути: DDoS атака, фізичне видалення вузлів мережі, велике навантаження на ділянки мережі.

Результати, наведені в [1], цілком придатні для моделювання атак на таку глобальну мережу, як Інтернет. Відомо, що вузли цієї мережі зв'язуються лініями зв'язку з різною пропускною здатністю.

Окремі сегменти Інтернет з'єднані в точки обміну трафіком, існують опорні канали. Можна констатувати, що сьогодні саме існування нашої цивілізації вже багато в чому залежить від зв'язності цієї мережі. Моделювання атак, т. е. розривів окремих зв'язків або видалення окремих, як показують розрахунки, далеко не всіх вузлів може порушити таку зв'язність і дають великі шанси терористам. Знаходження «слабких» ділянок глобальної мережі, проектування

резервних вузлів і каналів вимагають точних розрахунків на базі теорії перколяції.

Слід зазначити, що вище весь час мова йшли вирізання (вимикання, ... руйнування) вузлів з ймовірністю P випадковим чином. У той же час можливо вирізати вузли, як в стандартній перколяційний задачі, так в інших типах складних мереж, цілеспрямованим чином, вибираючи такі вузли, під час вирізання яких мережа руйнується максимально швидко. В мережі Інтернет таке спрямоване виведення з ладу вузлів (серверів) називається «запланована атака». Під виведенням з ладу вузлів розуміється виведення сервера з його працездатного стану, наприклад шляхом DDoS-атаки або атаки на переповнення буфера. При цьому виведення з ладу близько 1% цілеспрямованих вузлів зменшує продуктивність мережі Інтернет в два рази.

Нажаль не існує єдиної математичної методики розрахунку «перколяційного кластеру» - порогового значення при якому мережа стрибкоподібно змінює свій стан. В більшості випадків такі значення обчислюються шляхом моделювання.

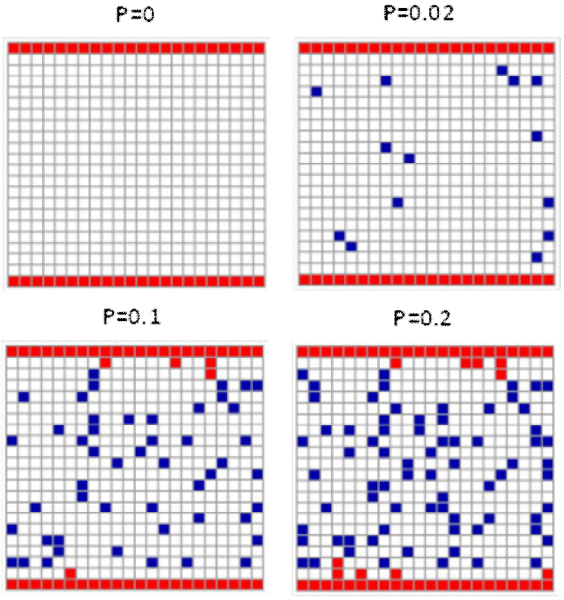
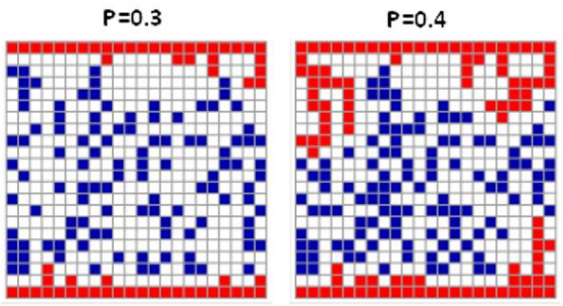


Рис.1 Моделювання створення перколяційного кластеру на прикладу квадратної решітки, при збільшенні коефіцієнтів зв'язків



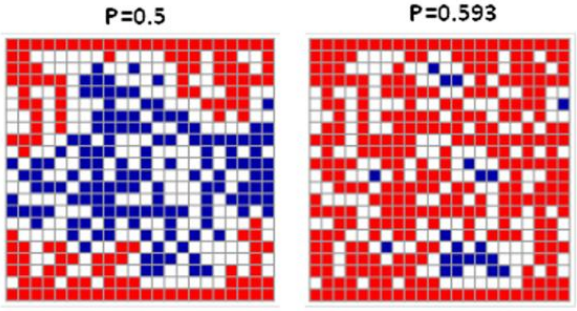


Рис.2 Моделювання створення перколяційного кластеру на прикладу квадратної решітки, при збільшенні коефіцієнтів зв'язків (4 схеми)

Як ми можемо спостерігати на Рисунку 2, при збільшенні коефіцієнтів зв'язків перколяційний кластер для однорідної квадратної решітки створюється при коефіцієнті заповнення **P=0,593**.

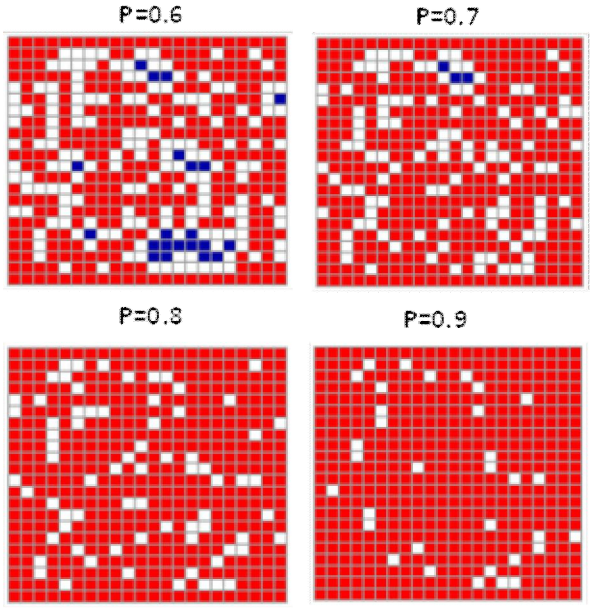


Рис.3 Моделювання створення перколяційного кластеру на прикладу квадратної решітки, при збільшенні коефіцієнтів зв'язків

Таким чином було проведено моделювання та отримано відображення процесу створення перколяційного кластеру для варіанту з'єднання - квадратна решітка.

Для інших варіантів з'єднання необхідно здійснювати окреме моделювання та відповідно окремий математичний розрахунок. Також слід розуміти що у цьому випадку коефіцієнт перколяції буде мати зовсім інше значення. Крім того варіанти з'єднання можуть мати ще й різну структуру що у свою чергу призведе до виникнення ще більш складеної задачі перколяції між принципово різними структурами.

Нижче наведено графік стрибкоподібного зміну стани системи при створенні або знищенні перколяційного кластеру.

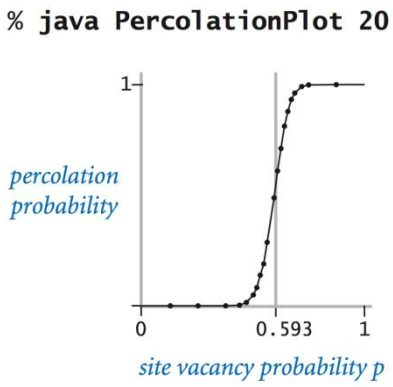
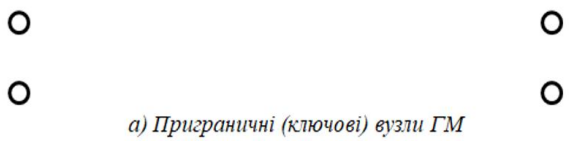


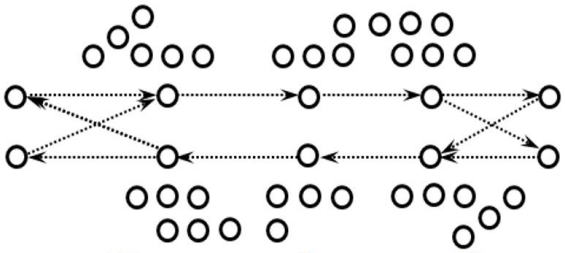
Рис.4 Графік стрибкоподібного зміну стану системи при створення або знищенні перколяційного кластеру (спрощений)

Рис.5 Алгоритм застосування теорії перколяції для оптимізації гетерогенної мережі

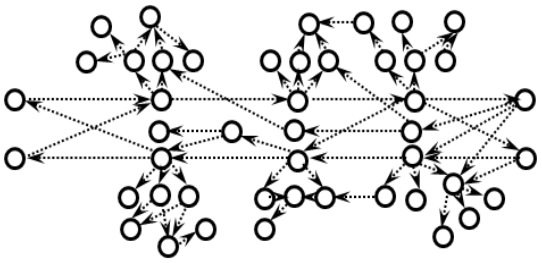


а) Пригранічні (ключові) вузли ГМ

б) Маршрути з ключових вузлів одна в одну



в) Працюючи вузли підсистеми провайдера



Кінцева структура ГМ

Рис.6 Оптимізація структури ГМ

Застосовуючи теорію перколяції для аналізу та визначення стійкості гетерогенної мережі (Рис.5,6), можливо добитися оптимальної структури с заданим коефіцієнтом перколяції.

Висновки й перспективи подальших досліджень

У результаті аналізу та тестового математичного моделювання зв'язків мережі, отримано підтвердження ефективності застосування теорії перколяції для оцінювання стійкості гетерогенної мережі.

Отримані результати доцільно використовувати для удосконалення існуючих та розробки нових методик побудови перспективних інформаційно-телекомунікаційних мереж для забезпечення інформаційних процесів із заданим рівнем стійкості в умовах кібератак.

Література

1. Тарасевич Ю.Ю. Перколяция: Теория, приложения алгоритмы. Изд.2.–М. URSS, 2012, - 112с. **2.** What is Percolation? http://www.statslab.cam.ac.uk/~grg/papers/perc/chap1.pdf **3. Radicchio F.** Percolation in real interdependent networks. Cornell University, 2015. http://homes.soic.indiana.edu/filiradi/Mypapers/percolation_arxiv_rev.pdf **4. Karrer**, M. E. J. Newman, and L. Zdeborova, Phys. Rev. Lett. 113, 208702, 2014. **5. F. Krzakala**, C. Moore, E. Mossel, J. Neeman, A. Sly, L. Zdeborova, and P. Zhang, Proc. Natl. Acad. Sci. USA 110, 20935, 2013.

ПРИМЕНЕНИЕ ТЕОРИИ ПЕРКОЛЯЦИИ ДЛЯ ОЦЕНКИ УСТОЙЧИВОСТИ ГЕТЕРОГЕННОЙ СЕТИ В УСЛОВИЯХ КИБЕРАТАК

***Мурасов Рустам Камилович** (канд. техн. наук)*
Кононенко Сергей Николаевич
Мельник Ярослав Вячеславович

Национальный университет обороны Украины имени Ивана Черняховського, Киев, Украина

В современных условиях функционирования гетерогенных сетей, возникает необходимость в оценке их надежности и оптимизации. Поскольку в настоящее время рост пропускной способности сетей уже достиг лимита, рассматривается возможность повышения устойчивости сетей путем оптимизации их структуры. В работе рассмотрено применение теории перколяции для оценки устойчивости гетерогенных сетей. В работах других авторов уже рассматривается успешное применение теории перколяции в областях физики, химии и других наук. Поскольку современные гетерогенные сети не структурированы и не имеют однородной структуры и вариантов соединения то теория перколяции позволяет описать эту сеть. Также будет найден «перколяционные порог» - минимальное количество соединений и узлов при которой сеть сохраняет способность функционировать. При определении значения «коэффициент надежности гетерогенной сети» можно будет моделировать и строить различные варианты сетей в зависимости от его значения. Это позволяет оценивать устойчивость сети на этапе проектирования и оптимизировать существующие сети до заданного уровня, а также позволит выявить слабые места для потенциальных DDoS атак.

***Ключевые слова:** перколяции; гетерогенные сети; кибербезопасность; устойчивость компьютерной сети; DDoS атаки.*

APPLICATION OF THE PERCOLATION THEORY FOR ASSESSING THE STABILITY OF HETEROGENEOUS NETWORKS UNDER CYBER ATTACK CONDITIONS

***Rustam K. Murasov** (Philosophy Doctor of Technical Sciences, Chief of the Science Laboratory)*
***Serhii M. Kononenko** (Chief of Simulation Centre)*
Yaroslav V. Melnyk (Senior Researcher of Simulation Centre)

National Defense University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine

In today's heterogeneous networks, there is a need to assess their reliability and optimization. Since the growth of network capacity has already reached the limit, the possibility of increasing the stability of networks by optimizing their structure is being considered. In this paper, the application of percolation theory to the stability of heterogeneous networks is considered. In the works of other authors, the successful application of percolation theory in the fields of physics, chemistry, and other sciences is already being considered. Since modern heterogeneous networks are not structured and do not have a homogeneous structure and connection options, the percolation theory makes it possible to describe this network. Also, the "percolation threshold" will be found - the minimum number of connections and nodes at which the network remains able to function. When determining the value of the "reliability factor of a heterogeneous network", it will be possible to model and build various variants of networks, depending on its value. This allows you to assess the stability of the network at the design stage and optimize existing networks to a specified level, and also to identify weaknesses for potential DDoS attacks.

***Key words:** percolation; Heterogeneous networks; Cyber Defense; The stability of the computer network; DDoS attack.*

References

1. Tarasevych Y.Y. Percolation: Theory, Applications, Algorithms. Edition 2. – M. URSS, 2012, 112 p. **2.** What is Percolation? http://www.statslab.cam.ac.uk/~grg/papers perc/ chap1.pdf**__3. Radicchio F.** Percolation in real interdependent networks. http://www.nature.com/nphys/ journal/v11/n7/full/nphys3374.html

4. B. Karrer, M. E. J. Newman, and L. Zdeborova, Phys. Rev. Lett. 113, 208702, 2014. **5. F. Krzakala**, C. Moore, E. Mossel, J. Neeman, A. Sly, L. Zdeborova, and P. Zhang, Proc. Natl. Acad. Sci. USA 110, 20935, 2013.

УДК 004.056.57

Вадим Іванович Пеньков
Роман Михайлович Штонда
Олександр Миколайович Гук
Ірина Робертівна Мальцева
Юлія Олександрівна Черниш

Військовий інститут телекомунікацій та інформатизації, Київ, Україна

МЕТОДИ ТА ЗАСОБИ ПРОТИДІЇ ШКІДЛИВОМУ ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННЮ

Інформаційні технології визначають процеси передачі, зберігання та обробки інформації, а також її використання в певних цілях. Ці процеси повинні бути швидкими, найменш витратними, максимально корисними, зручними і автоматизованими. З цієї причини основною тенденцією розвитку інформаційних технологій є їх подання в цифровому вигляді, перехід до цифрових інформаційно-телекомунікаційних баз, заснованим на цифровій взаємодії комп'ютерів, розроблених з найрізноманітнішими функціональними алгоритмами. Впровадження персональних комп'ютерів в інформаційну сферу й застосування телекомунікаційних засобів зв'язку визначили новий етап розвитку інформаційних технологій.

Розвиток Інтернету змінив ставлення до проблем безпеки, піднявши питання про захищеність локальних і глобальних комп'ютерних мереж. Ще донедавна ці проблеми не були актуальними. Розробники перших комп'ютерних мереж в першу чергу прагнули збільшити швидкість і надійність передачі даних, часом досягаючи бажаного результату на шкоду безпеці.

Збільшення швидкості передачі інформації, обсягів і значимості оброблюваних в обчислювальних мережах даних відкриває перед кіберзлочинцями все більш широкі можливості. Поширення по всьому світу шкідливого програмного забезпечення займає лічені дні або навіть години. Сотні мегабайт оперативної пам'яті дозволяють виконувати практично будь-які дії непомітно для користувача. Спектр можливих цілей, таких як паролі, карткові рахунки, ресурси віддалених комп'ютерів представляє величезне поле для діяльності.

Ключові слова: *шкідливе програмне забезпечення, антивірусні програми, комп'ютерний вірус, комп'ютерна система, комп'ютерна мережа.*

Вступ

Шкідливі програми і боротьба з наслідками їх діяльності протягом останнього десятиріччя є однією з найсерйозніших проблем для всіх, хто працює за комп'ютером, від IT-директорів до домашніх користувачів. Постійне оновлення антивірусних програмних засобів – невід'ємний атрибут будь-якої корпоративної мережі, серверів Інтернет-провайдерів і значної частини особистих комп'ютерів. Останнім часом користувачі Інтернет все частіше відчувають потребу в отриманні подібних засобів або безпосередньо у складі операційних систем і серверних продуктів, або у вигляді додаткових послуг від постачальників зазначених категорій програмних засобів.

Постановка проблеми. За створення, використання і розповсюдження шкідливих програм передбачена відповідальність, у тому числі і кримінальна, в законодавстві багатьох країн світу.

У Кримінальному Кодексі України термін "шкідливий програмний засіб" детально не визначений. Але попри це Стаття 361-1 КК України передбачає покарання за "Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку."

Критерії, за якими програмні продукти можуть бути віднесені до категорії "шкідливих програмних засобів" досі ніде чітко не обумовлені. Відповідно, для того, щоб твердження про шкідливість програмного засобу мало юридичну силу, необхідно провести програмно-технічну експертизу з дотриманням всіх встановлених чинним законодавством формальностей.

Аналіз останніх досліджень і публікацій. Проблемам виявлення шкідливих програмних засобів та захисту від них присвячено ряд робіт, серед яких треба виділити праці Безрукова М. [1], Гульєва І. [2], Козлова Д.А. [3], Собейкіса В.Г. [4], Шаньгіна В. [5] та інших. В цих працях здебільшого розкриваються напрямки, методи та засоби протидії шкідливим програмам.

Метою статті є визначення методів та засобів захисту комп'ютерних систем від

шкідливих програмних засобів.

Виклад основного матеріалу дослідження

В даний час в теорії і практиці інформаційної безпеки склалися два принципово різних напрямки реалізації способів протидії шкідливим програмам.

Перший напрямок заснований на концепції структурно незалежних механізмів захисту інформації і припускає незалежність інформаційних процесів, і процесів протидії таким програмам. В цьому напрямку засоби протидії шкідливим програмам та програмному забезпеченню захищених інформаційних систем проектуються і розробляються незалежно один від одного, причому засоби протидії шкідливим програмам придані до вже розроблених програмних засобів. Особливістю механізму протидії в цьому випадку є те, що функції виявлення шкідливих програм реалізуються шляхом періодичного контролю цілісності обчислювального середовища захищених інформаційних систем з метою реєстрації несанкціонованих змін, викликаних шкідливими програмами.

Другий напрямок заснований на концепції структурно-залежних механізмів захисту інформації і передбачає залежність цих процесів. Згідно з цим напрямом реалізується дворівнева система ідентифікації впливів шкідливих програм: ідентифікація факту впливу та ідентифікація слідів впливу. У свою чергу, ідентифікація факту впливу шкідливої програми представляється дворівневим механізмом контролю процесів функціонування захищеної інформаційної системи, реєструючи некоректну поведінку її програмних засобів:

шляхом порівняння поточних результатів виконання функцій обробки інформації та функцій контролю, отриманих в динаміці функціонування програмних засобів;

шляхом виконання операцій порівняння поточних параметрів обчислювального процесу в захищеній інформаційній системі із заздалегідь відомими еталонними величинами.

Особливістю такої сукупності засобів контролю є те, що кожен такий засіб окремо має обмежені контролюючими характеристиками шкідливі функції, так як може охопити лише деякі, в основному неявні, ознаки та прояви шкідливих програм. Для правильного прийняття рішення проводиться аналіз некоректного функціонування програмних засобів захищеної інформаційної системи. В результаті формуються ідентифікації фактів впливу значущих ознак такого функціонування (трасологія впливу). При цьому аналізується послідовність всіх контрольних точок і викликів елементів програмних засобів відповідно до ієрархії їх побудови, з метою отримання інформації про час, місце та умови прояву впливу шкідливої програми та наслідків такого впливу.

Однак, у більшості випадків, наявність встановленої антивірусної програми, може виявитися недостатнім для повноцінного захисту. Як показано на рис. 1 один антивірусний засіб не завжди може гарантувати стовідсотковий захист від шкідливих програм [6].

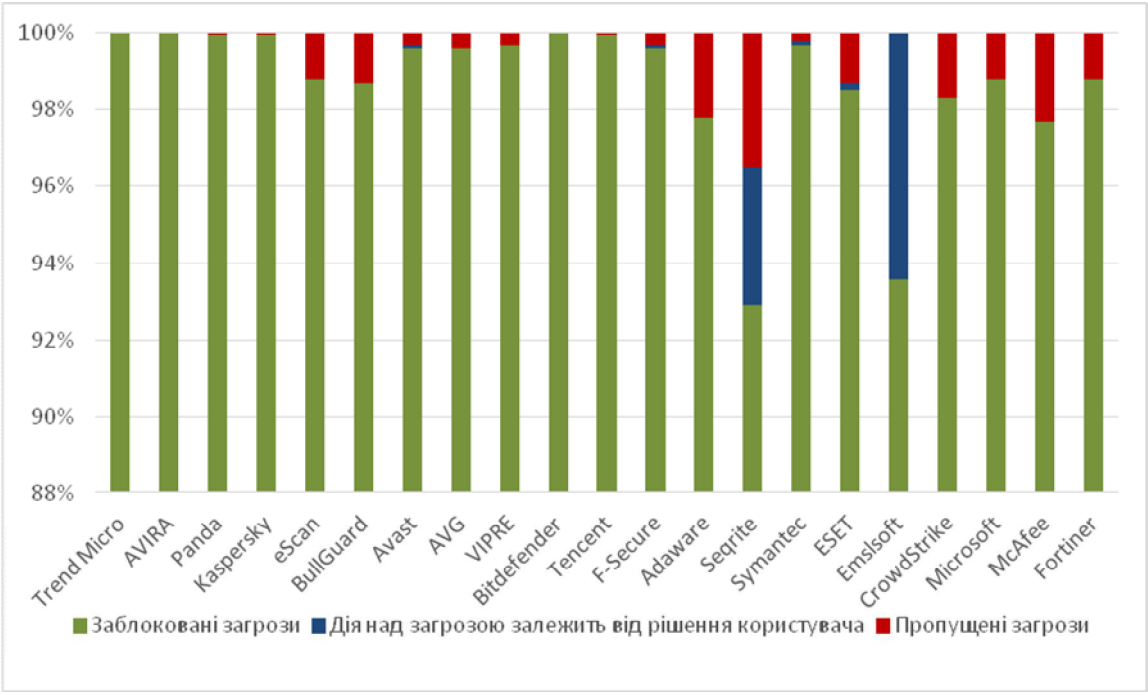


Рис. 1. Тест антивірусних засобів на захист від шкідливих програм

Тому в більшості випадків потрібно використовувати додаткові методи та способи.

Зазвичай через неправильне використання антивірусних програм, ігнорування порад щодо їх встановлення та самої роботи виробника антивірусних програм, методи та способи захисту можна розділити на три типи: правові, організаційні та технічні.

Правові методи зводяться до встановлення відповідальності за створення і поширення шкідливих програм, і заподіяння збитку. Слід зазначити, що довести авторство і умисність створення таких програм досить важко.

Організаційний захист полягає у виробленні та неухильному здійсненні заходів, спрямованих на попередження проникнення шкідливих програм в інформаційні системи, виявлення зараження, нейтралізацію негативного впливу і ліквідацію наслідків.

Технічні методи спрямовані на зміни в комп'ютерній системі, і полягають у використанні додаткових засобів захисту, які розширюють і доповнюють можливості антивірусних програм.

Такими засобами захисту можуть бути:

брандмауери-програми, що захищають від атак по мережі;

засоби боротьби зі спамом;

виправлення, що усувають "дірки" в операційній системі, через які можуть проникати віруси;

інші різні спеціальні утиліти для дослідження системи.

Крім того, можуть використовуватися спеціальні пристрої, що перешкоджають проникненню шкідливих програм на комп'ютер, пристрої резервного копіювання даних і так далі.

Технології, що використовуються в антивірусних програмах, можна розбити на дві групи:

технології сигнатурного аналізу;

технології імовірнісного аналізу.

Найпершою технологією пошуку шкідливих програм був сигнатурний аналіз.

Сигнатурний аналіз – метод виявлення вірусів, що полягає в перевірці наявності в ділянках коду сигнатур вірусів [5]. Сигнатурний аналіз є найбільш відомим методом виявлення вірусів і використовується практично у всіх сучасних антивірусних програмах.

Сам принцип роботи сигнатурного аналізу також визначає межі його функціональності – можливість виявляти лише вже відомі віруси, проти нових вірусів сигнатурний сканер безсилий, тому бази сигнатур необхідно оновлювати регулярно.

Грамотна реалізація вірусної сигнатури дозволяє виявляти відомі віруси зі стовідсотковою ймовірністю

В той час як еволюціонували віруси, ускладнювалися і розвивалися технології їх детектування.

Технології імовірнісного аналізу (несигнатурні технології) в свою чергу можна розбити на три категорії:

евристичний аналіз – технологія, заснована на імовірнісних алгоритмах, результатом роботи яких є виявлення підозрілих об'єктів. У процесі евристичного аналізу перевіряється структура файлу, його відповідність вірусним шаблонам. Найбільш популярною евристичною технологією є перевірка вмісту файлу на предмет наявності модифікацій уже відомих сигнатур вірусів та їх комбінацій. Евристичний аналіз застосовується для виявлення невідомих вірусів, і, як наслідок, не передбачає лікування;

поведінковий аналіз – технологія, в якій рішення про характер об'єкта, що перевіряється приймається на основі аналізу операцій, які ним виконуються. Поведінковий аналіз нечасто застосовується на практиці, оскільки більшість дій, характерних для вірусів, можуть виконуватися і звичайними додатками. Поведінкові аналізатори не використовують для роботи додаткових об'єктів, подібних вірусних баз і, як наслідок, нездатні розрізняти відомі й невідомі віруси - всі підозрілі програми апріорі вважаються невідомими вірусами;

аналіз контрольних сум – це спосіб відстеження змін в об'єктах комп'ютерної системи. На підставі аналізу характеру змін – одночасність, масовість, ідентичність змін довжин файлів – можна зробити висновок про зараження системи. Подібні технології застосовуються в сканерах при першій перевірці з файлу знімається контрольна сума і розміщується в кеші, перед наступною перевіркою того ж файлу сума знімається ще раз, порівнюється, і в разі відсутності змін файл вважається незараженим.

Поза всяким сумнівом, головною зброєю в боротьбі з вірусами завжди були антивірусні програми. Вони дозволяють не тільки виявляти віруси, що використовують різні методи маскування, але і видаляти їх з комп'ютера. Розрізняють наступні види антивірусних програм: вакцини; детектори; ревізори; охоронці; монітори; поліфаги; евристичні аналізатори.

Останнім часом, розробники антивірусних програм, пропонують користувачам комплексні рішення, які включають в себе більшу частину або навіть всі вищевказані програми.

Вакцини – це програми, призначені для запобігання зараження файлів від якого-небудь одного, конкретного вірусу. Вакцини застосовуються, якщо відсутні програми, що можуть знешкодити даний вірус. Вакцинація можлива тільки від відомих вірусів, які можна виявити, але неможливо знешкодити. Програма-вакцина модифікує програму, яка захищає комп'ютерну систему таким чином, щоб це не відображалося на її роботі, але при цьому справжній вірус вважав цю програму зараженою. Дії програм-вакцин засновані на одній з базових властивостей комп'ютерних вірусів – не заражати повторно вже інфіковану програму. З цією метою, при зараженні програм, віруси використовують так звану "чорну мітку", яка б дозволяла відрізняти вже інфіковані програми від неінфікованих. Це може бути, наприклад установка часу створення файлу в 24 години 1 хвилину і 62 секунди. Так як нормальні програми не можуть мати подібного часу створення, то, виявивши, що файл створений в цей час, вірус вважає, що він заражений і не намагається інфікувати його повторно.

Таким чином, програма-вакцина просто створює "чорну мітку" конкретного вірусу в програмі, що захищає не змінюючи її виконуваного коду, а вірус, виявляючи таку мітку, уже не намагається заразити даний файл.

"Детектори" або "сканери" – це програми, які здійснюють пошук характерної для конкретного вірусу сигнатури, в оперативній пам'яті комп'ютера або в файлах на жорсткому диску, і при виявленні, видають відповідне повідомлення. Недоліком цього класу антивірусних програм є те, що вони можуть знаходити тільки ті віруси, які відомі розробникам.

"Ревізори" – це програми, які належать до найбільш надійних засобів захисту від вірусів. Заражаючи комп'ютер, вірус робить зміни на жорсткому диску: дописує свій код в заражений файл, змінює системні області диска і таке інше. На виявленні таких змін ґрунтується робота антивірусних програм ревізорів. Вони побудовані на принципі, зворотного принципу побудови сканерів. Ревізори не знають в обличчя конкретні віруси, але вони запам'ятовують інформацію про кожен конкретний логічний диск і при зміні цієї інформації, дозволяють надійно виявляти, як відомі, так і нові, невідомі віруси. У разі виявлення зміни відомостей в комп'ютерній системі, вся відповідна інформація про змінений об'єкт надається користувачеві. Він вже сам повинен прийняти рішення: чи варто, наприклад, перевіряти даний файл на вірус (якщо це виконавчий файл) або проігнорувати повідомлення, якщо файл змінювався самим користувачем. Як правило, порівняння станів проводиться відразу після завантаження операційної системи. При порівнянні перевіряються довжина файлу, його контрольна сума, дата і час модифікації, і деякі інші параметри. Програми-ревізори мають достатньо розвинуті алгоритми, що дозволяють виявляти навіть віруси таких класів як "стелс"-віруси і "поліморфні" віруси, а деякі навіть можуть відновити вихідну версію програми, що перевіряється, видаливши зміни, внесені вірусом.

Перевагою ревізорів є – висока швидкість перевірки дисків (у багато десятків разів перевищує швидкість роботи сканерів) і висока надійність виявлення навіть невідомих вірусів.

"Охоронці" – це невеликі резидентні програми, призначені для виявлення підозрілих дій, що виникають при роботі користувача на комп'ютері, і характерних для вірусів.

Одним з найбільших недоліків програм цього класу є те, що при неправильному (а іноді навіть і при правильному) налаштуванні, вони буквально "засипають" користувача попередженнями, в результаті чого їх зазвичай відключають.

"Монітори" (або програми-фільтри) – це антивірусні програми які використовують для виявлення вірусів бази даних та їх сигнатури. Антивірусний монітор розташовується резидентно в пам'яті комп'ютера, і перевіряє на наявність вірусів тільки ті програми, над якими робить будь-які маніпуляції користувач, або операційна система.

Програми-фільтри є корисними з тієї точки зору, що допомагають користувачеві виявити вірус на ранній стадії його існування, ще до того моменту, коли поширення вірусу прийме характер епідемії.

"Поліфаги" – це програми, які здатні благополучно видалити вірус і відновити працездатність зіпсованих програм.

Для кожного вірусу, шляхом аналізу його коду, способів зараження файлів і таке інше виділяється деяка, характерна тільки для нього, послідовність байтів. Ця послідовність називається сигнатурою даного вірусу. Пошук вірусів, у найпростішому випадку, зводиться до пошуку їх сигнатур. Після виявлення вірусу в тілі програми (або завантажувального сектора, який теж, містить програму початкового завантаження) поліфаг знешкоджує його. Для цього розробники антивірусних засобів ретельно вивчають роботу кожного конкретного вірусу: що він псує, як він псує, де він ховає те, що зіпсує та інше. Сканування є найбільш традиційним методом пошуку вірусів. Воно полягає в пошуку сигнатур, виділених з раніше виявлених вірусів. Вірусні бази сучасних сканерів містять більше 40 000 масок вірусів.

Недоліком простих сканерів є їх нездатність виявляти "поліморфні" віруси, що повністю міняють свій код. Сучасні поліфаги використовують інші методи пошуку таких вірусів. Для цього вони використовують більш складні алгоритми пошуку, що включають евристичний аналіз перевірки програм. Враховуючи, що постійно з'являються нові віруси, програми-детектори та програми-поліфаги швидко застарівають, і потрібно регулярне оновлення версій баз даних, що містять сигнатури нових вірусів. Як результат, сканери застарівають вже в момент виходу нової версії.

Евристичні аналізатори – перевіряють програми і виявляють дії, характерні для вірусів. Завдяки цьому евристичні аналізатори здатні знаходити "поліморфні" віруси також легко, як і звичайні віруси, які не використовують механізму маскування, крім того, вони можуть виявляти віруси, раніше невідомі авторам антивірусної програми.

Для виявлення зазначених вірусів використовуються спеціальні методи. До них можна віднести метод емуляції процесора. Метод полягає в імітації виконання процесором програми і підсовування вірусу фіктивних керуючих ресурсів. Обманутий таким чином вірус, що знаходиться під контролем антивірусної програми, розшифровує свій код. Після цього, сканер порівнює розшифрований код з кодами зі своєї бази даних сканування.

Для більш надійного захисту комп'ютерних систем від вірусних атак все більшого поширення набувають антивірусні комплекси.

Антивірусний комплекс – набір антивірусів, що використовують однакове антивірусне ядро, яке призначено для вирішення практичних проблем щодо забезпечення антивірусної безпеки комп'ютерних систем. В антивірусний комплекс також в обов'язковому порядку входять засоби відновлення антивірусних баз.

Будь-яка локальна мережа, як правило, містить комп'ютери двох типів: робочі станції, за якими безпосередньо працюють люди, і мережеві сервери, що використовуються для службових цілей. Відповідно до характеру виконуваних функцій сервери поділяються на:

мережеві, які забезпечують централізоване сховище інформації: файлові сервери, сервери додатків та інші;

поштові, на яких працює програма, що служить для передачі електронних повідомлень від одного комп'ютера до іншого;

шлюзи, що відповідають за передачу інформації з однієї мережі в іншу. Наприклад, шлюз необхідний для з'єднання локальної мережі з Інтернетом.

Відповідно, розрізняють чотири види антивірусних комплексів: для захисту робочих станцій, файлових серверів, поштових систем і шлюзів.

Робочі станції – це комп'ютери локальної мережі, за якими безпосередньо працюють користувачі. Головним завданням комплексу для захисту робочих станцій є забезпечення безпечної роботи на розглянутому комп'ютері – для цього необхідна перевірка в режимі реального часу, перевірка на вимогу і перевірка локальної електронної пошти.

Мережеві сервери – це комп'ютери, спеціально виділені для зберігання або обробки інформації. Вони зазвичай не використовуються для безпосередньої роботи за ними, і тому, на відміну від робочих станцій, перевірка електронної пошти на наявність вірусів тут не потрібна. Отже, антивірусний комплекс для файлових серверів повинен проводити перевірку в режимі реального часу і перевірку на вимогу.

Антивірусний комплекс для захисту поштових систем призначений для перевірки всіх електронних листів на наявність в них вірусів. Тобто перевіряти інші файли, розміщені на цьому комп'ютері, він не зобов'язаний (для цього існує комплекс захисту мережевих серверів). Тому до нього пред'являються вимоги щодо наявності програми для перевірки всієї поштової кореспонденції в режимі реального часу і додатково механізму перевірки на вимогу поштових баз даних.

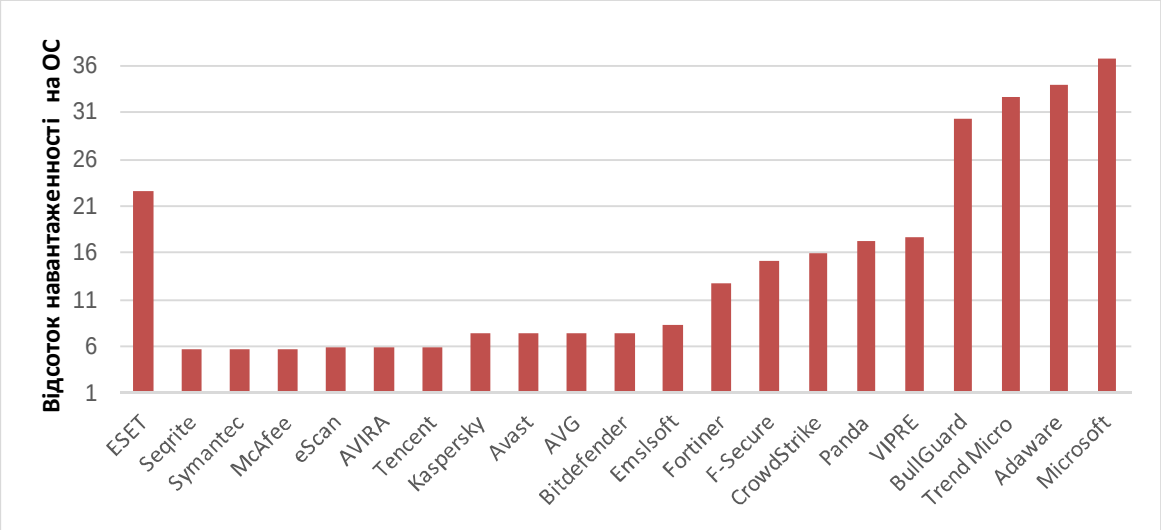
Аналогічно, згідно зі своїм призначенням, антивірусний комплекс для шлюзу здійснює перевірку даних, що проходять через шлюз.

Оскільки всі перераховані вище комплекси використовують сигнатурний аналіз, то в обов'язковому порядку в них повинен входити засіб для підтримки антивірусних баз в актуальному стані, тобто механізм їх оновлення. Часто виявляється корисним модуль для віддаленого централізованого управління, який дозволяє системному адміністраторові зі свого робочого місця налаштовувати параметри роботи антивірусу, запускати перевірку на вимогу і оновлення антивірусних баз.

Якщо розглядати технології захисту від шкідливих програм не окремо, а узагальнено, з точки зору представленої моделі, то складається наступна картина.

Технічний компонент технології відповідає в основному за такі її характеристики, як навантаження на систему (і як наслідок – її швидкодія), безпека та захищеність.

Навантаження на систему – це частка процесорного часу і оперативної пам'яті, безперервно або періодично задіяних у забезпеченні захисту і обмежує швидкодію системи. Емуляція виконується повільно, незалежно від реалізації: на кожну проемульовану інструкцію доводиться кілька інструкцій штучного середовища. Те ж можна сказати і про віртуалізацію. Моніторинг системних подій також безумовно рівномірно гальмує всю систему. На рис. 2 показаний графік впливу антивірусних засобів на операційну систему персонального комп'ютера за травень місяць 2017 року [6].



Під "безпекою" мається на увазі ступінь ризику, якому піддається операційна система і дані користувача в процесі ідентифікації потенційно шкідливого коду. Такий ризик існує завжди, коли шкідливий код виконується реально, в операційній системі. Для систем моніторингу подій таке реальне виконання коду архітектурно обумовлено, в той час як емуляція і файлове сканування можуть виявити шкідливий код ще до того, як він почав виконуватися.

Захищеність, цей параметр відображає уразливість технології, те, наскільки шкідливий код може ускладнити процес ідентифікації себе. Протистояти файловому детектуванню дуже легко: достатньо добре упакувати файл, зробити його поліморфним, або скористатися руткіт-технологією для приховування файлу. Протистояти емуляції трохи складніше, але також можливо для цього використовуються численні трюки, вбудовані в код шкідливої програми. Але сховатися від системного моніторингу програми вже складно – з тієї причини, що практично неможливо приховати поведінку.

В середньому, чим менш абстрактний захист, тим він безпечніше, але й тим простіше його обійти.

Аналітичний компонент технології відповідає за такі характеристики, як проактивність (і залежну від неї необхідну частоту оновлення антивірусу), відсоток помилкових спрацьовувань і навантаження на користувача.

Під проактивністю мається на увазі здатність технології виявляти нові шкідливі програми, які ще не потрапили до рук фахівців. У міру зростання складності аналітичної системи, зростає і її проактивність. З проактивністю безпосередньо пов'язана і така характеристика системи захисту, як необхідність постійного оновлення.

Наприклад, бази сигнатур потрібно постійно оновлювати, в той час як більш складні евристичні системи залишаються адекватними до поточної ситуації більш тривалий термін, а експертні аналітичні системи можуть успішно функціонувати без оновлень місяцями.

Відсоток помилкових спрацьовувань так само безпосередньо пов'язаний зі складністю технології аналізу. Якщо шкідливий код ідентифікується жорстко заданою сигнатурою або послідовністю дій, за умови достатньої довжини сигнатури.

Під навантаженням на користувача мається на увазі ступінь його участі у формуванні політики захисту – правил, винятків, білих і чорних списків – і участі в процесі винесення вердикту – підтвердження або спростування "підозр" аналітичної системи.

Чим складніша аналітична система, тим вона могутніша, але і тим вище відсоток помилкових спрацювань.

Висновки й перспективи подальших досліджень

На даний момент більшість рішень в області комп'ютерної безпеки реалізуються, як комплекс декількох технологій. У класичних антивірусах сигнатурні детектування зазвичай використовується в парі з тією чи іншою реалізацією моніторингу системних подій, емулятора, пісочниці.

Перш за все, слід пам'ятати, що не існує ні універсального, ні "найкращого" рішення. У кожної технології є свої плюси і мінуси. Наприклад, моніторинг подій в системі постійно займає процесорний час, але його найважче обманути; процесу емуляції можна перешкодити використанням в коді певних команд, але при її використанні виявлення шкідливого коду виконується в попереджуючому режимі, система залишається захищеною. Вибір технології – це вибір золотої середини з урахуванням конкретних потреб і обставин.

Існує безліч методик виявлення невідомого шкідливого програмного засобу. Кожна з них має свої переваги, недоліки та особливості використання. Але на даний момент не існує методики, яка б повністю вирішувала завдання виявлення невідомого шкідливого програмного засобу з прийнятною ефективністю для будь-яких видів шкідливих програмних засобів і за будь-яких вимог до системи виявлення шкідливих програмних засобів. Теоретично об'єднання декількох методик може вирішити цю проблему.

Для проведення ефективного дослідження комп'ютера, пошуку і знищення шкідливих програм потрібно комбінувати всі методи, способи і засоби, які висвітлені в цій статті.

Література

1. Безруков Н. Компьютерная вирусология. /Безруков Н.// - К.: УРЕ, 1991. с. 15. **2. Гульев И.** Компьютерные Вирусы. Взгляд Изнутри. /Гульев И.// - М.: ДМК 1998. с. 58-62. **3. Козлов Д.А.** Энциклопедия компьютерных вирусов. /Козлов Д.А., Парандовский А.А., Парандовский А.К.// Издательство: СОЛОН - Р, 2010. с. 343. **4. Собейкис В.Г.** Азбука хакера 3. /Собейкис В.Г.// - С.: Компьютерная вирусология, 2014. с. 26-28. **5. Шаньгин В.** Защита информации в компьютерных системах и сетях. /Шаньгин В.// - ДМК Пресс 2013. с. 65. **6. AV-Comparatives** – Незалежні тести антивірусного програмного забезпечення. / [Електронний ресурс] // - Режим доступу: www.av-comparatives.org – Назва з екрану.

МЕТОДЫ И СРЕДСТВА ПРОТЕВОДЕЙСТВИЯ ВРЕДОНОСНОМУ ПРОГРАМНОМУ ОБЕСПЕЧЕНИЮ

Вадим Иванович Пеньков
Роман Михайлович Штонда
Александр Николаевич Гук
Ирина Робертовна Мальцева
Юлия Александровна Черныш

Военный институт телекоммуникаций и информатизации, Киев, Украина

Информационные технологии определяют процессы передачи, хранения и обработки информации, а также её использование в определенных целях. Эти процессы должны быть быстрыми, менее затратными, максимально полезными, удобными и автоматизированными. По этой причине основной тенденцией развития информационных технологий является их представление в цифровом виде, переход к цифровым информационно-телекоммуникационных базам, основанным на цифровом взаимодействия компьютеров, разработанных с самыми разнообразными функциональными алгоритмами. Внедрение персональных компьютеров в информационную сферу и применение телекоммуникационных средств связи определили новый этап развития информационных технологий.

Развитие Интернета изменило отношение к проблемам безопасности, подняв вопрос о защищенности локальных и глобальных компьютерных сетей. Еще недавно эти проблемы не были столь актуальными. Разработчики первых компьютерных сетей в первую очередь стремились увеличить скорость и надежность передачи данных, порой достигая желаемого результата в ущерб безопасности.

Увеличение скорости передачи информации, объемов и значимости обрабатываемых в вычислительных сетях данных открывает перед киберпреступниками все более широкие возможности. Распространение по всему миру вредоносного программного обеспечения занимает считанные дни или даже часы. Сотни мегабайт оперативной памяти позволяют выполнять практически любые действия незаметно для пользователя. Спектр возможных целей, таких как пароли, карточные счета, ресурсы удаленных компьютеров представляет огромное поле для их деятельности.

Ключевые слова: *вредоносное программное обеспечение, антивирусные программы, компьютерный вирус, компьютерная система, компьютерная сеть.*

METHODS AND MEANS OF PROTECTION FROM MALICIOUS SOFTWARE

Vadym I. Penkov, Roman M. Shtonda, Oleksandr M.Guk,
Iryna R. Maltseva, Yuliia A. Chernysh

Military Institute of Telecommunications and Information, Kyiv, Ukraine

Information technologies define the processes of transmission, storage and processing of information, as well as its use for certain purposes. These processes should be fast, less expensive, as useful as possible, convenient and automated. For this reason, the main trend in the development of information technologies is their presentation in digital form, the transition to digital information and telecommunications bases based on the digital interaction of computers developed with a wide variety of functional algorithms. The implementation of personal computers into the information sphere and the use of telecommunications means of communication have determined a new stage in the development of information technologies.

The development of the Internet has changed attitudes to security issues, raising the issue of the security of local and global computer networks. Until recently, these problems were not so relevant. Developers of the first computer networks primarily sought to increase the speed and reliability of data transmission, sometimes achieving the desired result to the detriment of security.

The increase in the speed of information transfer, the volumes and significance of data processed in computer networks opens up wider opportunities for cybercriminals. Distribution around the world of malicious software takes a few days or even hours. Hundreds of megabytes of random access memory allow you to perform virtually any actions imperceptibly for the user. A range of possible goals, such as passwords, card accounts, remote computer resources, is a huge field for their activities.

Keywords: *malicious software, antivirus software, computer virus, computer system, computer network.*

References

1. Bezrukov N. (1991) Computer virology. [*Komp'yuternaya virusologiya.*]- K.: URE, p. 15. **2. Gul'yev I.** Computer viruses. View from the inside [*Komp'yuternyye Virusy. Vzglyad Iznutri*] - M.: DMK 1998. pp. 58-62. **3. Kozlov DA,** Parandovsky AA, Parandovsky A.K. (2010) Encyclopedia of computer viruses. [*Entsiklopediya kompyuternyih virusov*] Publisher: SOLON-R p. 343. **4. Sobeykis V.G.** (2014) The ABC of the hacker 3. [*Azbuka hakera 3*] S.: Computer virology pp. 26-28. **5. Shanguin V.** (2013) Protection of information in computer systems and networks. [*Zaschita informatsii v kompyuternyih sistemah i setyah.*] DMK Press p. 65. **6. AV-Comparatives** (2017) Independent Tests of Anti-Virus Software [*Nezalezhni testy antyvirusnoho prohramnoho zabezpechennia*], www.av-comparatives.org.

УДК 621.396

Юрій Борисович Прібилєв *(кандидат технічних наук, доцент)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

МЕТОД СИНТЕЗУ СТРУКТУРИ КОНТРОЛЬНО-ВИПРОБУВАЛЬНОЇ СТАНЦІЇ

У статті розроблений метод синтезу структури контрольно-випробувальної станції на базі уніфікованого ряду апаратно-програмних модулів. Запропонований метод передбачає визначення потрібних апаратно-програмних модулів з ряду уніфікованих модулів для забезпечення заданих вимог з контролю об'єктів контролю при мінімальних витратах на побудову контрольно-випробувальної станції. Основні етапи методу включають: визначення вихідної множини уніфікованих апаратно-програмних модулів; розробка спеціальних апаратно-програмних модулів; синтез структури контрольно-випробувальної станції як сукупності апаратно-програмних модулів, яка забезпечує задані вимоги з достовірності контролю та тривалості контролю при мінімальної вартості контрольно-випробувальної станції; вибір ЕОМ базового модулю контрольно-випробувальної станції та розробка програми контролю; апаратна побудова та комплексне налагодження контрольно-випробувальної станції. Розроблений метод дозволяє побудувати перспективну універсальну автоматизовану контрольно-випробувальну станцію зі змінною конфігурацією, яка зможе проводити автоматизований контроль і діагностування несправностей усіх зразків ракетного озброєння, що є на озброєнні Збройних Сил України та перспективних ракет, що зараз розробляються.

Ключові слова: *контрольно-випробувальна станція, об'єкт контролю, апаратно-програмний модуль.*

Вступ

Хід антитерористичної операції на південному сході України показав, що загроза застосування Російською Федерацією (РФ) засобів повітряного нападу (ЗПН) залишається високою. Порівняно з винищувальною авіацією, застосування засобів протиповітряної оборони (ППО) є менш витратним способом захисту від ЗПН противника. Однак існуючі темпи оновлення озброєння ППО відстають від темпів старіння техніки. Ще тривалий час основою парку зенітних ракетних комплексів (ЗРК) буде залишатись озброєння радянського виробництва, яке потребує відновлення, капітального ремонту та модернізації [1]. Для підтримання боєздатного стану ця застаріла техніка потребує застосування сучасних методів контролю технічного стану (ТС) та достовірної діагностики несправностей.

Постановка проблеми. У складі кожного ЗРК є технічні засоби, що призначені для надання обслуговуючому персоналу достовірної інформації про технічний стан зенітних керованих ракет (ЗКР). Основним джерелом такої інформації є проведення регламентних та контрольно-випробувальних робіт з ЗКР за допомогою штатних контрольно-випробувальних станцій (КВС).

Слід зауважити, що запланована глибока модернізація ЗРК [2] (інколи з заміною до 90% елементної бази радіоелектронної апаратури) обов'язково передбачає модернізацію КВС, які повинні бути здатними забезпечити достовірний контроль технічного стану та випробування модернізованих ЗКР. Але у більшості випадків модернізація існуючих КВС є економічно недоцільною. Ці КВС, побудовані на неуніфікованих агрегатах та елементній базі, є морально та технічно застарілими, вузькоспеціалізованими та жорстко прив'язаними до конкретного зразка ЗКР [3].

Скоротити витрати на обслуговування модернізованих ЗКР (та нових ЗКР, що зараз розробляються) дозволить побудова єдиної універсальної автоматизованої КВС, яку доцільно побудувати за базово-модульним принципом із застосуванням новітніх інформаційних технологій та яка буде здатна проводити контроль і випробування ЗКР декількох типів (множини об'єктів контролю (ОК)). Для побудови такої КВС необхідною є розробка сучасних методів проектування та побудови КВС.

Аналіз остатніх досліджень і публікацій. ЗРК є складною технічною системою, яка характеризується певною сукупністю показників та складається з великої кількості різнорідних елементів, які взаємодіють між собою [4-7]. Удосконалення методів технічної експлуатації і ремонту ЗРК, як основного способу підтримання технічної готовності ЗРК в сучасних умовах, розглянуто у [8].

Питання розвитку систем контролю технічного стану і діагностування ЗРК розглядали автори у [9]. Класичні методи проектування систем контролю ракет детально розглянуті у [10], але ці методи розроблені на основі неуніфікованих апаратних засобів без урахування взаємовпливу апаратних і програмних засобів та не забезпечують раціональних характеристик КВС.

Метою статті є розробка методу синтезу структури КВС на базі уніфікованого ряду апаратно-програмних модулів (АПМ), що забезпечує скорочення витрат та термінів на розробку і побудову сучасних КВС при заданих вимогах до якості КВС.

Виклад основного матеріалу дослідження.

У [10] запропонована методика синтезу КВС на базі ряду уніфікованих апаратних модулів. Але для скорочення термінів і вартості проектування та побудову КВС необхідно здійснювати як апаратно-програмну систему на основі взаємозв'язку програмних і апаратних засобів.

Структура КВС складається з сукупності АПМ, що забезпечують виконання заданих завдань контролю. При наявності уніфікованого ряду АПМ проектування структури КВС зводиться до визначення складу АПМ з необхідними характеристиками.

Тобто метод проектування КВС базується на виборі вихідної множини АПМ з ряду уніфікованих АПМ для забезпечення заданих вимог з контролю ОК, визначення оптимального складу АПМ при мінімальних витратах на КВС, і подальшого проектування апаратної і програмної частин КВС.

Запропонований метод синтезу КВС як апаратно-програмної системи складається з 9 етапів, які розглянемо нижче.

1. Визначається вихідна множина уніфікованих АПМ, виходячи з вимог за характеристиками контрольованих і стимулюючих сигналів ОК з урахуванням заданої моделі ОК.

2. Для сигналів, що не забезпечуються уніфікованим рядом АПМ, розробляються спеціальні АПМ, які включаються у вихідну множину.

3. Для заданого переліку контрольованих і стимулюючих сигналів і алгоритмів контролю проводиться синтез складу АПМ, виходячи з критеріїв ефективності проектованої КВС – забезпечення мінімальної вартості при забезпеченні заданих вимог за достовірністю контролю, тривалістю контролю, об'ємом пам'яті ЕОМ КВС. В результаті для кожного контрольованого і стимулюючого сигналу визначається конкретний АПМ. За результатами синтезу складу АПМ формуються склад уніфікованих апаратних и програмних модулів та склад спеціальних АПМ.

4. На етапі вибору стандартних рішень на основі ряду уніфікованих АПМ вибирається ЕОМ КВС та системне програмне забезпечення.

5. Для обраних спеціальних АПМ розробляються спеціальні апаратні засоби та програмне забезпечення (ПЗ) спеціальних АПМ. Після чого формується повний склад апаратних модулів та повний склад програмних модулів для побудови КВС.

6. На базі повного складу апаратних засобів проводиться апаратне проектування КВС (розробляються схема з'єднань КВС, схема розміщення апаратних засобів в конструкції КВС).

7. З сукупності складу програмних модулів АПМ проводиться розробка вихідних програм контролю ОК з урахуванням розроблених при проектуванні уніфікованих АПМ уніфікованих описів сигналів, уніфікованих описів завдань контролю, уніфікованих операцій управління АПМ, а також програм самоконтролю КВС.

8. Здійснюється розробка описів АПМ. На основі цих описів і з урахуванням опису з'єднань КВС розробляється база даних КВС для забезпечення трансляції модулів програм контролю.

9. Після розробки бази даних КВС здійснюється трансляція вихідних програм контролю та їх налагодження. Модулі програми контролю розробляються незалежно від неї. Після виготовлення зразка КВС проводиться комплексне налагодження програм контролю та ПЗ КВС, стикування КВС з ОК. По завершенню зазначених робіт проводяться випробування КВС.

Проектування КВС для множини ОК передбачає визначення сукупності засобів контролю для множини завдань контролю. При проектуванні КВС як апаратно-програмної системи потрібно на основі заданих моделей ОК визначити склад уніфікованих АПМ, що реалізують задані завдання контролю з мінімальною вартістю.

Таким чином, формалізована постановка завдання синтезу КВС для множини ОК на основі уніфікованих АПМ буде наступною.

1. Нехай задана сукупність завдань контролю $A\{A_n\}$, $n=\overline{1,N}$. Для кожного завдання контролю задані: перелік контрольованих параметрів $X_n\{X_i\}$, $i=\overline{1,I_n}$, перелік стимулюючих і контрольованих сигналів $R_n\{R_m\}$, $m=\overline{1,M_n}$, де m від 1 до h – стимулюючі сигнали та від $(h+1)$ до M_n – контрольовані сигнали.

Під сигналом розуміється стимулюючий або контрольований сигнал на певному контакті ОК; $W_n\{W_i\}$ – алгоритми контролю параметрів. Відомо необхідне число КВС для кожного завдання j_n. Для параметрів, що контролюються, відомі закони розподілу ймовірностей значень параметрів $f\{x_i\}$ і допустимі межі їх зміни.

Відомі описи стимулюючих і контрольованих сигналів – для всіх завдань контролю і опис загальної вихідної множини АПМ B_0, на підставі яких визначено вихідну множину АПМ за типами сигналів і ОК (для кожного сигналу кожного ОК) $B\{B_u\}$, $u=\overline{1,U}$.

2. Сукупність апаратних засобів вихідної множини АПМ $B\{B_u\}$ утворює вихідну множину

пристроїв $Q\{Q_k\}$, $k=\overline{1,K}$.

Кожен АПМ характеризується:

– часом виконання $t_в$;

– похибкою (видачі, перетворення сигналу) $d_п$;

– множиною пристроїв $Q_u\{Q_k\}$, $k \in K_u$,

де K_u – множина індексів пристроїв, що використовуються АПМ B_u;

– об'ємом пам'яті для зберігання програм АПМ P_u;

– вартістю розробки програми АПМ $C_{рп}$;

– вартістю настройки ПЗ АПМ $C_{нп}$.

Для кожного пристрою Q_k задана вартість $C_k(j_k)$, як функція від обсягу виробництва j_k:

$$C_k(f_k)=\begin{cases} a_k+b_k f_k, & \text{якщо } f_k>0 \\ 0, & \text{якщо } f_k=0 \end{cases}, \qquad (1)$$

де a_k – вартість розробки пристрою Q_k, яка не залежить від обсягу його виробництва, b_k – вартість виготовлення пристрою.

3. Необхідно визначити набір АПМ, який забезпечує виконання заданих вимог за достовірністю контролю та часу контролю для кожного завдання контролю A_n при мінімальній вартості С рішення всіх задач контролю.

4. Зв'язки між різними множинами АПМ описуються матрицями відповідності:

$$x_{mu}=\begin{cases} 1, & \text{якщо для стимулюючого(контролюємого)} \\ & \text{сигналу } R_m \text{ використовується АПМ } B_u; \\ 0, & \text{в іншому випадку.} \end{cases}$$

$$h_{mu}=\begin{cases} 1, & \text{якщо для АПМ } B_u \text{ є} \\ & \text{необхідним пристроєм } Q_k; \\ 0, & \text{в іншому випадку.} \end{cases}$$

$$g_{mu}=\begin{cases} 1, & \text{якщо сигнал } R_m \text{ використовується} \\ & \text{при контролі параметра } X_i; \\ 0, & \text{в іншому випадку.} \end{cases}$$

Крім того вводяться коефіцієнти:

e_{mi} – коефіцієнт впливу похибки формування або вимірювання сигналу R_m на похибку контролю параметра X_i.

c_{mi} – коефіцієнт впливу часу перетворення або видачі сигналу R_m на час контролю параметра X_i.

Достовірність контролю ОК, як функція достовірності контролю кожного параметра, розраховується за виразом: $D_n=\prod_{i=1}^{I_n} D_i$, де D_i – достовірність контролю параметра X_i є відомою функцією похибки контролю параметра $D_i=f(d_i)$.

Похибка d_i визначається похибками видачі стимулюючих і перетворення контрольованих сигналів, що беруть участь в контролі параметра і для кожного з яких вибирається один з АПМ B_u^*. Тобто похибка d_i є функцією похибок АПМ, що використовуються для контролю параметра X_i. Вплив похибок АПМ на похибку контролю параметра встановлюється за алгоритмом контролю параметрів $W_n(W_i)$. Найбільш часто [11] сумарну похибку контролю параметра визначають як:

$$s_i=\sqrt{\sum_{m=1}^{M_n} e_{mi}^2 \sum_{u=1}^{U} x_{mu} s_u^2}, \qquad (2)$$

при умові $\sum_{u=1}^{U} x_{mu}=1$ для $m=\overline{1,M}$.

Показниками достовірності є ймовірність "помилкової відмови" $P_{пв}$ і ймовірність "незнайденої відмови" $P_{нв}$. Ці показники обчислюються через ймовірності працездатності для *n*-го ОК $P_W^n=\prod_{i=1}^{I_n} P_{W_i}$, ймовірності отримання результату "ОК придатний" для *n*-го ОК $P_W^n=\prod_{i=1}^{I_n} P_{W_i}$ і спільної ймовірності зазначених подій $P_{Wx}^n=\prod_{i=1}^{I_n} P_{W_i w_i}$: $P_{пв}^n=P_W^n-P_{Ww}^n$, $P_{нв}^n=P_W^n-P_{Ww}^n$.

Імовірність P_{W_i} визначається розподілом ймовірностей значень і-го параметра, а ймовірності P_{w_i} і $P_{W_i w_i}$ залежать від розподілів ймовірностей параметра і похибки його контролю:

$$P_{W_i}=f_1\left(\sqrt{\sum_{m=1}^{M_n} e_{mi}^2 \sum_{u=1}^{U} x_{mu} s_u^2}\right) \qquad (3)$$

$$P_{w_i}=f_2\left(\sqrt{\sum_{m=1}^{M_n} e_{mi}^2 \sum_{u=1}^{U} x_{mu} s_u^2}\right) \qquad (4)$$

$$P_{W_i w_i}=f_3\left(\sqrt{\sum_{m=1}^{M_n} e_{mi}^2 \sum_{u=1}^{U} x_{mu} s_u^2}\right) \qquad (5)$$

Вид функцій f_1, f_2, f_3 для обчислення ймовірностей в залежності від похибки контролю параметра наведено в [11]. Таким чином, достовірність контролю для кожного завдання A_n може бути визначена як:

$$P^n_{пв} = \prod_{i=1}^{I_n} \left[f_1 \left(\sqrt{\sum_{m=1}^{M_n} e^2_{mi} \sum_{u=1}^{U} x_{mu} s^2_u} \right) - f_3 \left(\sqrt{\sum_{m=1}^{M_n} e^2_{mi} \sum_{u=1}^{U} x_{mu} s^2_u} \right) \right]$$

$$P^n_{нв} = \prod_{i=1}^{I_n} \left[f_2 \left(\sqrt{\sum_{m=1}^{M_n} e^2_{mi} \sum_{u=1}^{U} x_{mu} s^2_u} \right) - f_3 \left(\sqrt{\sum_{m=1}^{M_n} e^2_{mi} \sum_{u=1}^{U} x_{mu} s^2_u} \right) \right]$$

Час контролю n-ой КВС t_n складається з часу виконання програми АПМ $t_{вп}$, часу, що визначаються затримками в ОК $t_{зп}$, часу, що пов'язаний з виконанням керуючої програми контролю $t_{кп}$: $t_n = t_{вп} + t_{зп} + t_{кп}$.

Значення $t_{вп}$ визначається за формулою:

$$t_{пв} = \sum_{i=1}^{I_n} \sum_{m=1}^{M_n} c_{mi} \sum_{u=1}^{U} x_{mu} t_u . \quad (6)$$

Об'єм пам'яті ЕОМ n-ой КВС V_n визначається сумою об'ємів пам'яті, що використовується АПМ $V_в$ і об'ємом пам'яті, яка займається керуючою частиною програм контролю $V_{пк}$. Значення об'єму пам'яті V_n визначається виразом:

$$V_n = V_{пк} + \sum_{u=1}^{U} V_u \operatorname{sgn}\left(\sum_{m=1}^{M_n} x_{mu} \right), \quad (7)$$

де $\operatorname{sgn}(z) = \begin{cases} 1, & \text{якщо } z > 0 \\ 0, & \text{якщо } z = 0 \end{cases}$.

Вартість контролю С КВС (всіх АПМ, на базі яких реалізується контроль для заданої сукупності задач) складається з наступних складових: вартості всіх пристроїв, що входять в АПМ, вартості розробки програм АПМ, вартості настроювання ПЗ АПМ.

Завдання полягає в мінімізації вартості КВС за умови, що її технічні характеристики відповідають вимогам за достовірністю, за часом контролю ОК, допустимим об'ємом пам'яті ЕОМ. Вартість всіх пристроїв, що входять до складу уніфікованих АПМ, визначається виразом [8]:

$$C = \sum_{k=1}^{K} \left[a_k \operatorname{sgn}\left(\sum_{n=1}^{N} \sum_{m=1}^{M_n} \sum_{u=1}^{U} x_{mu} h_{uk} \right) \right] + \sum_{n=1}^{N} \left[b_k \operatorname{sgn}_n \max_i \left(\sum_{m=1}^{M_n} \sum_{u=1}^{U} x_{mu} h_{uk} g_{im} \right) \right]. \quad (8)$$

Функція max(…) використовується для тих випадків, коли при контролі деякого параметра ОК може знадобитися більше одного однотипного АПМ. Тому в таких випадках доцільно присвоювати таким АПМ різні номери, при цьому вартість пристроїв запишеться у вигляді:

$$C = \sum_{k=1}^{K} \left[a_k \operatorname{sgn}\left(\sum_{n=1}^{N} \sum_{m=1}^{M_n} \sum_{u=1}^{U} x_{mu} h_{uk} \right) \right] + \sum_{n=1}^{N} \left[b_k \operatorname{sgn}_n \left(\sum_{m=1}^{M_n} \sum_{u=1}^{U} x_{mu} h_{uk} \right) \right] \quad (9)$$

Вартість розробки ПЗ АПМ дорівнює:

$$C_{пр} = \sum_{u=1}^{U} C_{up} \operatorname{sgn}\left(\sum_{n=1}^{N} \sum_{m=1}^{M_n} x_{mu} \right). \quad (10)$$

Вартість настроювання ПЗ АПМ дорівнює:

$$C_{пн} = \sum_{u=1}^{U} C_{uн} \operatorname{sgn}\left(\sum_{n=1}^{N} \sum_{m=1}^{M_n} x_{mu} \right). \quad (11)$$

Використовуючи отримані вирази, математичне формулювання задачі синтезу КВС для множини ОК має наступний вигляд:

$$\min_{x_{mu}} C = \sum_{k=1}^{K} \left[a_k \operatorname{sgn}\left(\sum_{n=1}^{N} \sum_{m=1}^{M_n} \sum_{u=1}^{U} x_{mu} h_{uk} \right) \right] + \sum_{n=1}^{N} \left[b_k \operatorname{sgn}_n \left(\sum_{m=1}^{M_n} \sum_{u=1}^{U} x_{mu} h_{uk} \right) \right] + \sum_{u=1}^{U} C_{up} \operatorname{sgn}\left(\sum_{n=1}^{N} \sum_{m=1}^{M_n} x_{mu} \right) + \sum_{u=1}^{U} C_{uн} \operatorname{sgn}\left(\sum_{n=1}^{N} \sum_{m=1}^{M_n} x_{mu} \right). \quad (12)$$

Вираз (12) отриманий при наступних обмеженнях:

– ймовірності помилкової відмови і незнайденої відмови при контролі кожного ОК повинні бути менше заданих значень:

$$P^n_{пв}(x_{mu}) = \prod_{i=1}^{I_n} \left[f_1 \left(\sqrt{\sum_{m=1}^{M_n} e^2_{mi} \sum_{u=1}^{U} x_{mu} s^2_u} \right) - f_3 \left(\sqrt{\sum_{m=1}^{M_n} e^2_{mi} \sum_{u=1}^{U} x_{mu} s^2_u} \right) \right] \le P^n_{пв\,пз}, n = \overline{1,N}, \quad (13)$$

$$P^n_{нв}(x_{mu}) = \prod_{i=1}^{I_n} \left[f_2 \left(\sqrt{\sum_{m=1}^{M_n} e^2_{mi} \sum_{u=1}^{U} x_{mu} s^2_u} \right) - f_3 \left(\sqrt{\sum_{m=1}^{M_n} e^2_{mi} \sum_{u=1}^{U} x_{mu} s^2_u} \right) \right] \le P^n_{іâ\,пç}, n = \overline{1,N} \quad (14)$$

– час контролю кожного ОК має бути менше заданого:

$$t_{пв}(x_{mu}) = \sum_{i=1}^{I_n} \sum_{m=1}^{M_n} c_{mi} \sum_{u=1}^{U} x_{mu} t_u \le t_{пз} - t_{nm} - t_{ny}, n = \overline{1,N}, \quad (15)$$

– об'єм пам'яті ЕОМ не повинен перевищувати заданий:

$$V_n(x_{mu}) = \sum_{u=1}^{U} V_u \operatorname{sgn}\left(\sum_{m=1}^{M_n} x_{mu} \right) \le V_{пк} - V_{ny}, n = \overline{1,N}, \quad (16)$$

– для кожного необхідного сигналу при контролі повинен бути призначений тільки один АПМ:

$$\sum_{u=1}^{U} x_{mu} \operatorname{sgn}\left(\sum_{i=1}^{I_n} g_{im} \right) = 1, \quad m = \overline{1,M_n}, \quad n = \overline{1,N}. \quad (17)$$

Вираз (17) визначає вибір для сигналу єдиного АПМ з уніфікованого ряду, і отже, єдине рішення завдання оптимізації при синтезі структури КВС.

Висновки й перспективи подальших досліджень

Таким чином, у статті запропонований метод синтезу КВС як апаратно програмної системи, який ґрунтується на виборі множини АПМ з уніфікованого ряду АПМ і при необхідності спеціальних АПМ для забезпечення заданих вимог з контролю ОК. Запропоновано математичне формулювання задачі синтезу складу КВС, яка полягає у визначенні набору АПМ, який забезпечує виконання заданих вимог до якості КВС (достовірність контролю, час контролю) при мінімальній вартості КВС.

Проектування КВС на основі уніфікованого ряду АПМ показало, що в порівнянні з існуючими методами на базі апаратних засобів процес різко спрощується. За досвідом створення модернізованого комплексу "Гурт-М" для контролю різних видів авіаційного озброєння на державному підприємстві "ДержККБ Луч", створення КВС зводиться практично на 80-90% (відсоток використання уніфікованого ряду АПМ) до вибору потрібної множини АПМ.

В результаті роботи, які пов'язані з розробкою методик контролю, структури контрольно-вимірювальних каналів, складу апаратних засобів, структурно-методичних варіантів контролю [12] не проводяться, що дає суттєву перевагу в зменшенні витрат на проектування та побудову КВС. Об'єм обладнання КВС, які побудовані на основі АПМ, приблизно в 2-3 рази менше обсягу обладнання КВС, побудованих на основі апаратних засобів, а терміни розробки конструкторської документації скорочуються в 2-3 рази. Напрямком подальших досліджень є складання алгоритму завдання синтезу КВС.

Література

1. Гриб Д.А., Ланецький Б.М., Лук'янчук В.В. Удосконалення методів технічної експлуатації і ремонту як основа підтримання боєготового стану зенітного ракетного озброєння в сучасних умовах: Науково-теоретичний та науково-практичний журнал "Наука і оборона". 2012. №3. С. 55–63. **2. Карпенко Д.В.** Стан та перспективи розвитку зенітного ракетного озброєння Повітряних Сил Збройних Сил України: Науковий журнал "Наука і техніка Повітряних Сил Збройних Сил України". 2017. № 2(27). С.75–78. **3. Прібилєв Ю.Б., Сакович Л.В.** Підхід до побудови уніфікованої універсальної автоматизованої контрольно-випробувальної станції ракетного озброєння: Науково-теоретичний та науково-практичний журнал "Наука і оборона". Київ. 2017. №1. С. 42–48. **4. Барзилович Е.Ю.** Модели технического обслуживания сложных систем. М.: Высш. шк. 1982. 230 с. **5. Месарович, М.** Общая теория систем: математические основы. [Текст] / М. Месарович, И. Такахара // Пер. с англ. М.: "Мир", 1978. – 312 с. **6. Берталанфи, Л. фон.** Общая теория систем – критический обзор. // Исследования по общей теории систем: Сборник переводов / Общ. ред. В. Н. Садовского и Э. Г. Юдина. – М.: Прогресс, 1969. – С. 23-82. **7. Гайдес, М. А.** Общая теория систем. (Системы и системный анализ) [Текст] / М.А. Гайдес. // – М.: Глобус-Пресс, 2005. – 201 с. **8. Пермяков О. Ю. Прібилєв Ю.Б., Дюбанов О.О.** Модель системи діагностування, технічного обслуговування та ремонту складних технічних систем військового призначення: Науково-теоретичний та науково-практичний журнал "Наука і оборона". 2016. № 2. С. 48–52. **9. Жердєв М.К., Вишнівський В.В., Пампуха І.В., Скуйбіда О.Ю.** Напрями розвитку систем контролю технічного стану і діагностування складних технічних систем: Зб. наук. праць ВІКНУ імені Тараса Шевченка. 2006. № 3. С. 22–25. **10. Гнедов Г.М., Росенбаули О.Б., Шумов Ю.А.** Проектирование систем контроля ракет. М.: Машиностроение, 1975. 224 с. **11. Пономарев Н.Н., Фрумкин И.С., Гусинский И.С.** и др. Проектирование внешних средств автоматизированного контроля радиоэлектронного оборудования. / Под ред. Н.Н. Пономарева. М.: Радио и связь. 1984. 296 с. **12. ДСТУ 2389–94.** "Технічне діагностування та контроль технічного стану. Основні терміни та визначення".

МЕТОД СИНТЕЗА СТРУКТУРЫ КОНТРОЛЬНО-ИСПЫТАТЕЛЬНОЙ СТАНЦИИ

***Юрий Борисович Прибылев** (канд. техн. наук, доцент)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье разработан метод синтеза структуры контрольно-испытательной станции на базе унифицированного ряда аппаратно-программных модулей, согласно которому выбираются необходимые аппаратно-программные модули из ряда унифицированных модулей для обеспечения заданных требований по контролю объектов контроля при минимальных затратах на строительство контрольно-испытательной станции. Основные этапы метода включают: определение исходного множества унифицированных аппаратно-программных модулей; разработку специальных аппаратно-программных модулей; синтез структуры контрольно-испытательной станции как совокупности аппаратно-программных модулей, которая обеспечивает заданные требования по достоверности контроля и времени контроля при минимальной стоимости контрольно-испытательной станции; выбор ЭВМ базового модуля контрольно-испытательной станции и разработка программы контроля;

аппаратное построение и комплексную наладку контрольно-испытательной станции. Разработанный метод позволяет построить перспективную универсальную автоматизированную контрольно-испытательную станцию переменной конфигурации, которая сможет проводить автоматизированный контроль и диагностирование неисправностей всех образцов современного ракетного вооружения Вооруженных Сил Украины и перспективных разрабатываемых ракет.

Ключевые слова: *контрольно-испытательная станция, объект контроля, аппаратно-программный модуль.*

THE METHOD OF SYNTHESIS OF STRUCTURE OF THE CONTROL AND TEST STATION

Yurii Pribyliev ***(Candidate of Technical Sciences, Associate Professor)***

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

There is developed a method of synthesis of the structure of control and test station on the basis of an unified number of hardware-software modules in the article. The proposed method involves the definition of the necessary hardware and software modules from a number of unified modules to provide for the specified requirements for control of objects of control with minimal costs for the construction of a test and testing station. The main stages of the method include: determining the source set of unified hardware and software modules; development of special hardware-software modules; the synthesis of the structure of the control and testing station as a set of hardware-software modules, which provides the specified requirements for the reliability of control and duration of control with a minimum cost of the test and testing station; selection of the base unit control and test station computer and control program development; hardware construction and complex setup of control and testing station. This developed method allows to construct a promising universal automated control and testing station with variable configuration, which will be able to carry out automated control and diagnostics of malfunctions of all samples of missile weapons, which are on the arming of the Ukrainian armed forces and the advanced missiles currently under development.

Keywords: *control-test station, object of control, hardware-software module.*

References

1. Ghryb D.A. Udoskonalennja metodiv tekhnichnoji ekspluataciji i remontu jak osnova pidtrymannja bojeghotovogho stanu zenitnogho raketnogho ozbrojennja v suchasnykh umovakh [Tekst] / D. A. Ghryb, B. M. Lanecjkyj, V. V. Luk'janchuk // Nauka i oborona. – 2012. – №3. – S. 55-63. **2. Karpenko D.V.** Stan ta perspektyvy rozvytku zenitnogho raketnogho ozbrojennja Povitrjanykh Syl Zbrojnykh Syl Ukrajiny. // Nauka i tekhnika Povitrjanykh Syl Zbrojnykh Syl Ukrajiny. – 2017. – # 2(27). – S.75–78. **3. Pribyljev Ju.B.,** Sakovych L.V. Pidkhid do pobudovy unifikovanoji universaljnoji avtomatyzovanoji kontroljno-vyprobuvaljnoji stanciji raketnogho ozbrojennja // Naukovo-teoretychnyj ta naukovo-praktychnyj zhurnal "Nauka i oborona". – Kyjiv. – 2017. – #1. – S. 42–48. **4. Barzilovich E. Yu.** Modeli tehnicheskogo obsluzhivaniya slozhnyih sistem / E. Yu.Barzilovich. – M.: Vyissh. shk. 1982. – 230 s.**5. Mesarovich, M.** Obschaya teoriya sistem: matematicheskie osnovyi. [Tekst] / M. Mesarovich, I. Takahara // Per. s angl. M.: "Mir", 1978. – 312 s. **6. Bertalanfi, L. fon.** Obschaya teoriya sistem – kriticheskiy obzor. // Issledovaniya po obschey teorii sistem: Sbornik perevodov / Obsch. red. V. N. Sadovskogo i E. G. Yudina. – M.: Progress, 1969. – S. 23-82. **7. Gaydes, M. A.** Obschaya teoriya sistem. (Sistemyi i sistemnyiy analiz) [Tekst] / M.A. Gaydes. // – M.: Globus-Press, 2005. – 201 s. **8. Permjakov O. Ju.**, Pribyljev Ju.B., Djubanov O.O. Modelj systemy diaghnostuvannja, tekhnichnogho obslughovuvannja ta remontu skladnykh tekhnichnykh system vijsjkovogho pryznachennja. // Nauka i oborona. – 2016. – # 2. – S. 48–52. **9. Zherdjev M.K.,** Vyshnivsjkyj V.V., Pampukha I.V., Skujbida O.Ju. Naprjamy rozvytku system kontrolju tekhnichnogho stanu i diaghnostuvannja skladnykh tekhnichnykh system // Zb. nauk. pracj VIKNU imeni Tarasa Shevchenka. – 2006. – # 3. – S. 22–25. **10. Gnedov G.M.,** Rosenbauli O.B., Shumov U.A. Proektirovanie system kontrilya raket. - M.: Mashinostroenie, 1975. – 224 s. **11. Ponomarev N.N.,** Frumkin I.S., Gusinskij Proektirovanie vneshnih sredsv avtomatizirovanogo kontrolya radioelektronogo oborudovaniya . – M.: Radio i svaz. – 1984. – 296 s. **12. DSTU 2389–94.** "Tekhnichne diaghnostuvannja ta kontrolj tekhnichnogho stanu. Osnovni terminy ta vyznachennja".

УДК 629.76

[1]Михайло Юрійович Ракушев (доктор технічних наук, с.н.с.)
[2]Сергій Валентинович Ковбасюк (доктор технічних наук, с.н.с.)

[1]Національний університет оборони України імені Івана Черняховського, Київ, Україна
[2]Житомирський військовий інститут імені С.П.Корольова, Житомир, Україна

ШЛЯХИ УДОСКОНАЛЕННЯ ТРАЄКТОРНОЇ ОБРОБКИ ДЛЯ КОСМІЧНИХ АПАРАТІВ ВИДОВОГО СПОСТЕРЕЖЕННЯ В СИСТЕМІ КОНТРОЛЮ ТА АНАЛІЗУ КОСМІЧНОЇ ОБСТАНОВКИ

Ведення гібридної війни проти України засвідчує, що використання космічних систем суттєво впливає на стан забезпеченості національної безпеки та оборони. Важливим питанням при застосуванні власних та протидії іноземним космічним системам є знання обстановки, що складається у навколоземному космічному просторі. В Україні для вирішення цього питання створено Систему контролю та аналізу космічної обстановки, центральним завданням якої є ведення каталогу космічних об'єктів.

Основу каталогу космічних об'єктів складають орбітальні параметри руху космічних об'єктів. За даними з цього каталогу проводиться оповіщення про прольоти іноземних космічних апаратів видового спостереження, що дозволяє звести до мінімуму виток відповідної інформації оборонного та народногосподарського характеру. Для якісного вирішення завдання оповіщення необхідно забезпечити високі характеристики з точності ведення каталогу космічних об'єктів.

На теперішній час, для визначення орбітальних параметрів руху космічних об'єктів використовуються підходи засновані на методі найменших квадратів. Вихідним припущенням при використанні зазначеного підходу є нормальний закон розподілу похибок траєкторних вимірювань. Останні дослідження свідчать, що таке припущення є припустимим для оптико-електронних засобів, і обмежено виконується для радіолокаційних засобів. Зазначене, призводить до незадовільних характеристик точності сумісної обробки траєкторних вимірювань і, відповідно, точності ведення каталогу космічних об'єктів та оповіщення про прольоту іноземних космічних апаратів видового спостереження.

У статті розглядаються шляхи до удосконалення проведення обробки траєкторних вимірювань від різнотипних вимірювальних засобів в системі контролю та аналізу космічної обстановки щодо підвищення точності ведення каталогу космічних об'єктів для якісного вирішення завдання оповіщення про прольоти космічних апаратів видового спостереження.

Ключові слова: *космічний об'єкт, траєкторні вимірювання, узгоджена обробка, орбітальні параметри, диференціальні перетворення, система контролю та аналізу космічної обстановки.*

Вступ

Забезпечення розвитку сучасних космічних технологій в Україні є важливим чинником, що визначає стратегічне місце держави у світі. Таким чином, актуальним є підвищення ефективності використання національного космічного потенціалу для вирішення нагальних завдань які відносяться до сфери національних інтересів. Зазначений аспект, ще більше загострився за умов збройної агресії проти України, так-як використання космічних систем суттєво впливає, на ефективність дій збройних сил зокрема, та на стан забезпечення національної безпеки та оборони у цілому.

Важливим питанням при застосуванні власних та протидії іноземним космічним системам є знання обстановки, що складається у навколоземному космічному просторі.

Постановка проблеми. На сучасному етапі використання космічного простору, повні системи контролю космічного простору (ККП) мають США (на її супроводженні знаходиться більше 40000 КО) та РФ. Розвиває власну систему ККП КНР, створює її елементи Європейське космічне агентство та багато інших країн [1, 2].

В Україні, завдання моніторингу космічного простору виконує система контролю та аналізу космічної обстановки (СКАКО), яка є стратегічною системою держави та призначена для стеження за усіма доступними космічними об'єктами (КО) штучного походження в навколоземному космічному просторі та діями іноземних країн з його використання [1, 3].

Організаційно в більшості країн системи ККП, підпорядковані воєнним відомствам. СКАКО входить до Державного космічного агентства України, яке виконує завдання, у тому числі, в інтересах національної безпеки та оборони.

Структурно СКАКО являє собою сукупність вимірювальних засобів, що системно об'єднані єдиним пунктом управління та обробки вимірювань. Центральною задачею СКАКО є ведення каталогу КО, яка передбачає інвентаризацію КО, що знаходяться у навколоземному просторі, у тому числі, селекцію

діючих космічних апаратів (КА): їх ідентифікацію, визначення цільового призначення, національної приналежності та т.і [1].

Основними вимогами, що висуваються до каталогу КО є його повнота, точність та оперативність оновлення.

На теперішній час, одним з першочергових завдань, що виконується на основі даних з каталогу КО для у сфері національної безпеки та оборони є проведення оповіщення про прольоти іноземних КА видового спостереження, що дозволяє зменшити виток інформації закритого характеру. Для проведення оповіщення використовується вся інформація з каталогу КО: орбітальні параметри та класифікаційні ознаки КА, його державна приналежність та характеристики бортової апаратури.

Аналіз останніх досліджень і публікацій. Для якісного вирішення завдання з оповіщення про прольоти іноземних космічних апаратів видового спостереження, необхідно забезпечити високі характеристики точності ведення каталогу КО. Зазначені характеристики каталогу КО в СКАКО визначаються можливостями наземних вимірювальних засобів з проведення траєкторних вимірювань та порядком їх подальшої сумісної обробки [4, 5].

Особливостями національної СКАКО є [1, 5]: по-перше, до її складу входить обмежена кількість різнотипних (радіолокаційних та оптико-електронних) вимірювальних засобів які є високовартісними та складними системами; по-друге, усі вимірювальні засоби дислоковані на географічно обмеженій державним кордоном території.

Зазначене визначає необхідність проведення складної обробки усіх наявних траєкторних вимірювань які (відповідно особливостей СКАКО): по-перше, отримані на основі різних фізичних принципів з суттєво різними характеристиками точності; по-друге, мають значні часові інтервали рознесення.

Описані особливості СКАКО ще більше ускладнили завдання ведення каталогу КО після тимчасової окупації Криму РФ, де дислоковані біля 40% вимірювальних засобів СКАКО.

На теперішній час, основними в СКАКО, є алгоритми обробки траєкторних вимірювань на основі методу найменших квадратів [5]. Однак, результуюча точність проведення обробки траєкторних вимірювань на їх основі вже не задовольняє високим сучасним вимогам, які висуваються до характеристик каталогу КО з боку споживачів інформації СКАКО, що виконують завдання у сфері національної безпеки та оборони. Все це, суттєво загострюється при веденні проти України агресивної гібридної війни та втрати частини національної території на якій дислокована значна частина вимірювальних засобів СКАКО.

Метою статті є пошук шляхів підвищення точності визначення орбітальних параметрів руху КО на основі обробки траєкторних вимірювань від різнотипних вимірювальних засобів СКАКО для ведення каталогу КО та якісного вирішення завдання оповіщення про прольоти КА видового спостереження. Зазначена мета є актуальною, за умов збройної агресії проти України та незначних вітчизняних фінансових спроможностях щодо кількісного нарощування наземних вимірювальних засобів СКАКО

Виклад основного матеріалу дослідження.

На теперішній час, для визначення орбітальних параметрів руху КО при обробці траєкторних вимірювань, використовуються підходи засновані на методі найменших квадратів (у більш загальному вигляді методі максимальної правдоподібності), що дозволяє отримувати кінцеві алгоритми траєкторної обробки які характеризуються задовільною точністю при прийнятній обчислювальній складності. При цьому, одним з вихідних припущень, що визначає можливість використання описаного підходу є нормальний закон розподілу похибок траєкторних вимірювань які отримуються вимірювальними засобами спостереження за КО. Останні дослідження визначають, що таке припущення є припустимим для оптико-електронних засобів, і обмежено виконується для радіолокаційних засобів [6]. Зазначене призводить до неможливості підвищення точності сумісної обробки траєкторних вимірювань від різнотипних засобів в СКАКО на існуючих підходах.

Крім вимоги з точності на характеристики алгоритмів обробки траєкторних вимірювань, додатково, накладається обмеження щодо їх прийнятної обчислювальної складності для забезпечення можливості їх реалізації на ЕОМ. Останнє обмеження є суттєвим, так як СКАКО є складною інформаційною системою масового обслуговування високої пропускної здатності, що працює у реальному масштабі часу. Це обумовлює те, що ведення каталогу КО для великої кількості КО вимагає наявності високопродуктивної ЕОМ вартість якої може бути занадто великою [4].

У цілому, за рахунок задовільної точності при прийнятній обчислювальній складності, що забезпечує можливість їх реалізації на ЕОМ, алгоритми обробки траєкторних вимірювань на основі методу найменших квадратів на теперішній час є основними в СКАКО (описаний підхід є основним і в системі контролю космічного простору РФ) [4]. Можна стверджувати, що зазначений підхід до проведення обробки траєкторних вимірювань на теперішній час досяг своїх максимальних характеристик з точності визначення орбітальних параметрів руху КО. З іншого боку, до точності ведення каталогу КО, з боку споживачів інформації СКАКО (насамперед, які виконують завдання у сфері національної безпеки та оборони) висуваються постійно зростаючи вимоги (наведена тенденція має місце і

в інших країнах які мають системи контролю космічного простору) [6].

В основі підходів до побудови алгоритмів обробки траєкторних вимірювань для визначення орбітальних параметрів руху КО лежить прийнятий критерій якості, який визначає відповідний статистичний метод траєкторної обробки. Вибір такого критерію обумовлюється рядом факторів, основними з яких є умови проведення вимірювань (спосіб комбінування похибок вимірювань та їх характеристики) [7]. Часто, на практиці, при виборі критерію якості, крім вказаних вище припущень, робляться ще сильніші припущення, насамперед, про вигляд кореляційної матриці похибок вимірювань. Як правило вважається, що вона є діагональною, або, квазідіагональною.

Суттєвим недоліком описаних підходів до обробки траєкторних вимірювань є використання сильних, і часто невиправданих припущень про вигляд законів розподілу та кореляційних матриць похибок вимірювань. Тому, ці підходи стають малоефективними при високих вимогах до точності визначення орбітальних параметрів КО.

Зазначена проблемна ситуація, щодо невідповідності між реальними умовами проведення траєкторної обробки та використовуваними при теоретичних побудовах основними припущеннями досліджувалась у працях П.Є.Ельясберга (Інституту космічних досліджень Академії наук СРСР) [8], одним з базових положень яких є те, що для похибок вимірювань задаються тільки області в яких вони знаходяться. В описаній постановці для обробки траєкторних вимірювань використовуються алгоритми на основі мінімаксного критерію якості, а самі оцінки автор називає – гарантованими.

Недоліками мінімаксного підходу є те, що отримані в результаті границі можливих значень похибок визначення величин параметрів, що оцінюються є, занадто розширеними та те, що у ньому погано використовуються інформаційні можливості всіх проведених траєкторних вимірювань, що негативно впливає на точність кінцевих результатів. Зазначені недоліки, призвели до того, що цей підхід не знайшов практичного застосування у системі контролю космічного простору СРСР.

Питанням розвитку мінімаксного підходу та досліджень щодо його практичної реалізації при обробці траєкторної інформації в системі контролю космічного простору РФ, присвячені публікації науковців Інституту прикладної механіки ім. Келдиша та ВАТ “МАК “Вимпел” [6, 9]. Зазначене обумовлене тим, що похибки вимірювань радіолокаційних засобів спостереження за КО значно ближчі до рівномірного закону, ніж до нормального. Запропонований у цих публікаціях підхід є ефективнішим за метод найменших квадратів щодо точності визначення орбітальних параметрів руху КО. Автори називають свій підхід нестатистичним [6]. Основним недоліком нестатистичного підходу є те, що його результуюча обчислювальна складність, у порівнянні з методом найменших квадратів, є суттєво вищою (до 2-х порядків). Саме цей недолік, через можливості наявних обчислювальних засобів, до теперішнього часу, не дозволяв його впровадження в системі контролю космічного простору РФ.

В Україні, проблематиці щодо відмови від припущення про нормальний закон розподілу похибок траєкторних вимірювань присвячені публікації Жечева М.М. (Інститут технічної механіки НАН України та ДКА України) та Шептуна А.Д. (ДКБ “Південне”). Автори, називають розроблений підхід – метод узгоджених вимірювань [10]. Відмінною особливістю цього підходу є використання в алгоритмі обробки траєкторних вимірювань матриці Якобі часткових похідних від вимірювальних функцій за шуканими параметрами орбіти КО, що дозволяє провести оцінку характеристик точності визначення орбітальних параметрів руху КО. Узгоджений підхід підвищує точність визначення орбітальних параметрів руху КО у порівнянні з методом найменших квадратів. Однак, його основним недоліком є занадто висока обчислювальна складність (яка додатково підвищується при визначенні матриці Якобі), що значно ускладнює його реалізацію в СКАКО. Окремо слід зазначити, що узгоджений підхід не застосовувався для обробки траєкторних вимірювань від різнотипних вимірювальних засобів.

Однією з основних складових алгоритму траєкторної обробки, яка напряму визначає його результуючу обчислювальну складність, є процедура прогнозування руху КО [7]. Прогнозування руху КО проводиться на основі інтегрування диференціального рівняння, що описує його орбітальний рух. На теперішній час у вітчизняній практиці, для високоточного прогнозування руху КО, використовуються числові кінцево-різницеві методи (а саме, 7-ми етапний метод Адамса, що використовується за екстраполяційно-інтерполяційною схемою, розгін якого проводиться методом Рунге-Кутта 4-го порядку). Основним недоліком числових методів є їх висока обчислювальна складність, який ще більше підсилюється при розрахунку матриці Якобі.

Якщо розглянути останні дослідження щодо впровадження інших методів інтегрування звичайних диференціальних рівнянь у практику рішення завдання прогнозування руху КО, то можна зазначити, що одними з перспективних є методи на основі диференціальних перетворень академіка НАН України Г.Є. Пухова [11]. Використання диференціальних перетворень для прогнозування руху КО, у порівнянні з традиційними числовими методами, дозволяє досягти скорочення обчислювальних витрат на прогнозування. Але, відомі методи на їх основі, не

враховують всіх особливостей диференціальних рівнянь руху КО ближнього космосу, що у підсумку, знижує їх обчислювальну ефективність.

У цілому, віддаючи перевагу вітчизняним науковим напрацюванням, можна зазначити, що дослідження з удосконалення описаного вище узгодженого підходу щодо обробки траєкторних вимірювань від різнотипних вимірювальних засобів в СКАКО та зменшення його обчислювальної складності на основі використання математичного апарата диференціальних перетворень є пріоритетними.

Висновки й перспективи подальших досліджень

Таким чином, визначені шляхи підвищення точності визначення орбітальних параметрів руху КО на основі обробки траєкторних вимірювань від різнотипних вимірювальних засобів СКАКО для ведення каталогу КО та якісного вирішення завдання оповіщення про прольоти КА видового спостереження. Впровадження зазначених шляхів дозволить реалізувати:

обробку траєкторних вимірювань від різнотипних за фізичними принципами функціонування засобів, а саме: оптико-електронних та радіолокаційних;

обробку траєкторних вимірювань які мають різні характеристики похибок вимірювань та не вимагають прийняття нормального закону їх розподілу;

можливість розробки алгоритмів траєкторної обробки які мають прийнятну для реалізації на ЕОМ обчислювальну складність.

Перспективними напрямами подальших досліджень є безпосередня розробка методів та кінцевих алгоритмів узгодженої траєкторної обробки з використанням диференціальних перетворень. Та подальша оцінка їх ефективності для вирішення завдання оповіщення про прольоти КА видового спостереження.

Література

1. Основи побудови системи контролю та аналізу космічної обстановки / **І.Д. Варламов, В.В. Зуйко та ін.** – К.: НУОУ, 2015. – 221 с. 2**. С.С. Вениаминов**. Космический мусор - угроза человечеству/ **Вениаминов С.С.** – М.: Механика управление и информатика, 2013. – 208 с. 3. Розпорядження № 238 КМ України від 30.03.2011 р. Про затвердження Концепції реалізації державної політики у сфері космічної діяльності на період до 2032 року. 4. **Хуторовский З.Н.** Методы обработки измерений при каталогизации КО в ЦККП / **З.Н. Хуторовский.** – М., 2009. – 36 с. 5. **Каневский Л.Б., Ковбасюк С.В.** Аналіз особливостей ведення каталогу космічних об'єктів за інформацією від вітчизняних оптичних засобів / **Л.Б. Каневский, С.В. Ковбасюк** // Вісник ЖДТУ. – Ж: ЖДТУ, №1 (56). 2011. С. 50-55. 6. **Режим доступу** http://lfvn.astronomer.ru/report/0000076/Vimpel.pdf.

7**. В.Н. Брандин, А.А. Васильев, А.А. Куницкий.** Экспериментальная баллистика космических аппаратов / **Брандин В.Н., Васильев А.А., Куницкий А.А.** – М.: Машиностроение, 1984. – 262 с. 8. **Эльясберг П.Е.** Определение движения по результатам измерений / **П.Е. Эльясберг.** – М.: Наука, 1976. – 416 с. 9. **Режим доступу** http://www.vimpel.ru/nauchnie-trudi-i-publikatsii/. 10. **М.М. Жечев, А.Д. Шептун.** Метод согласованных измерений определения движения космических летательных аппаратов / **Жечев М.М., Шептун А.Д.** // Техническая механика. – Днепропетровск: ИТМ НАНУ НКАУ, №2. 2002. С. 36-44. 11. **Ракушев М.Ю.** Прогнозування руху космічних апаратів на основі диференціально-тейлорівських перетворень: монографія / **М. Ю. Ракушев**. – Ж. Видавець О.О.Євенок, 2015. – 324 с.

ПУТИ УСОВЕРШЕНСТВОВАНИЯ ТРАЕКТОРНОЙ ОБРАБОТКИ ДЛЯ КОСМИЧЕСКИХ АППАРАТОВ ВИДОВОГО НАБЛЮДЕНИЯ В СИСТЕМЕ КОНТРОЛЯ И АНАЛИЗА КОСМИЧЕСКОЙ ОБСТАНОВКИ

[1]Михаил Юрьевич Ракушев *(доктор техн. наук, с.н.с, доцент кафедры)*
[2]Сергей Валентинович Ковбасюк *(доктор техн. наук, с.н.с., п.н.с. научного центра)*

[1]Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина
[2]Житомирский военный институт имени С.П.Королева, Житомир, Украина

Ведение гибридной войны против Украины показывает, что использование космических систем существенно влияет на состояние обеспеченности национальной безопасности и обороны. Важным вопросом при применении собственных и противодействия иностранным космическим системам является знание обстановки, которая складывается в околоземном космическом пространстве. В Украине для решения этого вопроса создана Система контроля и анализа космической обстановки, центральной задачей которой является ведение каталога космических объектов.

Основу каталога космических объектов составляют орбитальные параметры движения космических аппаратов. По данным из этого каталога производится оповещение о пролетах иностранных космических аппаратов видового наблюдения, что позволяет свести к минимуму утечку соответствующей информации оборонного и народнохозяйственного характера. Для качественного решения задачи оповещения необходимо обеспечить высокие характеристики по точности ведения каталога космических объектов.

В настоящее время, для определения орбитальных параметров движения космических объектов, используются подходы основанные на методе наименьших квадратов. Исходным предположением при

использовании указанного подхода является нормальный закон распределения погрешностей траекторных измерений. Последние исследования показывают, что такое предположение допустимо для оптико-электронных средств, и ограничено выполняется для радиолокационных средств. Указанное, приводит к неудовлетворительным характеристик точности совместной обработки траекторных измерений и, соответственно, точности ведения каталога космических объектов и оповещения о пролетах иностранных космических аппаратов видового наблюдения .

В статье рассматриваются пути к совершенствованию проведения обработки траекторных измерений от разнотипных средств измерений в системе контроля и анализа космической обстановки по повышению точности ведения каталога космических объектов для качественного решения задачи оповещения о пролетах космических аппаратов видового наблюдения.

Ключевые слова: *космический объект, траекторные измерения, согласованная обработка, орбитальные параметры, дифференциальные преобразования, система контроля и анализа космической обстановки.*

Ways of improvement of trajectory processing for space observation devices in the Space environment control system

[1]***Mikhailo Yu. Rakushev*** *(Doctor of Technical Science, Senior researcher, Associate professor of chair)*
[2]***Sergei V. Kovbasjuk*** *(Doctor of Technical Science, Senior researcher, Leading researcher of research centre)*

[1]***National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine***
[2]***Zhitomir Military Institute named after S.P.Korolev, Zhitomir, Ukraine***

Driving a hybrid war against Ukraine shows that the use of space systems has a significant impact on the state of national security and defense. An important issue when using own and countering foreign space systems is the knowledge of the near-earth space environment. In Ukraine, the Space Environment Control System (SECS) was created to address the issue.

The main task of the SECS is to maintain a space object directory based on orbital parameters of the movement of space objects (SO). According to the data from this catalog, alerts are made of spans of foreign satellite vehicles of species observation, which minimizes the turn of relevant information of defense and national economic nature. For qualitative solution of the problem of notification it is necessary to ensure high characteristics of the accuracy of the catalog of SO.

At present, approaches for determining the orbital parameters of the SO are based on the least squares method. The basic assumption for using this approach is the normal law of errors in trajectory measurements. Recent studies indicate that this assumption is acceptable for optoelectronic devices, and is limitedly used for radar equipment. The said, leads to unsatisfactory characteristics of the accuracy of the coherent processing of trajectory measurements and, accordingly, the accuracy of the catalog of SO and the notification of the flight of foreign spacecraft of species surveillance.

The article considers ways to improve the processing of trajectory measurements from different types of measuring instruments in SECS in order to improve the accuracy of the catalog of space objects for the qualitative solution of the problem of alert of spatial objects of satellite observation devices.

Keywords: *Space object, trajectory measurements, coherent processing, orbital parameters, differential transformations, the Space Environment Control System*

References

1. Varlamov I.D., Zuiko VV, etc. (2015), Fundamentals of the system of control and analysis of the space environment. [Osnovy pobudovy systemy kontrolyu ta analizu kosmichnoyi obstanovky], K.: NUOU, 221 p. **2. Veniaminov S.S.** (2013), Space debris is a threat to humanity [Kosmicheskiy musor - ugroza chelovechestvu]. - Moscow: Mechanics of Control and Informatics, - 208 p. **3. Decree** № 238 of the Cabinet of Ministers of Ukraine as of March 30, 2011 the Consept of state space policy realization for the period to 2032. **4. Khutorsky Z.N.** (2009), Methods of processing measurements in the cataloging of SO in the *SESC*. [Metody obrabotki izmereniy pri katalogizatsii KO v TSKKP]. - M. - 36 p. **5. Kanevsky L. B., Kovbasyuk S.V.** (2011). Analysis of the peculiarities of cataloging space objects according to information from domestic optical means. [Analiz osoblyvostey vedennya katalohu kosmichnykh ob□yektiv za informatsiyeyu vid vitchyznyanykh optychnykh zasobiv]. Bulletin of ZhDTU. ZhDTU, No. 1 (56). S. 50-55. **6. Access** mode http://lfvn.astronomer.ru/report/0000076/Vimpel.pdf. **7. Brandin V.N., Vasiliev A.A., Kunitsky A.A.** (1984). Experimental ballistics of space vehicles. [Eksperimental'naya ballistika kosmicheskikh apparatov]. Moscow: Mechanical Engineering, - 262 p. **8. Elyasberg P.E.** (1976). Determination of motion based on measurement results. [Opredeleniye dvizheniya po rezul'tatam izmereniy]. – M.: Nauka, - 416 p. **9. Access** mode http://www.vimpel.ru/nauchnie-trudi-i-publikatsii/.
10. Zhechev M.M., Sheptune A.D. (2002). Method of consistent measurements of the motion of spacecraft. [Metod soglasovannykh izmereniy opredeleniya dvizheniya kosmicheskikh letatel'nykh apparatov]. Technical mechanics. - Dnipropetrovsk: ITM NASU, N2. P. 36-44. **11. Rakushev M.Yu** (2015). Spacecraft motion prediction on the basis of the taylor differential transformations: monograph. [Prohnozuvannya rukhu kosmichnykh aparativ na osnovi dyferentsial no-teylorivs kykh peretvoren : monohrafiya] - Zh. Publisher O.O.Yevenok, - 324p.

УДК 629.7:001.57.001.63

Петро Васильович Фриз *(канд. техн. наук, доцент)*

Житомирський військовий інститут ім. С. П. Корольова, Житомир, Україна

УДОСКОНАЛЕНИЙ НАУКОВО-МЕТОДИЧНИЙ АПАРАТ ДЛЯ МОДЕЛЮВАННЯ НЕЗБУРЕНОГО РУХУ КОСМІЧНИХ АПАРАТІВ

У статті систематизовано та вдосконалено відомий науково-методичний апарат для моделювання незбуреного руху космічних апаратів (КА) у прикладних завданнях як на етапах створення космічних систем (КС), так і під час їх цільового застосування. Значно розширено математичний апарат для моделювання просторо-часового положення КА за рахунок модифікацій базових векторів. Аналітичні викладки доповнено переходами між векторами за допомогою оригінальних гіперграфів, що суттєво спрощує процес моделювання. Наведено методики перерахунків одних елементів орбіт в інші, розкрито підхід до розв'язку трансцендентного рівняння Кеплера методом ітерацій. Запропоновано алгоритм переходу від безперервних функцій польотного часу до їх дискретної форми.

Ключові слова: *незбурений рух; моделювання; параметри орбіт; вектор просторово-часового положення; космічний апарат; TLE-файли.*

Вступ

Відомо, що на етапах розроблення та цільового застосування КС математичне моделювання як інструмент їх дослідження відіграє ключову роль, оскільки "замінює" ще не створені КС або "наближує" до персоналу вже існуючі віддалені космічні засоби, що функціонують у складних умовах.

Особливо ефективним видається моделювання *орбітального руху* КА, оскільки для цього існує добре відпрацьований математичний апарат, а також використовуються макети, посібники, кінцеві формули, готові програмні продукти та ін.

При цьому традиційно вважається, що в першу чергу варто досліджувати *збурений* (тобто реальний) орбітальний рух КА, оскільки природно він відбувається у багатофакторному просторі зі слабко передбачуваними параметрами і випадковими процесами. І це насправді так.

Однак з методичного погляду простіше, а іноді і достатньо спочатку вивчити або дослідити *незбурений* (ідеальний) рух КА, а далі враховувати збурювальні фактори та їх вплив на орбітальний рух у цілому. З огляду на останнє зауваження дана стаття орієнтована якраз на незбурений орбітальний рух як основу для подальших досліджень реальних КС та процесів у них.

Постановка проблеми. Оскільки в теперішній час теорія незбуреного руху достатньо вивчена, то наслідком цього є добре розвинутий відповідний математичний апарат. Але, на жаль, він розосереджений у різних джерелах, має різну семантику, не завжди пристосований для моделювання та аналітичних розрахунків у реальних умовах.

Через це існує певне *протиріччя* між зростаючими об'ємами математичних викладок теорії орбітального руху та обмеженими можливостями щодо їх практичного використання. Крім того, потребує вдосконалення або розроблення сама методика розрахунків, оцінювання отриманих результатів та прийняття відповідних рішень.

У зв'язку з цим **метою статті** є *систематизація та вдосконалення* відомого науково-методичного апарату для моделювання незбуреного руху КА як передумови подальших досліджень.

Огляд останніх досліджень і публікацій. Питанням моделювання орбітального руху КА присвячено значну кількість сучасних наукових робіт [1–9]. Але в них тільки вибірково висвітлюється застосований математичний апарат або не приводиться взагалі. Більшість із цих робіт мають вузько спрямоване застосування або вирішують тільки окремі специфічні завдання. У ряді зарубіжних розробок [8, 9] акцент зроблено на порядок їх використання без наведення математичних моделей.

Викладення основного матеріалу. У загальному випадку для опису (моделювання) просторово-часового положення КА при їх незбуреному русі використовують вектор орбітальних параметрів або вектор кеплерових елементів еліптичної орбіти вигляду [10, 11]:

$$\mathbf{R_0} = \{a, e, w, i, W, t_П\}, \qquad (1)$$

де a і e – велика піввісь і ексцентриситет еліпса (розміри і форма орбіти);

w, i, W – аргумент перигею, нахилення та інерціальна довгота висхідного вузла (ВВ) орбіти;

$t_П$ – момент знаходження КА в перигеї орбіти.

Але на практиці [12] найчастіше розміри і форму орбіти первісно описують через висоту її апогею H_A та перигею $H_П$. Тому *велика піввісь* еліптичної орбіти обчислюється (рис. 1) як [10]

$$a = 0{,}5\,(r_A + r_П) = 0{,}5(H_A + H_П + 2R_з), \qquad (2)$$

де $r_A = R_з + H_A$ – відстань від центра Землі до апогею орбіти A;

$r_П = R_з + H_П$ – відстань від центра Землі до перигею орбіти П;

$R_з = 6371$ км – середній радіус Землі.

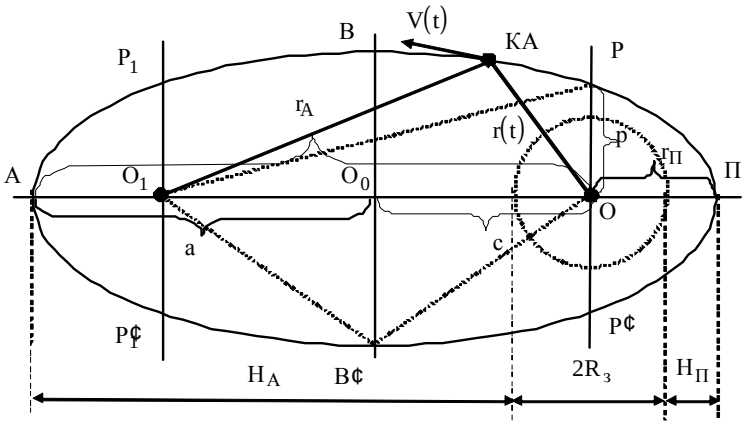


Рис. 1. До визначення елементів орбіти

Для розрахунків *ексцентриситету* можна користуватись залежностями [10]

$$e = \frac{c}{a} = \frac{H_A - H_П}{H_A + H_П + 2R_з} = \frac{H_A - H_П}{2a}, \qquad (3)$$

де $c = OO_0$ – половина міжфокусної відстані еліпса орбіти.

Отже, як видно із аналізу виразів (2) і (3), замість класичного вектора (1) можна користуватись модифікованим вектором, більш пристосованим до реальних задач:

$$\mathbf{R_Ф} = \{H_A, H_П, w, i, W, t_П\}, \qquad (4)$$

Більше того, розміри і форму орбіти можна характеризувати комплексним показником – *фокальним параметром:*

$$p = a(1 - e^2). \qquad (5)$$

Враховуючи (5), можна запропонувати ще один модифікований вектор орбітальних параметрів:

$$\mathbf{R_Ф} = \{a, p, w, i, W, t_П\} = \{p, e, w, i, W, t_П\}. \qquad (6)$$

Вектор (6) менш зручний для практики, оскільки фокальний параметр (5), що входить до його складу, має меншу інформативність порівняно з парою його компонентів $\{a, e\}$ внаслідок їх "згортання" через арифметичні операції над ними. Тому виникає потреба доповнювати його одним із своїх же компонентів.

Із формул (2), (3) та (5) можна отримати і такі співвідношення, придатні для моделювання еліптичних орбіт при незбуреному русі КА:

$$\begin{aligned} r_A &= a(1+e) = p/(1-e); \\ r_П &= a(1-e) = p/(1+e); \end{aligned} \qquad (7)$$

$$\begin{aligned} H_A &= H_П\frac{1+e}{1-e} + 2R_з\frac{e}{1-e}; \\ H_П &= H_A\frac{1-e}{1+e} - 2R_з\frac{e}{1+e}, \end{aligned} \qquad (8)$$

причому формули (8) оприлюднюються вперше.

Поряд з висотами орбіт на практиці часто використовують *сидеричний період* обертання КА, який однозначно обчислюється за формулою [10]

$$T = 2p\sqrt{a^3/m_0}, \qquad (9)$$

де $m_0 = 398602\ км^3/с^2$ – гравітаційний параметр Землі.

Із сидеричним періодом однозначно пов'язана середня кутова швидкість КА, названа в теорії польоту *середнім рухом* КА, який для еліптичних орбіт обчислюється за формулою

$$n = 2p/T = \sqrt{m_0/a^3}. \qquad (10)$$

Тому вектор (1) можна подати як

$$\mathbf{R_Ф} = \{T, e, w, i, W, t_П\} = \{n, e, w, i, W, t_П\}. \qquad (11)$$

Теоретично в разі $e = 0$ говорять про *колові* орбіти, але на практиці скоріш за все використовують *майже колові* орбіти, коли $e \approx 0$, внаслідок чого із залежностей (5) та (7)–(10) отримаємо ряд прикладних формул:

$$\begin{aligned} &H_A \approx H_П \approx H_o; \\ &r_A \approx r_П \approx r_o \approx H_o + R_з; \\ &a \approx H_o + R_з \approx r_o \approx p; \end{aligned} \qquad (12)$$

$$T_o = 2p\sqrt{r_o^3/m_0}; \quad n_o = 2p/T_o = \sqrt{m_0/r_o^3}.$$

Крім того, оскільки у *колових* орбіт не існує апогею і перигею, то аргумент перигею w у складі векторів (1), (4) та (6) втрачає смисл, а замість моменту $t_П$ слід використовувати момент перетинання КА площини екватора t_W.

В таких ситуаціях достатньо користуватись модифікованим вектором

$$\mathbf{R_o} = \{H_o, e \approx 0, i, W, t_W\}. \qquad (13)$$

Якщо *колова* орбіта *пряма приекваторіальна* ($i \approx 0$), що можна подати логіко-аналітичним виразом:

$$(e \approx 0) \dot{U} (i \approx 0) = 1,$$

то втрачають смисл інерціальна довгота ВВ W і момент часу t_W. Натомість для визначеності можна використовувати географічну довготу КА як функцію польотного часу l_t, який відносно конкретного спостерігача являє собою місцевий або всесвітній час.

Тоді вектор (13) набуває вигляду

$$\mathbf{R_{oo}} = \{H_o, e \approx 0, i \approx 0, l_t\}. \qquad (14)$$

І, нарешті, у разі стаціонарних орбіт висота колової екваторіальної орбіти $H_o \approx 35800$ км, тому виконується умова [11]:

$$(e \approx 0) \wedge (i \approx 0) \wedge (H_o \approx 35800) = 1.$$

У цьому випадку КА залишається нерухомим відносно обертової Землі, "зависаючи" на географічній довготі λ_0, а вектор (14) перетворюється до вигляду

$$\mathbf{R_{ст}} = \{H_o \approx 35800, e \approx 0, i \approx 0, \lambda_t \approx \lambda_0\}. \quad (15)$$

На основі такого підходу можна отримати ряд інших векторів, які однозначно описують незбурені орбіти КА та зручні для практичного застосування.

Поряд з вектором кеплерових елементів (1) та його модифікаціями (4), (6) та (11) використовують й інші вектори, які комплексно характеризують параметри орбіти та параметри орбітального руху КА. Одним із них є вектор [10,11]

$$\mathbf{R_t} = \{r(t), V(t), \theta(t), u(t), \Omega, i\}, \quad (16)$$

де $r(t)$ і $V(t)$ – поточні модулі радіуса-вектора КА та його лінійної швидкості (рис. 2);

$\theta(t)$ і $u(t)$ – поточні кут місцевого горизонту та аргумент широти КА;

t – польотний час КА, відлік якого ведеться від моменту $t_П$.

Радіус-вектор КА $\bar{r} = \bar{r}(t)$ з'єднує центр Землі і центр мас КА. Модуль радіуса-вектора змінюється у межах $r_П \le r \le r_A$, а його поточна величина визначається із *рівняння орбіти* у полярних координатах:

$$r(t) = \frac{p}{1 + e\cos J(t)}, \quad (17)$$

де $J(t)$ – істинна аномалія КА (див. далі).

Для колових орбіт при $e \approx 0$ із формули (17) одержимо $r(t) = r_o = p = a = \text{const}$.

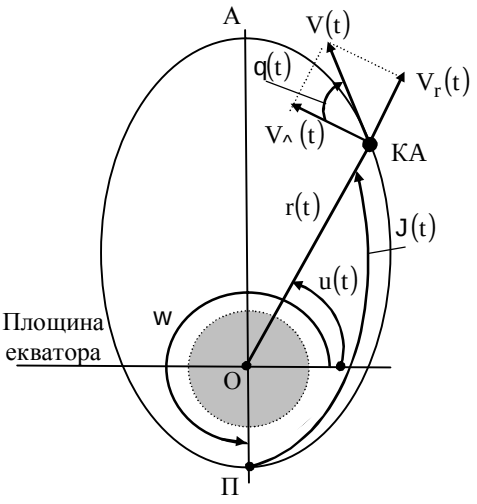


Рис. 2. Зв'язок між параметрами орбітального руху

Лінійна швидкість КА $\bar{V} = \bar{V}(t)$ являє собою швидкість *поступального* руху центра мас КА у площині орбіти відносно інерціального простору. Цей вектор завжди спрямований по дотичній до орбіти у точці знаходження КА (див. рис. 2).

Модуль *лінійної еліптичної* швидкості КА визначається як [10]

$$V(t) = \sqrt{\mu_0 \left(\frac{2}{r(t)} - \frac{1}{a}\right)}. \quad (18)$$

Формула (18) універсальна, оскільки вона придатна і для колових орбіт як часткового випадку еліптичних. Якщо КА рухається по *коловій* орбіті з радіусом $r = a = r_o$, то із рівняння (18) одержимо формулу для його *лінійної колової* швидкості:

$$V_o = \sqrt{\mu_0 / r_o} = \text{const}. \quad (19)$$

Радіальна складова $\bar{V}_r = \bar{V}_r(t)$ являє собою проекцію вектора лінійної швидкості КА на його радіус-вектор $\bar{r}$. Вона характеризує швидкість зміни модуля (довжини) радіуса-вектора КА і може бути обчислена за формулою [10]

$$V_r(t) = \sqrt{\frac{\mu_0}{p}}\, e \sin J(t). \quad (20)$$

Як випливає із цього виразу, для еліптичних орбіт радіальна швидкість може бути додатною (КА віддаляється від центра Землі), від'ємною (КА наближається) або такою, що дорівнює нулю (КА перебуває в апогеї або перигеї).

Максимального значення модуль радіальної швидкості досягає у точках P та P′ (див. рис. 1), тобто при $\sin J(t) = \pm 1$ або $J = 90^0$ і $J' = 270^0$. Для колових орбіт ($e \approx 0$) завжди виконується умова $V_r \approx 0$.

Трансверсальна складова $\bar{V}_\wedge = \bar{V}_\wedge(t)$ – це проекція вектора лінійної швидкості КА на лінію місцевого горизонту (перпендикуляр до радіального напрямку). Вона завжди більше нуля, характеризує швидкість поступального переміщення кінця радіуса-вектора під час руху КА та обчислюється як [10]

$$V_\wedge(t) = \sqrt{\frac{\mu_0}{p}}\,[1 + e\cos J(t)]. \quad (21)$$

Для еліптичних орбіт в апогеї і перигеї трансверсальна швидкість дорівнює лінійній швидкості КА в цих же точках. Для колових орбіт (при $e \approx 0$)

$$V_r \approx 0;\ V_\wedge \approx V \approx \text{const}.$$

Як видно із рис. 2, на еліптичних орбітах для будь-якого моменту часу справедливі такі співвідношення:

$$V_r = V\sin\theta;\ V_\wedge = V\cos\theta;$$
$$V = \sqrt{V_r^2 + V_\wedge^2}. \quad (22)$$

У цих формулах $\theta = \theta(t)$ – *кут місцевого горизонту* – кут нахилення вектора лінійної швидкості до місцевого горизонту, відлічуваний за годинниковою стрілкою.

Як випливає із формул (22), поточні значення цього кута

$$\theta = \arcsin(V_r / V) = \arccos(V_\wedge / V). \quad (23)$$

Кут місцевого горизонту може отримувати додатні значення (при віддаленні КА від центра Землі), від'ємні (при наближенні КА), а також нульові в апогеї і перигеї орбіти. Із виразу (23) видно також, що для колових орбіт кут $\theta(t) \approx 0$.

Аргумент широти КА $u = u(t)$ являє собою поточне кутове положення КА у площині орбіти, відлічуване від площини екватора Землі по ходу орбітального руху КА. Його можна знайти через аргумент перигею ω та істинну аномалію КА $\vartheta = \vartheta(t)$ як

$$u(t) = \omega + \vartheta(t). \qquad (24)$$

Істинна аномалія КА $\vartheta = \vartheta(t)$ теж являє собою кутове положення КА у площині орбіти, але відлічуване від точки перигею орбіти по ходу орбітального руху КА. Її можна знайти через ексцентричну аномалію КА $E = E(t)$ як

$$\vartheta(t) = 2\operatorname{arctg}\left[\sqrt{\frac{1+e}{1-e}}\,\operatorname{tg}\frac{E(t)}{2}\right]. \qquad (25)$$

Ексцентрична і *середня аномалії* пов'язані між собою рівнянням Кеплера, що *явно* описує елементи орбіт і параметри руху КА *в часі* у вигляді

$$E(t) - e\sin E(t) = M(t), \qquad (26)$$

де $M = M(t)$ – середня аномалія КА, яку можна обчислювати через середній рух n та польотний час КА t відносно моменту його перебування в перигеї t_{Π} як

$$M(t) = n(t - t_{\Pi}). \qquad (27)$$

Із викладеного випливає, що вектори (1) та (16) однозначно пов'язані між собою, наочно описують просторово-часове положення КА, мають зрозумілий геометричний смисл і через це широко застосовуються при вивченні теорії орбітального руху та проведенні наукових досліджень.

Однак на практиці найбільш вживаним є підхід до просторово-часового опису КА за допомогою TLE-файлів (*Two-Line Element set* – дворядкові елементи), які можна знайти за адресою: *http://celestrac.com/NORAD/documentation/tle-fmy.htm* [13, 14].

Приклад реального TLE-файла наведено у табл. 1, його структуру подано у табл. 2, а семантику вживаних позначень можна знайти в [10].

Таблиця 1

Реальний TLE-файл з казахського КА KAZEOSAT 1

KAZ 1
1 39731U 14024A 17104.79072753 .00000003 00000-0 14338-4 0 9993
2 39731 98.4208 184.7429 0001376 91.2441 268.8898 14.42003118155755

Таблиця 2

Структура TLE-файлів

Назва КА (не більше 24 символів)										
1	CCCCC	U	YY№№№A	DDDDD.dddddddd	.GGGGGGGG	PPPPPP-P	QQQQQQ-Q	0	SSS	Z
2	CCCCC	iii.iiii	WWWWWWW	eeeeeee	WWW.WWWW	MMM.MMMM	NN.NNNNNNNN	OOOOO		Z

Аналіз змісту TLE-файлів показує, що із їх складу можна виділити лише ті параметри, які подібно векторам (1) та (2) характеризують просторово-часове положення КА:

$$\mathbf{R_{tle}} = \{t_D, i, \Omega, e, \omega, M, N, Q\}, \qquad (28)$$

де t_D – епоха □ момент часу, в який сформовано даний TLE-файл;

M – середня аномалія КА на момент t_D;

N – середньодобовий рух КА (кількість витків орбіти за добу);

$Q = \{G, P, O, D\}$ – решта даних (перша G та друга P похідні від середньодобового руху, кількість витків на епоху O та інші D).

Аналіз векторів (1), (16) та (28) показує, що між ними існує певний взаємозв'язок, що дозволяє однозначно переходити від відомих компонентів одного вектора до шуканих компонентів іншого за схемою: $\mathbf{R_{tle}} \ll \mathbf{R_0}$, $\mathbf{R_0} \ll \mathbf{R_t}$, $\mathbf{R_{tle}} \ll \mathbf{R_t}$, – а далі проводити моделювання за допомогою найбільш придатного із них.

На практиці найчастіше постає завдання переходу від вектора (28) до векторів (1) $\mathbf{R_{tle}} \to \mathbf{R_0}$ та (16) $\mathbf{R_0} \to \mathbf{R_t}$.

Методика переходу $\mathbf{R_{tle}} \to \mathbf{R_0}$ в разі *незбуреного* руху КА може бути такою (рис. 3):

По-перше, при незбуреному орбітальному русі КА елементи i, Ω, e, ω векторів (1) та (28) збігаються і перерахунків не потребують.

По-друге, знайти велику піввісь a для вектора (1) із формули (12) як

$$a = \sqrt[3]{\mu_0 / n^2}, \ [n] = c^{-1}. \qquad (29)$$

По-третє, оскільки в TLE-файлах надається *середньодобовий* рух КА $N = \text{const}$ як кількість витків за середньосонячну добу $T_{сд} = 86400^s$, то для знаходження середнього руху n слід скористатись очевидною залежністю:

$$n = N / T_{сд} = N / 86400^s. \qquad (30)$$

По-четверте, для розрахунків моменту проходження КА через перигей орбіти t_{Π} у складі вектора (1) застосувати формулу (27).

Справді, прийнявши $t = t_D$ і скориставшись відомою із TLE-файла середньою аномалією $M(t) = M(t_D) = M$ та середнім рухом КА (30), із виразу (27) знайдемо

$$t_{\Pi} = t_D - M / n. \qquad (31)$$

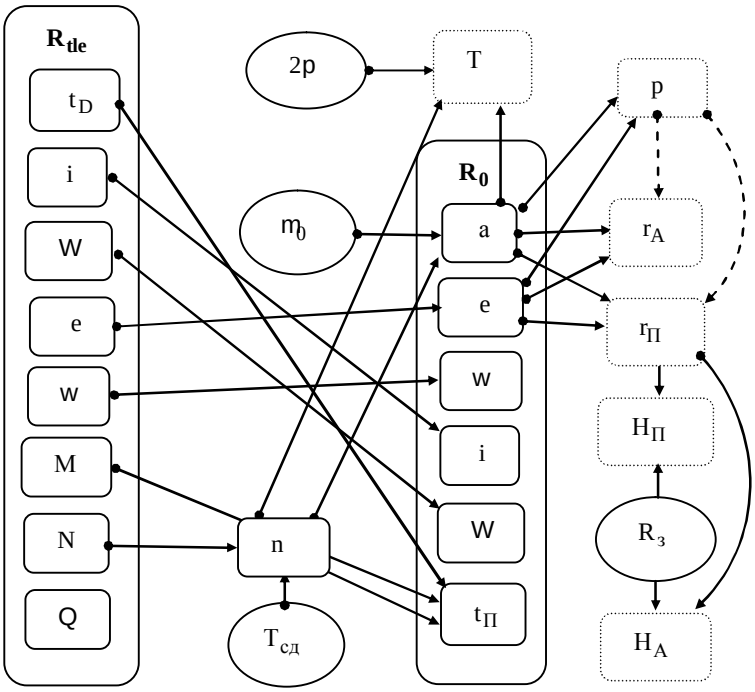


Рис. 3. Гіперграф переходів від вектора $\mathbf{R_{tle}}$ до вектора $\mathbf{R_0}$ та його модифікацій

По-п'яте, при моделюванні безперервних у часі процесів слід перейти від аналогових величин до дискретних за алгоритмом (рис. 4):

$$t_0 = t_п \to t_1 = t_0 + dt \to t_2 = t_0 + 2dt \to \\ \to t_j = t_0 + jdt \to t_J = t_0 + Jdt, \qquad (32)$$

де $j = \overline{0, J}$ – номери дискрет (натуральні числа від 0 до J);

$J \geq 2$ – загальна кількість дискрет (натуральне число);

$dt = Dt / J$ – розмір однієї дискрети (дискретизація рівномірна);

$Dt = |t_к - t_п|$ – заданий часовий інтервал моделювання;

$t_к$, $t_п$ – кінцевий і початковий моменти часу.

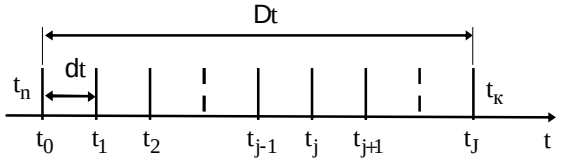


Рис. 4. До перетворення часових інтервалів у дискретну форму

При такому підході формула (27), наприклад, перетвориться до вигляду

$$M(t_j) = n(t_j - t_П), \; j = \overline{0, J}, \; t_j = t_{j-1} + dt, \\ dt = Dt / J, \qquad (33)$$

де $Dt = T$ – сидеричний період обертання КА.

По-шосте, використовуючи формули (5), (7–10) та (12), можна перейти від вектора (1) до його модифікацій (4), (6), (11) або (13–15), елементи яких показано на рис. 3 пунктиром.

Методика переходу $\mathbf{R_0} \to \mathbf{R_t}$ у разі *незбуреного* руху КА полягає у такому (рис. 5):

По-перше, при незбуреному орбітальному русі КА елементи i, W векторів (1) та (16) збігаються і перерахунків не потребують.

По-друге, для зручності перерахунків доцільно від вектора (1) перейти до його розширеної модифікації (див. рис. 5):

$$\mathbf{R_0^*} = \{T, p, a, e, w, i, W, t_П\}, \qquad (34)$$

де T і p – сидеричний період обертання та фокальний параметр, розраховані за формулами (9) та (5) відповідно.

По-третє, через відомий сидеричний період обертання T за формулою (10) отримати середній рух КА n.

По-четверте, оскільки відомий момент часу $t_П$, коли КА перебуватиме в перигеї орбіти, то використовуючи знайдений середній рух n, за формулою (27) з урахуванням (33) знайти середню аномалію КА $M(t_j)$ на будь-який фіксований момент польотного часу $t = t_j$.

По-п'яте, для цього ж моменту із трансцендентного рівняння (26) методом ітерацій обчислити ексцентричну аномалію як

$$E_{i+1}(t_j) = M(t_j) - e \sin E_i(t_j); \; i = \overline{0, I}, \; j = \overline{0, J}, \qquad (35)$$

поклавши $E_0(t_j) = M(t_j)$.

Для практичних цілей досить прийняти $I = 6$ і, отже, остаточним значенням шуканої ексцентричної аномалії вважати $E(t_j) = E_6$.

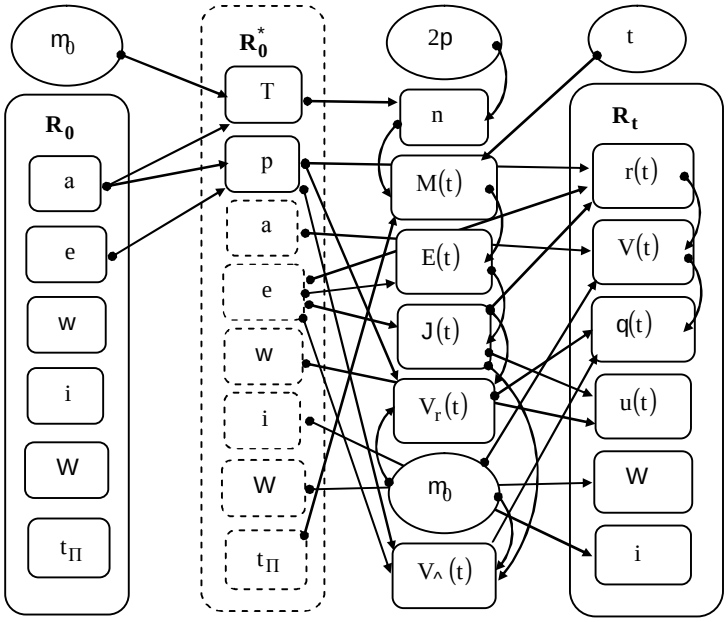


Рис. 5. Гіперграф переходів від вектора $\mathbf{R_0}$ до вектора $\mathbf{R_t}$

По-шосте, за формулою (25) розрахувати істинну аномалію КА $J(t_j)$, а далі за виразом (24) знайти шуканий аргумент широти $u(t_j)$.

По-сьоме, у разі необхідності можна об'єднати гіперграфи, зображені на рис. 4 і 5, і на цій основі здійснити глобальний перехід $\mathbf{R_{tle}} \to \mathbf{R_0} \to \mathbf{R_t}$.

Висновки й перспективи подальших досліджень:

1. У статті систематизовано ряд відомих із теорії орбітального руху КА залежностей та доповнено їх новими, що дало змогу отримати вдосконалений науково-методичний апарат, пристосований для моделювання незбуреного руху КА. Його основу становлять аналітичні залежності, оригінальні алгоритми та методичні рекомендації щодо їх застосування.

2. Цей апарат може стати базовим інструментом для опису і прогнозування збуреного руху КА, а також моделювання їх положення як у космічному просторі, так і відносно заданих наземних об'єктів спостереження і пунктів прийому цільової інформації.

Література

1. Артюшенко М. В. Моделирование и синтез орбитальной группировки космических аппаратов зонального наблюдения территории Украины / М. В. Артюшенко, С. С. Дугин, А. Д. Федоровский // Космічна наука і технологія. – К. : Вид. дім "Akademperiodika", 2011. – Т. 17. – № 5. – С. 50–57. **2. Куренков В. И.** Методы исследования эффективности ракетно-космической техники : электрон. учеб. пособ. / В. И. Куренков, М. Ю. Гоголев. – Самара : Изд-во Самар. гос. аэрокосм. ун-та, 2012. – 285 с. **3. Лабуткина Т. В.** Математическая модель для анализа кинематики сопровождения орбитальных объектов наземными антеннами / Т. В. Лабуткина // Вісник Дніпропетр. ун-ту. Ракетно-космічна техніка. – Т. 17. – 2011. – С. 40–50. **4. Матюшин М. М.** Моделирование сценариев оперативного управления полетом космического аппарата / М. М. Матюшин / Наука и образование. – М. : МГТУ им. Н. Э. Баумана. Эл. №ФС 77-48211, 2011. – С. 1–17. **5. Ручинская Е. В.** Математическое моделирование управляемого движения космических аппаратов : дис. кандидата техн. наук / Е. В. Ручинская. – М. : – 2010. – 175 с. [Электронный ресурс]. – Режим доступа: www.dissercat.com. **6. Сомова Т. Е.** Моделирование и анимация пространственного движения маневрирующего спутника землеобзора / Т. Е. Сомова // Известия Самарского науч. центра РАН. – Самара : Самарский НЦ РАН, 2012. – Т. 14. – № 6. – С. 125–128. **7. Спиридонов А. А.** Моделирование движения сверхмалого космического аппарата / А. А. Спиридонов, В. А. Саечников, И. А. Шалатонин // Гелиофизические исследования. – М. : Институт прикладной геофизики им. акад. Е. К. Федорова. – 2015. – С. 1–4. **8. Stoff S.** Orbitron – Satellite Tracking System // Stoff.pl: website. [Electronic resource]. – Mode of access: http://www.stoff.pl. **9. STK** overview [Electronic resource]. URL: http://www.agi.com/products/by-producttype/ applications/stk/default.aspx. **10. Фриз П. В.** Основи орбітального руху космічних апаратів : підручник / П. В. Фриз. – Житомир : ЖВІ НАУ, 2012. – 348 с. : іл. **11. Фриз П. В.** Теоретико-множинний підхід до опису просторово-часового положення космічних апаратів в задачах спостереження Землі / П. В. Фриз // Наука і техніка Повітряних сил Збройних Сил України : наук.-техн. журнал. – Х. : ХУПС, 2013. – Вип. 1(10). – С. 205–208. **12. Практикум** з використання програмних комплексів Orbitron та WXtrack для моделювання процесів у космічних інформаційних системах / П. В. Фриз, С. П. Фриз. – Житомир : ЖВІ, 2017. – 52 с. **13. NORAD** Two-Line Element Set Format // Celestrak.com: website [Electronic resource]. – Mode of access: http://celestrak.com/NORAD/ documentation/tle-fmt.asp. **14. Hoots F. R.** Models for Propagation of NORAD Element Sets. / F. R. Hoots, R. L. Roehrich // Space track Report no. 3. Colorado Springs: Peterson AFB, CO, 1980. – 91 p [Electronic resource]. – Mode of access : http://www.celestrak.com/NORAD/ documentation/spacetrk.pdf.

УСОВЕРШЕНСТВОВАННЫЙ НАУЧНО-МЕТОДИЧЕСКИЙ АППАРАТ ДЛЯ МОДЕЛИРОВАНИЯ НЕВОЗМУЩЕННОГО ДВИЖЕНИЯ КОСМИЧЕСКИХ АППАРАТОВ

Петр Васильевич Фриз *(канд. техн. наук, доцент, профессор кафедры)*

Житомирский военный институт им. С. П. Королева, Житомир, Украина

В статье систематизирован и усовершенствован известный научно-методический аппарат для моделирования невозмущенного движения космических аппаратов в прикладных задачах как на этапах создания космических систем, так и в процессе их целевого применения. Значительно расширен математический аппарат для моделирования пространственно-временного положения КА за счет модификаций базовых векторов. Аналитические выкладки дополнены переходами между векторами с помощью оригинальных гиперграфов, что существенно упрощает процесс моделирования. Приведены методики пересчета одних элементов орбит в другие, раскрыто подход к решению трансцендентного уравнения Кеплера методом итераций. Предложен алгоритм перехода от непрерывных функций полетного времени до их дискретной формы.

Ключевые слова: *невозмущенное движение; моделирование; параметры орбит; вектор пространственно-временного положения; космический аппарат; TLE-файлы.*

IMPROVED SCIENTIFIC AND METHODICAL APPARATUS FOR MODELING UNBELIEVED MOVEMENT OF SPACE APPLIANCES

Petr V. Frees *(Candidate of Technical Sciences, Associate Professor, Professor of the Department)*

Zhitomir Military Institute named after S. P. Korolev, Zhitomir, Ukraine

In the article, a well-known scientific and methodical apparatus for modeling the unperturbed motion of space vehicles in applied problems both at the creation stages of space systems and in the process of their targeted application is systematized and improved. The mathematical apparatus for modeling the space-time position of the spacecraft due to modifications of the base vectors has been significantly expanded. Analytic calculations are supplemented by transitions between vectors with the help of original hypergraphs, which greatly simplifies the modeling process. Methods are given for recalculating some elements of orbits into others, the approach to solving the Kepler transcendental equation is described by the iteration method. An algorithm for the transition from continuous flight time functions to their discrete form is proposed.

Keywords: *unperturbed motion; modeling; parameters of orbits; vector of space-time position; spacecraft; TLE files.*

References

1. Artyushenko M.V. Modeling and synthesis of the orbital constellation of space vehicles for the zonal observation of the territory of Ukraine / MV Artyushenko, SS Dugin, AD Fedorovskii // Cosmic Science and Technology-Giya. - K.: View. Dim "Akademperiodika", 2011. - T. 17. - № 5. - P. 50-57. **2. Kurenkov V. I.** Methods of researching the effectiveness of rocket and space technology: electron. Training. Help. / VI Kurenkov, M. Yu. Gogolev. - Samara: Samara Publishing House. State. Aerospace. University, 2012. - 285 with. **3. Labutkina T. V.** Mathematical model for the analysis of the kinematics of tracking of orbital objects by terrestrial antennas / TV Labutkina // Visnik Dnipropetr. Un-tu. Rocket and space technology. - T. 17. - 2011. - P. 40-50. **4. Matyushin M. M.** Modeling scenarios for operational control of the space vehicle's flight / MM Matyushin / Science and education. - M.: MSTU them. NE Bauman. El. No. FS 77-48211, 2011. - P. 1-17. **5. Ruchinskaya E. V.** Mathematical modeling of controlled motion of space vehicles: dis. Candidate tehn. Sciences / EV Ruchinskaya. - M.: - 2010. - 175 p. [Electronic resource]. - Access mode: www.dissercat.com. **6. Somova T. E.** Simulation and animation of the spatial motion of the maneuvering earth survey satellite / T. Somova // Izvestiya Samarskogo nauchn. Center of the Russian Academy of Sciences. - Samara: Samara Scientific Center of RAS, 2012. - T. 14. - № 6. - P. 125-128. **7. Spiridonov A. A.** .Modeling of the motion of an ultra-small spacecraft / AA Spiridonov, VA Saechnikov, IA Shalatonin // Heliophysical Investigations. - M.: Institute of Applied Geophysics. Acad. E. K. Fedorova. - 2015. - pp. 1-4. **8. Stoff S**. Orbitron - Satellite Tracking System // Stoff.pl: website. [Electronic resource]. - Mode of access: http://www.stoff.pl. **9. STK** overview [Electronic resource]. URL: http://www.agi.com/products/by-producttype/ applications / stk / default.aspx. **10. P. V. Friz.** Fundamentals of the orbital motion of space vehicles: a textbook / PV Friz. - Zhitomir: ZhVI NAU, 2012. - 348 p. : Ill. **11. P. V. Friz.** The set-theoretic approach to the description of the space-time position of space vehicles in the problems of Earth observation / PV Friz // Science and Technology of the Air Force of the Armed Forces of Ukraine: Sciences.-Tech. Journal. - H.: HUPS, 2013. - Vip. 1 (10). - P. 205-208. **12. Workshop** on the use of Orbitron and WXtrack software complexes for modeling processes in space information systems / PV Friz, SP Friz. - Zhitomir: ZhVI, 2017. - 52 with. **13. NORAD** Two-Line Element Set Format // Celestrak.com: website [Electronic resource]. - Mode of access: http://celestrak.com/NORAD/ documentation / tle-fmt.asp. **14. Hoots F. R.** Models for Propagation of NORAD Element Sets. / F. R. Hoots, R. L. Roehrich // Space track Report no. 3. Colorado Springs: Peterson AFB, CO, 1980. - 91 p [Electronic resource]. - Mode of access: http://www.celestrak.com/NORAD/ documentation / spacetrk.pdf.

УДК 004.932

Худов Геннадій Володимирович [1] ***(докт. техн. наук, професор)***
Худов Владислав Геннадійович [2]
Хижняк Ірина Анатоліївна [1]
Новікова Ірина Вікторівна [3]

[1] ***Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна***
[2] ***Харківський національний університет радіоелектроніки, Харків, Україна***
[3] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

ОЦІНКА ВІДСТАНІ КУЛЬБАКА-ЛЕЙБНЕРА ПРИ ТЕМАТИЧНОМУ СЕГМЕНТУВАННІ ОПТИКО-ЕЛЕКТРОННОГО ЗОБРАЖЕННЯ МЕТОДОМ КАННІ

Результат дешифрування зображень, що отримані з бортових систем оптико-електронного спостереження, залежить від якості сегментування зображень, особливо з урахуванням особливостей їх отримання (різнорідний фон, варіабельність різних частин зображення, наявність шумів). Проаналізовані основні методики, критерії і показники сегментування зображень, їх переваги та недоліки. Запропоновано провести оцінку інформаційного показника (відстані Кульбака-Лейбнера) тематичного сегментування оптико-електронного зображення методом Канні. Проведено аналіз основних етапів методу Канні: згладжування, пошук градієнту, придушення хибних максимумів, подвійна порогова фільтрація, трасування області невизначеності. Наведено результат сегментування оптико-електронного зображення методом Канні, проведено розрахунок відстані Кульбака-Лейбнера на її залежність від масштабного коефіцієнта вихідного зображення.

Ключові слова: *дешифрування, об'єкт; космічний апарат; оптико-електронне зображення; обробка; сегментування; показник ефективності; відстань Кульбака-Лейбнера; метод Канні; згладжування;фільтрація; інформаційний показник; піксель.*

Вступ

В сучасних умовах ведення мережецентричних, гібридних війн, антитерористичної операції на території Донецької та Луганської областей близько 80% розвідувальних завдань, 60% завдань по забезпеченню охорони та 50% завдань по забезпеченню вогневого ураження вирішується за допомогою інформації, що отримується з бортових систем спостереження (безпілотні літальні апарати, космічні системи спостереження) [1, 2].

Ефективність дешифрування інформації, що отримана з бортових систем спостереження, може бути представлена чотирма категоріями [3]:

- «А» - впевнене дешифрування без використання додаткових матеріалів;
- «В» - дешифрування можливе камеральним способом при використанні додаткових матеріалів;
- «С» - дешифрування можливе лише з використанням польового дослідження»
- «D» - дешифрування неможливо.

В таблиці 1 наведені зведені результати можливості дешифрування об'єктів по оптико-електронним зображенням, що отримані з космічних апаратів (КА) Pleiades, WorldView та при виконанні аерофотозйомки з використанням камери VisionMap A3 [3]. Проаналізовано 236 об'єктів наступних типів:

- рельєф суші;
- гідрографія;
- населені пункти;
- соціально-економічні об'єкти;
- дорожні мережі та дорожні споруди;
- рослинний покров та ґрунти.

Таблиця 1

Зведені результати можливості дешифрування об'єктів

Тип вихідних даних	Кількість об'єктів			
	A	B	C	D
КА Pleiades	103	92	21	20
КА WorldView	106	90	19	21
Камера Vision A3	126	78	16	16

З аналізу результатів, наведених в табл. 1, видно, що для трохи менше половини обєктів дешифруються впевнено (категорія «А»), приблизно 10% об'єктів дешифрувати неможливо (категорія «D») та приблизно 50% об'єктів можуть бути дешифровані за допомогою додаткових матеріалів. При наявності навіть додаткових матеріалів складнощі виникають при вирішенні завдання дешифрування різних типів об'єктів, що мають невеликі розміри, точкових та малопротяжних об'єктів та обєктів.

Результат дешифрування зображень, що отримані з бортових систем оптико-електронного спостереження, залежить від якості сегментування зображень, особливо з урахуванням особливостей їх отримання (різнорідний фон, варіабельність різних частин зображення, наявність шумів) [4]. При використанні відомих методів сегментування зображення не завжди вдається забезпечити стійкість методів сегментування до варіацій різних параметрів зображення (топологічних, геометричних,

фотометричних).

Постановка проблеми. Проведемо сегментування оптико-електронного зображення, що отримане з бортової системи оптико-електронного спостереження. У якості методу сегментування оберемо метод Канні [5]. Метод виділення контурів Канні є оптимальним по наступним параметрам [5]:

- критерію виділення контурів – метод повинен виділяти як можна більше існуючих на зображенні границь;
- локалізації країв – контури, що виділені, повинні розташовуватися як можна ближче до границі на зображенні;
- мінімізації кількості відкликів одного краю – кожен контур повинен відмічатися один раз і, якщо можливо, контури не повинні створюватися з причини шумів.

У якості показника ефективності сегментування оберемо інформаційний показник – відстань Кульбака-Лейбнера [6, 7].

Аналіз останніх досліджень і публікацій. Відомо [8, 9], що основні методики сегментування зображень поділяються на:

1. Суб'єктивні.
2. Об'єктивні.
   2.1. Системні.
   2.2. Прямі.
      2.2.1. Аналітичні.
      2.2.2. Емпіричні.
         2.2.2.1. Контрольовані.
         2.2.2.2. Неконтрольовані (автоматичні).

Одним з ключових елементів методики порівняльного тестування є критерій оцінки якості сегментування зображення. На теперішній час основні критерії і показники розроблені для двох основних підходів до сегментування зображення [8, 10, 11]:

1) розділення зображення контурами на області зі схожими характеристиками (в англійській термінології – edge-based methods (boundary-based, contour-based);

2) об'єднання пікселів зображення в групи на основі близькості деяких кількісних ознак (region-based methods).

Для оцінки результатів роботи методів першої групи використовуються, в основному критерії і показники такі ж самі, що і для детекторів границь (такі показники наведені в [8, 9]). Критерії оцінки якості методів сегментування зображення, що відносяться до другої групи наведені в [9].

Основними ознаками якісного сегментування є [8, 9-11]:

- однорідність області по характеристикам (в першу чергу, по кольору та текстурі);
- відмінність значень обраних характеристик для суміжних областей зображення;
- гладкість границь кожного сегменту зображення;
- незначна кількість «дірок» у сегменті.

По відповідності указаним ознакам і класифікуються відомі показники якості сегментування зображення [8].

1. Перша група – це показники, які засновані на порівнянні з еталонним сегментуванням.

1.1. Кількість пікселів, що віднесені при сегментуванні не до свого сегменту. Оцінюється шляхом побудови матриці неточності (таблиця 2) [8]. Стовбці матриці відповідають класу, до якого пікселі дійсно належать, а строки – класу, до якого пікселі віднесені при сегментуванні. Таким чином, правильно класифіковані пікселі відносяться до елементів матриці, що знаходяться на головній діагоналі, неправильно класифіковані – до всіх інших елементів матриці [8].

Таблиця 2

Приклад матриці неточності [8]

	BK	PA	RD	CY	NU	Total
BK	909	2		2		913
PA						
RD			111	10		121
CY	37	3	67	802	1	910
NU				87	419	506
Total	946	5	178	901	420	

Показники, що використовуються при цьому, наступні. Перший – процентне відношення неправильно класифікованих пікселів даного k-го класу до загальної кількості пікселів цього класу на еталонному зображенні (вираз (1)):

$$M_1^k = 100\frac{\left(\sum_{i=1}^{n} C_{ik}\right) - C_{kk}}{\sum_{i=1}^{n} C_{ik}}, \qquad (1)$$

де n - кількість класів;

C_{kk} - кількість правильно класифікованих пікселів k-го класу;

$\sum_{i=1}^{n} C_{ik}$ - кількість пікселів, що дійсно належать до k-го класу.

Другий показник – це процентне відношення пікселів, що помилково віднесені до k-го класу до загальної кількості пікселів других класів на еталонному зображенні (вираз (2)):

$$M_2^k = 100\frac{\left(\sum_{i=1}^{n} C_{ki}\right) - C_{kk}}{\left(\sum_{i=1}^{n}\sum_{k=1}^{n} C_{ik}\right) - \sum_{i=1}^{n} C_{ik}}, \qquad (2)$$

де $\sum_{i=1}^{n} C_{ki}$ - кількість пікселів, що віднесені до k-го класу;

$\sum_{i=1}^{n}\sum_{k=1}^{n} C_{ik}$ - загальна кількість пік селів на зображенні k-го класу;

C_{kk} - кількість правильно класифікованих пікселів k-го класу;

$\sum_{i=1}^{n} C_{ik}$ - кількість пікселів, що дійсно належать до k-го класу.

Третій показник – імовірність помилки сегментування $p(err)$. Імовірність того, що піксель вихідного зображення буде віднесений на сегментованому зображенні до об'єкту $p_s(o)$ може бути представлена виразом (3):

$$p_s(o) = p(o)p(o/o) + p(b)p(o/b), \quad (3)$$

де $p(o)$, $p(b)$ - імовірності того, що випадковим образом обраний піксель вихідного зображення належить об'єкту або фону, при цьому $p(o) + p(b) = 1$;

$p(o/o)$ - імовірність того, що піксель, що належить об'єкту, при сегментуванні також буде віднесений до об'єкту;

$p(o/b)$ - імовірність того, що піксель, що належить фону, при сегментуванні буде помилково віднесений до об'єкту.

Імовірність того, що піксель вихідного зображення буде віднесений на сегментованому зображенні до фону $p_s(b)$ може бути представлена виразом (4):

$$p_s(b) = p(b)p(b/b) + p(o)p(b/o), \quad (4)$$

де $p(b/b)$ - імовірність того, що піксель, що належить фону, при сегментуванні також буде віднесений до фону;

$p(b/o)$ - імовірність того, що піксель, що належить об'єкту, при сегментуванні буде помилково віднесений до фону.

Імовірність $p(err)$ визначається виразом (5):

$$p(err) = p(o)p(b/o) + p(b)p(o/b). \quad (5)$$

В роботі [11] наведено ще декілька узагальнень показника (5) на випадок довільної кількості сегментів.

1.2. Показники, що характеризують неправильне місце розташування класифікованих пікселів. Перший показник - e (вираз (6)):

$$e = \frac{\sqrt{\sum_{i=1}^{N} d_i^2}}{A} x100, \quad (6)$$

де N - кількість помилково класифікованих пікселів;

A - загальна кількість пікселів на зображенні;

d_i - евклідова відстань між i-им помилково класифікованим пікселом, що дійсно відноситься до даного класу.

Інтервал значень, що приймає e: від 0 (при ідеальному сегментуванні) до e_{max}, яке залежить від розмірності зображення n, та розраховується для квадратного зображення розміром (nxn) за виразом (7):

$$e_{max} = \begin{cases} 100\sqrt{\frac{7}{6} - \frac{3}{2n} + \frac{1}{3n^2}}, \text{якщо n - чітне} \\ 100\sqrt{\frac{7}{6} - \frac{3}{2n} - \frac{1}{6n^2} + \frac{1}{2n^2}}, \text{якщо n - нечітне.} \end{cases} \quad (7)$$

Другий показник – FOM (figure of merit) [11] – емпірична відстань даного пікселя від його дійсного розташування. Існують дві різновиди показника FOM – вирази (8), (9):

$$FOM = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{1+\gamma d_i^2}, \quad (8)$$

$$FOM_l = \begin{cases} \frac{1}{N_e}\sum_{i=1}^{N}\frac{1}{1+\gamma d_i^2}, N_e > 0 \\ 1, N_e = 0. \end{cases} \quad (9)$$

де N - кількість пікселів на зображенні;

d_i - відстань i-го пікселя зображення до найближчого пікселя, що віднесений до того ж класу на еталоному зображенні;

γ - масштабний множник;

N_e - помилково класифіковані пікселі.

Існують ще декілька емпіричних показників якості сегментування зображення, наприклад, - показник Хаусдорфа – вираз (10):

$$Hausdorff(I_t, I_s) = \max(h(I_t, I_s), h(I_s, I_t)), \quad (10)$$

де I_t, I_s - множини пікселів різних областей;

$h(I_s, I_t)$ - відстань між відповідними областями;

$$h(I_t, I_s) = \max_{t_i \in I_t} \min_{s_i \in I_s} \|t_i = s_i\|. \quad (11)$$

Якщо $h(I_t, I_s) = d$, то це означає що всі пікселі множини I_t знаходяться не дальше, ніж на відстані d від множини пікселів I_s.

Використовують також показники [11]:

- RMS (root mean squared error) – середньоквадратична похибка (вираз (12)):

$$RMS(I_1, I_2) = \left[\frac{1}{card(X)}\sum_{x \in X}(I_1(x) - I_2(x))^2\right]^{\frac{1}{2}}, \quad (12)$$

де $card(X)$ - кількість пікселів в множині X;

$I_i(x)$ - інтенсивність пікселя x в I_i;

X - множина пікселів на сегментованому зображенні;

- показник Баддели (вираз (13):

$$Baddeley(I_1, I_2) = \left[\frac{1}{card(X)}\sum_{x \in X}\left|d(x, I_1) - d(x, I_2)\right|^p\right]^{\frac{1}{p}}, \quad (13)$$

де $d(x, I) = \min_{y \in I} d(x, y)$;

$p \geq 1$,

та інші. Показники за виразами (8)-(13) також називають супервізорними показниками оцінки якості сегментування зображення [8].

1.3. Показники, що характеризують ступінь фрагментації зображення (вираз (14)):

$$FRAG = \frac{1}{1+\left|a(n_R - n_l\right|^b}, \qquad (14)$$

де n_R - кількість сегментів на сегментованому зображенні;

n_l - кількість сегментів на еталонному зображенні;

a, b - масштабні коефіцієнти.

1.4. Показники, що характеризують значення характеристик вихідного зображення, що використовуються для сегментування (вираз (15)):

$$FOC = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{1+\left|y\,(f_i - m_j)\right|^d}, \qquad (15)$$

де N - кількість пікселів на зображенні;

f_l - значення інтенсивності пікселя i вихідного зображення;

m_j - репрезентативне значення інтенсивності j-го сегменту, до i-тий піксель був віднесений при сегментуванні;

y, d - масштабні параметри.

2. Друга група – показники, які не потребують наявності еталонного сегментування.

2.1. Показник, що враховує однорідність сегментів, який заснований на обчисленні дисперсії величини відповідної ознаки зображення, що використовується для сегментування. Нехай f_i - значення ознаки F в пікселі i. Тоді дисперсія ознаки F для сегменту зображення R_j визначається наступним чином:

$$s_j^2 = \sum_{i\in R_j}\frac{(f_i - \bar{f}_j)^2}{A_j}, \qquad (16)$$

де $\bar{f}_j = \sum_{i\in R_j}\frac{f_i}{A_j}$;

A_l - площина сегменту R_j.

Міра однорідності області W, яка складається з сегментів R_j, визначається виразом (17):

$$U_W = 1 - \sum_{R_i\in W}\frac{w_j s_j^2}{N}, \qquad (17)$$

де w_j - вага, що визначає вклад сегменту R_j в U_W;

$N = s_{max}^2 \sum_{R_j\in W} w_j$ - нормуючий коефіцієнт;

$s_{max}^2 = \frac{1}{2}(f_{max} - f_{min})^2$;

f_{max}, f_{min} - максимальне та мінімальне значення ознаки F в області W.

2.2. Показник, що враховує контраст між сегментами.

$$c_{ij} = \frac{\left|\bar{f}_i - \bar{f}_j\right|}{\bar{f}_i + \bar{f}_j}, \qquad (18)$$

де $\bar{f}_i$, $\bar{f}_j$ - середні значення ознаки F в сегментах R_i та R_j відповідно.

2.3. Комплексний показник, який, наприклад, враховує як однорідність сегментів, так і їх кількість (вираз (19)):

$$F = \frac{1}{1000N}\sqrt{R}\sum_{i=1}^{R}\frac{e_i^2}{\sqrt{A_i}}, \qquad (19)$$

де N - кількість пікселів на зображенні;

R - кількість сегментів;

A_i - площина i-го сегмента;

e_i - величина, що характеризує ступінь однорідності i-го сегмента.

Однак, наведені вище показники оцінки якості сегментування зображення мають наступні недоліки:

- іноді результати сегментування, які є найкращими з точки зору експертів, мають більш високий відсоток помилково класифікованих пік селів;

- не враховується розташування помилкових пікселів відносно відповідного сегменту – тому помилка на границі та помилка в центрі сегменту повинні штрафуватися по різному;

- не враховується різниця у важності окремих ділянок зображення для сегментування – помилки для різних сегментів зображення повинні мати різну вагу;

- відсутня інформація по клас пікселів, що вносить найбільшу помилку.

Метою статті є оцінка інформаційного показника якості (відстані Кульбака-Лейбнера) тематичного сегментування оптико-електронного зображення методом Канні.

Виклад основного матеріалу дослідження.

В роботах Канні, наприклад [5], введено поняття Non-Maximum Suppression, яке означає, що пікселями границь є точки, в яких досягається максимум градієнта у напрямку вектору градієнта. Етапи методу Канні наводяться нижче.

1. Згладжування. Проводиться з метою зменшення впливу шумів на визначення границь, для чого використовується фільтр Гауса (вираз (20)):

$$f(x,y) = \frac{1}{2\pi s}e^{\left(-\frac{x^2+y^2}{2s^2}\right)}, \qquad (20)$$

де (x, y) - координати пікселя на зображенні;

$f(x, y)$ - яскравість зображення;

s - параметр розмиття.

Значення параметра розмиття необхідно обрати таким, що забезпечує найбільше придушення шуму. Більше значення параметра використовується для виділення крупних границь, менше – для виділення

маленьких деталей.

2. Пошук градієнту. Для визначення градієнту на зображенні після фільтру Гауса (20) будемо використовувати оператор Собеля [12], схема просторової фільтрації з використанням якого наведена на рис. 1 [12].

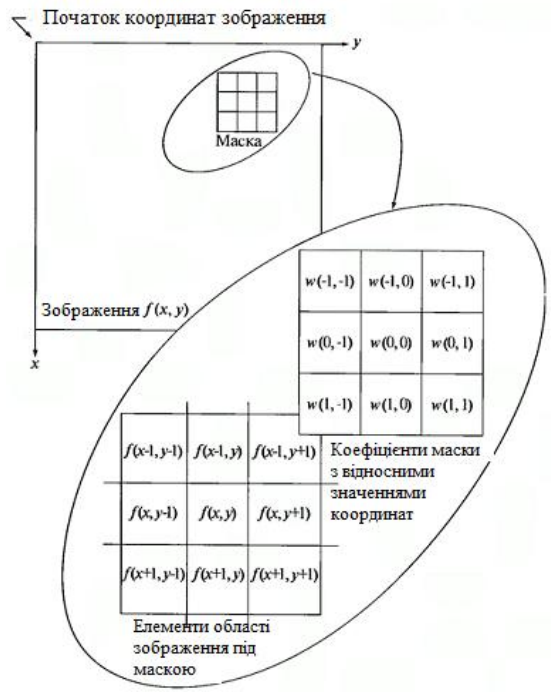


Рис. 1. Схема просторової фільтрації з використанням оператору Собеля [12]

Основою перетворення Собеля є припущення, що функція розриву яскравості на гранях єстановиться значно більше. З цього припущення можна зробити висновок, що для знаходження граней достатньо здійснити диференціювання функції яскравості $f(x, y)$ (вирази (21), (22)):

$$\frac{\partial f(x,y)}{\partial x} = Dx = \frac{f(x+dx, y) - f(x,y)}{dx}, \qquad (21)$$

$$\frac{\partial f(x,y)}{\partial y} = Dy = \frac{f(x, y+dy) - f(x,y)}{dy}. \qquad (22)$$

В дискретних зображеннях dx та dy можна вимірювати в кількості пікселів між двома точками з використанням виразів (23), (24):

$$Dx = f(i+1, j) - f(i, j), \qquad (23)$$

$$Dy = f(i, j+1) - f(i, j). \qquad (24)$$

Вираз для визначення величини градієнту G можна записати наступним чином (вираз (25)):

$$G = \sqrt{(Dx)^2 + (Dy)^2}, \qquad (25)$$

а напрямок q (вираз (26):

$$q = \arctan\left(\frac{Dy}{Dx}\right). \qquad (26)$$

У виразах (25), (26) оцінка градієнту проводиться з використанням масок (2x2):

$$Dx = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \qquad (27)$$

$$Dy = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}. \qquad (28)$$

Основний недолік використання масок (27), (28) – велика кількість помилок з причини наявності шуму [12]. Крім того, використання масок парного порядку не дає можливості проводити оцінку на основі пікселя, що розташований по центру маски. Тому, будемо використовувати оператор Собеля з масками (29), (30):

$$K_{G_x} = \begin{pmatrix} 1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{pmatrix}, \qquad (29)$$

$$K_{G_y} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{pmatrix}. \qquad (30)$$

З аналізу виразів (29), (30) (у порівнянні з (27), (28)) видно використання коефіцієнту 2 для середніх елементів. Цей факт використаний з роботи [13], а збільшене значення коефіцієнту використовується для зменшення ефекту згладжування за рахунок надання більшої ваги середнім точкам. Значення та напрямок величини градієнту G приймають вид (31), (32), відповідно:

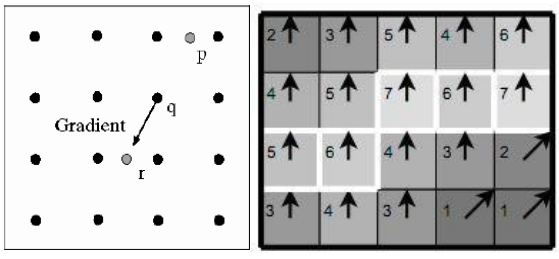
$$G = \sqrt{G_x^2 + G_y^2}, \qquad (31)$$

$$q = \arctan\left(\frac{|G_x|}{|G_y|}\right). \qquad (32)$$

Після використання оператора Собеля інтенсивність кожного пікселя вихідного зображення дорівнює градієнту вектора яскравості.

3. Придушення хибних максимумів. Мета цього етапу – перетворити «розмити» границі в «чітки». Це досягається збереженням локальних максимумів та видаленням всього іншого. Для кожного пікселя виконуються наступні дії:

- напрямок градієнту округлюється до найближчого значення, що кратне 45° (рис. 2а) [5];
- якщо у поточній точці досягається локальний максимум у напрямку градієнту, то вона є частиною границі;
- у противному випадку точка видаляється (рис. 2).



а) б)

Рис. 2. Пошук локальних максимумів [5]: а) (максимуми p та r інтерполюються (видаляються)); б) принцип придушення хибних максимумів

Принцип придушення проілюстрований на рис. 2б. Всі пікселі на рис. 2б мають «орієнтацію вверх», тому значення градієнту в цих точках буде порівняно з нижче та вище розташованими пікселями. Пікселі, що обведені білим кольором на рис. 2б залишаться у вихідному зображенні, інші – будуть придушені.

4. Подвійна порогова фільтрація (рис. 3 [5]). Сутність – кожен піксель, що перевищує верхній поріг, відмічається як «сильний», кожен піксель, що попадає між двома порогами, - «слабий» (яскравість таких пікселів приймає фіксоване середнє значення та буде уточнюватися на наступному етапі), пікселі, що менше нижнього порогу, видаляються.

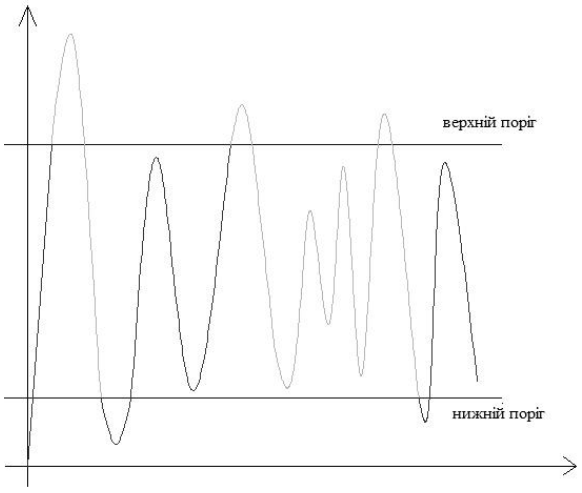


Рис. 3. Використання двох порогів в методі Канні [5]

Використання подвійного порогу дозволяє зменшити вплив шуму (за рахунок верхнього порогу) та не втратити «хвости» (за рахунок нижнього порогу).

5. Трасування області невизначеності. Задача зводиться до виділення груп пік селів, що отримали на попередньому етапі проміжне значення та віднесенню їх до границі (якщо вони з'єднанні з однією з встановлених границь) або їх придушенню (в противному випадку).

Результат сегментування вихідного зображення (рис. 4) методом Канні наведений на рис. 5.

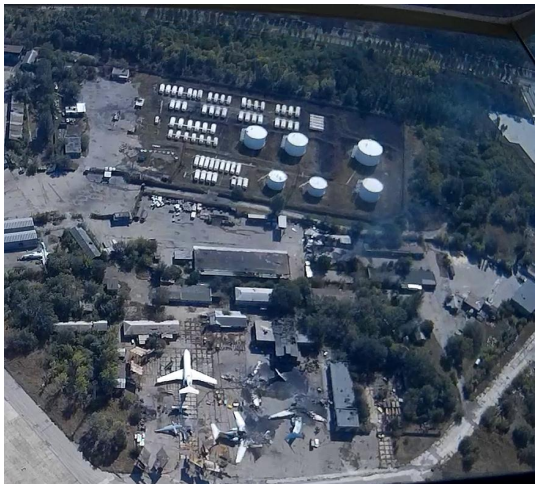


Рис. 4. Вихідне зображення [14]

Рис. 5. Результат сегментування вихідного зображення (рис. 4) методом Канні

Показником якості сегментування вихідного зображення (рис. 4) методом Канні оберемо інформаційний показник – відстань Кульбака-Лейбнера $K(p_x, p_h)$ (вираз (33)) [6, 7]:

$$K(p_x, p_h) = \int_{R^2} p_x(x) \log \frac{p_x(x)}{p_h(x)} dx , \quad (33)$$

де p_x - розподіл яскравості на вихідному зображенні (рис. 4);

p_h - розподіл яскравості на сегментованому зображенні (рис. 5);

R^2 - площина зображення.

На рис. 6 наведена крива залежності відстані Кульбака-Лейбнера від зміни коефіцієнту масштабування m вихідного зображення (рис. 4) при сегментуванні зображення з використанням методу Канні.

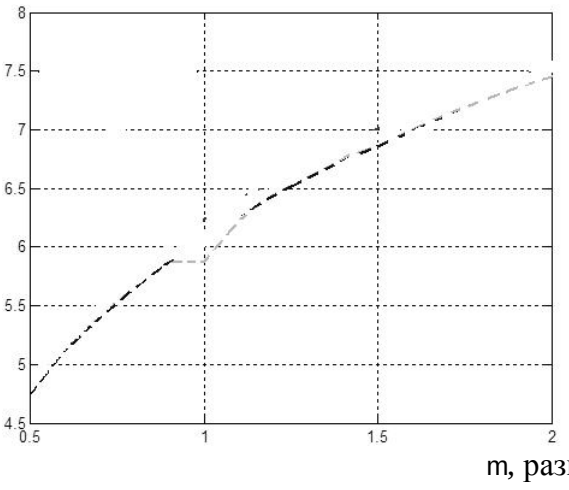


Рис. 6. Залежність відстані Кульбака-Лейбнера від зміни коефіцієнту масштабування вихідного зображення (рис. 4) при сегментуванні зображення з використанням методу Канні

Відстань Кульбака-Лейбнера розраховувалась за виразом (33) з використанням логарифму за основою 2, отже відстань Кульбака-Лейбнера вимірюється у бітах, а для зображення в градаціях $(0...255)$ максимальне значення відстані Кульбака-Лейбнера дорівнює 8.

Висновки й перспективи подальших досліджень

Таким чином, встановлено, що результат дешифрування зображень, що отримані з бортових систем оптико-електронного спостереження, залежить від якості сегментування зображень, особливо з урахуванням особливостей їх отримання (різнорідний фон, варіабельність різних частин зображення, наявність шумів). Проаналізовані основні методики, критерії і показники сегментування зображень, їх переваги та недоліки. Запропоновано провести оцінку інформаційного показника (відстані Кульбака-Лейбнера) тематичного сегментування оптико-електронного зображення методом Канні. Проведено аналіз основних етапів методу Канні: згладжування, пошук градієнту, придушення хибних максимумів, подвійна порогова фільтрація, трасування області невизначеності. Наведено результат сегментування оптико-електронного зображення методом Канні, проведено розрахунок відстані Кульбака-Лейбнера на її залежність від масштабного коефіцієнта вихідного зображення.

Напрямком подальших досліджень є порівняння різних методів сегментування з використанням інформаційного показника – відстані Кульбака-Лейбнера.

Література

1. Савин Л.В. Сетецентрическая и сетевая война. Введение в концепцию. - М.: Евразийское движение, 2011. - 130 с. **2. Bayuk J.L., Healey J., Ronmeyer P., Sachs M.H, Schmidt J., Weiss J.** Cyber security policy guidebook. – New Jersey.: Wiley, 2017. – 270 p. **3. Кобзева Е.А.** Оценка потенциала снимков с КА Pleiades для создания цифровых топографических карт и планов. – Геопрофи, 2013. № 1. - С. 52-57. **4. Худов В.Г.** Мультиагентний метод сегментування зображень, що отримані з бортових систем оптико-електронного спостереження. Системи озброєння і військова техніка, 2016. № 3 (47). - С. 116-119. **5. Canny J.F.** A Computational Approach to Edge Detection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1986. № 8. - PP. 679-698. **6. Kullback S., Leibler R.A.** On information and sufficiency. The Annals of Mathematical Statistics, 1951. V.22. № 1. - P. 79-86. **7. Теребиж В.Ю.** Восстановление изображений при минимальной априорной информации. Успехи физических наук, 1995. Т. 165. № 2. - С. 143-176. **8. Рубан І.В., Худов В.Г., Худов Р.Г.** Показники якості сегментування оптико-електронних зображень. Системи управління, навігації та зв'язку, 2017. Вип. 2 (42). - С. 143–146. **9. Захаров А.В., Кольцов П.П., Котович Н.В., Кравченко А.А., Куцаев А.С., Осипов А.С**. Некоторые методы сравнительного исследования детекторов границ. Труды НИИСИ РАН, 2012. Том 2. № 1. - С. 4-13. **10. Захаров А.В., Кольцов П.П., Котович Н.В., Кравченко А.А., Куцаев А.С., Осипов А.С**. Критерии оценки качества сегментации изображений. Труды НИИСИ РАН, 2012. Том 2. № 2. - С. 87-99. **11. Zhang H. Fritts J.E., Goldman S.A.** Image segmentation evaluation: A survey of unsupervised methods. Computer Vision and Image Understanding, 2008. Vol. 110. Issue 2. - PP.260-280. **12. Гонсалес Р., Вудс Р.** Цифровая обработка изображений. М.: Техносфера, 2005. – 1072 с. **13. Senthilkumaranl N., Rajesh R.** Edge Detection Technigues for Image Segmentation – A Survey of Soft Computing Approaches. International Journal of Recent Trends in Engineering, 2009. Vol. 1. № 2. - PP. 26-37. **14. Електронний ресурс.** Режим доступу http://www.satimagingcorp.com/gallery/ikonos.

ОЦЕНКА РАССТОЯНИЯ КУЛЬБАКА-ЛЕЙБНЕРА ПРИ ТЕМАТИЧЕСКОЙ СЕГМЕНТАЦИИ ОПТИКО-ЭЛЕКТРОННЫХ ИЗОБРАЖЕНИЙ МЕТОДОМ КАННИ

Геннадий Владимирович Худов [1] ***(докт. техн. наук, профессор)***
Владислав Геннадиевич Худов [2]
Ирина Анатольевна Хижняк [1]
Ирина Викторовна Новикова [3]

[1] ***Харковский национальный университет Воздушных Сил имени Ивана Кожедуба, Харьков, Украина***
[2] ***Харьковский национальный университет радиоэлектроники, Харьков, Украина***
[3] ***Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина***

Результат дешифрирования изображений, полученных с бортовых систем оптико-электронного наблюдения, зависит от качества сегментации изображений с учетом особенностей их получения (разнородный фон, вариабельность разных частей изображения, наличие шумов). Проанализированы основные методики, критерии и показатели сегментации изображений, их преимущества и недостатки. Предложено провести оценку информационного показателя (расстояния Кульбака-Лейбнера) тематической сегментации оптико-электронного изображения метом Канни. Проведено анализ основных этапов метода Канни: сглаживание, поиск градиента, подавление ложных максимумов, двойная пороговая фильтрация, трассировка областей неопределенности. Приведен результат сегментации оптико-электронного изображения методом Канни, проведен расчет расстояния Кульбака-Лейбнера и его зависимость от масштабного коэффициента исходного

изображения.

Ключевые слова: *дешифрирование; объект; космический аппарат; оптико-электронное изображение; обработка; сегментация; показатель эффективности; расстояние Кульбака-Лейбнера; метод Канни; сглаживание; фильтрация; информационный показатель; пиксель.*

ESTIMATION OF THE DISTANCE OF THE KULBAK-LEIBNER AT THE THEMATIC SEGMENTATION OF OPTIC-ELECTRONIC IMAGES BY THE CANNI'S METHOD

Hennadii V. Khudov[1] ***(Doctor of Technical Sciences, Professor)***
Vladislav H. Khudov[2]
Irina A. Khizhnyak[1]
Irina V. Novikova[3]

[1]Kharkov National Air Force University named after Ivan Kozhedub, Kharkov, Ukraine
[2]Kharkov National University of Radio Electronics, Kharkov, Ukraine
[3]National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The result of decoding the images obtained from on-board optic-electronic surveillance systems depends on the quality of image segmentation, taking into account the features of their production (heterogeneous background, variability of different parts of the image, the presence of noise). The main methods, criteria and indicators of image segmentation, their advantages and disadvantages are analyzed. It is suggested to evaluate the information indicator (Kulbak-Leibner distance) of the thematic segmentation of the optic-electronic image by the Canni's method. The analysis of the main stages of the Canni's method is carried out: smoothing, gradient search, suppression of false maxima, double threshold filtering, tracing of uncertainty areas. The result of segmentation of the optic-electronic image by the Canni's method is given, the Kulbak-Leibner distance calculation and its dependence on the scale factor of the original image are carried out.

Keywords: *decoding; an object; spacecraft; optic-electronic image; treatment; segmentation; performance indicator; Kulbak-Leibner distance; Canni's method; smoothing; filtration; information indicator; pixel.*

References

1. Savin L.V. (2011), Network-centric and network war. Introduction to the concept. [*Setetsentricheskaya i setevaya voyna. Vvedeniye v kontseptsiyu*], Moscow: The Eurasian Movement, 130 p. 2. **Bayuk J.L., Healey J., Ronmeyer P., Sachs M.H, Schmidt J., Weiss J.,** (2017) Cyber security policy guidebook. – New Jersey.: Wiley. – 270 p. **3. Kobzeva E.A.** (2013), Estimation of the potential of images from the Pleiades spacecraft for creating digital topographic maps and plans [*Otsenka potentsiala snimkov s KA Pleiades dlya sozdaniya tsifrovykh topograficheskikh kart i planov*], Geoprofi. No. 1. - P. 52-57. **4. Khudov V.G.** (2016), Multiagent image segmentation method derived from on-board optoelectronic monitoring systems [*Mul□tyahentnyy metod sehmentuvannya zobrazhen□, shcho otrymani z bortovykh system optyko-elektronnoho sposterezhennyai*], Armament and military equipment systems. No. 3 (47). - P. 116-119. **5. Canny J.F.** (1986), A Computational Approach to Edge Detection. IEEE Transactions on Pattern Analysis and Machine Intelligence. № 8. - P. 679-698. **6. Kullback S., Leibler R.A.** (1951), On information and sufficiency. The Annals of Mathematical Statistics. V.22. № 1. - P. 79-86. **7. Terebyzh V.Yu.** (1995), Restore images with minimal a priori information [*Vosstanovleniye izobrazheniy pri minimal'noy apriornoy informatsii*], Progress in Physical Sciences. T. 165. № 2. - P. 143-176. **8. Ruban I.V., Khudov V.G., Khudov R.G.** (2017), Quality Indicators for Segmentation of Optoelectronic Imagery [*Pokaznyky yakosti sehmentuvannya optyko-elektronnykh zobrazhen□*], Control, Navigation and Communication Systems. Vip. 2 (42). - P. 143-146. **9. Zakharov A.V., Koltsov P.P., Kotovich N.V., Kravchenko A.A., Kutsaev A.S., Osipov A.S.** (2012), Some methods of comparative study of boundary detectors Imagery [*Nekotoryye metody sravnitel'nogo issledovaniya detektorov granits*], Proceedings of NIISI RAS. Volume 2. № 1. - P. 4-13. **10. Zakharov A.V., Koltsov P.P., Kotovich N.V., Kravchenko A.A., Kutsaev A.S., Osipov A.S.** (2012), Criteria for assessing the quality of image segmentation [*Kriterii otsenki kachestva segmentatsii izobrazheniy*], Proceedings of NIISI RAS. Volume 2. № 2. - P. 87-99. **11. Zhang H. Fritts J.E., Goldman S.A.** (2008), Image segmentation evaluation: A survey of unsupervised methods. Computer Vision and Image Understanding. Vol. 110. Issue 2. - PP.260-280. **12. Gonzalez R., Woods R.** (2005), Digital Image Processing Imagery [*Tsyfrovaya obrabotka izobrazhenii*], Moscow: Technosphere. - 1072 p. **13. Senthilkumaranl N., Rajesh R.** (2009), Edge Detection Technigues for Image Segmentation – A Survey of Soft Computing Approaches. International Journal of Recent Trends in Engineering. Vol. 1. № 2. - PP. 26-37. **14. Electronic resource.** Access mode http://www.satimagingcorp.com/gallery/ikonos.

УДК (623.094)

Vadym Bunakov

Central Research Institute of Arms and Military Equipment of the Armed Forces of Ukraine, Kyiv , Ukraine

ON ASSESSING THE IMPACT OF EMERGING TECHNOLOGY ON THE ARMED FORCES OVER THE NEXT 10 YEARS

The article outlines the main emerging technologies that will have the greatest influence on the Armed Forces of the advanced countries over the next 10 years. Based on the analysis of the main areas of development of these emerging technologies, it is concluded that the most probable is the further improvement of existing technologies with the parallel increase of the influence on the Armed Forces of such technologies as cyberspace, autonomous (robotic) systems, and weapons of direct energy transmitter of energy. It is concluded that over the next ten years, further transformation of combat operations from the classical, built on the theory of the war of Clausewitz, into non-traditional, hybrid combat operations, which more closely correspond to the theoretical works in the field of military art had ex-pressed by Sun-Tzu, will take place.

Keywords: *Armed Forces, emerging technologies, doc-trine, balance of power.*

The introduction

Over the next 10 years the emerging technologies such as cyberspace, autonomous systems, direct energy transmission technologies and even the combination of existing ones will greatly affect the military capabilities and the doctrines of the Armed Forces, and even the balance of power in the world. However, for transferring the emerging technologies into weapon systems needs takes some time.

Based on an analysis of existing trends, it can be assumed that over the next 10 years period the armed struggle grounded on the transfer of kinetic energy will remain the main form of rivalry, but, on the other hand, emerging technologies and combinations of existing ones, due to the reduction in mass-dimensional characteristics of weapons, to simultaneously increasing destructive ability of new types of weapons will lead to improve tactical and technical characteristics of weapons.

Formulation of the problem. At present, considerable attention is paid to assessing the possible impact of the emerging technology on the Armed Forces and the nature of future conflicts. However, these studies do not assess the possible impact on a certain period of time. Therefore, the article seeks to assess the possible impact of the emerging technology on the Armed Forces and the nature of future conflicts over the next 10 years.

Analysis of literature. Today, the great attention of the leading arms manufacturers of the world (the USA, China and Russia) is focused on creating new weapons that will allow them to dominate over the world. The achievement of this goal is possible through the creation of new weapons or the improvement of the existing one. We can predict about the enormous impact of emerging technologies on the Armed Forces in the near future. Already today, emergent technologies change the ways in which combat operations are conducted by the Armed Forces, the doctrines of their use and the balance of power. However, in their publications, the authors do not consider the impact of technology on the Armed Forces in the next 10 years, nor does it fully assess the possibilities to improve the characteristics of existing weapons.

Purpose of the article. To define the idea of emerging technologies, the sufficiency of a tenyear period for the emerging technologies to radically change the Armed Forces. Assess the impact of emerging technologies on the combat potential of the Armed Forces, on the doctrines and the influence of emerging technologies on the balance of power.

FIELDS OF EMERGING TECHNOLOGY

For an assessment of the impact of emerging technologies on Armed Forces during the next 10 years, it is necessary to define what type of technologies are emerging (give the definition of the emerging technologies and identify the most important part of them). Moreover, it also would be interesting to gauge the possibilities for the implementation of such technologies in armament over the next 10 years.

When it comes to emerging technologies it is implied, that these technologies are completely new, their impact on the character of future conflicts is unpredictable and the dynamics of their development indicate their rapid growth and possible significant consequences over a considerable period (Daniele Rotolo, 2015)[9].

If we analyze the emerging technologies that are consistent with the above-identified assets and that might have impact on the nature of Armed Forces in the foreseeable future, we would highlight some the most important parts of them: (Raytheon, 2016) [27], (Jitendra S. Tate, 2015)[15]:

- Cyberspace;
- Autonomous systems (Robotic systems);
- Direct energy transmission technologies;
- Nanotechnology;
- Biotechnology;
- Artificial Intelligence and Intellect.

In addition to these above-mentioned technologies, it is also interesting to note the issue of existing technologies and combination of them, that with their

complex use and with relatively insignificant resource costs can considerably improve the qualitative characteristics of existing weapons.

Cyberspace (a space that exists in the virtual world and is built on information) has significantly changed the conduct of combat operations and has a huge impact on real aspects of the world now. Covering all spheres and management processes of human life Cyberspace allowed achieving huge effects with low costs. Cyber-attacks undermine the confidence in the banking system of many states, break down nuclear plants, turn off electro stations, and affect the minds and hearts of entire nations. The influence of cyberspace and conducting operations on the armed forces in it for the next 10 years will only be increased (Geers, 2015)[12].

Among the technologies that directly transfer energy, various kinds of electromagnetic energy emitters (laser and electromagnetic guns) are being used. Today manufacturers have announced the creation of different armament based on this technology. The leading developers (General Atomics, BAE Systems) are testing weapon samples on new physical principles of land, air and sea-based aiming the destruction of mines, shells, un-manned aircraft, marine and ground systems and deactivating of all existing electronic systems. Electromagnetic munitions were used in the Gulf War to suppress virtually all radio electronic facilities operating on the principle of receiving and converting electromagnetic waves (Nass, 2007)[22]. Within the future 5-6 years period Electromagnetic rail-gun fires is believed to go into service with the US Navy (O'Rourke, 2017)[24]. General Atomics Aeronautical Systems announced the creation of a tactical combat solid-state high-energy laser which is capable of destroying drones and small marine boats and which will be a base for short-range defence system for military ships (Warwick, 2015) [32].

Autonomous systems (Robotic systems) are fully capable of performing the functions of a soldier (human presupposition is necessary only for the performance of management and control functions) during warfare. Such robotic systems, as unmanned aircraft, marine and ground systems have already significantly changed the nature of combat operations. If on the one side, we have an ordi-nary soldier with his fragile biological structure, which does not allow increasing speed, acceleration, maneuverability, depth and height of the use of military systems, the modern autonomous robotic systems on the other side don't have this shortcoming. The robotic systems enable to increase the depth of reconnaissance on the enemy territory, significantly improve the speed of obtaining intelligence information, and accelerate the accuracy of fire support and, most important-ly, the ability to reduce the number of losses among own forces and the population. The significant influence of robotic systems on the character of contemporary conflicts will be kept up in the next 10 years (Кричевский, 2016) [40].

To replace a person in the decision-making process, robotic systems must possess the required intelligence. The ability of machines 'to think', 'judge' and 'behave' like a human is the main task of arms manufacturers all over the world. Today, most advanced Armed Forces are using decision support systems that are able to offer best solutions in accordance with the current situation. If during the next 10 years period, this technology will be able to shift to the level of creating an artificial intelligence, this would represent invaluable military means. However, in connection with the huge demands on the computing power together with its expensiveness the number of such funds in the Armed Forces will be limited.

Nanotechnology, that is used to create materials with required structure at the level of nanometers had already allowed to generate materials with qualities that are not inferior to exist; some of them such as hardness, resistance to rupture and thermal conduction are better than existing natural analogues (Wiśniewski, 2007) [36], (Víctor M. Castaño, 2013) [34]. During the period of 2010-2012 armoured vests with the use of materials based on nanomaterials (carbon nanotubes) were created, which by their characteristics significantly exceed existing analogues (Tiwari, 2012) [31]. In the next 10 years, nanomaterials will create an ability to produce weapons with much smaller weight and dimensional characteristics. However, the estimated price of such materials together with their limited number, will not allow a significant influence on the Armed Forces during the upcoming years.

Technology aiming to improve the quality of living organisms, with assistance of other living ones (biotechnology) is already used in modern medicine. Regeneration of non-functional limbs is one of the successful achievement. (Bionics, 2009). Working process of how to create other parts of human body is still ongoing and this is believed to allow the full restoration of lost or damaged parts of human organism within the next 10 years period. However, as in the case of nanomaterials, the price of such technologies is enormously high and therefore the possibilities for their implementation are limited so far.

Over the past few decades, the significant shift of thinking in modern science and technology made it possible to improve existing technologies. Mobile phones, these smart de-vises with implemented technologies in of transmission and reception of electromagnetic waves, information processing, coding and decoding and displaying them on the screen are the most significant example of the symbiosis of existing technologies with their highly improved quality characteristics.

A brief look at the 'life cycle' of armament enables us to assess the impact of emerging technologies on Armed Forces. It is a time from the moment, where technologies emerged to the time of arriving of the new weapons built on these emerged technologies to the arsenals of Armed Forces (Daniele Rotolo, 2015)[9]. The implementation of achievements of emerging technologies in exciting armament or the creation of new type of weaponry needs a time. For example, the creation and placement on the Global Positioning System that allowed the implementation of navigation technology took about 15 years (Mai, 2015)[20]. Only after 22 (from creation to its mass production) years the F-22 fighter aircraft could use

the "STEALTH" technology (Boeing, 2014).[6] The creation of anti-tank missile system AT-14 "Spriggan", with its implemented laser targeting technology took exactly ten years, and the creation of a bulletproof vest on the basis of nanotechnology took about 9 years. Consequently, a ten-year period is the minimum requirement and in most cases insufficient for systemic changes in the Armed Forces.

Thus, from the technologies listed above, the cyberspace, robotic technologies, weapons of direct energy transmitter, as well as a combination of existing technologies (Matts-son, 2015) will have the most potent quantitative, qualitative and cost indicators. Mutual penetration and additions of existing technologies will create new quality and improve the tactical and technical characteristics of weapon systems, although the emergent technologies will affect the Armed Forces only if they will be successfully implemented in new weapon systems and armament.

MILITARY CAPABILITIES

The technological level of armament is one of the components of the military capabilities, together with the structure of the Armed Forces and their readiness to conduct combat operations. In the future 10 years perspective, as a result of the introduction of new systems on the basis of emerging technologies there definitely will be changes in the military capabilities of the Armed Forces (Ashley J. Tellis, 2000). [1]

During the Second World War, the possession and availability of radar technology enabled the Royal Air Force, with information on take-off and flight direction together with significantly fewer aircraft to inflict considerable damage to the Luftwaffe and ultimately win The Battle of Britain. De-ciphering the codes of control channels al-lowed Allies to sink a considerable number of the Kriegsmarine submarines during The Battle of the Atlantic. The possession of computer technology and the creation of advanced automated computer-based control systems contributed to NATO, winning the Cold War with the USSR. The possession of nuclear weapon technology and its usage re-sulted in changing the balance of power in the world and forced imperial Japan to sign an agreement of capitulation.

The tactical and technical characteristics by using existing technologies and their new combination will be greatly improved in the next 10 years period. However, the main method to struggle will remain a physical armed struggle based on the transfer of kinetic and electromagnetic energies for the destruction of enemy troops by its weapons, military equipment, facilities and environment (Slipchenko, 1999) [29].

Further increase of combat capabilities concerning the accuracy of the target acquisition, due to the use of global positioning systems, unmanned systems, new nanomaterials, should lead to a reduction the number of de-vices to be engaged to destroy a target, to a significant increase in its payload and destructive power, to a higher survivability and protection (Lambeth, 1997)[17]. It is planned, that for 2027 in the arsenal of he USA, Russian and Chinese Armies will be a significant number of robots that will operate before and on the frontline with the soldiers.

The development of microelectronics will significantly expand the possibilities for further development of new types of precision weapons and weapons on ’new physical principles‘. They will be built on the most advanced ultra-high-speed, ultra-large inte-grated circuits and ultra-sensitive sensors of different frequency bands. The new nano-materials with the new element base of radio electronics will allow creating control and guidance systems and of high-precision armament much less and easier than now, and thus several times to increase the effective-ness of the warhead without increasing the power of the rocket's power plant.

New weapons and military equipment will not only sharply increase the combat capabilities of the Armed Forces, but also radically decrease the quantity of them, change their composition, structure, the character of con-ducting combat operations and the nature of possible wars (Loo, 2009)[18]. Participation in the armed struggle with a large number of different offensive and defensive weapons based on the emerging technologies will complicate the nature of this struggle (Gerasimov, 2013)[13].

In order to change military capabilities the emerging technologies, in case of their realisation, should have the same significant con-sequences and impact as it was the case of nuclear technology. Besides this, the numbers of new weapons of destruction need to be significantly large as for example it was the case with tanks and aircraft. Besides, the development of appropriate methods for the use of new armament bears high importance as the lack of understanding and possibilities of new technologies leads to catastrophic effects. In the beginning of World War II, for example, the Soviet army in spite of having a large quantity of high-tech armament lost all initial battles.

The impact of emerging technologies on the military capabilities of the Armed Forces is not limited. In the next 10 years, new weapons systems, in which today's emerging technologies will be implemented, will significantly change the doctrine, but the latter in turn will significantly affect the emerging technologies (Blasko, 2011).[5]

ARMED FORCES, EMERGING TECHNOLOGIES AND DOCTRINES

The US and Russia set themselves the task of being able to conduct an operation any-where in the world and strike on any object within a timeframe one hour after taking the decision to engage (Woolf, 2017) [37]. Being the second largest economic power after the United States, China has a huge gap in high-tech weapons compared with the US. Under-standing its considerable gap with the advanced powers in high-tech weapons, China is trying to implement Anti Access Anti denial (A2/AD) based on the existing technical level of weapons (Ou, 2014) [25]

Today the US is the world leader in the economy and politics. The US military budget in 2016 exceeded the military expenditures of the five states following it taken together (SIPRI, 2017) [28]. As the world leader, the Unit-ed States set itself a global goal to dominate all corners of the world. For achieving this ambitious goal, the US must have the most advanced Armed Forces in the world that in turn is a result of equipping them with the most advanced systems of

armament. These goals set new tasks for the scientific and industrial complex of the US to develop new types of weapons and, accordingly, the development of new technologies. To meet these requirements, the country is developing the Conventional Prompt Global Strike pro-gram, which will be based on hypersonic de-livery and defeat systems (a combination of existing technologies resulting to creation of new weapons systems with new qualities) (Blasko, 2011) [5], (Woolf, 2017) [37]. New systems (the X-37B, the RQ-4 Global Hawk) have been already tested. Adopting such systems in the Armed Forces within the next 10 years will create the possibility to implement the requirements for applying a precision strike anywhere in the world.

Russia with its army modernization plan until 2025 is the second example of mutual impact of doctrine and emerging technologies. Setting itself the task to be back to the world leader's club, Russian leadership is considering the possibility of realizing this task through deep military reform, using a military modernization program like locomotive of economy, and the creation and rearmament of its Armed Forces with new weapons (Bukkvoll, 2011).[7] The development of technologies is a consequence of growing demands of Armed Forces. To the end of 2020, Russia's Armed Forces will possess nearly 70 % of modernised armament and by 2025 all Armed Forces will be modernized. (Petraitis, 2015) [26].

The basis of the military doctrine of Beijing is inseparable from the theoretical works of Sun-Tzu and traditional Chinese culture who aim to win the war without a single battle. Achieve victory even before the first shot is the main desire of the modern Armed Forces. To accomplish this, it is planned to widely use cyber operations and new high-tech weapons (Newmyer, 2010)[23]. In accordance with the views of the military leadership of China, in future wars the knowledge and the skills of the soldier will be the decisive factor of victory. In China's military thinking the future war will be technological and be accompanied by the massive application of modern radio electronic means and precision weapons. Having only advanced technologies would not be enough to win in the future war. Unconventional thinking, the ability to make quick and non-standard decisions will always defeat the enemy's high-tech forces, because no matter how high-tech the enemy is, he might have weaknesses on which it is necessary to strike (Blasko, 2011). [5]

China's political and military leadership is carrying out a series of measures aiming to develop and create new weapons (aircraft J-20, aircraft carrier Liaoning), with the high use of technologies obtained from Russia (successful production of the Russian Su-27 clone) (Cheung, 2016)[8]. So, the creation a new J-20 fighter and aircraft carrier Liaoning similar to which the Chinese People's Army has never had before, will take at least 5-6 years to change and develop the doctrine, to assess possible changes and to take into ac-count the new capabilities of these systems (Кривопалов, 2016) [39]. New technologies, being the driver of military reforms, lead to optimizing the number of the Chinese Armed Forces, changing their structure from quantitative indicators to qualitative ones, influencing on command and control system and changing the doctrine of the Chinese Armed Forces (Blasko, 2011) [5].

Mutual impact of emerging technology and doctrine of China can be seen on its A2/AD concept. Having bitter experience of the negotiation with Taiwan in 1996, when American's aircraft carriers were sent to the area to improve this relationship (Ou, 2014) [25], the basis of the Chine's A2/AD will be the anti-aircraft ballistic missile DF-21D (Кривопалов, 2016), which is an example of using existing technology to change and improve submarine's ballistic missiles for new purpose. Realizing the existence of a huge gap in military technology compared to the US, China's political leadership tasked of the industry to decrease this gap by modernizing existing armaments and creating new ones (Ou, 2014) [25].

Having a significant backlog in the development of military science and technology, China's leadership relies on the development of domestic emerging technologies and the receipt of emerging technologies from other countries (Defence, 2016)[10], primarily from Russia (Cheung, 2016)[8]. New high-tech weapons systems define China's modern doc-trine and in the next 10 years period with the introduction of new, high-tech systems and complexes, this trend will carry on.

Within the next 10 years, the mutual influence of emerging technologies and doc-trines will be strengthened and will be deter-mined by the geopolitical goals of the state and the level of development of science and technology of these countries. The US and Russia are setting themselves the goal of geopolitical domination, developing doctrines in accordance with which the Armed Forces are tasked to carry out an operation anywhere in the world. For the implementation of these goals, the Armed Forces of both countries will try to receive the most advanced weapons in the next 10 years period. Thus, the Doctrines of the United States and Russia determine the requirements for the capabilities of the Armed Forces and, in turn, the Armed Forces determine the requirements for emerging technologies.

However, as in the case of the Chinese nuclear program, when, as a result of technology diffusion from the USSR, China obtained the technology of creating nuclear weapon and became a member of the nuclear club, the emerging technologies can not only affect the doctrine but can also influence on the balance of power in the world.

ARMED FORCES, EMERGING TECHNOLOGIES AND THE BALANCE OF POWER

Today, the world order is determined by the Westphalian system of international relations in which the state-nation is the basis of the system. The relations between states are built on the principles of national state sovereignty and non-interference in internal affairs of other sovereign states, on the priority of national interests and the principle of the balance of power (Beaulac, 2004). [3] Possession of technologies for creating nuclear weapons is the main driving force of the existing world order.

Attack on the US on 9/11 showed that in-

ternational terrorism, concentrated in the Islamic countries, challenged the world dominated by the US. With the outbreak of the war in Afghanistan, the US Armed Forces started fighting with an adversary whose organization did not have a hierarchical structure. The nature of the fighting in Afghanistan and Iraq showed that the US and its al-lies faced with such non-linear adversaries. It can be certainly said that, the Armed Forces of the US started the first non-linear war be-tween the state and non-state organization. (Иванов, 2008) Traditionally, the military is organized in accordance with a strict hierarchy from the general and down to the soldier. Unlike them, networks straighten the command structure. This proves the growing strength of networks as a threat to the USA national security and the existing balance of power in the world (Baluyevsky, 2012) [2].

The terrorist organizations conducted asymmetric military operations and targeted the political will of the enemy, rather than his military power (Иванов, 2008). They are distributed, dispersed, active and mobile, acting impromptu, widely used the Internet for propaganda, searched for the new recruits and realized the concept of the asymmetric war. Asymmetric warfare is the battle of numerous and organized small units, against conventional military forces, which are structured into large formations (Иванов, 2008). This makes them effective and difficult to track and destroy. Losing the conventional war, the international terrorist organizations launched the operations in the battlefields of cyberspace.

The 10 years' experience of using cyber-space (perhaps the most significant one from emerging technologies) illustrates this technology has significant advantages over the conventional means of destruction. Today the cyberspace has changed the course of military operations and in the next 10 years, its impact on the Armed Forces and therefore on the balance of power will only be increased with an effect not less than the effect of creating nuclear technology.

'[…] cyber technology have allowed to create a completely new type of weaponry, which has no analogues in world history and the next war will begin in cyberspace' (Kissinger, 2014) [16].

For example, in November 2009 American and Israeli military specialists conducted an attack using the malicious computer program Stuxnet against the Iranian company in Natanz, which resulted in the disruption of more than 20% of the functioning centrifuges (Wirtz, 2015) [35]. In the opinion of Israeli experts, the damage caused was no less than if the physical operations for the destruction of centrifuges using conventional weapons had been carried out (Wedermyer, 2012) [33].

In case of Russia, Gerasimov's doctrine defined new forms and methods of warfare in which cyberspace has priority (Gerasimov, 2013) [13]. During the operations by Russian cyber special services to stop the provision of power supply systems for the population of western Ukraine in 2015, two out of three electricity supply stations were put out of operation, as a result 230,000 people were without electricity for a considerable period of time (Geers, 2015)[12].

In contrast, even with nuclear deterrence, cyber-attacks cannot be prevented. Their results are visible only after a successful attack on vital objects. Today, a small organization of well-trained professionals located in different parts of the world, with relevant knowledge and skills can be a very powerful fighting unit. In such a situation it is extremely difficult to agree on common rules (as it was done in the case of nuclear weapons) and deterrence principles. But what is happening now makes us think about fundamentally new principles of organizing the world order.

Given the fact that North Korea and Iran widely support all kinds of terrorist organizations around the world, the likelihood of such technologies to be disposed into the hands of leaders of such entities is high.

Thus, emerging technologies such as cyberspace and the proliferation of nuclear technologies will make it possible in the next 10 years to shift the focus of strategic rivalry between states in the field of competition between the state and non-state (semi-state organizations).

The importance of cyberspace as a means of achieving their geopolitical goals and therefore aiming to at change the existing world order is perfectly understood by Russia and China.

Accordance to Gerasimov's doctrine '[…] it is necessary to carry out asymmetric actions for remote impact on the enemy, to destroy his facilities throughout the entire territory, to neutralize the enemy's superiority in the armed struggle' (Gerasimov, 2013) [13].

Right now, Russia is waging wars for the minds and hearts of the Russian and other population using computer networks («in contact», «odnoklassniki»), aiming to realize the concept of victory without a battle (Crimea).

The leadership of the Chinese People's Army also attaches great importance to the ability to influence the balance of power in the world and especially in the Indo-Pacific region. Deterrence of China, is reduced to the resolution of military situations by non-military means and the implementation of concepts of victory without a battle and victory before entering the battle (Newmyer, 2010)[23], which were voiced by the Chinese philosopher Sun-Tzu. Cyber deterrence of China is a strategic tool, and because of the significant consequences that may result from attacks on vital systems of support for society and control systems, the initial phase, hidden in cyberspace, will have the decisive role in achieving victory over the enemy (Ou, 2014) [25].

At the same time, the consequences of the cyberspace clashes will even exceed the consequences of conventional military operations using high-precision weapons and their destructive power. Given that such clashes will not lead to direct human losses, it is possible to assume with a high probability that such operations will precede in the foreseeable future, and subsequently supersede conventional military operations.

CONCLUSION

The Armed Forces, prepared and trained to war using the means and methods of con-ducting past wars, are doomed to failure be-fore the outbreak of hostilities. The high technological level of the Armed

Forces is one of the conditions for creating superiority over the enemy. Emerging technologies will make it possible to conduct almost contact-less operations, in which Armed Forces should be prepared for conducting operations in all relevant dimensions, air, land, sea, space and cyberspace.

Over the next 10 years, emerging technologies such as cyberspace, autonomous (robotic) systems, weapons of direct energy transmitter and the combination of existing technologies might lead to increasing numbers of high-tech weapons and a reduction of numbers of Armed Forces. As in the case of nuclear weapons technology, the emerging technologies and especially the cyberspace will have a significant potential to change military capabilities, doctrines and influence on the balance of power in the world.

Win the war without a single battle; achieve victory even before the first shot it is the main goal of future Armed Forces. To achieve these goals, Armed Forces should be ready to conduct conventional operation on the full depth of the enemy's space, prepare for conduct the cyber-operation in cyber-space aimed to disrupt the command and control systems of enemy (these actions will have a hidden character, the consequences of which the enemy will understand after the outbreak of hostilities). They should be ready to use new high-precision armament, much less, much easier, with several times increasing the destruction power, based on the transfer of kinetic and electromagnetic energy with the wide use of autonomous systems of sea, land and air. In addition, they should be prepared to conduct network-centric operations against conventional and not-conventional adversary in the virtual and real world, aimed primarily at suppressing the enemy's will for resistance.

However, possession of high-tech weapons does not guarantee victory in a future war.

Unconventional thinking, the ability to make quick and non-standard decisions will always defeat the enemy's high-tech forces, because no matter how technically advanced the enemy is, he would always have weak-nesses on which it is possible to strike (Blasko, 2011).

References

1. Ashley J. Tellis, Janice Bially. 2000. Measuring National Power in the Postindustrial Age. RAND corporatio. 2000.

2. Baluyevsky, Yury. 2012. Security Index of A Globalized World: The Russian Dimension. 1(81), 25 Apr 2012, Vol. 13, pp. 27-38.

3. Beaulac, Stéphane. 2004. The westphalian model in defining international law: challenging the myth. 2004.

4. Bionics, Touch. 2009. Touch Bionics unveils world's first bionic finger. Touch Bionics. [В Интернете] 6 Dec 2009 г. [Цитировано: 26 Apr 2017 г.] http://www.touchbionics.com/news-events/news/touch-bionics-unveils-world%E2%80%99s-first-bionic-finger.

5. Blasko, Dennis J. 2011. 'Technology Determines Tactics': The Relationship between Technology and Doctrine in Chinese Military Thinking. 2011 г., Т. 34:3, стр. 355-381.

6. Boeing. 2014. F-22 Raptor. http://www.boeing.com. [В Интернете] 2014 г. [Цитировано: 26 Apr 2017 г.] http://www.boeing.com/history/products/f-22-raptor.page.

7. Bukkvoll, Tor. 2011. Iron Cannot Fight – The Role of Technology in Current Russian Military Theory. 2011, Vol. 34:5, pp. 681-706.

8. Cheung, Tai Ming. 2016. Innovation in China's Defense Technology Base: Foreign Technology and Military Capabilities. 11 Sep 2016, Vols. 39:5-6, pp. 728-761.

9. Daniele Rotolo, Diana Hicks, Ben Martin. 2015. What Is an Emerging Technology? 7 July 2015.

10. Defence, US Department of 2016. Military & security developments involving the People's Republic of China 2016. May 2016 г.

11. Engels, Marx. 1843-44. Selected works of Marx and Engels. s.l. : Lawrence & Wishart Electric Book, 1843-44. p. 211. Vol. 3. ISBN-13: 978-0717804146.

12. Geers, Kenneth. 2015. Cyber war in perspective: Russian aggression against Ukraine. Tallinn : NATO CCD COE Publications, 2015. ISBN 978-9949-9544-4-5.

13. Gerasimov, Valeriy. 2013. The Value of Science is in the Foresight. Voyenno-Promyshlennyy Kuryer. 2013 г.

—. 2013. The Value of Science is in the Foresight. Voyenno-Promyshlennyy Kuryer. 2013 г.

14. Isserson, G.S. 2016. G.S. Isserson and the War of the Future: Key Writings of a Soviet Military Theorist. s.l. : McFarland & Co Inc, 2016. 1476662363.

15. Jitendra S. Tate. 2015. Military and national security implications. 2015 г., Т. 41, 1.

16. Kissinger, Henry. 2014. World order. Reflections on the character of nations and the course of history. New York : Penguin Press, 2014. p. 200. ISBN 978-0-698-16572-4.

17. Lambeth, Benjamin S. 1997. The technology revolution in air warfare. 1997, Vol. 39:1, pp. 65-83.

18. Loo, Bernard Fook Weng. 2009. Decisive Battle, Victory and the Revolution in Military Affairs. 2009, Vol. 32:2.

19. Macaulay, Thomas. 2017. The future of technology in warfare: From AI robots to VR torture. [Online] 13 Jan 2017. [Cited:] http://www.techworld.com/security/future-of-technology-in-warfare-3652885/.

20. Mai, Thuy. 2015. Global Positioning System History. www.nasa.gov. [В Интернете] 31 July 2015 г. [Цитирова-но: 04 05 2017 г.] https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html.

21. Mattsson, Peter A. 2015. Russian military thinking – a new generation. 2015, Vol. 1, 1.

22. Nass, Meryl. 2007. Meryl Nass, MD, Director of Pulmonary Rehabilitation, Mount Desert Island Hospital Bar Harbor, Maine. U.S. Senate Committee on Veterans' Affairs. [В Интернете] 25 September 2007 г. [Цитировано: 26 Apr 2017 г.] https://web.archive.org/web/20071103025251/http://www.senate.gov/~veterans/public/index.cfm?pageid=16&release_id=11326&sub_release_id=11373&view=all.

23. Newmyer, Jacqueline. 2010. The Revolution in Military Affairs with Chinese Characteristics. 2010, Vol. 33:4.

24. O'Rourke, Ronald. 2017. Navy Lasers, Railgun, and Hypervelocity Projectile: Background and Issues for Congress. Congressional Research Service. 2017.

25. Ou, Si-Fu. 2014. China's A2AD and Its Geographic Perspective. 2014.

26. Petraitis, Daivis. 2015. The New Face of Russia's Military. 2015, Vols. 2014-2015, Volume 13.

27. Raytheon. 2016. Securing tomorrow, future warfare, cultivating emerging technologies. 2016.

Sanchenko, O. 2014. The structures, methods and models use of consciental weapons in the social communication. 2014 г., Т. 7.

28. SIPRI. 2017. World military spending: Increases in the USA and Europe, decreases in oil-exporting countries. 24 April 2017.

29. Slipchenko, Vladimir. 1999. Voyna budushchego. Nongovernmental Science foundation. 1999 г.

30. The National Academy of Sciences. 2010. PERSISTENT FORECASTING OF DISRUPTIVE TECHNOLOGIES. N.W. Washington : s.n., 2010. ISBN: 978-0-309-11660-2.

31. Tiwari, Anupam. 2012. Military nanotechnology. 2012 г., Т. 2, 4, стр. 825 – 830

32. Warwick, Graham. 2015. General Atomics: Third-Gen Electric Laser Weapon Now Ready. aviationweek. [В Ин-тернете] 20 Apr 2015 г. http://aviationweek.com/technology/general-atomics-third-gen-electric-laser-weapon-now-ready.

33. Wedermyer, Landon J. 2012. The Changing Face of War: The Stuxnet Virus and. 2012.

34. Víctor M. Castaño, Rogelio Rodríguez. 2013. Nanotechnology for ballistic materials: from concepts to products. [ред.] Universidad Nacional Autónoma de México, Boulevard Juriquilla 3001, Santiago de Centro de Física Ap-licada y Tecnología Avanzada. 2013 г., Т. 47, 3.

35. Wirtz, James J. 2015. Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. 2015.

36. Wiśniewski, Adam. 2007. Nanotechnology for body protection. 2007.

37. Woolf, Amy F. 2017. Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues. Congressional Research Service. 2017.

38. Иванов Олег. 2008. Американская революция в во-енном деле и ее влияние на военно-политичесКую стра-тегию. 2008 г.

39. Кривопалов. 2016. Kitayskaya voennaya mosch kak faktor mirovoy politiki. 2016 г.

40. Кричевский, Герман. 2016. НБИКС-технологии и концепция современной войны. [В Интернете] 2016 г. http://www.nanonewsnet.ru/articles/2016/nbics-tekhnologii-dlya-mira-voiny-anons-knigi-german-evseevich-krichevskii

ОЦІНКА ВПЛИВУ ТЕХНОЛОГІЙ, ЩО ЗАРОДЖУЮТЬСЯ НА ЗБРОЙНІ СИЛИ ПРОТЯГОМ НАСТУПНИХ 10 РОКІВ

Вадим Петрович Бунаков

Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ, Україна

У статті проаналізовані основні технології, що зароджуються, які будуть мати найбільший вплив на Збройні Сили розвинутих країн світу на протязі наступних 10 років. Спираючись на аналіз основних напрямків їх розвитку, робиться висновок, що найбільш імовірним є подальший розвиток існуючих технологій передачі кінетичної енергії, за рахунок зменшення маса-габаритних характеристик зброї та одночасного зростання деструктивної здатності нових типів озброєння та подальше підсилення впливу на Збройні Сили таких технологій, як кіберпростір, автономні (роботизовані) системи та озброєння прямої передачі енергії. Зроблено висновок, що на протязі наступних 10 років відбудеться подальша трансформація бойових дій від класичних (теоретичні роботи Клаузевіца) до нетрадиційних, гібридних бойових дій, що відповідає теоретичним роботам Сан-Цзи.

Ключові слова: *технології, що зароджуються, Збройні Сили, доктрина, баланс сил.*

ОЦЕНКА ВЛИЯНИЯ ЗАРОЖДАЮЩИХСЯ ТЕХНОЛОГИЙ НА ВООРУЖЕННЫЕ СИЛЫ В ТЕЧЕНИЕ СЛЕДУЮЩИХ 10 ЛЕТ

Вадим Петрович Бунаков

Центральный научно-исследовательский институт вооружения и военной техники Вооруженных Сил Украины, Киев, Украина

В статье проанализированы основные зарождающиеся технологии, которые будут иметь наибольшее влияние на Вооруженные Силы развитых стран в течение следующих 10 лет. Основываясь на анализе основных направлений их развития, делается вывод, что наиболее вероятным является дальнейшее совершенствование существующих технологий передачи кинетической энергии, за счет уменьшения масса-габаритных характеристик оружия и одновременного роста деструктивной способности новых типов вооружения, с параллельным усилением влияния на Вооруженные Силы таких технологий, как киберпространство, автономные (роботизированные) системы и оружие прямой передатчи энергии. Сделан вывод, что в течение следующих десяти лет произойдет дальнейшая трансформация боевых действий от классических (теоретические роботы Клаузевица) к нетрадиционным, гибридным боевым действиям, соответствующим теоретическим работам Сан-Цзы.

Ключевые слова: *зарождающиеся технологии, Вооруженные Силы, доктрина, баланс сил.*

УДК 355.014

Вдовенко Сергій Григорович
Даник Юрій Григорович *(д-р техн. наук, професор)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

КОНЦЕПТУАЛЬНІ НАПРЯМИ КОМПЛЕКСНОГО ВИРІШЕННЯ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ СКРИТОГО УПРАВЛІННЯ ЗБРОЙНИХ СИЛ

Досліджений стан забезпечення скритого управління в Збройних Силах, тенденції розвитку організаційно-технічних заходів у сфері у цій сфері. Запропоновані нові підходи щодо побудови систем захисту інформації в Збройних Силах.

Ключові слова: *захист інформації, інформаційна безпека, кібербезпека, криптографічний захист інформації, протидія технічним розвідкам, скрите управління військами, спеціальний зв'язок.*

Вступ

Постановка проблеми. Актуальність статті. Досвід збройних конфліктів останніх десятиліть XX століття та початку XXI століття, в тому числі антитерористичної операції на території Донецької та Луганської областей свідчить про зростання вимог до організаційно-технічних засад забезпечення безпеки інформації, яка циркулює в інформаційному просторі при вирішенні задач управління військами. Однією з вимог до управління є скритність [1,2].

Скрите управління військами (силами) (далі - СУВ) - управління військами (силами), що організоване з дотриманням вимог скритності, яка має за мету забезпечення збереження в таємниці від технічних розвідок заходів щодо керівництва військами (силами) і визначає комплекс заходів щодо використання наявних засобів засекречування, шифрування, кодування, захищених автоматизованих систем управління, засобів криптографічного захисту службової інформації з одночасним виконанням заходів щодо введення противника в оману, протидії технічним розвідкам, забезпечення охорони державної таємниці, технічного захисту інформації та захисту іншої інформації з обмеженим доступом [3]. Тобто виявлення та закриття каналів, через які можливий витік секретних даних, в тому числі з використанням засобів криптографічного захисту інформації (далі - КЗІ), є одним з основних завдань СУВ .

Інтенсивний розвиток інформаційних технологій значно підвищив спроможності держав, їх збройних сил та спеціальних служб у сфері технічних розвідок. Кіберпростір визнано сферою ведення бойових дій [4]. Значно зросли можливості криптоаналізу.

Зважаючи на це, розробку та розвиток форм і способів застосування власних засобів та комплексів КЗІ слід розглядати як складову частину забезпечення кібербезпеки, а також ефективної протидії засобам технічної розвідки (далі - ПДТР) противника [5,6].

В провідних країнах світу проводяться постійні інтенсивні дослідження в цій сфері. Розроблені інноваційні організаційно-технічні заходи, системи (комплекси) КЗІ, які дозволяють в певному сенсі вирішувати зазначені питання. Але, необхідний рівень ефективності, як в організаційному так і технічному плані, досягнуто тільки в найбільш розвинених країнах.

Тому розгляд питань, які пов'язані з підвищенням цієї ефективності, є своєчасним і актуальним.

Аналіз останніх досліджень і публікацій.

До середини 70-х років XX століття, дослідження і публікації в сфері криптографії були переважно закритими, а їх результатами користувалися урядові і військові структури. У 1975 р. математики із США У.Диффи, (W. Diffie) та Э. Хэллмэн (A.Hellman) опублікували роботу "Захищеність та імітостійкість. Введення у криптографію", в якій обгрунтували принцип шифрування з відкритим ключем. Ця дата вважається початком відкритою криптографії. Серед іноземних авторів відмічається також В. Столингс (W. Stallings), який першим запропонував принцип асиметричного шифрування, але йому не було дозволено оприлюднити результати досліджень. Вітчизняні вчені також приділяють

значну увагу дослідженням в галузі криптографічного захисту інформації, такі роботи провадяться в Інституті кібернетики ім. В.М. Глушкова НАНУ, Харківському національному університеті ім. В.Н. Каразіна, Національному технічному університеті України "КПІ" ім. І.Сікорського, Національному авіаційному університеті, Житомирському військовому інституті імені С.П. Корольова, науково-навчальних закладах Державної служби спеціального зв'язку та захисту інформації України. Заслуговують на увагу публікації Горбенка І.Д., Горбенка Ю.І., Кузнєцова О.О., Потія О.В.

До цього часу опубліковано дуже мало робіт вітчизняних фахівців, присвячених питанням криптографічного захисту інформації в системі СУВ. Нажаль досвід та аналіз не чисельних публікацій щодо проведення антитерористичної операції на сході України (далі - АТО) свідчить, що у військах досі приділяється недостатньо уваги питанням забезпечення захисту інформації. [7, 8]

Аналіз показує, що основними факторами, які негативно впливають на досягнення мети щодо недопущення витоку інформації в умовах ведення антитерористичної операції є:

низька ефективність протидії щодо ведення противником комплексної розвідки із всебічним застосуванням технічних засобів (відсутність штатних підрозділів технічного захисту інформації (далі – ТЗІ) та ПДТР в тактичній ланках управління);

відсутність або недостатня кількість в усіх ланках управління ЗС України, особливо в тактичній, апаратури криптографічного захисту мовної та документальної інформації;

низький рівень підготовки особового складу з питань, які розглядаються, відсутність необхідного досвіду та нехтування правилами скритого управління.

Всі фактори, які впливають на скритність управління, умовно можна поділити на організаційно-правові та науково-технічні.

В організаційних заходах пріоритетними є підходи щодо визначення єдиних засад і вимог щодо комплексної протидії технічним розвідкам, включно питань КЗІ. При цьому, мають розроблятися і впроваджуватися концепції, засади, форми, способи, методи їх застосування, правила роботи, заходи щодо безпеки тощо. [6].

Характерною рисою підходів, які розглядаються, є комплексність застосування засобів КЗІ, що функціонують в складі систем управління, зв'язку та інформаційних систем (далі - ІС) всіх рівнів, побудованих на різних алгоритмічних та технологічних принципах. Системність такого рішення забезпечується шляхом комплексного закриття всіх інформаційних потоків, при чому самі засоби КЗІ мають бути рівномірно розподілені між органами спеціального зв'язку системи управління угрупованням, зі створенням необхідних запасів, що сприяє підвищенню їх ефективності та живучості.

Однак з урахуванням недостатньої кількості сучасних національних засобів КЗІ з одного боку, та зростанням можливостей технічних видів розвідки (радіоелектронної, кібернетичної тощо), радіоелектронної боротьби та криптоаналізу з іншого, проблема скритності управління військами вирішується недостатньо ефективно з системним запізненням відносно розвитку зазначених засобів.

Враховуючи це **метою статті** є визначення концептуальних напрямів комплексного вирішення проблеми захисту інформації в системі скритого управління в Збройних Силах.

Виклад основного матеріалу дослідження

Одним із основних елементів який забезпечує вирішення проблеми захисту інформації в системі скритого управління в Збройних Силах є підсистема КЗІ.

Ефективність КЗІ залежать від:

інтенсивного розвитку та розширення переліку типів, класів і можливостей комплексів (засобів) технічних видів розвідки і РЕБ, а також варіантів, форм, способів, масштабів та наслідків їх застосування, і продуктивності криптоаналізу;

наявності і стану розвитку засобів, способів, методів, моделей, і тактики протидії технічним розвідкам, зокрема, у сфері КЗІ;

наявності відповідних висококваліфікованих фахівців та інтегрованої навчально-науково-виробничої бази.

При цьому, комплекс криптографічного захисту інформації є сукупністю взаємодіючих апаратно-програмних засобів з різним ступенем інтегрованості та автоматизації, які забезпечують виконання завдань щодо криптографічного перетворення інформації та передачі криптограм.

Найбільш небезпечним, з точки зору СУВ є втрата (компрометація) КЗІ, або взяття його під контроль.

З метою запобігання таким загрозам та ризикам розробляються та здійснюються організаційно-технічні заходи щодо забезпечення безперервності, оперативності, достовірності та стійкості скритого зв'язку.

Тому, до систем КЗІ, що розробляються мають бути визначені ряд вимог щодо їх захисту від усіх можливих загроз, насамперед – щодо криптостійкості [9, 25]. Вперше ці вимоги сформульовані ще у 1883 році Огюстом Керкгоффсом. Одна з вимог, відома як принцип Керкгоффса, така: "Система не має вимагати секретності й у разі потрапляння до ворога не має втрачати надійності". [10, 11]

Відомий американський математик і криптограф К. Шеннон (Cl. Shannon) в своїй доповіді Конгресу США 1 вересня 1945 року, під назвою "Теорія зв'язку в секретних системах" сформулював тезу про необхідність припущення

щодо наявності у противника будь-якого обладнання, необхідного для перехоплення і запису сигналів секретних повідомлень. В якості єдиної потенційної загрози криптосистемі розглянуто здатність противника щодо дешифрування криптограм, тобто його можливості щодо криптоаналізу (рис.1) [11]. За таких умов єдиною необхідною й достатньою вимогою щодо безпеки інформації можна було вважати – криптостійкість.

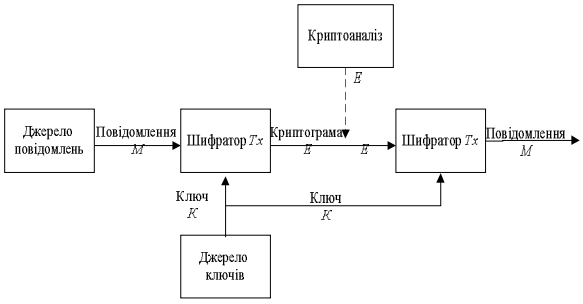


Рис. 1. Схема секретної системи (за Шенноном).

З розвитком інформаційних технологій, широким їх застосуванням в системах державного і військового управління, розвідки, модель загроз безпеці інформації змінилася в бік ускладнення

У загальному вигляді загрози можна умовно поділити на три групи: техногенні, антропогенні та такі, що обумовлені стихійними подіями. Загрози третьої і значною мірою другої групи нівелюються організаційними, правовими, освітніми та оперативно-розшуковими заходами. Задача запобігання, або зниження рівня техногенних та частини антропогенних загроз, досягається вирішенням науково-технічних та організаційно-технічних задач [9, 25].

Тому, головним завданням при створенні засобів (комплексів) КЗІ є розробка методу криптографічних перетворень та математичне доведення його гарантованої стійкості проти криптоаналізу, за умов забезпечення високої продуктивності алгоритму за програмною, програмно-апаратною та апаратною реалізацією та оптимального підходу до порівняльної простоти побудови та вартості технічної та технологічної реалізації проекту [12,13]. При цьому, слід враховувати важливість вирішення ряду задач, які безпосередньо не пов'язані з криптографією. Наприклад, максимальне зниження імовірності витоку інформації по каналам побічних електромагнітних випромінювань та наведень (далі - ПЕМВН), недопущення несанкціонованого доступу (далі - НСД) до інформації та обладнання, забезпечення кібербезпеки тощо (рис.2) [13, 14].

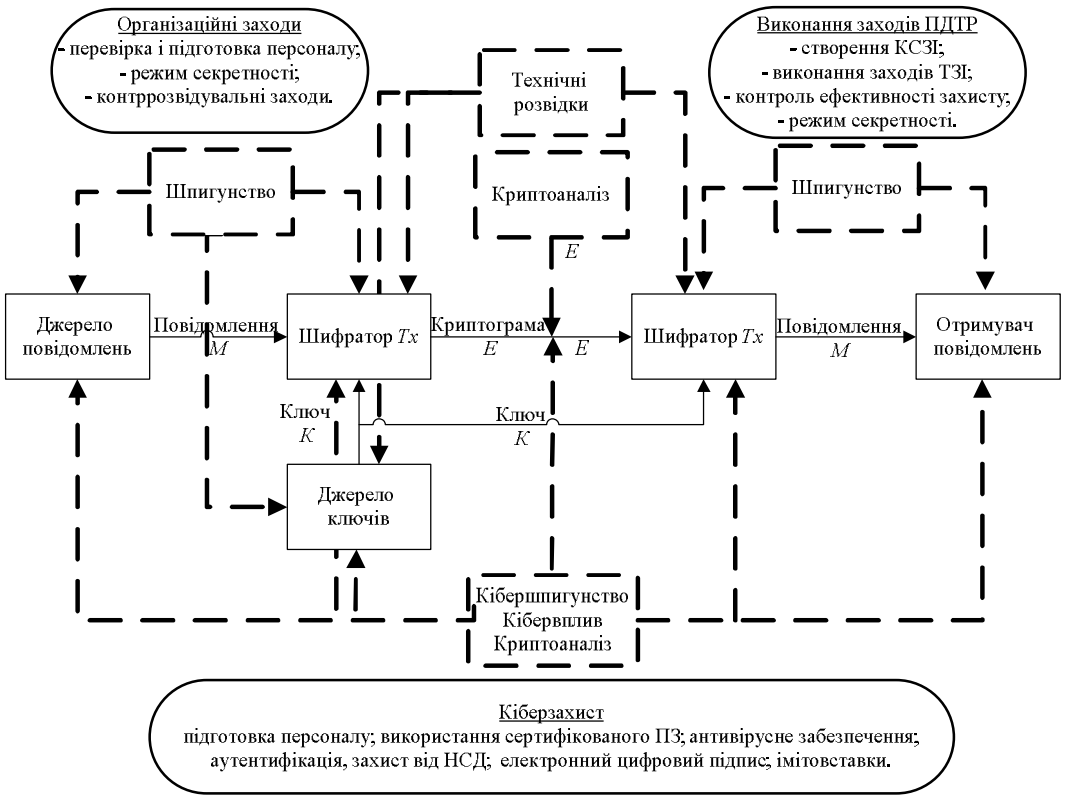


Рис. 2. Схема потенційних загроз техногенного і антропогенного характеру та варіанти заходів щодо запобігання їм

Сучасні підходи до оборонного планування вимагають раціонального використання наявних у держави можливостей і ресурсів [15, 16]. Ефективність застосування засобів і комплексів КЗІ визначається співвідношенням між важливістю і обсягами завдань, які можуть бути вирішені за їх допомогою та вартістю їх розроблення, виробництва й експлуатації. [12]

Таким чином, комплексна організаційно-технічна система захисту інформації, має бути адекватною загрозам, але не більш вартісною ніж цінність самої інформації.

Традиційно вважається, що система спеціального зв'язку (криптографічного захисту інформації) має повноцінно функціонувати як в мирний час так і в особливих умовах та бути готовою до функціонування особливий період, включно стан війни.

В Збройних Сил України протягом 1992-2016 років здійснювалися організаційно-правові, науково-технічні, освітні та інші заходи по переходу від системи шифрованого зв'язку та режиму секретності, яка залишилась у спадок від збройних сил колишнього СРСР, до системи охорони державної таємниці Збройних Сил України, яка складається з підсистем:

режиму секретності та секретного документального забезпечення;

захисту інформації (технічного і криптографічного) та підсистеми технічного забезпечення.

На сьогодні в ЗС України завдання безпосередньо КЗІ, а також ряд пов'язаних з ними, виконують Центральне управління охорони державної таємниці та захисту інформації, Головне управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України та безпосередньо або функціонально підпорядковані їм військові частини і структурні підрозділи (рис.3).

Рис. 3. Існуюча модель організації криптографічного захисту інформації в ЗС України

Відсутність державної програми реформування системи охорони державної таємниці, хронічне недофінансування науково-дослідних та дослідно-конструкторських робіт з розробки національних засобів КЗІ, а також незначні обсяги закупівель засобів КЗІ розроблених вітчизняних виробниками, негативно вплинули на ефективність скритого управління [17]. Окупацію Криму та воєнну агресію на Сході України [15], Збройні Сили, інші військові формування та правоохоронні органі нашої держави зустріли маючи на озброєнні (забезпеченні) різнотипні засоби спеціального зв'язку і криптографічного захисту інформації, іноді з різними криптоалгоритмами. Збройні Сили України, переважно застосовували апаратуру колишнього СРСР, в тому числі таку, що визнавалася морально й фізично застарілою (включно мобілізаційний запас). Мережі зв'язку та інформаційних систем Збройних Сил, інших військових формувань і правоохоронних органів (далі - ІВФ і ПрО) мали різну ступінь інтегрованості, були побудовані з урахуванням визначених їм завдань та обсягів фінансування. Їх системи управління перебували на різних етапах реформування. Збройні Сили, виходячи з ряду об'єктивних і суб'єктивних причин, знаходилися в не самому кращому положенні. Польова (мобільна) компонента системи зв'язку та ІС була побудована на радянських засобах, переважно аналогових. Слід також відмітити, що під час анексії Криму, з метою запобігання захоплення противником, було екстрено знищено значну кількість засобів КЗІ, ключових засобів до них тощо.

З метою виправлення ситуації, було вжито ряд заходів спрямованих на термінову закупівлю засобів зв'язку, технічного й криптографічного захисту інформації. За відсутності вітчизняних

конкурентоспроможних інформаційних технологій було надано перевагу технічним засобам оброблення інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують захист інформації. Комунікаційне обладнання іноземного виробництва, яке використовується у мережах зв'язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються. За таких умов створилися можливості витоку інформації, порушення її цілісності та блокування [8, 9 ,17].

Витік (розголошення) інформації, яка становить державну та іншу передбачену законом таємницю, службової інформації тощо — це одна з основних можливих загроз національній безпеці України в інформаційній сфері [18].

На протязі 2015 — 2016 років на державному рівні були визначені стратегічні цілі та завдання щодо:

реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом;

удосконалення законодавства у сфері криптографічного та технічного захисту інформації з урахуванням норм і стандартів ЄС та НАТО;

розвитку та вдосконалення системи технічного і криптографічного захисту інформації, системи захищених телекомунікацій на сучасній технологічній базі за стандартами (вимогами), що використовуються провідними європейськими державами з урахуванням практики держав - членів НАТО та ЄС;

організації розроблення уніфікованих сучасних **вітчизняних** комплексів та засобів спеціального зв'язку і захисту інформації, модернізації наявних та забезпечення їх виробництва з урахуванням реальних потреб суб'єктів сектору безпеки і оборони;

забезпечення кібербезпеки і безпеки інформаційних ресурсів;

створення системи підготовки кадрів у сфері кібербезпеки та захисту інформації для потреб органів сектору безпеки і оборони [7, 12].

Слід відмітити, що в розвинених державах світу при визначенні ряду завдань державного і воєнного управління акцентується увага на обов'язковості наявності національних рішень щодо захисту інформації.

Так, Стратегія національної безпеки республіки Польща розглядаючи питання охорони інформації з обмеженим доступом, зокрема в системах спеціального зв'язку та підкреслюючи важливість співпраці з НАТО та ЄС, вирішальне значення надає розвитку та впровадженню національних рішень в галузі криптографії [19].

Доктрина інформаційної безпеки РФ до основних напрямків інформаційної безпеки в галузі державної безпеки відносить заходи щодо забезпечення захисту інформації що містить державну таємницю, іншу інформацію з обмеженим доступом за рахунок впровадження відповідних інформаційних технологій, в тому числі наукових досліджень та дослідних розробок зі створення власних перспективних технологій та засобів забезпечення інформаційної безпеки [20].

З огляду на зазначене вважається за необхідне та доцільне розробити Концепцію розвитку системи охорони державної таємниці (захисту інформації) держави.

На підставі Концепції розробити Державну програму розвитку системи охорони державної таємниці (захисту інформації), яку затвердити Указом Президента України після розгляду в Раді Національної безпеки і оборони України.

Під час розробки Концепції і Державної програми розвитку системи охорони державної таємниці використовувати досвід та напрацювання насамперед Збройних Сил України.

На наш погляд, на відміну від існуючої системи охорони державної таємниці основною парадигмою має стати **захист інформації з обмеженим доступом.**

До виконання завдань із їх розроблення слід залучити Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, Генеральний штаб Збройних Сил України, науково-дослідні установи та вищі навчальні заклади, у тому числі військові**.**

У Концепції та Державній програмі необхідно передбачити розвиток систем технічного та криптографічного захисту інформації [17].

Обов'язково мають бути передбачені заходи щодо:

визначення вичерпного переліку напрямів наукових досліджень та профільних науково-дослідних установи в галузі КЗІ та ТЗІ;

встановлення інституту генерального (головного) конструктора засобів КЗІ;

визначення порядку і джерел фінансування фундаментальних наукових досліджень, НДДКР тощо, з урахуванням авторського права;

визначення порядку обов'язкового погодження з Генеральним штабом ЗС України оперативно-тактичних й тактико-технічних вимог на засоби і комплекси спеціального зв'язку та криптографічного захисту інформації, які плануються до розроблення в інтересах ІВФ та ПрО.

Аналіз світових тенденцій розвитку систем зв'язку та інформаційно-телекомунікаційних систем свідчить що за умов постійного ускладнення інформаційно-телекомунікаційних технологій, проблему скритності управління, зокрема безпеки інформації, неможливо вирішити

тільки створенням і застосуванням апаратури КЗІ. Вона може бути вирішена тільки за рахунок комплексного підходу до створення озброєння, військової техніки, в тому числі автоматизованих систем управління та зв'язку, якій має враховувати необхідність захисту інформації в їх складових частинах [21, 22].

Так, сучасна программа модернізації засобів криптографічного захисту інформації ЗС США передбачає:

розвиток технологій криптографічного захисту даних в локальних радіомережах командних пунктів, підтримка інфраструктури відкритих ключів, розробка нових алгоритмів програмування систем криптографічного захисту;

збільшення довжини ключової послідовності;

удосконалення апаратно-програмних систем автоматичної генерації і розподілу ключів шифрування;

підвищення швидкодії шифрувального обладнання та збільшення кількості каналів зв'язку, що обслуговуються одним засобом криптографічного захисту;

підвищення рівня оперативно-технічної сумісності засобів криптографічного захисту інформації на національному та коаліційному рівнях;

збільшення обсягів постачання мережевого обладнання з функцією IP-шифрування. [21]

Вважається що реалізація програм модернізації засобів криптографічного захисту інформації в США значно покращить надійність функціонування інформаційних систем і систем управління та одночасно обмежить можливості сторонніх осіб щодо НСД до інформаційного ресурсу. При цьому, в США й в інших державах, для вирішення окремих завдань розробляються та застосовуються такі типи апаратно-програмних засобів криптографічного захисту інформації:

зовнішні, до яких віднесені магістральні (on line) та абонентські (off line, on line) шифратори;

вбудовані безпосередньо в апаратуру зв'язку модулі, плати, чипи шифрування. [21]

В Росії, де традиційно розробляються та виготовляються зовнішні апаратно-програмні засоби попереднього й лінійного шифрування, для побудови магістрального високошвидкісного дуплексного IP-шифратора на базі криптографічного алгоритму ГОСТ 28147-89 розроблено інноваційний для РФ модуль криптографічних перетворень АВС – 10. Апаратна реалізація виробу суттєво підвищує швидкість шифрування, виключає можливість втручання в процес криптографічних перетворень [23].

В Україні розробку і виробництво засобів і комплексів криптографічного захисту інформації здійснюють декілька підприємств, які мають потужній науково-технічний потенціал: акціонерне товариство "Інститут інформаційних технологій" (м. Харків), Науково-впроваджувальна фірма "Криптон " (м.Київ), товариство з обмеженою відповідальністю "Трител " (м.Київ), науково-технічний комплекс "Імпульс " (м.Київ). Продукція підприємств є цілком конкурентоспроможною та може експортуватися [26, 27, 28, 29, 30].

Криптографія й надалі буде активно розвиватися. Головним завданням її сьогодення є розробка та впровадження швидкісних методів криптографічних перетворень із забезпеченням високого рівня секретності. Це обумовлено сучасними інформаційно-комунікаційними можливостями та підходами до побудови мереж зв'язку та інформаційних систем, в яких циркулюють надвеликі обсяги інформації. Вирішення питання знаходиться в площині ускладнення криптосистем, підвищення криптографічної стійкості алгоритмів, мінімізації обсягів блоків даних.

Перспективним напрямком подальшого розвитку криптографії розглядається створення квантових систем, особливо для захисту важливих стратегічних державних і військових каналів зв'язку. Перетворення на основі квантових обчислень в майбутньому дозволять вирішувати всі завдання значно швидше ніж на звичайних комп'ютерах [24]. В нашому контексті слід розглядати суттєве підвищення можливостей криптоаналізу.

Звичайно, можливості класичної криптографії ще не вичерпані, але слід визначитися щодо перспектив застосування криптоалгоритмів колишнього СРСР, зокрема ГОСТ 28147-89.

Тим більш, що національний блочний шифр «Калина» має значно більшу продуктивність та криптостійкість ніж модифікований російський ГОСТ 28147-89 та алгоритм AES (США) з аналогічною довжиною ключа [12, 13, 25].

Враховуючи різноманітність завдань органів військового управління різних рівнів та військових частин і підрозділів Збройних Сил України, а також факторів та умов, що впливають на їх бойову діяльність, для забезпечення ефективного функціонування мереж спеціального зв'язку та інших інформаційних систем військового призначення, їх спроможності виконати поставлені завдання з високою якістю та у визначені терміни, необхідно мати на озброєнні (забезпеченні) декілька типів засобів криптографічного захисту інформації та спеціального зв'язку, які б відповідали наступним вимогам:

функціональна гнучкість, адаптивність модульність, компактність та конструктивна простота засобів і комплексів спеціального зв'язку та КЗІ;

доступність, надійність, різноманітність, простота застосування, гнучкість та адативність до загроз (атак) національних криптографічних алгоритмів та ключових систем, реалізація розумного балансу між необхідністю швидко передавати величезні обсяги інформації та довжиною ключової послідовності засобів КЗІ;

можливість застосування багаторівневого криптографічного захисту інформації (безпосередньо корисної інформації та технологічної інформації систем, що забезпечують);

можливість одночасної реалізації (опційно) двох алгоритмів криптографічного захисту (національного і коаліційного, або національного і колишнього СРСР – на перехідний період);

забезпечення вимог щодо технічного захисту інформації, зокрема щодо заборони витоку інформації по каналам ПЕМВН, захисту від НСД тощо;

багатоваріантність виконання криптографічних модулів (чипів, плат, блоків, виробів) для забезпечення їх спільної роботи в єдиній мережі;

адаптивна стандартність інтерфейсів та операційних систем;

автоматизоване здійснення обробки інформації та даних;

реалізація багаторівневої системи контролю безпеки та захисту від помилок персоналу;

можливість застосування в якості засобів спеціального зв'язку різноманітного периферійного й допоміжного обладнання;

малогабаритність, забезпечення вимог засобів щодо рухомості, кліматичних обмежень, впливу механічних навантажень, електроживлення, електромагнітного впливу тощо.

Висновки й перспективи подальших досліджень

Таким чином, для забезпечення конфіденційності, достовірності, цілісності, автентичності інформації з обмеженим доступом в системах управління держави, ЗС, ІВФ і ПрО необхідно виконати значну кількість різноманітних організаційно-правових, науково-технічних, військово-технічних та фінансово-економічних заходів.

В практичній реалізації задачі вважається за можливе й доцільне використання у сфері оборони теоретичних засад та технологічних рішень науково-технічних (впроваджувальних) підприємств України щодо асиметричних криптосистем з відкритим ключем. Зокрема, для створення систем шифрування мовної та документальної інформації тактичного рівня, систем державного впізнавання для поля бою, забезпечення захисту технологічної інформації інформаційних систем, аутентифікації користувачів, а також для запобігання несанкціонованому застосуванню засобів ураження.

Отже, основний потік найбільш важливих оперативних документальних розпоряджень і повідомлень слід захищати із застосуванням симетричних системи шифрування, що забезпечують високий ступінь секретності, іншу інформацію – за допомогою порівняльно повільних асиметричних криптографічних систем.

Між інших переваг, таке рішення веде до заощадження бюджетних коштів та певним чином знижує ефективність системи РЕР та кіберрозвідки противника, що є актуальним в особливий період.

В статті розглянуті концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління військами Збройних Сил України.

В подальшому будуть досліджені вимоги до побудови засобів і комплексів криптографічного захисту інформації систем управління військового призначення, їх криптографічних алгоритмів, ключових систем.

Література

1. Управление войсками в операциях. підручник М. ВА ГШ, 1975. – 380 с.
2. **Розум І. Ю.**. Застосування телекомунікаційних систем у процесі управління військами: посібник для вищих військових навчальних закладів / Розум І. Ю., Савісько П. А., Огороднійчук М. Д. та ін. – К.: НУОУ, 2016. – 164 с.
3. Звід відомостей, що становлять державну таємницю, затверджений наказом СБУ від 12.08.2005 №440, зареєстрований в Міністерстві юстиції України 17.08.2005 за № 902/11182, зі змінами
4. Стратегія кібербезпеки України затверджена Указом Президента України від 15 березня 2016 року № 96/2016
5. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015
6. Концепція розвитку сектору безпеки і оборони України, введена в дію Указом Президента України від 14.03.2016 №92/2016
7. Радіо для прибиральників. Зв'язок у ЗСУ – сучасний, але не військовий. АНАЛІЗ армійського досвіду. Режим доступу: http://texty.org.ua/pg/article/solodko/read/73135/Radio_dla_prybyralnykiv_Zvjazok_u_ZSU_
8. **Гуманенко В.** Где грань между безграмотностью генералов и откровенным предательством? http://fakeoff.org/war/gde-gran-mezhdu-bezgramotnostyu-generalov-i-otkrovennym-predatelstvom
9. **Даник Ю.Г.** Основи захисту інформації / Даник Ю.Г., Вдовенко С.Г., Шестаков В.І., Писарчук О.О., Грищук Р.В., Куліківський М.В., Ходаківський В.М.: навчальний посібник. Житомир – 2015, 219 с.
10. **Керкгоффс О**. Военная криптография. Режим доступу:https://ru.wikipedia.org/wiki/военная_криптография
11. **Шеннон К**. Работы по теории информации и кибернетике / Издательство иностранной литературы, – Москва – 1963 – 832 с.
12. **Горбенко І.Д**. Прикладаная криптології. Теорія. Практика. Застосування. / монографія. / Горбенко І.Д., Горбенко Ю.І.Видання 2-ге, перероблене й доповнене. Харків-2012, видавництво «Форт», 877 с.
13. **Кузнецов О.О.** Обгрутування вимог, побудова та аналіз перспективних симетричних криптоперетворень на основі блочних шифрів / Кузнецов О.О, Олійников Р.В., Горбенко Ю.І., Пушкарьов А.І., Дирда О.В., Горбенко І.Д. // Прикладная радіоелектроніка – 2014 – №3 – С. 124-141.
14. **Чеховский С.А.** Электромагнитные излучения компьютерных систем и защита информации науково - технічний журнал / Захист інформації – 2003 – № 3 – С.18 - 29.
15. Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015.

16. Стратегічний оборонний бюлетень України, введений в дію Указом Президента України від 6 червня 2016 року № 240/2016
17. **Вдовенко С.Г.** Сучасні вимоги до охорони державної таємниці та захисту інформації з обмеженим доступом в особливий період / Імперативи розвитку цивілізації – 2015 – №2. Київ – ФОП О.С.Ліпкан, С. 93-96.
18. Закон України Про основи національної безпеки України від 19 червня 2003 року № 964-IV, зі змінами (Відомості Верховної Ради України (ВВР), 2003, № 39, ст.351)
19. National Security Strategy Of The Republic Of Poland, The National Security Bureau – Warsaw –2014.
20. Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. Режим доступу: http://base.garant.ru/71556224/
21. **Морозов Д.А.** Шифровальное оборудование вооружённых сил США / Зарубежное военное обозрение 2016, № 3, С. 38-43.
22. **Букашкин С.А.** История развития шифрующей аппаратуры в России / Цифровая обработка сигналов – 2011 – №4, Режим доступу: http://www.dspa.ru/articles/year2011/jour11_4/art11_4_1.pdf
23. Модуль криптографических преобразований для построения перспективной шифраппаратуры. Режим доступу: http://www.citis.ru/citis_project_3.html.
24. Дошина А. Д., Михайлова А. Е., Карлова В. В. Криптография. Основные методы и проблемы. Современные тенденции криптографии // Современные тенденции технических наук: Материалы IV Междунар. науч. конф. Казань – 2015 — С. 10-13. Режим доступу: https://moluch.ru/conf/tech/archive/163/8782/
25. **Горбенко Ю.І.** Побудування та аналіз систем. Протоколів і засобів криптографічного захисту інформації. Частина 1. Методи побудування та аналізу, стандартизації та застосування криптографічних систем. монографія. / Харків – 2015, видавництво «Форт», 959 с.
26. ПАО ІІТ. Режим доступу: https://iit.com.ua//
27. ПАО ІІТ. Режим доступу: http://ksystems.com.ua/iit/
28. НВФ Кріптон. Режим доступу: http://www.crypton.ua/index.php/uk/
29. ООО Трітел. Режим доступу: http://www.tritel.ua/index.php/uk/
30. НТК Імпульс. Режим доступу: http://ntkimpuls.com.ua/uk/

КОНЦЕПТУАЛЬНЫЕ НАПРАВЛЕНИЯ КОМПЛЕКСНОГО РЕШЕНИЯ ПРОБЛЕМЫ ЗАЩИТИ ИНФОРМАЦИИ В СИСТЕМЕ СКРЫТОГО УПРАВЛЕНИЯ ВООРУЖЁННЫХ СИЛ

Вдовенко Сергей Григорьевич (доцент кафедры связи и информационных систем)
Даник Юрий Григорьевич (д-р техн. наук, професор, начальник института информационных технологий)

Национальный университет оборони Украины имени Ивана Черняховского, Киев, Украина

Целью статьи *является определение концептуальных направлений комплексного решения проблемы защиты информации в системе скрытого управления войсками.*

Интенсивное развитие информационных технологий значительно повысило возможности государств, их вооружённых сил и специальных служб в сфере технической разведки. Киберпространство признано сферой ведения боевых действий. Значительно возросли возможности криптоанализа. Это требует существенных затрат на осуществление мероприятий по противодействию техническим разведкам, и в частности на криптографическую защиту информации. Вместе с тем современные подходы к оборонному планированию требуют рационального использования имеющихся у государства возможностей и ресурсов.

В статье рассмотрены концептуальные направления комплексного решения проблем защиты информации и намечены подходы к формированию единых основ в системе скрытого управления войсками, направленные на снижение эффективности системы радиоэлектронной разведки противника и экономию бюджетных средств, что актуально в особый период.

Ключевые слова: *защита информации, информационная безопасность, кибербезопасность, криптографическая защита информации, скрытое управление войсками, противодействие техническим разведкам, специальная связь.*

CONCEPTUAL APPROACHES FOR COMPLEX SOLUTION OF INFORMATION SECURITY IN THE CODE C2 OF THE ARMED FORCES

Serhii G. Vdovenko *(Associate Professor of the Communication and Information Systems Department)*
Yury G. Danik *(doctor of technical sciences, Professor, Head of Information Technologies Institute)*

Ivan Chernyakhovsky National Defense University of Ukraine, Kiev, Ukraine

The purpose of this article *is to define conceptual approaches for a comprehensive solution on information protection in the code C2 of troops.*

The intensive development of information technologies has significantly increased the capabilities of countries, their armed forces and special services in the field of electronic warfare. Cyberspace is recognized as a place of warfare. Possibilities of cryptanalysis have been significantly increased and require increasing funds for counter measures against electronic warfare activities, and in particular, for the information cryptographic protection. At the same time, modern approaches to defence planning require rational use of the state's capabilities and resources.

The article considers conceptual approaches for complex solution of information security problems and outlines approaches to the formation of unified bases for information security in the system of code C2 of

troops to reduce the effectiveness of the enemy's electronic reconnaissance system and saving budget funds, what is relevant in a crisis period.

Key words: *information security, cyber security, information cryptographic security, troops code C2, countermeasures against the electronic warfare, special purpose communication.*

References

1. Command of troops in operations. (1975) [*Upravlenye voiskamy v operatsyiakh*], Textbook M. VA GHS, - 380 p.
2. **Rozum I. Yu.,** Savis'ko P. A., Ogorodniychuk M. D. et al. (2016), Application of telecommunication systems in the process of command of troops: a manual for higher military educational institutions [*Zastosuvannia telekomunikatsiinykh system u protsesi upravlinnia viiskamv*], - Kyiv. NUOU, 164 p.
3. The number of offers to become a holder of a title. [*Zvid vidomostei, shcho stanovliat derzhavnu taiemnytsiu*], the instructions issued by the Security Service of Ukraine on 12.08.2005 No. 440, registrations in the Ministry of Justice of Ukraine on 08/17/2005 for No. 902/11182
4. The strategy of cyber security of Ukraine. [*Stratehiia kiberbezpeky Ukrainy*], was approved by the Decree of the President of Ukraine dated March 15, 2016, No. 96/2016.
5. The National Security Strategy of Ukraine. [*Stratehiia natsionalnoi bezpeky Ukrainy*], *approved by the Decree of the President of Ukraine dated 05/26/2015 № 287/2015.*
6. *Concept of development of the security and defense sector of Ukraine* [*Kontseptsiia rozvytku sektoru bezpeky i oborony Ukrainy*], *put into effect by the Decree of the President of Ukraine dated March 14, 2016, No. 92/2016.*
7. *"Radio for cleaners. Communication with the Armed Forces is modern, but not military. ANALYSIS OF ARMY EXPERIENCE. "* ["*Radio dlia prybyralnykiv. Zviazok u ZSU – suchasnyi, ale ne viiskovyi. ANALIZ armiiskoho dosvidu.*"]. available at: http://texty.org.ua/pg/article/solodko/read/73135/Radio_dla_prybyralnykiv_Zvjazok_u_ZSU_
8. ***Gumanenko V.*** *"Where is the line between illiteracy of generals and frank betrayal?"* ["*Gde gran mezhdu bezghramotnostiu generalov y otkrovennym predatelstvom?"*] *available at:* http://fakeoff.org/war/gde-gran-mezhdu-bezgramotnostyu-generalov-i-otkrovennym-predatelstvom
9. **Danik Yu.G.**, Vdovenko S.G., Shestakov V.I., Pysarchuk O.O., Gryshchuk R.V., Kulikovsky M.V., Khodakivsky V.M. (2015) Fundamentals of information protection [Osnovy zakhystu informatsii], textbook. Zhytomyr . 219 p.
10. ***Kerkhoffs O.*** *"Military cryptography"*. ["*Voennaya kriptografiya*"], *available at*: https://ru.wikipedia.org/wiki/военная _криптография
11. **Shannon K.** Works on the theory of information and cybernetics (1963) [*Rabotyi po teorii informatsii i kibernetike*], Foreign Literature Publishing, Moscow, p. p. 333 -402.
12. **Gorbenko I.D.**, Gorbenko Yu.I. (2012). An example of cryptology. Theory. Practice. Application. Monograph. [*Prykladana kryptolohiia. Teoriia. Praktyka. Zastosuvannia. Monohrafiia.*], Issue 2-th, processed and supplemented. Kharkov, publishing house "Fort", 877 p.
13. **Kuznetsov O.O.**, Oliynikov R.V., Gorbenko Yu.I., Pushkarev A.I., Dirda O.V., Gorbenko I.D. (2014) Requirements survey, construction and analysis of perspective symmetric cryptographic transformations based on block ciphers [*Obhrutuvannia vymoh, pobudova ta analiz perspektyvnykh symetrychnykh kryptoperetvoren na osnovi blochnykh shyfriv*]. Applied electronics. No. 3. p. p.. 124-141.
14. **Chekhovsky S.A**. (2003). "Electromagnetic radiation of computer systems and information protection." ["*Elektromagnitnyie izlucheniya kompyuternyih sistem i zaschita informatsii."*]. Scientific and technical journal. Information protection. No. 3. p.p..18 -29.
15. The Strategy of National Security of Ukraine [*Stratehiia natsionalnoi bezpeky Ukrainy*], approved by the Decree of the President of Ukraine dated May 26, 2015, No. 287/2015.
16. The Strategic Defense Bulletin of Ukraine [*Stratehichnyi oboronnyi biuleten Ukrainy*], enacted by the Decree of the President of Ukraine dated June 6, 2016 No. 240/2016
17. **Vdovenko S.G**. (2015). "Modern requirements for the protection of state secrets and the protection of information with restricted access in a crisis period". ["*Suchasni vymohy do okhorony derzhavnoi taiemnytsi ta zakhystu informatsii z obmezhenym dostupom v osoblyvyi period* "]. Imperatives of the development of civilization, No.2. Kyiv, FOP O.S.Lipkan, pp. 93-96
18. The Law of Ukraine On the Basis of National Security of Ukraine [*Zakon Ukrainy Pro osnovy natsionalnoi bezpeky Ukrainy*] of June 19, 2003 No. 964-IV, as amended (Vidomosti of the Verkhovna Rada of Ukraine (VVR), 2003, No. 39, p.351)
19. National Security Strategy Of The Republic Of Poland (2014). The National Security Bureau. Warsaw..
20. *The doctrine of information security of the Russian Federation* [*Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii*], *approved by Decree of the President of the Russian Federation dated December 5, 2016, No. 646. available at*: http://base.garant.ru/71556224/
21. **Morozov D.A.** (2016) "USF Encryption Equipment" ["*Shifrovalnoe oborudovanie vooruzhyonnyih sil SShA* "], Foreign Military Review, No. 3, pp. 38-43.
22. *Bukashkin S.A. (2011). "The history of the development of encryption equipment in Russia"*. ["*Istoriya razvitiya shifruyuschey apparaturyi v Rossii*"] *Digital signal processing. No. 4, available at*: http://www.dspa.ru/articles/year2011/jour11_4/art11_4_1.pdf
23. *"The module of cryptographic transformations for the construction of perspective cipher equipment."* ["*Modul kriptograficheskih preobrazovaniy dlya postroeniya perspektivnoy shifrapparaturyi.*"] *available at*: http://www.citis.ru/citis_project_3.html.
24. *Doshina A.D., Mikhailova A.E., Karlova V. V. (2015)* "*Cryptography. Basic methods and problems. Modern Trends of Cryptography*". ["*Kriptografiya. Osnovnyie metodyi i problemyi. Sovremennyie tendentsii kriptografii*"]. *Modern Trends in Technical Sciences: Materials IV International. scientific conf. Kazan, pp. 10-13*. available at: https://moluch.ru/conf/tech/archive/163/8782/
25. **Gorbenko Yu.I.** (2015). Building and analyzing systems. Protocols and means of cryptographic protection of information. Part 1. Methods of construction and analysis, standardization and application of cryptographic systems. Monograph. [*Pobuduvannia ta analiz system. Protokoliv i zasobiv kryptohrafichnoho zakhystu informatsii. Chastyna 1. Metody pobuduvannia ta analizu, standartyzatsii ta zastosuvannia kryptohrafichnykh system. Monohrafiia.*] Kharkiv, Fort Publishing, 959 p.
26. *IIT*. available at*:* https://iit.com.ua//
27. *IIT*. available at*: http:*//ksystems.com.ua/iit/
28. *Kripton.* available at*:* http://www.crypton.ua/index.php/uk/
29. *Tritel. available at*: http://www.tritel.ua/index.php/uk/
30. *Impuls. available at*: http://ntkimpuls.com.ua/uk/

УДК 316.259+355.01

Олександр Миколайович Гук[1]
Олексій Юрійович Чередниченко[1]
Роман Михайлович Штонда[1]
Ігор Олексійович Диба[2]

[1]***Військовий інститут телекомунікацій та інформатизації, Київ, Україна***
[2]***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

ДІЇ В КІБЕРПРОСТОРІ ПІД ЧАС ПІДГОТОВКИ ТА ВЕДЕННЯ МЕРЕЖЕЦЕНТРИЧНОЇ ВІЙНИ

У статті розглянуто зміни характеру ведення сучасних війн і ознаки переходу до мережецентричної моделі управління бойовими діями, спектр воєнних дій держави, основні напрямки та умови досягнення інформаційної переваги над противником. Визначено роль та місце дій в кіберпросторі під час підготовки та ведення мережецентричних війн та їх вплив на системи контролю та комунікацій життєво і стратегічно важливих об'єктів держави. Обґрунтовано необхідність захисту від кібератак об'єктів критичної інфраструктури держави та розвитку власних кіберозброєнь.

Ключові слова: *інформаційна війна, кіберпростір, мережецентризм, спектр воєнних дій держави, поріг оголошення війни, кібератака, кібербезпека, інформаційна перевага, мережецентрична війна, кібернетична зброя, кібернетичний вплив.*

Вступ

Аналіз останніх локальних війн і збройних конфліктів показав докорінні зміни у тактиці і стратегії ведення збройної боротьби. Супротивник, який має технологічну перевагу, замість зіткнення з противником по фронту, застосовує сили та засоби на всю глибину його території. Кількість військ, що розгорнуті на певному напрямі, вже не грає вирішальної ролі в досягненні мети операції. Для забезпечення переваги над противником вже недостатньо мати в своєму розпорядженні певний бойовий потенціал, а важливо застосувати його в потрібному місці та в потрібний час.

Постановка проблеми. Інформаційні війни в теперішній час є складовою частиною ведення сучасного військового протиборства. Головною метою ведення інформаційної війни є дезінформація, психологічне та інформаційне подавлення військ противника, а також порушення роботи систем управління військами, органів державного управління, систем цивільної оборони та життєзабезпечення країни.

Оборонний потенціал будь-якої держави може бути значно знижений противником через кіберпростір ще до початку бойових дій. Це необов'язково може бути вплив на бойові системи. В державі є банківські системи та структури державного управління, які використовують глобальну мережу. Порушення сталого функціонування цих систем або кіберсистем їх контрагентів може призвести до зниження обороноздатності та сприяти досягненню противником політичних цілей війни.

Аналіз остатніх досліджень і публікацій.

Питання, що стосуються сутності мережецентричних операцій та особливостей управління військами у ході їх ведення, досить широко висвітлюються у різних виданнях.

Основна модель ведення війн, діюча в арміях США і країн НАТО, заснована на концепції «мережецентричної війни». Модель «мережецентричної війни» представляється як система, що складається з трьох решіток-підсистем: інформаційної, сенсорно-розвідувальної та бойової. Основу системи складає інформаційна решітка, на яку накладаються сенсорна і бойова решітки, що взаємно перетинаються. Інформаційна решітка-підсистема пронизує собою всю систему в повному обсязі. Елементами сенсорної підсистеми є засоби розвідки, а елементами бойової решітки - засоби ураження. Ці дві групи елементів об'єднуються органами управління та командуванням. [1]

Значна увага приділяється нормативному регулюванню діяльності в кібернетичному просторі, порядок визначення шкоди, завданої кібератаками, визначення механізмів притягнення до відповідальності за її завдавання, а також співвідношення національних та міжнародних механізмів і засобів забезпечення безпеки кіберпростору.

Метою статті є визначення ролі та місця дій (операцій) в кіберпросторі під час підготовки та ведення мережоцентричної війни, а також основних завдань таких дій, та пріоритетних напрямів втілення такого досвіду в Україні.

Виклад основного матеріалу дослідження.

Термін "мережецентризм" вперше з'явився в американській комп'ютерній індустрії і став результатом прориву в інформаційних технологіях, які дозволили організовувати взаємодію між комп'ютерами не дивлячись на використання в них різних операційних систем. Відповідно до "мережецентричної моделі обчислень" користувачу не потрібно володіти усім програмним забезпеченням

для вирішення прикладних задач, а достатньо мати лише спрощене обчислювальне обладнання (мережевий комп'ютер) для звернення до віддаленої центральної бази, яка здійснює всі необхідні обчислення і забезпечує користувача усією необхідною інформацією. Пізніше ідея "мережецентризму" була взята на озброєння спеціалістами армії США. [2]

У будь-якій військовій операції має місце такий цикл подій: розвідка противника – оцінка обстановки – прийняття рішення – дії відповідно до обраного плану. Такий цикл умовно можна розділити на дві фази: інформаційну та кінетичну. Остання, в основному, визначається можливостями засобів ураження. Раніше як вітчизняні, так і закордонні вчені займались пошуком технічних рішень, пов'язаних в першу чергу із другою фазою, а саме – підвищенням мобільності, точності та вогневої міці засобів збройної боротьби. Така модель управління отримала назву "платформоцентричної", відповідно до якої розвиток військової техніки відбувався у напрямку створення та удосконалення окремих "бойових платформ", а бойовий потенціал підрозділів визначався їх кількісним нарощуванням. Але, як показує практика, для підвищення ефективності кінетичної фази є певні обмеження, крім того суттєво підвищується і вартість розробок.

Рисунок 1. Спектр воєнних дій держави

На рисунку 1 показано поділ воєнних дій на дві фази: інформаційну і кінетичну. Зверніть увагу, що ці фази не виключають одна одну, а всі дії розподіляються по спектру між суто кінетичними або суто інформаційними. Чим вище дія по спектру, тим вона більш сильна; найвища тяжкість дій – це ядерний удар або кібератака, що руйнує національну енергосистему. Дії над червоною лінією, здебільшого, загальновизнано відповідають порогу оголошення війни; дії під червоною лінією або юридично неоднозначні, або явно нижче порогу оголошення війни. Зверніть увагу, що інформаційні дії, як правило, більш юридично неоднозначні через відсутність чіткого розуміння в результаті більш короткого історичного контексту використання інформаційної війни. Хоча кібератака, яка критично порушує фінансовий сектор, потенційно може бути настільки ж руйнівною або навіть більш руйнівною, ніж терористична атака, що спонсується державою або звичайне вторгнення, область інформаційної війни (особливо кібервійни) має тенденцію бути більш двозначною через проблеми із тлумаченням суверенітету, оскільки вона пов'язана з фізичними та логічними межами комп'ютерних мереж і серверів.

Вкрай важливо, що більшість дій війни потрапляють в сферу правової неоднозначності. Це не означає, що дії в сірій зоні є законними відповідно до міжнародного права, скоріше, відсутній консенсус щодо того, як країни вважають за краще інтерпретувати свою законність. Фактично, більшість цих дій під строгим тлумаченням міжнародно-правового кодексу вважаються незаконними. Розглянемо випадок використання Росією «Патріотичних хакерів» в 2007 році для проведення розподілених атак на відмову в

обслуговуванні на державних сайтах Естонії, тим самим завдаючи шкоду здатності Естонії здійснювати управління. За словами міністра оборони Естонії, ця кібератака стала «ситуацією в області національної безпеки», що спричинило прохання про надання підтримки НАТО та подальшому створенні Центру співпраці в області кібербезпеки НАТО в Таллінні, Естонія. Ясно, що естонці вважали, що цей напад є застосування сили. Очевидно, що росіяни, маючи намір використовувати силу, зуміли спотворити міжнародне сприйняття цього використання національної сили, щоб уникнути великого, невигідного конфлікту. [3]

За таких умов була створена нова – "мережецентрична" система поглядів на управління збройними силами і бойовими засобами, покликана збільшити їх бойовий потенціал за рахунок створення єдиної інформаційно-комунікаційної мережі. Принципи ведення "мережецентричних" війн (принаймні на даному етапі розвитку їх теорії і практики) перше за все спрямовані на досягнення інформаційної переваги над противником.

Інформаційна перевага – це не передача у великій кількості інформації "бойовим платформам", а досягнення більш глибокого, яке відповідає обстановці, усвідомлення і розуміння ситуації на полі бою, більш точного з'ясування своїх переваг та недоліків противника, здатність сформувати задум дій, в якому ці переваги будуть максимальною мірою реалізовані, а недоліки противника використані у своїх цілях, випереджене прийняття й негайне доведення до підлеглих та сусідів рішень, цілком адекватних обстановці, безперервний контроль їх виконання. Нові можливості для удосконалення мережевих організаційних форм відкриває значний розвиток засобів інформатизації, оскільки для ефективності дій подібних формувань необхідно, щоб швидкість і якість обміну інформацією між ланками мережі були набагато вищими, ніж у ієрархічних структурах.

Мережецентрична війна – війна, орієнтована на досягнення інформаційної переваги. Це концепція ведення бойових дій, що передбачає збільшення бойової потужності угруповання об'єднаних сил за рахунок утворення інформаційно-комутаційної мережі, що поєднує джерела інформації (розвідки), органи управління та засоби ураження (придушення), що забезпечує доведення до учасників операцій достовірної та повної інформації про обстановку практично в реальному масштабі часу. За рахунок цього досягається прискорення процесу управління силами та засобами, підвищення темпу операцій, ефективності ураження сил супротивника, живучості своїх військ та рівня самосинхронізації бойових дій.[4]

Враховуючи особливість "мережевої" війни стосовно будь якого театру військових дій передбачається чотири основні фази ведення бойових дій:

досягнення інформаційної переваги за допомогою випереджуючого знищення (виводу з ладу, придушення) системи розвідувально-інформаційного забезпечення супротивника (засобів та систем розвідки, мережеутворюючих вузлів, центрів обробки інформації та управління);

завоювання переваги (панування) в повітрі за рахунок придушення (знищення) системи ППО супротивника;

поступове знищення залишених без управління та інформації засобів ураження супротивника, в першу чергу ракетних комплексів, авіації артилерії, бронетехніки;

остаточне придушення або знищення осередків спротиву ворога.

Успішне здійснення кожної з фаз ґрунтується на значно меншій тривалості бойового циклу "виявлення-впізнання-цілевказання-ураження" порівняно з супротивником, на більш точних та повних відомостях про угруповання супротивника, що протистоїть. [2]

Проведення операцій в кібернетичному просторі дозволяє дистанційно вивести з ладу системи життєзабезпечення, державного та військового управління, саме тому обґрунтування ефективності, стратегії та тактики даних операцій привертає значну увагу військових спеціалістів з інформаційної безпеки, збройні сили яких планують ведення "мережецентричних війн".

З військової точки зору кіберпростір являє собою специфічну складову частину більш широкого – інформаційного або інформаційно-комунікаційного простору. В структурному відношенні кіберпростір включає в себе апаратно-програмні комплекси та комп'ютерні мережі, в яких накопичується, зберігається та циркулює інформація. [4]

Необхідність порушення функціонування інфраструктури та системи життєзабезпечення населення, дозволяє зробити висновок про те, що цілями кібернетичних атак стануть системи контролю та комунікацій життєво і стратегічно важливих об'єктів:

інформаційні та комунікаційні ресурси країни;

ядерна та хімічна промисловість;

автоматизовані системи управління

технологічні процеси на стратегічно важливих підприємствах;

фінансова і банківська сфери;

енергетична система життєзабезпечення;

дорожній рух і транспортні мережі;

системи управління та зв'язку держави, поліції і армії.

Характерними рисами дій в кіберпросторі у військових цілях є:

високий темп проведення кібервпливу;

не завжди явний характер деструктивного впливу;

не завжди явне джерело деструктивного впливу;

необмежені масштаби впливу;

непередбачуваність місця і часу кібервпливу противника;

загроза незворотних катастрофічних наслідків деструктивного впливу.[1]

Збройні сили будуть вести реальні дії в кіберпросторі у військових цілях тільки з початком війни, а в мирний час вони повинні займатися всебічною підготовкою до їх ведення, маючи, у своєму кіберарсеналі такі засоби і способи дій, які в мирний час можуть навіть кваліфікуватися як негуманні, незаконні, катастрофічні за наслідками.

Слід чітко розуміти, що кіберпростір як поле

ведення протиборства двох або більше сторін буде набувати все більшого значення. Вже сьогодні бюджети відомств безпеки розвинених країн, задіяних в системі кібербезпеки держави (а кількість структур, які в цих процесах задіяні, постійно збільшується), складають мільярди доларів, і жодна з країн ще не зменшувала витрат за цими статтями (Рис.2). Не варто думати, що ці кошти вкладаються виключно в системи "оборони" і "захисту", – неформально майже всі держави займаються розробкою кіберозброєння.

Ще з моменту анексії Криму Російська Федерація використовувала кібератаки як складову своєї гібридної війни проти нашої держави. Різноманітні спеціальні підрозділи структур безпеки нашого супротивника здійснювали атаки на державні інформаційні ресурси і на персональні дані окремих політиків і громадських діячів. Найбільш відомі випадки таких дій – DDoS-атаки на урядові ресурси (МЗС , сайт Президента України , сайти органів сектору безпеки та оборони), цільові атаки на державні органи за допомогою шахрайських електронних листів, спроби порушити роботу системи ЦВК під час виборів Президента і на парламентських виборах 2014р а також функціонування вірусу Uroboros, який, з високою долею ймовірності, ідентифікований як російський.

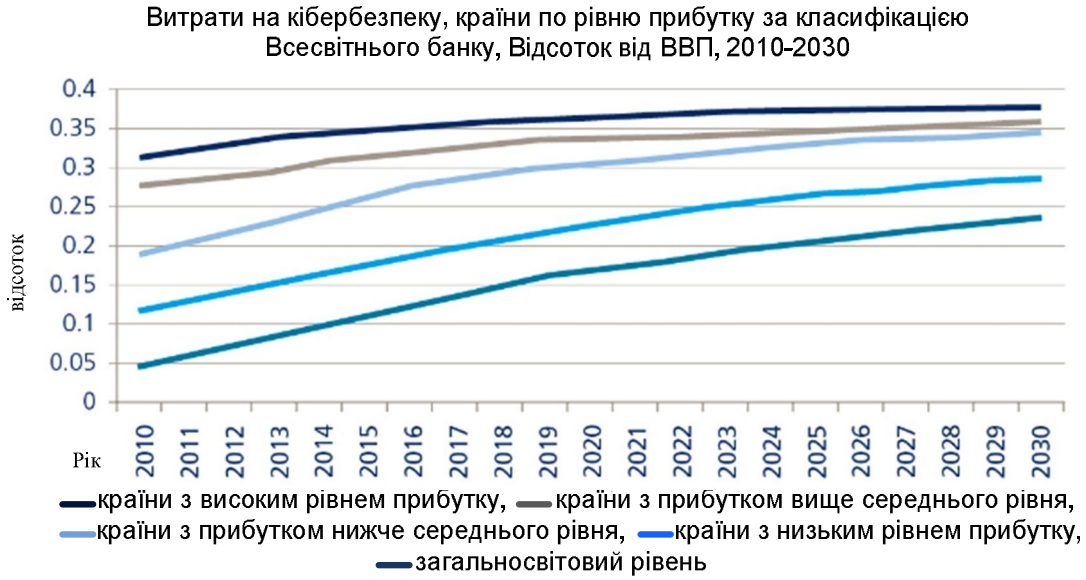


Рисунок 2. Витрати на кібербезпеку країн світу. [6]

Противник повинен знати, що намагаючись використовувати кіберпростір на шкоду національним інтересам України, він може зіткнутися з діями у відповідь. Це, у свою чергу, призведе до зростання його витрат на оборону, що і може бути однією з цілей асиметричної відповіді.[7] Саме тому потрібно приділяти більше уваги розвитку кіберозброєнь та кіберзахисту.

Висновки й перспективи подальших досліджень

Таким чином дії (операції) в кіберпросторі є невід'ємною складовою підготовки та ведення "мережецентричних війн". Зазвичай проводяться в рамках інформаційної операції (хоча не виключено проведення окремої операції в кіберпросторі), на першій фазі бойових дій, під час здобуття інформаційної переваги над противником. Відмінними ознаками дій в кіберпросторі у військових цілях є: наявність чітко сформульованої мети кібервпливу (узгодженої за цілями і завданнями операції, бою, битви); ретельне планування дій з досягнення поставленої мети і наявність відповідного комплекту сил і специфічних засобів кібервпливу. Кібернетична зброя вже зараз володіє потенціалом поразки, порівнянним зі зброєю масового ураження, а зі збільшенням комп'ютеризації державних, інфраструктурних та життєзабезпечуючих об'єктів потенціал даного виду зброї буде тільки зростати.

Література

1. Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне/Спецтехника и связь №3, 2011. **2. Тітов І. В.** Мережоцентрична концепція ведення війни XXI сторіччя / І. В. Тітов // Системи озброєння і військова техніка. – 2008. – № 3. **3. Jason Rivera.** Understanding and Countering Nation-State Use of Protracted Unconventional Warfare./ Jason Rivera//Режим доступу:http://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare **4. Alberts, David S. (David Stephen)**, Network centric warfare : developing and leveraging information superiority, 2nd Edition (Revised) / David S. Alberts, John J. Garstka, Frederick P. Stein. Second printing February 2000. **5. Дубов Д. В.** Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.**6. Overcome by cyber risks? Economic benefits and costs of alternate cyber futures**./ Zurich Insurance Group's and the Atlantic Council's Brent Scowcroft Center's on International

Security report//Available at: http://publications.atlantic-council.org/cyberrisks//**7. Горбулін В.П.** У пошуках асиметричних відповідей: кіберпростір у гібридній війні. – 2015. Режим доступу: https://gazeta.dt.ua /internal /u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni-_.html

ДЕЙСТВИЯ В КИБЕРПРОСТРАНСТВЕ ВО ВРЕМЯ ПОДГОТОВКИ И ВЕДЕНИЯ СЕТЕЦЕНТРИЧЕСКОЙ ВОЙНЫ

***Александр Николаевич Гук*[1]**
***Алексей Юрьевич Чередниченко*[1]**
***Роман Михайлович Штонда*[1]**
***Игорь Алексеевич Дыба*[2]**

[1] *Военный институт телекоммуникаций и информатизации, Киев, Украина*
[2]*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

В статье рассмотрены изменения характера ведения современных войн и признаки перехода к сетецентрической модели управления боевыми действиями, спектр военных действий государства, основные направления и условия достижения информационного превосходства над противником. Определена роль и место действий в киберпространстве во время подготовки и ведения сетецентрических войн и их влияние на системы контроля и коммуникаций жизненно и стратегически важных объектов государства. Обоснована необходимость защиты от кибератак объектов критической инфраструктуры государства и развития собственных кибервооружений.

Ключевые слова: *информационная война, киберпространство, сетецентризм, спектр воен действий государства, порог объявления войны, кибератака, кибербезопасность, информацио преимущество, сетецентрическая война, кибернетическое оружие, кибернетическое влияние*

ACTIONS IN CYBERSPACE DURING THE PREPARATION AND CONDUCT OF NETWORK CENTRIC WARS

***Oleksandr M. Guk*[1]**
***Oleksiy Y. Cherednychenko*[1]**
***Roman M. Shtonda*[1]**
***Ihor O. Dyba*[2]**

[1]*Military Institute of Telecommunications and Informatization, Kyiv, Ukraine*
[2]*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

The article considers changes in the nature of conducting modern wars and signs of transition to a network-centric model of combat management, the spectrum of military actions of the state, the main directions and conditions for achieving information superiority over the enemy. The role and place of actions in cyberspace during the preparation and conduct of network centric wars and their influence on the control and communication systems of vital and strategically important objects of the state were determined. The necessity of protection of the state's critical infrastructure objects and development of own cyber weapons is grounded.

Keywords: *information warfare, cyberspace, net-centric, the spectrum of state military operations, the threshold of war, cyberattack, cybersecurity, information superiority, network centric warfare, cybernetic weapons, cybernetic influence.*

References

1. Makarenko S. I. Perspectives and problems of employment of the cybernetic weapon by in the modern net-centric war [Problemyi i perspektivyi primeneniya kiberneticheskogo oruzhiya v sovremennoy setetsentricheskoy voyne] /Special equipment and communication №3, 2011. **2. Titov I.V.** Network centric warfare concept of conducting war of XXI century [Merezhotsentrychna kontseptsiia vedennia viiny XXI storichchia]/I.V. Titov // Weapons systems and military equipment. – 2008. – № 3. **3. Jason Rivera.** Understanding and Countering Nation-State Use of Protracted Unconventional Warfare./ Jason Rivera// Access mode: http://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare **4. Alberts, David S. (David Stephen)**, Network centric warfare : developing and leveraging information superiority, 2nd Edition (Revised) / David S. Alberts, John J. Garstka, Frederick P. Stein. Second printing February 2000. **5.** Dubov D. V. Cyberspace as a new dimension of geopolitical rivalry: monograph [Kiberprostir yak novyi vymir heopolitychnoho supernytstva : monohrafiia]/ D. V. Dubov. – K. : NISS, 2014. – 328 pg. **6. Overcome by cyber risks? Economic benefits and costs of alternate cyber futures**./ Zurich Insurance Group's and the Atlantic Council's Brent Scowcroft Center's on International Security report// Access mode: http://publications.atlantic-council.org/cyberrisks// **7. Gorbulin V.P.** Finding asymmetric responses: cyberspace in hybrid warfare. [U poshukakh asymetrychnykh vidpovidei: kiberprostir u hibrydnii viini.] – 2015. Access mode: https://gazeta.dt.ua /internal/u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni-_.html

УДК 344.14+343.2.01

Роман Володимирович Дужий
Віталій Іванович Пазиніч

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ХАРАКТЕРИСТИКА ФОРМ ТА ВИДІВ КОНТРОЛЮ ЗА ДІЯЛЬНІСТЮ ОРГАНІВ І УСТАНОВ ВИКОНАННЯ ПОКАРАНЬ

У статті розглянуто правовий статус суб'єктів, які здійснюють державний контроль за діяльністю органів і установ виконання покарань. Особливого значення набуло розгляд умов перебування особового складу в постійному інформаційно-психологічному впливі.

Стаття піднімає питання які розкривають зміст, забезпечення законності в діяльності органів і установ виконання покарань та запобігання будь-яким можливим порушенням прав і законних інтересів як засуджених, так і персоналу.

Системний розгляд даного питання розкривається через форми державного контролю за діяльністю установ виконання покарань: перевірка; спостереження; опитування; моніторинг; інспектування; ревізія; огляд; інвентаризація; аудит; ознайомлення із статистичною звітністю; одержання пояснень; вивчення та аналіз матеріалів, які містяться в засобах масової інформації або у зверненнях громадян.

***Ключові слова**: правовий статус, державний контроль, запобігання порушенням прав і законних інтересів, контролю за діяльністю установ виконання покарань.*

Вступ

Система установ і органів виконання покарань є частиною правоохоронних органів України, яка вирішує такі завдання, як боротьба зі злочинністю та її попередження. Оскільки до цього завдання має відношення все суспільство, воно через систему державних і громадських інститутів встановлює постійний соціальний контроль за діяльністю правоохоронних органів. Не є винятком також діяльність персоналу установ та органів виконання покарань, контроль за яким має свої особливості. Насамперед, у процесі контролю забезпечується дотримання законності під час виконання кримінальних покарань [1, С. 57].

Постановка проблеми. Саме для забезпечення законності в діяльності органів і установ виконання покарань та запобігання будь-яким можливим порушенням прав і законних інтересів як засуджених, так і персоналу, чинним законодавством (Глава 4 КВК України, ст. 27, 29 Закону України «Про Державну кримінально-виконавчу службу України») передбачені такі інститути як контроль та нагляд.

Формами державного контролю за діяльністю установ виконання покарань визначено: перевірку; спостереження; опитування; моніторинг; інспектування; ревізію; огляд; інвентаризацію; аудит; ознайомлення із статистичною звітністю; одержання пояснень; вивчення та аналіз матеріалів, які містяться в засобах масової інформації або у зверненнях громадян [3].

Аналіз остатніх досліджень і публікацій. Проблемні питання діяльності установ виконання покарань були предметом наукових досліджень А.О. Галай, С.К. Гречанюка, О.М. Джужи, В.А. Льовочкіна, В.П. Пєткова, О.Б. Пташинського, Г.О. Радова, О.В. Романенко, А.Х. Степанюка, В.М. Трубникова, С.Я. Фаренюка та інших науковців. Проте, у вітчизняній юридичній науці висвітлено недостатньо правовий статус суб'єктів, які здійснюють державний контроль за діяльністю установ виконання покарань [2].

Останніми роками науковці приділяють особливу увагу підвищенню ефективності управління місцями позбавлення волі та утримання ув`язнених, поліпшенню фізичного та морального здоров`я ув'язнених, а також належній підтримці та сприянню працівникам пенітенціарних установ у підвищенні професійного рівня та особистих якостей. Так, у працях О.М. Бандурки, О.В. Беци, І.І. Іванькова, А.Х. Степанюка, В.М. Трубнікова, І.С. Яковець особлива увага приділяється дотриманню прав людини при виконанні кримінальних покарань в установах кримінально-виконавчої служби.

Мета статті полягає в піднятті питання які розкривають зміст, забезпечення законності в діяльності органів і установ виконання покарань та запобігання будь-яким можливим порушенням прав і законних інтересів як засуджених, так і персоналу.

Виклад основного матеріалу дослідження.

За роки незалежності в Україні здійснюється поступова гуманізація відбування кримінальних покарань, реалізується низка важливих заходів, спрямованих на удосконалення пенітенціарної системи України відповідно до міжнародних та європейських стандартів. Проте умови тримання засуджених та осіб, взятих під варту, поводження

із ними не відповідають вимогам як національного законодавства, так і міжнародним та європейським нормам і стандартам забезпечення дотримання прав людини і громадянина в місцях позбавлення волі.

Як правильно відзначає В.М. Трубников, ефективне вирішення проблем кримінальної юстиції і забезпечення правопорядку в Україні можливо не тільки в рамках держави, його елементів і структур, але суспільства в цілому. Проте, враховуючи нові історичні, політичні, економічні і соціальні умови, а також беручи до уваги досвід розвитку країн Західної Європи та потреба в переході до Європейських пенітенціарних стандартів, необхідності формування цивільного суспільства і правової держави, а звідси формувати нову кримінальну і кримінально-виконавчу політику і лише тоді ми зможемо вирішити поставлене завдання вдосконалення чинного законодавства і використання в практиці його застосування міжнародно-правових стандартів [7, С. 134].

Неможливо не погодитись із твердженням професора Трубникова та інших вищевказаних професорів і вважаю, що нам потрібно формувати нову кримінально-виконавчу політику, беручи до уваги досвід розвитку країн Західної Європи.

Відповідно до статті 24 Кримінально-виконавчого кодексу, без спеціального дозволу в будь-який час безперешкодно відвідувати установи виконання покарань для здійснення контролю та проведення перевірок мають право: Президент України або спеціально уповноважені ним представник; Прем'єр-міністр України; Уповноважений Верховної Ради України з прав людини; члени Комісії при Президентові України у питаннях помилування; Міністр юстиції України; Міністр внутрішніх справ України; члени Європейського комітету з питань запобігання катуванням чи нелюдському або такому, що принижує гідність, поводженню чи покаранню; народні депутати України; Генеральний прокурор України, а також уповноважені ним прокурори і прокурори, які здійснюють на відповідній території нагляд за додержанням законів при виконанні судових рішень у кримінальних справах.

Необхідно виокремити три групи суб'єктів державного контролю за діяльністю органів і установ виконання покарань: надвідомчих, внутрівідомчих та комплексних. До перших необхідно віднести: Верховну Раду України; Президента України; Кабінет Міністрів України; центральні та місцеві органи виконавчої влади; судові органи України. До другої: Державна пенітенціарна служба України та її територіальні та локальні органи управління. Треті комплексні суб'єкти державного контролю за діяльністю установ виконання покарань, які складаються як з представників державних органів, так і з представників самоврядних та громадських органів.

У роботі органів та установ виконання покарань громадськість бере участь через спостережні комісії та інші громадські об'єднання. У ст. 93 Європейських пенітенціарних правил в редакції січня 2006 р. окремо приділяється увага незалежному нагляду за умовами тримання засуджених та поводженню з ними. Акцентується увага на тому, що такий нагляд має здійснюватися незалежними органами чи організаціями та результати його мають бути публічно доступними. Навіть у статті 5 Конституції України визнається громадський контроль, тобто органи державної влади та органи місцевого самоврядування є підконтрольними народу в цілому, оскільки джерелом влади в Україні є народ. Громадський контроль здійснюється спостережними комісіями, та іншими утвореннями громадян. У своїй роботі вони керуються: Конституцією України, Європейськими пенітенціарними правилами. Нові Європейські пенітенціарні правила мають суто рекомендаційний характер для адміністрації установ виконання покарань, проте вони накладають моральні та політичні зобов`язання на ті держави, які їх прийняли.

Однією з головних функцій омбудсмена у світі є контроль за діяльністю виконавчих та інших органів державної влади шляхом розгляду скарг громадян на дії тих чи інших органів або посадових осіб, що призвели до порушення прав та свобод людини і громадянина. В цьому сенсі важливим невід'ємним правом омбудсмена є право проводити розслідування, у тому числі й за власною ініціативою, і на їх підставі вносити рекомендації щодо шляхів відновлення порушених прав у конкретному випадку, вносити пропозиції стосовно змін до законодавства або перегляду неправомірної адміністративної практики органів державної влади. Процедура звернення до омбудсмена максимально неформальна та гнучка, а доступ до нього є безплатним і відкритим для всіх громадян держави [5].

З початку антитерористичної операції (АТО) на Донбасі з в'язниць окупованого Донбасу на підконтрольну Україні територію передали близько 130 засуджених і тут зусиль докладала уповноважений з прав людини. Але під час перевірок виявлені численні порушення в діяльності адміністрацій виправних установ щодо забезпечення належного режиму відбування покарання засуджених. Встановлені непоодинокі випадки незаконного притягнення до дисциплінарної відповідальності осіб, які відбувають міру кримінального покарання Так, у слідчих ізоляторах зони АТО виявлені порушення норм Закону України "Про попереднє ув'язнення" в частині роздільного тримання ув'язнених та засуджених осіб та інше [8].

Перевірки проводяться за заявами та іншими повідомленнями про порушення законності, що вимагають прокурорського реагування, а за наявності підстав — також з власної ініціативи прокурора. Прокуратура не підміняє органи відомчого управління та контролю і не втручається в оперативну діяльність, якщо така

діяльність не суперечить чинному законодавству [4]. Прокурорський нагляд за додержанням і застосуванням законів є по суті видом діяльності спеціально уповноважених органів державної влади, що здійснюється від імені держави шляхом використання передбачених законом повноважень та правових засобів їх забезпечення з метою з'ясування стану додержання Конституції України та законів, вжиття заходів до усунення порушень законів, притягнення винних до встановленої законом відповідальності, поновлення порушених прав. При здійсненні контролю за діяльністю органів і установ виконання покарань прокуратура керується насамперед: Конституцією України, Закону України «Про прокуратуру», та іншими нормативно-правовими актами [5]. Згідно статистичних даних по відвідуванню прокурором виправної колонії №86 за перший квартал 2015 року, ним було розглянуто 7 справ про порушення прав засуджених. Під час проведення службової перевірки дані факти порушення не були підтвердженні.

Омбудсмен є посадовою особою, статус якої визначається Конституцією України, Законом України «Про Уповноваженого Верховною Радою з прав людини», Законом України «Про державну службу». Уповноважений здійснює свою діяльність незалежно від інших державних органів та посадових осіб. Діяльність омбудсмена доповнює існуючі засоби захисту конституційних прав і свобод людини і громадянина, і забезпечує захист і поновлення порушених прав і свобод [5].

Отже, розглянувши дане питання можна зауважити те, що хоча і контроль за діяльністю органів і установ виконання покарань здійснюється згідно чинного законодавства з боку органів які уповноважені здійснювати цей контроль, але він можна так сказати носить суто формальний характер. Це пояснюється тим, що органи які здійснюють контроль є державними, ну і як відомо з практики майже всі державні органи співпрацюють між собою. Це добре знають засуджені особи, тому вони і не довіряють даним органам які здійснюють контроль за діяльністю органів і установ виконання покарань. Якщо ж брати до уваги громадський контроль, то переваги даного контролю це саме незалежність від держави, тобто громадський контроль здійснюється без втручання державних органів. У держави основне завдання являється покарати злочинця, тобто фактичне відбуття засудженою особою призначеного покарання, а вже саме суспільство є зацікавленим у тому, щоб особи, які відбули покарання, не становили суспільної небезпеки, одним із чинників чого є неухильне дотримання прав засуджених під час відбування кримінальних покарань. Тому засуджені більше будуть довіряти громадському контролю, а не державним органам, які здійснюють даний контроль.

Висновки й перспективи подальших досліджень

Таким чином, отримані результати дозволяють визначити, що приведення підходів до організації внутрішніх комунікацій у Збройних Силах України до стандартів НАТО потребує реорганізації відповідних органів управління морально-психологічним забезпеченням у Збройних Силах України, вивчення нових форм і способів діяльності, прийнятих в НАТО та їхньої реалізації в практичній роботі керівного складу військових частин (підрозділів) Збройних Сил України.

За умови проведення відповідних змін, внутрішні комунікації стануть невід'ємною частиною стратегічних комунікацій Міністерства оборони України та Збройних Сил України, що, в свою чергу, дасть змогу комплексно та узгоджено використовувати для інформування та мотивації особового складу всі комунікативні можливості.

Література

1. Кримінально-виконавче право України (загальна частина). Навчально-методичний посібник – К : Інститут кримінально-виконавчої служби, 2014 – 112 с. **2. Макаренко Т.В.** Суб'єкти, які здійснюють державний контроль за діяльністю установ виконання покарань /Т.В.Макаренко // Форум права. – 2010. – №1. – [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/ejournals/1.FP/2010-1/11knu.pdf **3.** Гаращук В.М. Система контролюючих органів та їх повноваження: загальний огляд // Державне будівництво та місцеве самоврядування. – Х., 2003. – Вип. 5. – [Електронний ресурс]. – Режим доступу: http://www.kyiv-gov.ua/gromadskij_kontrol_za_dotrimannj **4. Степанюк А.Х.** (ред.) Кримінально-виконавче право України Підручник / за ред. А. Х. Степанюк Х.: Право, 2010 – 320 с. **5. Давиденко Є.** «Служба омбудсмена в Україні»\\Право України, 2001 -№ 6. – [Електронний ресурс]. Режим доступу: http://www.bestreferat.ru/referat-190825.html **6. Прокурорський нагляд в Україні.** Підручник для юрид. вузів і факультетів (І. Є. Марочкін, П. М. Каркач, Ю.М. Грошевий та ін.). За ред. проф. Марочкіна І. Є., Каркача П. М. Харків 2004. . – [Електронний ресурс]. – Режим доступу: http://radnuk.info/pidrychnuku/prokyratyra/508-2004.html **7. Трубников В.М.** Роль і значення цивільного суспільства і правової держави у формуванні кримінальної і кримінально-виконавчої політики / В.М. Трубников // Державна політика у сфері кримінальної юстиції та забезпечення правопорядку в Україні: Матер. наук.-практ. семінару (28 лютого 2008 року), Дніпропетровський державний університет внутрішніх справ). – Д. : Дніпроп. держ. ун-т внутр. Справ, 2008. – 232 с. **8. Прокуратура виявила порушення прав засуджених і ув'язнених у колоніях та СІЗО Донбасу** – [Електронний ресурс]. – Режим доступу: https://dn.depo.ua/ukr/dn/prokuratura-viyavila-porushennya-prav-zasudzhenih 24112016111100

ХАРАКТЕРИСТИКА ФОРМ ТА ВИДІВ КОНТРОЛЮ ЗА ДІЯЛЬНІСТЮ ОРГАНІВ І УСТАНОВ ВИКОНАННЯ ПОКАРАНЬ

Роман Володимирович Дужий
Віталій Іванович Пазиніч

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье рассмотрены правовой статус субъектов, осуществляющих государственный контроль за деятельностью органов и учреждений исполнения наказаний. Особое значение в статье приобрело рассмотрение условий пребывания личного состава в постоянном информационно-психологическом воздействии.

Статья поднимает вопросы, которые раскрывают содержание, обеспечение законности в деятельности органов и учреждений исполнения наказаний, и предотвращения любых возможных нарушений прав, и законных интересов как осужденных, так и персонала.

Система рассмотрение данного вопроса раскрывается через формы государственного контроля за деятельностью учреждений исполнения наказаний: проверка; наблюдения; опрос; мониторинг; инспектирования; ревизия; осмотр; инвентаризация; аудит ознакомления со статистической отчетностью; получения объяснений; изучение и анализ материалов, содержащихся в средствах массовой информации или в обращениях граждан.

Ключевые слова: *правовой статус, государственный контроль, предупреждение нарушений прав и законных интересов, контроля за деятельностью учреждений исполнения наказаний.*

CHARACTERISTICS OF THE FORMS AND TYPES OF CONTROLLING ACTIVITY BODIES AND INSTITUTIONS OF CARRIAGE

Roman V. Dujiy
Vitaliy I. Pazunich

National Defense University of Ukraine named after Ivan Cherniakhsovsky, Kyiv, Ukraine

The article considers the legal status of subjects exercising state control over the activities of bodies and institutions for the execution of sentences. Particular importance in the article has become the consideration of the conditions of staying in the permanent staff in the informational and psychological impact.

Indeed, the article raised issues that reveal the content, the maintenance of legality in the activities of bodies and institutions for the execution of punishments and to prevent any possible violations of the rights and legitimate interests of both convicted and staff.

System review of this issue is disclosed through the forms of state control over the activities of institutions for the execution of penalties: verification; Observation; Poll; Monitoring; Inspection; Audit; Inspection; Inventory; Audit of familiarization with statistical reporting; Getting explanations; Studying and analyzing materials contained in mass media or citizen appeals.

Keywords: *legal status, state control, prevention of violations of rights and legitimate interests, control over the activities of penitentiary institutions.*

References

1. Criminal-executive law of Ukraine (general part). Educational Manual - K: Criminal Execution Service Institute, 2014 - 112 p. **2. Makarenko T.V.** Subjects exercising state control over the activities of penitentiary institutions /TVMakarenko // Forum of rights. - 2010. - No. 1. - [Electronic resource]. - Access mode: http://www.nbuv.gov.ua/ejournals/1.FP/2010-1/11kn.pdf. **3. Garashchuk V.M.** The system of controlling bodies and their powers: a general overview // State construction and local self-government. - Kh., 2003. - Vip. 5. - [Electronic resource]. - Access mode: http://www.kyiv-obl.gov.ua/gromadskij_kontrol_za_dotrimannjam_prav_zasudzhenih_ponjattja_ta_zmist. **4. Stepanyuk A.H.** (Ed.) Criminal enforcement law of Ukraine Textbook / ed. A. Kh. Stepaniuk X .: Right, 2010. - 320 p. **5. Davydenko E.** "The Ombudsman's Service in Ukraine" \\ The Law of Ukraine, 2001-No. 6. - [Electronic resource]. - Mode of access: http://www.bestreferat.ru/referat-190825.html **6. Prosecutor's Supervision in Ukraine. Legal textbook.** Universities and faculties (I. E. Marochkin, P. M. Karkach, Yu.M. Groshevy, etc.). Ed. Prof. Marochkina I. E., Karkach P. M. Kharkiv 2004. - [Electronic resource]. -Modeofaccess: http://radnuk.infopidrychnuku /prokyratyra/508-marochkina/11074-2004.html

7. V. Trubnikov The role and significance of civil society and the rule of law in the formation of criminal and penal policy / V.M. Trubnikov // State policy in the field of criminal justice and ensuring law and order in Ukraine: Mater. Sci. Pract. Seminar (February 28, 2008), Dnipropetrovsk State University of Internal Affairs). - D.: Dnipropetrovsk State Yn-t inside True, 2008 - 232 p. **8. The prosecutor's office found violations of the rights of prisoners and prisoners in the colonies and SIZO of Donbass** - [Electronic resource]. - Access mode: https://dn.depo.ua/ukr/dn/prokuratura-viyavila-porushennya-prav-zasudzhenih 24112016111100

УДК 35.48

Віталій Олександрович Кацалап *(канд. військ. наук)*
Олександр Володимирович Войтко *(канд. військ. наук)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ОЦІНЮВАННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В ІНТЕРЕСАХ БОЙОВИХ ДІЙ ВІЙСЬК (СИЛ)

Дослідження сценаріїв та ситуацій воєнного характеру дозволяє визначити можливі причини (умови) виникнення кризи та етапи ведення будь-яких бойових дій (операцій). Одним із перспективних таких наукових досліджень є оцінювання інформаційно-психологічного впливу в інтересах бойових дій військ (сил). Таке оцінювання пов'язане з визначенням показників: пронозу обстановки; вірогідного масштабу бойових дій; наслідків від застосування того чи іншого способу інформаційно-психологічного впливу. У кожному способі інформаційно-психологічного впливу необхідно визначити напрямок зосередження основних зусиль, кількість сил і засобів, які залучаються до ведення бойових дій. Враховуючи, що зазначені складові мають свою послідовність моделювання яка містить ряд обмежень врахування яких дозволить спрогнозувати можливі наслідки від інформаційно-психологічного впливу противника.

Ключові слова: *сценарії, ситуації, інформаційно-психологічний вплив, способи інформаційно-психологічного впливу, бойові дії військ (сил).*

Вступ

Спираючись на характеристику інформаційних викликів та загроз національній безпеці України, визначені пріоритети державної політики з питань національної безпеки і оборони, у ході розробки Державних програм [1] різного типу, в яких проаналізовано широкий спектр імовірних ситуацій застосовуватимуться Збройні Сили України, як на довгострокову так і середньострокову перспективу. Ці ситуації об'єднані сценаріями. Сценарії стали базовими для визначення можливого інформаційно-психологічного впливу противника на Збройні Сил України.

Постановка проблеми. Визначення наслідків від інформаційно-психологічного впливу противника пов'язана з урахування ряду умов та чинників: імовірний розвиток обстановки, вірогідні масштаби та наслідки; завдання своїх військ (сил), що повинні бути досягнуті; можливі етапи розвитку ситуації; загальний порядок застосування військ (сил); розрахунки потреб у силах і засобах для протидії. Запорукою адекватної протидії для ефективного застосування військ (сил) є прогнозування впливу зазначених чинників в можливих ситуація та сценаріях.

Аналіз остатніх досліджень і публікацій. Розгляд джерел [2-4] свідчить, що сценарії можуть містити можливі причини (умови) виникнення кризи, цілі, які можуть ставитися протилежною стороною. Для прогнозу цілей протилежної сторони (противника) у кожному сценарії визначають напрямок зосередження основних зусиль, кількість сил і засобів, які залучаються до ведення бойових дій, а також можливі способи інформаційно-психологічного впливу противника. Враховуючи, що зазначені складові мають свою послідовність моделювання яка не скоординована за місцем і часом в силу того, що застосовуються різні підходи до моделювання. Це дає можливість стверджувати те, що за таких умов визначити можливі наслідки від інформаційно-психологічного впливу противника сьогодні досить складно.

Метою статті є визначення набору параметрів можливих показників які необхідні для оцінювання інформаційно-психологічного впливу в інтересах бойових дій військ (сил).

Виклад основного матеріалу дослідження.

Базуючись на аналізі викликів та загроз національній безпеці України в Стратегічному оборонному бюлетені до 2025 року [3] розглядається спектр імовірних ситуацій, у яких можуть застосовуватися війська (сили). Ці ситуації об'єднані сценаріями, які стали базовими для моделювання інформаційно-психологічного впливу, а саме:

здійснення стримування та відбиття збройної агресії проти України;

терористичні акти проти України;

втручання у внутрішні справи України з боку інших держав;

внутрішня нестабільність;

порушення цілісності кордонів України;

надзвичайні ситуації природного, техногенного, соціального та воєнного характеру;

надзвичайні ситуації природного, техногенного, соціального та воєнного характеру;

протидія (участь у припиненні дій) організованої злочинності за участю Збройних Сил України;

ведення миротворчих операцій ЗС України;

захист життя громадян України і державної власності за кордоном;

надання військової допомоги Україною іншим державам в рамках багатосторонніх угод.

За своїм змістом сценарій є загальним описом низки кризових ситуацій з визначенням переліку та змісту способів інформаційно-психологічного впливу, які має запровадити держава, цілей, які планується при цьому досягти, та базових даних для проведення подальшого застосування військ (сил). Так, одному сценарію табл. 1 відповідає 4-8 ситуацій. Загальна кількість ситуацій може бути близько – 64. Кожний сценарій містить можливі причини (умови) виникнення кризи, сфери зіткнення інтересів (предмет суперечок); цілі, які можуть ставитися протилежною стороною, імовірний розвиток кризи (обстановки), вірогідні масштаби та наслідки; цілі України, що мають бути досягнуті; функції та завдання військ (сил); загальний порядок застосування військ (сил); розрахунки потреб у силах і засобах для протидії інформаційно-психологічного впливу противника.

У кожному сценарії визначено повноваження органів державної влади та ступінь їх участі у виконанні завдань щодо нейтралізації кризових ситуацій. Це дало можливість спланувати для залучення оптимальну кількість сил безпеки і оборони, забезпечивши тим самим достатню ефективність їх застосування та економію ресурсів держави. Такий розподіл визначає орган державної влади, що є відповідальним за врегулювання кризових ситуацій за тим чи іншим сценарієм, а також тих, хто бере участь у виконанні цього завдання (таблиця 1).

Таблиця 1

Варіант участі Сектору безпеки і оборони України в кризових сценаріях

№ з/п	Найменування сценаріїв	Найменування органів виконавчої влади та інших структур						
		Кризовий центр	ЗСУ	СБУ	МВС	МНС	ДПСУ	Держспецзв'язу
1.	Здійснення стримування та відбиття збройної агресії проти України		ГВ	БУ	БУ	БУ	БУ	
2.	Терористичні акти проти України	КЗ	БУ	ГВ	БУ	ДР	БУ	БУ
3.	Втручання у внутрішні справи України з боку інших держав	КЗ	ДР	БУ	БУ		ДР	БУ
4.	Внутрішня нестабільність	К	ДР	БУ	ГВ		ДР	ДР
5.	Порушення цілісності кордонів України	К	БУ	БУ	БУ		ГВ	БУ
6.	Надзвичайні ситуації природного, техногенногот характеру	К	БУ	ДР	БУ	ГВ	ДР	
7.	Протидія (участь у припиненні дій) організованої злочинності за участю Збройних Сил України	КЗ		БУ	ГВ		БУ	ДР
8.	Ведення миротворчих операцій ЗС України	КЗ	ГВ	ДР	БУ	БУ	ДР	ДР
9.	Захист життя громадян України і державної власності за кордоном	КЗ	БУ	ДР	БУ	ДР		БУ
10.	Надання військової допомоги Україною іншим державам в рамках багатосторонніх угод	КЗ	К	ДР				БУ

Умовні позначення:

К - керівництво; БУ - безпосередня участь;

КЗ - координація зусиль (дій, заходів); ДР - допоміжна роль;

ГВ - головна відповідальність; Зб - забезпечення (дипломатичне, законодавче, організаційне, ресурсне, інформаційне).

Аналіз сучасних викликів і загроз для національної безпеки України, визначення ймовірних кризових ситуацій дозволяє класифікувати сценарії в яких будуть застосовуватись війська (сили):

бойові дії високої інтенсивності (регіональна війна) – війна за участю двох і більше держав (коаліцій, груп держав) зі всіма ознаками найрішучіших воєнно-політичних цілей проти України, що несе загрозу втрати незалежності, суверенітету та територіальної цілісності нашої

держави. Він може стати результатом ескалації воєнних конфліктів більш низької інтенсивності. Бойові дії сухопутних угруповань можуть вестися в межах одного регіону (операційної зони), а збройна боротьба може розповсюдитися на всю територію держави та прилягаючі акваторії морів, повітряний і космічний простір;

бойові дії середньої інтенсивності (локальна війна) – війна між двома і більше державами, торкається переважно інтересів тільки цих держав. Бойові дії можуть вестися в межах одного регіону (операційній зоні), а збройна боротьба розповсюджуватися на значну територію;

бойові дії низької інтенсивності (прикордонний конфлікт) – сторони, як правило, будуть намагатися досягнути певних результатів оперативно-тактичного характеру. Він може стати наслідком розростання збройного інциденту, збройної акції, прикордонного та інших збройних зіткнень обмеженого масштабу на ґрунті територіальних, економічних, політичних або інших суперечок.

Сучасний стан та тенденції розвитку воєнно-політичної обстановки свідчить, що широкомасштабна збройна агресія проти України на середньострокову перспективу дуже ймовірна.

Вивчення озброєної боротьби немислиме без встановлення залежностей між кількісними характеристиками протидіючих сторін і можливими результатами їх зіткнення. Уміння передбачати переваги тій або іншій системи озброєння, способу інформаційно-психологічного впливу являється складним і досить кропітким завданням. Тому прорахунки в зазначеному будуть виключати можливість виправлення помилкового рішення. Якщо у минулому для досягнення різкого перелому в битві воєначальник нерідко мав моральне право приймати вкрай ризиковані рішення, сподіваючись на щасливий випадок або зберегти за собою можливість відходу від вибраного плану, то нині однією з вимог військової науки є вироблення таких рішень під час бойових дій військ (сил), які зводять до мінімуму ризик опинитися в програшній ситуації.

Стосовно негативного інформаційно-психологічного впливу на особовий склад військ (сил) слід зауважити, що він може здійснюватися як загальний (на військовослужбовця як людину в суспільстві) переважно у мирний час, так і як спеціальний (на воїна та захисника) переважно в особливий період.

Як в мирний час, так і в особливий період метою здійснення негативного інформаційно-психологічного впливу з боку кожної із протидіючих сторін на особовий склад військ (сил) є погіршення морально-психологічного стану особового складу військ (сил) противника, що є умовою зниження їх психологічної готовності до діяльності або відмови її здійснювати. Мета досягається результатами:

деморалізації особового складу збройних сил;

збудження у солдат і офіцерів страху та невпевненості у майбутньому;

формування недовіри до командирів;

переконання військовослужбовців до невиконання своїх обов'язків, невчинення опору противнику та здачі у полон.

У сучасних умовах ведення бойових дій військ (сил) спрогнозувати ефект від інформаційно-психологічного впливу противника визначити являється складним завданням. Складність у проведенні розрахунків із визначення наслідків інформаційно-психологічного впливу пов'язана з вимогами до показників та критеріїв які для цього застосовуються. Так, в роботах [5] для оцінки інформаційного впливу використовуються методи експертного оцінювання. Це в свою чергу спрощує зміст показника оцінювання та вводить ряд суб'єктивних факторів пов'язаних із судженнями експертів. На скільки буде зменшена похибка в судженнях експертів тим точнішими будуть розрахунки та їх достовірність.

Як приклад для оцінювання інформаційно-психологічного впливу можемо застосувати метод визначення віддаленої ваги оцінок [6]. Сутність методу полягає в поєднанні експертного методу шкальних оцінок та методу визначення медіани та квартілей.

На першому етапі в методі визначення медіани та квартілей проводиться експертне опитування результати якого є розрахунок коефіцієнтів відносної важливості способів інформаційно-психологічного впливу.

Другим етапом є формування варіантів інформаційних дій, необхідних при виробленні рекомендацій щодо способів інформаційно-психологічного впливу якими буде досягається поставлена мета.

Наступним кроком буде розрахунок коефіцієнтів відносної важливості необхідних для обґрунтування важливості того або іншого способу інформаційно-психологічного впливу залежно від поставлених цілей і завдань.

Під час проведення експертного опиту складається матриця, в яку вписуються основні способи інформаційно-психологічного впливу, цілі і завдання. Клітки матриці заповнюються значеннями коефіцієнтів відносної важливості вказаних способів, виражених в долях одиниць, але так, щоб сума коефіцієнтів в стовпцях дорівнювала одиниці.

Привласнення коефіцієнтів відносній важливості проводиться в декілька турів. Після здобуття перших результатів група розробників підраховує середнє значення коефіцієнтів і вибирає дані тих фахівців, в яких коефіцієнти значно відрізняються в ту або іншу сторону від середніх. Потім проводиться другий тур привласнення коефіцієнту його значення.

Після визначення коефіцієнтів знов підраховується середнє значення отриманих результатів. Кількість таких турів у великій мірі

залежить від кваліфікації фахівців і їх досвіду. Вважається, що в середньому достатнє трьох турів голосування для груп, що складаються з 10-12 експертів.

Погоджені результати заносяться в таблицю як елементи матриці (табл.2.1 та 2.2).

В даному випадку можливими інформаційними діями стратегічного характеру є:

A_1 – активні інформаційні дії з метою зриву підготовки противника до агресії;

A_2 – демонстративні дії з метою віддзеркалення можливого нападу противника;

A_3 – ультимативні дії з метою захвату стратегічної ініціативи;

A_4 – інформаційне упередження з метою створення вигідних умов для швидкого закінчення бойових дій операцій;

A_5 – інформаційне зіткнення з метою забезпечення боєздатності Збройних Сил;

A_6 – інформаційна експансія з метою визначення ключових об'єктів впливу.

В таблицях 2.1 та 2.2 моделюються наступні способи інформаційно-психологічного впливу:

1. Попередження;
2. Спонукання;
3. Ізолювання;
4. Залякування;
5. Дезінформація;
6. Компрометація;
7. Дискредитація.

Порівнюючи властивості кожного способу інформаційно-психологічного впливу

Таблиця 2.1

Результати моделювання способів інформаційно-психологічного впливу

№ з/п	Коефіцієнти інформаційних дій			Заг. коеф.
	A_1	A_2	A_3	
1.	0,2	0,5	0,4	1,1
2.	0,05	0,05	0,05	0,15
3.	0,14	0,11	0,05	0,3
4.	0,4	0,2	0,425	1,025
5.	0,06	0,05	0,025	0,135
6.	0,05	0,05	0,025	0,125
7.	0,1	0,04	0,025	0,165
Заг. сум.	1	1	1	3

Таблиця 2.2

Результати моделювання способів інформаційно-психологічного впливу

№ з/п	Коефіцієнти інформаційних дій			Заг. коеф.
	A_4	A_5	A_6	
1.	0,1	0,25	0,3	1,75
2.	0,05	0,025	0,2	0,425
3.	0,05	0,025	0,02	0,395
4.	0,5	0,5	0,2	2,225
5.	0,05	0,125	0,13	0,44
6.	0,05	0,05	0,1	0,325
7.	0,2	0,025	0,05	0,44
Заг. сум	1	1	1	3

Такий підхід мав ряд позитивних сторін, але йому були властиві і істотні недоліки. Як і при уявному моделюванні, тут різко виявлявся суб'єктивізм, бо адекватність цих значень повністю залежала від досвіду експерта. Крім того, експерт не завжди може врахувати всі фактори та чинники, які впливатимуть на ситуацію.

Рідше звертають увагу на інший недолік зазначеного підходу, пов'язаний з процесом вибору показників та критеріїв оцінювання. У реальних бойових діях фактор інформаційно-психологічного впливу на особовий склад має доволі суттєве значення. Величенна якого безпосередньо впливає на виконання бойових завдань особовим складом.

Висновки й перспективи подальших досліджень

Таким чином, запропонований підхід дозволяє оцінити інформаційно-психологічний вплив противника в інтересах бойових дій військ (сил). Зазначене оцінювання характеризує зміст способів інформаційно-психологічного впливу противника та являється основою для прогнозу поведінки особового складу під час виконання ним бойових завдань. Визначено послідовність моделювання складових способів інформаційно-психологічного впливу противника.

Важливо продовжити докладне вивчення способів інформаційно-психологічного впливу противника із широким залученням науковців, військових експертів з метою розроблення комплексної методики протидії інформаційно-психологічному впливу противника. При цьому слід урахувати можливі варіанти участі Сектору безпеки і оборони України в кризових сценаріях.

Література

1. Указ Президента України "Про затвердження Державної програми реформування Збройних Сил України на 2011 – 2015 роки". **2.** "Про оборону України" від 6.12.91 р. N 1932-XII. **3**. Указ Президента України "Про рішення Ради національної безпеки і оборони України "Про Стратегічний оборонний бюлетень України на період до 2025 року". **4**. Указ Президента України "Про затвердження Плану заходів зі стабілізації ситуації у Збройних Силах України на 2010 рік". **5. Горбулін В.П., Биченок М.М.** Проблеми захисту інформаційного простору України. - К .: Видавництво "Інтертехнологія", 2009. – 136 с. **6. Тараканов К.В.** Математика и вооруженная борьба. – М .: Воениздат, 1974. – 240 с.

ОЦЕНКА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВЛИЯНИЯ В ИНТЕРЕСАХ БОЕВЫХ ДЕЙСТВИЙ ВОЙСК (СИЛ)

Виталий Александрович Кацалап *(канд. воен. наук)*
Александр Владимирович Войтко *(канд. воен. наук)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Исследование сценариев и ситуаций военного характера позволяет определить возможные причины (условия) возникновения кризиса и этапы ведения боевых действий (операций). Одним из перспективных таких научных исследований есть оценивание информационно-психологического влияния в интересах боевых действий войск (сил). Такое оценивание связано с определением показателей : проныру обстановки; достоверного масштаба боевых действий; последствий от применения того или другого способа информационно-психологического влияния. В каждом способе информационно-психологического влияния необходимо определить направление сосредоточения основных усилий, количество сил и средств, которые привлекаются к ведению боевых действий. Учитывая, что отмечены составляющие имеют свою последовательность моделирования которая содержит ряд ограничений учета которых позволит спрогнозировать возможные последствия от информационно-психологического влияния противника.

Ключевые слова: *сценарии, ситуации, информационно-психологическое влияние, способы информационно-психологического влияния, боевые действия войск (сил).*

ASSESSMENT OF THE INFORMATION AND PSYCHOLOGICAL INFLUENCE FOR THE BENEFIT OF MILITARY TROOPS (FORCES) ACTIONS

Vitaliy O. Katsalap *(Candidate of Military Sciences)*
Oleksandr V. Voitko *(Candidate of Military Sciences)*

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

Researching of military scenarios and situations allows us to determine the possible causes (conditions) of a crisis and stages of conducting any military actions (operations). One of the perspective research is assessment of information and psychological influence for the benefit of military troops (forces) operations. This assessment is connected with the definitions like: situation prognosis; probable scale of combat actions; consequences of usage of different methods of information and psychological influence. In each method of information and psychological influence it is necessary to determine the direction of concentration of the main efforts, the number of forces and means involved in combat actions. These components have their own simulation sequence, which contains a number of limitations, taking them into concideration allows to predict the possible consequences of the enemy's informational and psychological influence.

Keywords: scenarios, situations, informatively-psychological influence, methods of informatively-psychological influence, battle actions of troops (forces).

References

1. Edict of President of Ukraine is "About claim of the Government program of reformation of Military Powers of Ukraine on 2011 - 2015". **2.** "About the defensive of Ukraine" from 6.12.91 N 1932 - XII. **3.** Edict of President of Ukraine "About the decision of national security and defensive of Ukraine Council "About the Strategic defensive bulletin of Ukraine on a period 2025 to". **4.** Edict of President of Ukraine "About claim of Plan of measures on stabilizing of situation in Military Powers of Ukraine on 2010". **5. Gorbulin V.P., Bichenok M. M.** Problems of defence of informative space of Ukraine. - К .: Publishing House "Intertehnologiya", 2009, 136 p. **6. Tarakanov K.V.** Mathematics of armed struggle. M .:Voyenizdat,1974,240 p.

УДК 681.5.01

Сергій Валентинович Ковбасюк *(д-р техн. наук, с. н. с., провідний науковий співробітник)*[1]
Дмитро Володимирович Пекарєв *(канд. техн. наук, с. н. с., начальник наукового центру)*[1]
Ірина Анатоліївна Беспалко *(молодший науковий співробітник)*[1]

[1]***Житомирський військовий інститут імені С. П. Корольова, Житомир, Україна***

ПРИНЦИПИ ОРГАНІЗАЦІЙНОЇ ПОБУДОВИ ТА ВИМОГИ ДО ФУНКЦІОНАЛЬНОСТІ СИСТЕМ ОПОВІЩЕННЯ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

У статті наведено результати аналізу побудови та функціонування існуючих систем оповіщення в різних сферах життєдіяльності суспільства, а також огляд наукових праць, присвячених питанням інформування та створення систем оповіщення. Визначено, що відомі підходи до створення систем оповіщення лише частково враховують особливості проведення оповіщення зі специфічних (оборонних) питань, не містять обґрунтування принципів організаційної побудови систем оповіщення спеціального призначення та не можуть бути взяті за прототип для зазначених систем.

У статті запропоновано класифікацію систем оповіщення, визначено переваги та недоліки кожного їх класу. Сформовано основні принципи організаційної побудови, яким повинна відповідати система оповіщення спеціального призначення, та визначено вимоги до її функціональності як до інформаційно-керуючої системи, що реалізує всі функції автоматизованих систем моніторингу та управління.

Ключові слова: *система оповіщення спеціального призначення, принципи організаційної побудови, функціональні вимоги, класифікація.*

Вступ

Сучасний період розвитку суспільства характеризується все більше наростаючими суперечностями та виникненням конфліктів у міжнародних відносинах, політичних і військових протиріч між державами (союзами, блоками). В умовах ризиків масштабних надзвичайних ситуацій (синергетичний розвиток природно-техногенних процесів, виникнення принципово нових (гібридних) загроз тощо) [1, 2], а також, економічної нестабільності та швидкого науково-технічного прогресу рівень навантажень на державну безпеку наближається до критичного і загрожує виникненням локальних конфліктів і гібридних війн. Неодмінною умовою сталого розвитку держави є її безпека, захищеність від впливу внутрішніх та зовнішніх загрозливих факторів. Одним із завдань забезпечення національної безпеки є оповіщення керівництва держави та/або її різних відомчих структур про виникнення загроз національній безпеці, стан поточної обстановки, розвиток подій тощо [1, 2].

Актуальність захисту населення і територій, своєчасного оповіщення та інформування керівництва держави та органів управління в цілому обумовлена масштабами наслідків аварій, катастроф, стихійних лих, а також можливістю виникнення збройних конфліктів.

В даному контексті інформуванням є надання відомостей про визначені події, процеси, обстановку тощо, з метою підвищення обізнаності відповідних посадових осіб (структур), оповіщенням є доведення до зазначених посадових осіб (структур) сигналів (повідомлень) про загрозу та/або виникнення тих чи інших ситуацій.

Для запобігання виникненню зазначених надзвичайних ситуацій та/або забезпечення їх ліквідації потрібні зосередження зусиль та організація взаємодії різних органів управління, сил і засобів, у цілому – провадження відповідної державної політики. Таким чином, одним із ключових елементів захисту населення і територій, досягнення тих чи інших цілей при запобіганні різноманітним природним та техногенним процесам або при застосуванні штучних засобів впливу на населення держави, об'єкти з критичною інфраструктурою, є система оповіщення (СО).

СО повинна бути організована згідно з вимогами відповідних керівних документів, нормативно-правових актів та з урахуванням структури державного управління, характеру і рівня загроз національній безпеці, наявності й місця розташування сил, які можуть залучатися до ліквідації наслідків цих загроз [3].

Постановка проблеми. На теперішній час назріла необхідність удосконалення організаційних заходів та технічних засобів існуючих СО з урахуванням вимог сучасності.

Створення комплексної системи інформування та оповіщення будь-якого призначення потребує розробки системи принципових положень та напрямків розвитку процесів інформування та оповіщення з метою своєчасного та гарантованого доведення достовірної інформації про загрози виникнення певної надзвичайної події (ситуації)

до керівництва держави та/або відповідних органів управління.

Аналіз останніх досліджень і публікацій. Огляд СО різного призначення висвітлено в деяких закордонних та вітчизняних публікаціях [4, 5]. У роботах вітчизняних авторів досить повно та всебічно відображено результати досліджень процесів оповіщення про загрози та виникнення надзвичайних ситуацій.

З точки зору узагальнення та класифікації СО провідне місце мають займати державні стандарти та нормативно-правові акти щодо безпосереднього оповіщення та створення СО [5–7], але вони лише описують систему, призначену для оповіщення населення в разі виникнення надзвичайних ситуацій природного та техногенного характеру.

Зазначимо, що в більшості робіт, присвячених даним питанням, розглянуто лише окремі класи СО та надано їх описи. Питання розробки подібних систем не вивчалися комплексно, відсутній узагальнений аналіз та визначення принципів організаційної побудови, а також вимог до функціональності СО спеціального призначення. Під СО спеціального призначення будемо розуміти СО зі специфічних (наприклад, оборонних) питань різних відомчих структур.

Метою статті є розробка й обґрунтування принципів організаційної побудови та вимог до функціональності СО спеціального призначення.

Методи дослідження

Дослідження проводилося в рамках низки науково-дослідних робіт за тематикою створення, вивчення функціонування та удосконалення СО спеціального призначення. При цьому використовувався аналіз нормативно-правової бази, теоретичних джерел та сучасних поглядів на особливості СО.

Виклад основного матеріалу дослідження

Принципи організаційної побудови СО спеціального призначення

Аналіз існуючих СО показав, що такі системи створюються як комплекс організаційно-технічних заходів і технічних засобів оповіщення, засобів та каналів зв'язку, призначених для своєчасного доведення до споживачів (замовників) сигналів та інформації з визначених питань.

СО можна класифікувати за основними критеріями, наведеними на рис. 1 [3, 4, 8–13].

За функціональним призначенням СО можна розділити на [8]:

трансляційні, що дозволяють передавати інформацію різного призначення з різноманітних джерел, наприклад, мовленеві (текстові) оголошення, інформаційні повідомлення тощо;

аварійні, які в тривожному режимі ручним чи автоматичним способом передають аварійні повідомлення (сигнали);

комбіновані – багатофункціональні системи, що мають декілька пріоритетів (аварійне повідомлення в них передається за високим пріоритетом, блокуючи нижчі в рейтингу).

Рис. 1. Класифікація систем оповіщення

За принципом побудови СО можна розділити на [8]:

багатозональні системи можуть транслювати службові чи екстрені повідомлення в конкретні зони (одну або декілька);

багатоканальні системи дозволяють одночасно чи окремо транслювати інформацію в різні зони за окремими каналами (якщо в системі передбачено можливість ручного керування за допомогою вхідних сигналів чи спрямування їх у різні канали, то такі системи називають матричними);

розподілені системи поєднують властивості багатозональних та багатоканальних з можливістю дистанційного керування (у них основні (виконавчі, термінальні) блоки можуть виноситись на великі відстані) [9].

За архітектурою СО можна розділити на [11]:

одноріневі (централізовані), побудовані як єдиний комплекс технічних засобів (на базі спеціалізованих станцій контролю та управління) та призначені для управління нескладними процесами, що відбуваються, як правило, автономно;

дворівневі (найпоширеніші) включають

розгалужену систему комунікації засобів зв'язку, що забезпечують обмін інформацією як між підсистемами одного рівня, так і між локальними системами управління та станціями контролю і відображення інформації;

багаторівневі системи, що призначені для управління об'єктами з просторово розподіленою структурою.

За способом управління СО можна розділити на:

автоматичні, що функціонують без участі оператора при активації засобів оповіщення;

автоматизовані, у яких оператори мають можливість здійснювати локальне або дистанційне управління, втручатись в процес оповіщення, з метою його призупинення або корегування;

системи ручного керування, які передбачають оповіщення оператором за визначеними ним зонами.

За конструктивним виконанням СО можна розділити на [8]:

компактні моноблоки, що мають просте конструктивне виконання та можуть монтуватися в стійки;

стійкові системи, які монтуються з набору блоків різного функціонального призначення та використовуються для встановлення в спеціалізовані електротехнічні шафи чи стійки;

модульні багатофункціональні системи, що складаються з окремих модулів та можуть монтуватися в декількох корпусах або електротехнічних шафах.

За способом передачі інформації (сигналу) СО можна розділити на [12]:

аналогові, у процесі роботи яких безперервно обробляються аналогові сигнали завдяки функціональним елементам;

цифрові, у процесі функціонування яких обробляються цифрові сигнали, а інформація подається в цифровій формі.

За типом каналів зв'язку СО можна розділити на [13]:

проводові, у яких передача інформації здійснюється проводовими каналами зв'язку, вони є найбільш розповсюдженими та відрізняються високою надійністю, зручністю експлуатації та обслуговування;

безпроводові, у яких передача інформації здійснюється радіоканалами, під час якої кінцеве обладнання хоча б одного із споживачів може вільно переміщатися із збереженням унікального ідентифікаційного номера в межах пунктів закінчення мережі. Основні типи: радіорелейна, супутникова, мобільна, пейджингова, трекінгова.

За сферами застосування СО можна розділити на [3]:

загальнодержавні, що забезпечують передачу інформації оповіщення від пунктів управління до регіональних центрів;

регіональні, які забезпечують передачу інформації оповіщення від пунктів управління регіональних центрів до підпорядкованих їм органів управління;

відомчі, що мають визначену приналежність, наприклад, СО цивільної оборони, СО про пожежу, система попередження про ракетний напад тощо;

об'єктові – локальні СО, що здійснюють оповіщення визначених об'єктів.

Переваги та недоліки різних СО з точки зору їх застосування як систем спеціального призначення наведені в табл. 1.

СО спеціального призначення повинна виконувати декілька основних завдань (моніторинг поточної обстановки, аналіз її стану та змін, формування інформації оповіщення), що мають певні пріоритети та вирішуються у визначений для кожного завдання час або за необхідності – негайно. Отже, недоліки трансляційних та аварійних систем є неприйнятними для СО спеціального призначення.

Однорівневість (централізованість) будь-якої СО призводить до зниження оперативності та достовірності інформації оповіщення у зв'язку з тривалим періодом її підготовки. Для усунення зазначених вище недоліків побудову архітектури СО спеціального призначення доцільно здійснювати за принципом *багаторівневості*, що дозволить за рахунок прийняття відповідних рішень на кожному рівні зменшити складність управління системою та підвищити її динамічність, а також забезпечити темп оновлення інформації в масштабі часу, близькому до реального.

Наявність декількох рівнів системи та можливість забезпечення її функціонування у складних умовах дозволяють визначити, що СО спеціального призначення має бути *комбінованою*.

Недоліки багатозональних та багатоканальних систем не мають критичного впливу на СО спеціального призначення, але для неї важливу роль відіграють переваги *розподіленого* типу, зокрема він дозволить: проводити децентралізовану обробку даних; використовувати розподілені в просторі та функціонально системи введення та виведення інформації; підвищити оперативність отримання інформації оповіщення та її точність.

Узагальнена типова структура розподіленої багаторівневої системи включає три пов'язані рівні (рис. 2):

рівень споживача (замовника) містить виконавчі механізми, які працюють з визначеними об'єктами управління, він повинен мати засоби візуалізації процесів, що відбуваються;

рівень управління – це спеціалізоване програмне забезпечення, призначене для обробки даних та передачі їх на операторський рівень, а також часткових баз даних до рівня споживача;

операторський рівень містить сервери баз даних та автоматизовані робочі місця обробки вхідної інформації та обміну обробленими даними з іншими рівнями.

Таблиця 1

Порівняльні характеристики різних типів СО

Тип СО	Переваги для СО спеціального призначення		Недоліки для СО спеціального призначення	
	важливі	неважливі	критичні	некритичні
1	2	3	4	5
За функціональним призначенням				
Трансляційна	Можливість використання за відсутності побутових електромереж; наявність розгалуженої мережі трансляційних ліній	Простота використання абонентського гучномовця; можливість застосування мережі цивільної оборони	Стаціонарне розташування (віддаленість засобів оповіщення від джерела інформації); обмежений об'єм інформації для транслювання	Використання звукових сигналів та їх низька якість
Аварійна	Простота інфраструктури; низька ймовірність спотворення сигналів оповіщення	Висока ймовірність доставки сигналів оповіщення	Одностороння передача інформації з низькою інформативністю	
Комбінована	Наявність декількох рівнів, що мають визначені функції й обладнання та поєднані між собою у єдину систему			Додаткові витрати на резервування каналів зв'язку з метою забезпечення функціонування системи в складних умовах
За принципом побудови				
Багатозональна	Можливість оповіщення за окремими або за всіма зонами		Централізованість управління процесом оповіщення	
Багатоканальна	Непрацездатність окремого каналу не впливає на роботу всієї системи	Передача інформації здійснюється одночасно декількома каналами		Відносна складність обладнання багатоканальної системи зв'язку
Розподілена	Висока швидкодія завдяки розподілу завдань між паралельними процесами; підвищена надійність та стійкість до відмов; простота в нарощуванні як структурного складу, так і функціональних можливостей; модульність системи			Технічна складність побудови та відносно висока вартість; необхідність налагодження каналів зв'язку; ускладнення контролю цілісності даних та захисту інформації; висока кваліфікація фахівців для розробки та обслуговування системи
За архітектурою				
Однорівнева (централізована)	Висока швидкість обміну даними між процесорним модулем та засобами введення-виведення інформації	Висока надійність через лінійність системи зв'язку та передачі даних; можливість реалізації ефективного контролю	Неможливість рознесення структурних елементів у просторі; низькі завадостійкість та стійкість до відмов системи	
Дворівнева	Порівняно спрощений процес оновлення програмного забезпечення та архівування даних		Обмеженість фізичними причинами (потужністю процесора, пропускною здатністю ліній передачі даних)	

Продовження таблиці 1

1	2	3	4	5
			зростання кількості користувачів бази даних; неможливість швидкого масштабування системи	
Багаторівнева	Невелика складність окремих систем управління (особливо на низьких рівнях); охоплення всіх рівнів управління; динамічність системи (на кожному рівні приймається відповідне рішення); можливість роботи в масштабі часу, близькому до реального			Складність забезпечення безпеки інформації за рахунок наявності численних зв'язків між рівнями; складність управління системою; великі відстані між вузлами; висока кваліфікація фахівців для обслуговування системи
За способом управління				
Автоматизована	Оброблення особою, що приймає рішення більш повної та достовірної інформації; оперативність контролю процесів у системі та гнучкість управління ними; зниження працевтрат на оброблення інформації	Чутливість системи до неправильних дій Оператора або формату вхідних даних; можливість статистичного аналізу результатів виконання завдань у системі		Вартість програмування системи; висока кваліфікація фахівців для її обслуговування
Автоматична		Скорочення фахівців для обслуговування за рахунок функціонування відповідно до заданого алгоритму	Необхідність спеціального обладнання	Висока кваліфікація фахівців для обслуговування системи
Ручного керування		Керованість розподілом етапів виконання завдання за часом	Складність контролю та управління; невисока завадостійкість; припинення функціонування системи за відсутності оператора	
За конструктивним виконанням				
Компактна	Багатофункціональність			Обмеження за потужністю
Стійкова	Наявність фізичного захисту блоків від несанкціонованого доступу	Забезпечення необхідного температурного режиму; відносно великий строк експлуатації обладнання	Громіздкість; стаціонарність; специфіка обслуговування обладнання	
Модульна	Масштабованість обладнання; наявність захисту блоків від несанкціонованого доступу; великий строк експлуатації обладнання			Необхідність узгодження роботи модулів; імовірність відсутності модуля для вирішення специфічного завдання; необхідність наявності специфічних знань у фахівців для обслуговування

Продовження таблиці 1

1	2	3	4	5
За типом обладнання				
Аналогова		Висока надійність та доступність за вартістю	Потреба в перетворенні аналогової інформації в цифрову; неможливість виявлення перешкоди в сигналі та необхідність застосування фільтрації сигналів у зв'язку з безперервністю області значень	
Цифрова	Можливість складнішої та багатоступеневої обробки даних; їх тривале зберігання; легкість у проектуванні та налагодженні цифрових пристроїв системи	Можливість організації необхідної захищеності від дії шумів, наведень і перешкод;		Потреба в узгодженні аналогової апаратури із цифровою; мала ємність цифрових сигналів за рахунок передачі інформації переважно двома рівнями
За способом передачі інформації				
Проводова	Наявність декількох рівнів захисту; відносно мала чутливість до перешкод; можливість використання резервного джерела живлення		Відносно складне встановлення дротових систем	Можливість виникнення складнощів при прокладанні або демонтажу
Безпроводова	Можливість встановлення в місцях без доступу до стаціонарного джерела живлення; здатність до розширення системи	Можливість підключення до телефону та/або комп'ютерних систем для віддаленого моніторингу		Необхідність в автономному джерелі живлення; чутливість до радіоперешкод та метеорологічних умов
За сферою застосування				
Загально-державна		Поширеність на всю територію країни	Складність контролю за виконанням оповіщення та вжиттям відповідних заходів захисту	
Регіональна			Територіальна обмеженість оповіщення; можливість витоку спеціальної інформації	
Відомча	Обмеженість оповіщення відомчою належністю об'єктів оповіщення та їх призначенням; можливість організації захисту від несанкціонованого доступу до інформації	Можливість організації ефективного контролю за процесом оповіщення та вжиттям відповідних заходів захисту		
Об'єктова			Локалізація оповіщення в межах визначеного об'єкту	

Окрім того, СО спеціального призначення має бути *автоматизованою*, оскільки оповіщення проводиться з використанням спеціалізованих програмно-технічних комплексів, що проводять розрахунки, але потребують супроводження оператором.

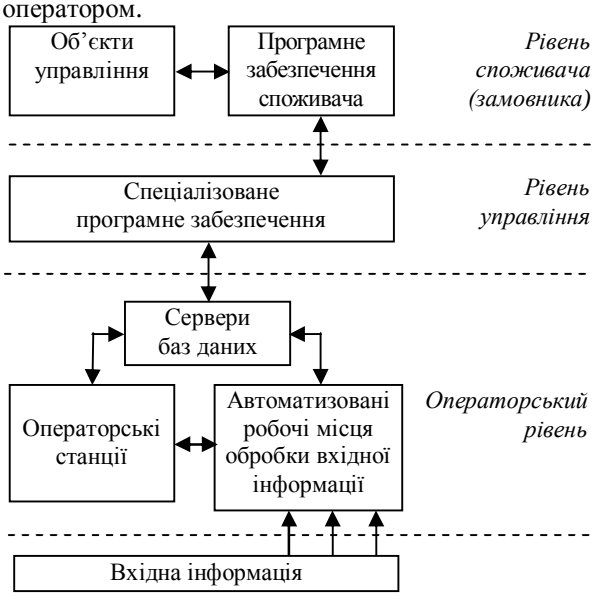


Рис. 2. Узагальнена типова структура СО

На даний час потужностей сучасної електронно-обчислювальної техніки достатньо для створення комплексної системи інформування та оповіщення. СО спеціального призначення повинні бути *модульними*, *цифровими* і побудованими на базі персональних електронно-обчислювальних машин (можливо, спеціалізованих).

Система зв'язку та передачі даних СО призначена для автоматизованого обміну даними. Для забезпечення надійного та оперативного обміну інформацією на великі відстані в СО спеціального призначення повинні використовуватися *проводові* цифрові канали зв'язку волоконно-оптичної лінії та, за необхідності, *безпроводові* (для реалізації функції мобільності та поширеності системи).

З урахуванням специфіки завдань, що вирішуються СО спеціального призначення, необхідності дотримання вимог нормативно-правових актів та керівних документів, зазначену СО доцільно будувати *відомчою*.

Таким чином, аналіз класифікації існуючих СО, загальної документації з їх стандартизації, важливих переваг та критичних недоліків різних їх типів дозволяє визначити принципи організаційної побудови СО спеціального призначення (табл. 2).

Вимоги до функціональності СО спеціального призначення

Оскільки СО реалізують усі функції автоматизованих систем моніторингу та управління, окрім зазначених організаційних принципів, реалізація СО спеціального призначення повинна задовольняти такі вимоги до функціональності (рис. 3) [14, 15].

Таблиця 2

Принципи організаційної побудови СО спеціального призначення

Принцип	Визначення
Функціональне призначення	Комбінована
Принцип побудови	Розподілена
Архітектура	Багаторівнева
Спосіб управління	Автоматизована
Конструктивне виконання	Модульна
Спосіб передачі інформації (сигналу)	Цифрова
Тип каналів зв'язку	Проводова + безпроводова
Сфера застосування	Відомча

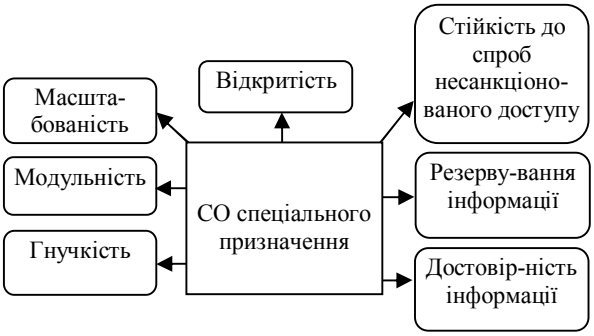


Рис. 3. Вимоги до функціональності СО спеціального призначення

Відкритість передбачає: можливість створення системи у вигляді єдиного комплексу на основі об'єднання підсистем; формування єдиних баз даних для різних підсистем автоматизації; наявність умов, сприятливих для створення територіально-розподілених систем з дотриманням вимог захисту інформації; допустимість надання даних зовнішнім споживачам при дотриманні вимог щодо захисту інформації та організації прав доступу тощо.

Масштабованість – це здатність системи адаптуватися до різкої зміни показників та підвищення вимог щодо вирішення поставлених завдань, передбачає наявність можливості нарощування системи шляхом включення необхідної кількості підсистем, нових об'єктів, збільшення кількості джерел інформації тощо.

Модульність передбачає створення системи вузлів типової структури, що забезпечить нарощування функціональних можливостей, інтеграцію до автоматизованих систем управління вищого рівня тощо.

Гнучкість визначається: розподіленою побудовою системи та реалізацією в ній алгоритмів прийняття рішення; швидким перенесенням програмного забезпечення на інше обладнання; розширенням функціональних можливостей та вирішуваних завдань; підходами до організації віддаленого доступу й налагодження інтерфейсу користувачів тощо.

Стійкість до несанкціонованого доступу передбачає: програмний та апаратний захист від

спроб несанкціонованого втручання; визначення порядку доступу персоналу до робочих місць тощо.

Резервування інформації має на меті забезпечення збереження та відновлення інформації у випадках, що можуть призвести до її пошкодження чи втрати.

Достовірність інформації визначається застосуванням: спеціалізованих систем кодування; алгоритмів контролю достовірності отриманої інформації; схем фіксації граничних показників процесу оповіщення тощо.

Таким чином, реалізація СО спеціального призначення відповідно до наведених принципів та вимог забезпечить її стійке функціонування, уникнення витоку інформації, гарантування оперативного отримання інформації споживачами (замовниками).

Висновки й перспективи подальших досліджень

За результатами аналізу існуючих СО різного призначення було узагальнено їх класифікацію, що відображає різноманітність підходів до побудови й організації СО. У результаті дослідження переваг та недоліків кожного класу СО було визначено основні принципи організаційної побудови СО спеціального призначення, відмінними рисами яких є одночасне використання розподіленої побудови та принципу багаторівневості.

Окрім зазначених організаційних принципів, до СО спеціального призначення висунуті вимоги до функціональності. Основними з них є масштабованість, модульність та гнучкість, обумовлені необхідністю відповідності СО спеціального призначення принципам розподіленості та багаторівневості, що забезпечить:

спрощення в організаційному та функціональному нарощуванні системи;

реалізацію алгоритмів формування інформації оповіщення та прийняття рішення посадовими особами;

використання, за необхідності, програмного забезпечення на іншому обладнанні;

застосування підходів до організації віддаленого доступу та налагодження інтерфейсу користувачів тощо.

Подальші дослідження зазначеного напрямку передбачають розробку структури конкретної СО спеціального призначення, що буде відповідати визначеним принципам та задовольняти вимоги до функціональності складних систем моніторингу й управління.

Література

1. Левченко О. В. Концептуальний підхід до комплексної оцінки стану інформаційної безпеки / О. В. Левченко // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – Вип. № 3 (20). – 2015. – С. 47–50. **2. Грищук Р. В.** Інформаційна та кібернетична безпека: роль та місце в умовах гібридної війни / Р. В. Грищук // Всеукр. наук.-практ. конф. [“Кібербезпека в Україні: правові та організаційні питання”] (Одеса, 21 жовт.). – Одеса : ОДУВС, 2016 р. – С. 16–17. **3. Воробієнко П. П.** Системи оповіщення цивільного захисту. навч. посіб. / П. П. Воробієнко, С. І. Білоусов – Одеса : ОНАС ім. О. С. Попова, 2012. – 76 с. **4. Кочнов О. В.** Особенности проектирования систем оповещения : учеб. пособ. / О. В. Кочнов, – Муром : Изд. “Стерх”, 2012. – 154 с. **5.** Безпека у надзвичайних ситуаціях. Захист населення у надзвичайних ситуаціях. Основні положення : ДСТУ 7095:2009. – [Введ. 2010–02–01]. – К. : Держспоживстандарт України, 2010. – 15 с. **6.** Системи протипожежного захисту : ДБН В.2.5-56-2014. – [Введ. 2015–07–01]. – К. : Мінрегіон України, 2015. – 133 с. **7.** Про затвердження Положення про організацію оповіщення і зв'язку у надзвичайних ситуаціях : постанова Кабінету Міністрів України від 15 лютого 1999 р. № 192. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/192-99-%D0%BF. **8. Основы построения систем оповещения.** [Электронный ресурс]. – Режим доступа : http://www.escortpro.ru/page/article/article105.htm.

9. Потомский С. Ю. Архитектура распределенной системы управления на основе реконфигурируемой многоконвейерной вычислительной среды [Электронный ресурс] / С. Ю. Потомский, Н. А. Полойко // L-Net Системный администратор. – 2014. – Вып. № 10 (143). – Режим доступа : http://samag.ru/archive/article/2806. **10. Гунько А. В.** Классификация АСУ ТП. [Электронный ресурс]. – Режим доступа : http://gun.cs.nstu.ru/ics/classification.pps. **11. Васильев К. К.** Теория автоматического управления (следящие системы) : учеб. пособ. – [2-е изд.]. – Ульяновск, 2001. – 98 с. **12. Преимущества и недостатки** проводной и беспроводной охранной системы. [Электронный ресурс]. – Режим доступа : http://dnt.net.ua/novosti/200-preimushchestva-i-nedostatki-provodnoj-i-besprovodnoj-okhrannoj-sistemy. **13.** Про телекомунікації : Закон України від 18.11.2003 № 1280-IV. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1280-15.

14. Черепаха Г. С. Функциональные требования к информационной системе управления командой проекта / Г. С. Черепаха // Восточно-Европейский журнал передовых технологий. – 2010. – Вып. № 9 (46), Том 4. – С. 53-57. **15.** Моніторинг об’єктів в умовах апріорної невизначеності джерел інформації / Ю. Я. Бобало, Ю. Г. Даник, Л. О. Комарова та ін. – Дрогобич; Львів : Коло, 2014. – 252 с.

ПРИНЦИПЫ ОРГАНИЗАЦИОННОГО ПОСТРОЕНИЯ И ТРЕБОВАНИЯ К ФУНКЦИОНАЛЬНОСТИ СИСТЕМ ОПОВЕЩЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Сергей Валентинович Ковбасюк *(д-р техн. наук, с. н. с., ведущий научный сотрудник)*[1]
Дмитрий Владимирович Пекарев *(канд. техн. наук, с. н. с., начальник научного центра)*[1]
Ирина Анатольевна Беспалко *(младший научный сотрудник)*[1]

[1]*Житомирский военный институт имени С. П. Королёва, Житомир, Украина*

В статье представлены результаты анализа построения и функционирования существующих систем оповещения в разных сферах деятельности и обзор научных трудов, которые посвящены вопросам оповещения и создания систем оповещения. Определено, что существующие подходы не в полной мере учитывают особенности проведения оповещения по специфическим (оборонным) вопросам, не содержат обоснования принципов организационного построения систем оповещения специального назначения и не могут быть взяты как прототип для указанных систем.

В статье предложена классификация систем оповещения, определены преимущества и недостатки каждого их класса. Сформированы основные принципы организационного построения, которым должна соответствовать система оповещения специального назначения, и определены требования к ее функциональности как к информационно-управляющей системе, которая реализует все функции автоматизированных систем мониторинга и управления.

Ключевые слова: *система оповещения специального назначения, принципы организационного построения, функциональные требования, классификация.*

THE PRINCIPLES OF ORGANIZATIONAL CONSTRUCTION AND FUNCTIONALITY REQUIREMENTS OF WARNING SYSTEM OF SPECIAL PURPOSE

Serghij V. Kovbasjuk *(Doctor of Technical Science, Senior researcher, Leading researcher of research centre)*[1]
Dmytro V. Pekariev *(Candidate of Technical Sciences, Senior researcher, Chief of research centre)*[1]
Iryna A. Bespalko *(Junior researcher of research centre)*[1]

[1]***S. P. Korolev Zhitomir Military Institute, Zhitomir, Ukraine***

The results of the analysis of construction and operation a warning systems in the different spheres of activity and review of scientific works that was devoted to the questions of creating of warning systems was presented in the article. It was determined that the existing approaches are not considered particularly special purpose warning systems on specific (defense) questions, do not contain any justification the principles of their organizational structure and couldn't to be a prototype of the special purpose warning systems.

The classification of warning systems, their advantages and disadvantages of each class of warning systems was suggested. The basic principles of organizational construction, which must comply with special purpose warning system was formed and the requirements for its functionality are defined as management information system, which implements all the functions of automated monitoring and control systems.

Keywords: *special purpose warning systems, the principles of organizational structure, functional requirements, classification.*

References

1. Levchenko A. V. (2015), Conceptual approach to a comprehensive assessment of information security. [*Konceptualjnyj pidkhid do kompleksnoji ocinky stanu informacijnoji bezpeky*], Science and Technology of the Air Force of Ukraine, No. 3 (20), pp. 47 – 50. **2. Grischuk R. V.** (2016), Information and cybernetic security: role and place in the hybrid war : National Scientific and Practical Conference "Cybersecurity in Ukraine: legal and organizational issues". [*Informaciyna ta kbernetichna bezpeka:rol ta misce v umovah hibrydnoyi vyini*], Odessa., ODUVS, pp. 16–17. **3. Vorobijenko P. P.**, Bilousov S. I. (2012), Warning system of civil protection: Tutorial. [*Systemy opovishhennja cyviljnogho zakhystu: navchaljnyj posibnyk*], Odesa, ONAT O. S. Popov, 76 p. **4. Kochnov O. V.** (2012), Features of the design of warning systems: a tutorial. [*Osobennosti proektirovanija sistem opoveshhenija: uchebnoe posobie*], Publishing house "Sterkh", 154 p. **5. DSTU 7095:2009** (2010), Safety in emergencies. Protecting the population in emergency situations. Basic provisions. [*Bezpeka u nadzvychajnykh sytuacijakh. Zakhyst naselennja u nadzvychajnykh sytuacijakh. Osnovni polozhennja*], K., Derzhspozhyvstandart of Ukraine, 15 p. **6. DBN V.2.5-56-2014** (2015), Fire protection systems. [*Systemy protypozhezhnogho zakhystu*], K., Ministry of Regional Development of Ukraine, 133 p. **7. "**Resolution of the Cabinet of Ministers of Ukraine dated February 15, 1999 No. 192 On Approval of the Provision on the Organization of Emergency Notification and Communication" [*"Pro zatverdzhennja Polozhennja pro orghanizaciju opovishhennja i zv'jazku u nadzvychajnykh sytuacijakh"*], available at: http://zakon2.rada.gov.ua/laws/show/192-99-%D0%BF. **8. "**Fundamentals of building warning systems" [*"Osnovy postroenija sistem opoveshhenija"*], available at: http://www.escortpro.ru/page/article/article105.htm. **9.** Potomskij S. Ju., Polojko N. A., "The architecture of a distributed control system based on a reconfigurable multicopy computing environment" [*"Arhitektura raspredelennoj sistemy upravlenija na osnove rekonfiguriruemoj mnogokonvejernoj vychislitel'noj sredy"*], available at: http://samag.ru/archive/article/2806. **10.** Gun'ko A. V., "Classification of ACS TP" [*"Klassifikacija ASU TP"*], available at: http://gun.cs.nstu.ru/ics/classification.pps. **11. Vasil'ev К. К.** (2001), The theory of automatic control (tracking system) : A Tutorial. [*Teorija avtomaticheskogo upravlenija (sledjashhie sistemy): Uchebnoe posobie*], 2nd ed, Ul'janovsk, 98 p. **12.** "Advantages and disadvantages of wired and wireless security system" [*"Preimushhestva i nedostatki provodnoj i besprovodnoj ohrannoj sistemy"*], available at : http://dnt.net.ua/novosti/200-preimushchestva-i-nedostatki-provodnoj-i-besprovodnoj-okhrannoj-sistemy. **13.** "About telecommunications" : The law of Ukraine [*"Pro telekomunikacyi : Zakon Ukrainy"*] 18.11.2003 № 1280-IV, available at : http://zakon2.rada.gov.ua/laws/show/1280-15. **14. Cherepaha G. S.** (2010), Functional requirements for the information management system of the project team. [*Funkcional'nye trebovanija k informacionnoj sisteme upravlenija komandoj proekta*], Eastern-European Journal of Eenterprise Technologies, No. 9 (46), pp 53-57. **15. Bobalo Ju. Ya.**, Danyk Ju. G., Komarova L. O. (2014), Monitoring of objects in conditions of a priori uncertainty sources. [*Monitoryngh ob'jektiv v umovakh apriornoji nevyznachenosti dzherel informaciji*], Droghobych, Ljviv, 252 p.

УДК 354.42

Олександр Миколайович Косогов *(кандидат військових наук)*

Військова частина А1906, Київ, Україна

МЕТОД ВИБОРУ РАЦІОНАЛЬНОГО СКЛАДУ СКЛАДНОЇ СИСТЕМИ НА БАЗІ МОДИФІКОВАНОГО МЕТОДУ TOPSIS

У статті виділені специфічні особливості задач вибору раціонального складу складної системи, зокрема системи інформаційної безпеки, що дозволяють ідентифікувати їх як завдання багатокритеріального аналізу і прийняття рішень в нечіткому середовищі. Запропоновано узагальнену концептуальну модель прийняття рішень в задачах вибору альтернативних варіантів складу системи, а також модифікацію методу TOPSIS. Ця модифікація полягає в інтегруванні до алгоритму прийняття рішень додаткової компоненти, яка забезпечує розрахунок на основі методу аналізу ієрархій коефіцієнтів компетенції експертів, а також зведення ієрархічної структури критеріїв вибору, що характеризує альтернативи, до одноступінчастої ієрархії

Ключові слова*: управління, складна система, прийняття рішень, нечітке середовище, інтелектуальні технології, багатокритеріальна оптимізація*

Вступ

В умовах ведення гібридної війни Російської Федерації проти України виникають особливості функціонування складних систем військового призначення (ССВП), які не притаманні завданням мирного часу та традиційним формам і способам збройної боротьби, особливо на етапах підготовки та початку війни, коли реальні наміри і дії противника приховуються або проводяться демонстративно під виглядом інших заходів.

Особливості умов застосування воєнної сили у гібридній війні, високій динамізм змін обстановки вимагає від ССВП відповідної адаптації, проведення необхідних системних заходів стосовно удосконалення функціоналу, взаємодії та структури для ефективного управління підпорядкованими силами і засобами в умовах збройної агресії.

Зазначене вище обумовлює актуальність наукових досліджень стосовно вирішення завдання обґрунтування раціонального складу та структури органів військового управління шляхом розробки та впровадження сучасних підходів для прийняття відповідних рішень.

Постановка проблеми. Проведений аналіз [1; 2; 5-8] свідчить, саме за таких умов функціонування ССВП застосування методів та алгоритмів багатокритеріального оцінювання дає змогу отримувати кращі результати на відміну від інших підходів. При цьому основним об’єктом дослідження є альтернативні варіанти структури органів військового управління.

Зменшення рівня невизначеності при обґрунтуванні раціональної структури органів військового управління досягається шляхом комплексного застосування процедур синтезу та аналізу, генерування одночасно кількох альтернативних варіантів комплекту, а також розробки механізмів їх коригування.

На теперішній час загальний підхід до обґрунтування структури ССВП здійснюється з недотриманням базових принципів системного підходу: не виконується принцип багатоальтернативності прийняття управлінських рішень (відповідні органи обмежуються розробкою тільки одного варіанта комплекту), формування управлінських рішень не базується на результатах оцінювання та аналізу ефективності функціонування системи, в якій зазначений ССВП є підсистемою нижчого рівня, в механізмі реалізації запропонованих рішень відсутні процедури їх корекції.

Питанням дослідження складних систем приділяється достатньо уваги [1–6], при цьому найбільш системно результати викладені у [7], де визначено, що специфічними особливостями завдання визначення раціонального складу складної системи військового призначення є:

неповнота й невизначеність вихідної інформації при функціонуванні системи в різних умовах обстановки;

багатокритеріальність завдання, що пов’язано з необхідністю врахування великої кількості часткових показників;

наявність кількісних і якісних показників, які необхідно враховувати;

неможливість застосування класичних методів оптимізації.

Враховуючи викладене, пошук шляхів визначення комплекту ССВП є актуальним науковим і практичним завданням.

Метою статті є викладення методу ранжирування альтернатив складу системи на основі оцінок експертів з урахуванням їх компетентності та подальшого вибору раціонального варіанта складу системи.

Викладення основного матеріалу

Нехай відомі такі компоненти складної системи :

1. $X = x_i, i = \overline{1,n}$ – множина альтернатив складу системи;
2. $K = \{K_i,\ j = 1,m\}$ – множина загальних критеріїв ефективності системи;
3. $K_j = \{K_{jt},\ t = 1,s_j\}$ – множина часткових критеріїв;
4. $E = \{e_l,\ l = 1,g\}$ – множина експертів;
5. $w_j,\ j = 1,m$ – коефіцієнти відносної важливості критеріїв ($K = \{K_i,\ j = 1,m\}$);
6. $w_{jt},\ t = l,s_j,\ j = 1,m$ – коефіцієнти відносної важливості часткових критеріїв ($K_j = \{K_{jt},\ t = 1,s_j\}$);
7. $v_l,\ l = 1,\ g$ – коефіцієнти компетентності експертів.

Вирішення завдання припускає виконання такої послідовності дій.

Крок 1. Для здійснення багатокритеріальної оптимізації завдань ІБ на базі методу TOPSIS необхідно насамперед позбутися від ієрархічної структурованості критеріїв (рис. 1). З цією метою на основі методу аналізу ієрархій (МАІ) Сааті за допомогою коефіцієнтів відносної важливості критеріїв і часткових критеріїв визначаються ваги [9,10], з якими останні ввійдуть у розрахунок інтегрального критерію К. У формалізованому вигляді добутком w_j,де $\sum_{j=1}^{m} w_j = 1$ та w_{jt},де $\sum_{t=1}^{s_j} w_{jt} = 1$ визначається w_{jt} – вага часткового критерію w_{jt}^{K} в розрахунку інтегрального критерію $K = \{k_j\}, j = \overline{1,m}$, тобто $w_{jt}^{K} = w_{jt} \cdot w_j$.

В результаті двоступінчаста ієрархічна структура критеріїв вибору K, що характеризує альтернативи, зводиться до одноступінчастої ієрархії (рис. 2).

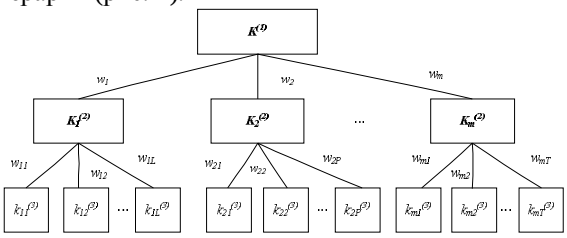


Рис. 1. Ієрархічна структурованість критеріїв вибору, що характеризують альтернативи

У подальших кроках для спрощення індексів усі часткові критерії об'єднуються в єдиній множині G.

$$G = \{k_{jt}, j = \overline{1,m}, t = \overline{1,s_j}\} = \{k_z, z = \overline{1,Z}\},$$
$$z = s_{j-1} + t, j = \overline{1,m}, \quad t = \overline{1,s_j}, \quad s_0 = 0,$$

де Z – загальне число часткових критеріїв, що характеризують альтернативи, тобто $Z = \sum_{j=1}^{m} s_j$.

У такому випадку. $w_z = w_{jt}$.

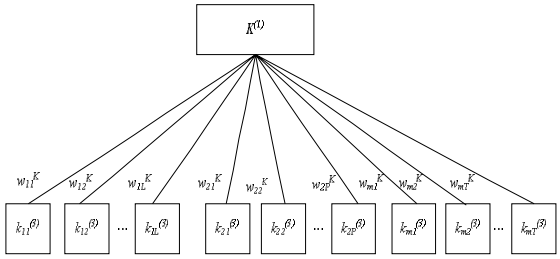


Рис. 2. Зведення критерію K до одноступінчастої ієрархії

Крок 2. Ступені належності (відповідності) альтернатив частковим критеріям оцінюються лінгвістичними значеннями (рис.3) і виражаються нечіткими трапецієподібними числами $R^l = (r_{iz}^l) = (a_{iz}^l, b_{iz}^l, c_{iz}^l, d_{iz}^l)$. Так, наприклад, якщо ступінь задоволення (належності) альтернативи x_i частковому критерію k_z експертом оцінена значенням “добре”, то це виражається як $r_{iz}^l = (7,8,8,9)$, а якщо експертом дана оцінка “дуже добре”, то $r_{iz}^l = (8,9,10,10)$ і т.ін. У результаті експертної оцінки ступенів належності альтернатив частковим критеріям отримуємо матрицю:

$$R^l = [r_{iz}^l], l = \overline{1,g} \leftrightarrow \{a_{iz}^l, b_{iz}^l, c_{iz}^l, d_{iz}^l\}, l = \overline{1,g}$$

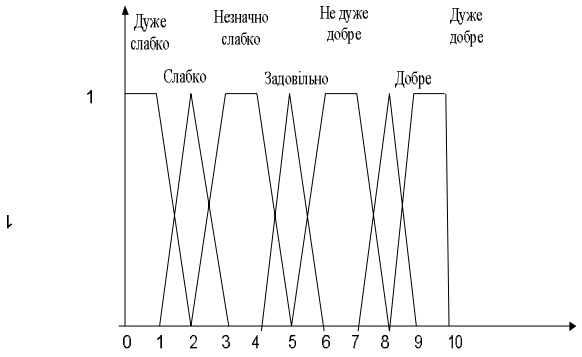


Рис.3. Ступені належності (відповідності) альтернатив частковим критеріям

Крок 3. Цей крок припускає попередній розрахунок коефіцієнтів компетентності експертів $v_l, l = \overline{1,g}$. З цією метою авторами застосована модифікація методу, що полягає в інтегруванні до алгоритму додаткового кроку, який припускає розрахунок коефіцієнтів компетентності експертів, що беруть участь у процедурі оцінювання альтернатив.

З урахуванням коефіцієнтів компетентності експертів $v_l, l = \overline{1,g}$ формується матриця

$$R^l = [r_{iz}^l], l = \overline{1,g} \leftrightarrow \{a_{iz}^{v_l}, b_{iz}^{v_l}, c_{iz}^{v_l}, d_{iz}^{v_l}\}, l = \overline{1,g}$$

Елементами цієї матриці є трапецієподібні числа, які виражають ступінь задоволення альтернативи x_i частковим критеріям k_z; з урахуванням компетентності експертів і розраховуються в такий спосіб:

$$a_{iz}^{v_l} = a_{iz}^{l} \cdot v_l;\ b_{iz}^{v_l} = b_{iz}^{l} \cdot v_l;\ c_{iz}^{v_l} = c_{iz}^{l} \cdot v_l;\ d_{iz}^{v_l} = d_{iz}^{l} \cdot v_l. \quad (3)$$

Крок 4. Визначається єдина – агрегована матриця:

$$R^l = [r_{iz}^l], l = \overline{1,g} \leftrightarrow \{a_{iz}^{v_l}, b_{iz}^{v_l}, c_{iz}^{v_l}, d_{iz}^{v_l}\},$$

$$l = \overline{1,g} \rightarrow R = [r_{iz}] \leftrightarrow \{a_{iz}, b_{iz}, c_{iz}, d_{iz}\}.$$

Елементи цієї матриці визначаються в такий спосіб:

$$a_{iz} = \{\min a_{iz}^{v_l};\ l = \overline{1,g}\};$$
$$b_{iz} = \frac{1}{g}\sum_{l=1}^{g} b_{iz}^{v_l};$$
$$c_{iz} = \frac{1}{g}\sum_{l=1}^{g} c_{iz}^{v_l};$$
$$d_{iz} = \{\max d_{iz}^{v_l};\ l = \overline{1,g}\}; \quad (4)$$

Елементи матриці множаться на ваги часткових критеріїв. У результаті цієї операції отримується зважена нечітка матриця:

$$a_{iz}^W = a_{iz} \cdot w_z;$$
$$b_{iz}^W = b_{iz} \cdot w_z;$$
$$c_{iz}^W = c_{iz} \cdot w_z; \quad (5)$$
$$d_{iz}^W = d_{iz} \cdot w_z.$$

Крок 6. Матриця (5) нормалізується. Для цього застосовується метод Hsu і Cehn [11], на основі якого визначаються $d_z^+ = \max d_{iz}^v, i = \overline{1,n}$. Далі на основі виразу

$$R_{iz}^N = [r_{iz}^N] \leftrightarrow \{a_{iz}^N, b_{iz}^N, c_{iz}^N, d_{iz}^N\} \leftrightarrow \left\{\frac{a_{iz}^W}{d_z^+}, \frac{b_{iz}^W}{d_z^+}, \frac{c_{iz}^W}{d_z^+}, \right.$$

визначаються елементи нормалізованої матриці прийняття рішень.

Крок 7. На основі зважених значень визначається ідеальне позитивне (найкраще) рішення (ІПР) X^+. З цією метою для кожного $k_z, (z = \overline{1,z})$ відбираються

$$d_{iz}^+ = \{\max d_{iz}^N;\ i = \overline{1,n}\} \quad (7)$$

формується матриця

$$X^+ = [d_z^+] = [(d_1^+, d_1^+, d_1^+, d_1^+), \ldots, (d_Z^+, d_Z^+, d_Z^+, d_Z^+)] \quad (8)$$

Відповідно до виразу (6) $d_Z^+ = 1$ для $\forall z$ тобто всі елементи матриці X^* дорівнюють одиниці.

Крок 8. Обчислюється ідеальне негативне (найгірше) рішення (ІНР) X^-. З цією метою для кожного $k_z\ z = \overline{1,z}$ відбираються

$$a_{iz}^- = \{\min a_{iz}^N;\ i = \overline{1,n}\} \quad (9)$$

і формується наступна матриця:

$$X^- = [a_z^-] = [(a_1^-, a_1^-, a_1^-, a_1^-), \ldots, (a_Z^-, a_Z^-, a_Z^-, a_Z^-)] \quad (10)$$

Крок 9. З використанням формули (2) за індивідуальним значенням кожного часткового критерію розраховується відстань альтернатив до ІПР:

$$D_z^+(x_i, X^+) = \sqrt{\frac{1}{4}((a_{iz}^N - d_z^+)^2 + (b_{iz}^N - d_z^+)^2 + (c_{iz}^N - d_z^+)^2 + (d_{iz}^N - d_z^+)^2)} \quad (11)$$

На основі отриманих результатів формується вектор $[D^+] = [D_1^+, \ldots, D_Z^+]$

Крок 10. За індивідуальним значенням кожного часткового критерію розраховується відстань альтернатив до ІНР:

$$D_z^-(x_i, X^-) = \sqrt{\frac{1}{4}((a_{iz}^N - a_z^-)^2 + (b_{iz}^N - a_z^-)^2 + (c_{iz}^N - a_z^-)^2 + (d_{iz}^N - a_z^-)^2)}. \quad (12)$$

На основі отриманих результатів формується вектор $[D^-] = [D_1^-, \ldots, D_Z^-]$

Крок 11. Визначається відстань кожної з альтернатив до ІПР:

$$D^+(x_i) = \sqrt{\sum_{z=1}^{Z}(D_z^+(x_i, X^+)^2}. \quad (13)$$

Крок 12. Визначається відстань кожної з альтернатив до ІНР:

$$D^-(x_i) = \sqrt{\sum_{z=1}^{Z}(D_z^-(x_i, X^-)^2}. \quad (14)$$

Крок 13. Розраховується інтегральний показник (коефіцієнт близькості) для кожної порівнюваної альтернативи як відношення обчисленого для неї відстані від ідеально найгіршого рішення до суми відстаней до найкращого й найгіршого рішень:

$$D(x_i) = D^+(x_i) + D^-(x_i)$$

$$\varphi(x_i) = \frac{D^-(x_i)}{D(x_i)}$$

У відповідності до значення коефіцієнта близькості $\varphi(x_i)$ є можливість ранжирування альтернатив. Так, чим ближче до одиниці значення коефіцієнта близькості $\varphi(x_i)$, тим переважніше порівнювана альтернатива. Найбільше значення інтегрального показника $\varphi(x_i)$ визначає найкращу альтернативу, тобто оптимальне рішення. Найменше значення $\varphi(x_i)$ відповідає найгіршій альтернативі.

Висновки

Запропоновано метод прийняття управлінських рішень щодо визначення структури складної системи з використанням багатокритеріальної оптимізації на базі методу TOPSIS. Використання методу TOPSIS у завданнях прийняття управлінських рішень дозволяє підвищити їх адекватність за рахунок приорітизации за ступенем близькості до ідеального рішення, забезпечує об'єктивність і транспарентність прийнятих управлінських рішень і надає можливості для розширення сфер застосування методів багатокритеріальної оптимізації. Застосована модифікація методу TOPSIS, що полягає в зведенні двоступінчастої ієрархії показників ефективності функціонування системи до одноступінчатої, а також інтегруванні в алгоритм додаткового кроку, що припускає розрахунок і введення коефіцієнтів компетентності експертів, які беруть участь у процедурі оцінки альтернатив.

Переваги запропонованого підходу до багатокритеріальної оптимізації на базі модифікованого методу TOPSIS для підтримки прийняття рішень зводяться до такого:

- відсутність необхідності в складанні бази нечітких правил;
- математична обґрунтованість і відносна простота розрахунків інтегральних показників, що дозволяють здійснити ранжирування альтернативних рішень, здійснювати подальший аналіз і вибір остаточного варіанта рішення;
- відсутність обмежень на кількість альтернатив і критеріїв, що характеризують об'єкт дослідження;
- урахування в алгоритмі прийняття рішень компетентності експертів, що беруть участь у процедурі прийняття рішень;
- урахування ієрархічної структурованості критеріїв, що описують альтернативи;
- можливість пріоритизации альтернатив за ступенем їх близькості до ідеального рішення.

Литература

1. Романченко, І. С. Використання таксономічних методів при проведенні досліджень у воєнній справі [Текст] / І. С. Романченко, О. М. Загорка // Зб. наук. пр. ЦНДІ ЗС України. – К., 2007. – № 3 (41). – С. 5–16. **2. Загорка.О.М.** Елементи дослідження складних систем військового призначення [Текст] / О. М. Загорка, С. П. Мосов, А. І. Сбитнєв, П. І. Стужук. – К.: НАОУ, 2005. – 100 с. **3. Корнеенко,** В. П. Методы оптимизации: учебник [Текст] / В. П. Корнеенко. – М.: Высш. шк., 2007. – 664 с. **4. Ahmadi,** H. Ranking the micro level critical factors of electronic medical records adoption using TOPSIS method [Text] / H. Ahmadi, M. S. Rad, M. Nilashi, O. Ibrahim, A. Almaee // Health Informatics – An International Journal. – 2013. – Vol. 2. – № 4, November. – P. 19–32. **5. Saelee,** S. Biomass type selection for boilers using TOPSIS multi-criteria model [Text] / S. Saelee, B. Paweewan, R. Tongpool, T. Witoon, J. Takada, K. Manusboonpurmpool // International Journal of Environmental Science and Development. – 2014, April. – Vol. 5. – № 2. – P. 181–186. 6. Baležentis, A. Multimoora-FG: a multi-objective decision making method for linguistic reasoning with an application to personnel selection [Text] / A. Baležentis, T. Baležentis, W. K. M. Brauers // Informatica. – 2012. – Vol. 23. – № 2. – P. 173–190. **7. Потьомкін, М. М.** Методика визначення раціонального складу складної системи військового призначення на основі модифікованого методу ELECTRE [Текст] / М. М. Потьомкін // Зб. наук. пр. ЦНДІ ЗС України. – К., 2008. – № 3 (45). – С. 62–68. **8. Косевцов В.О.**, Телелим В.М., Лобанов А.А. До питання оцінювання ефективності функціонування системи забезпечення воєнної безпеки держави// Наука і оборона. – 2010. - № 3. – С. 8-12. **9. Косогов О. М.** Методичний підхід до розрахунку показників ефективності функціонування системи інформаційної безпеки Головного управління розвідки Міністерства оборони України / О. М. Косогов, А. О. Сірик, Д. В. Косаренко // Зб. наук. праць. – К. : – НДІ ГУР МО України, 2015. – Вип. 41. – С. 51–60. **10. Романченко І.С.** Метод TOPSIS-ядро та його використання для багатокритеріального порівняння альтернатив/ І.С.Романченко, М.М.Потьомкін// Системи обробки інформації : збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2016. – Вип. 1 (138). – С. 103 – 106 **11. Hsu, H. M**. Fuzzy credibility relation method for multiple criteria decision-making problems [Text] / H. M. Hsu, C. T. Chen // Information Sciences. – 1997. – Vol. 96, Issue 1–2. – P. 79–91. doi: 10.1016/s0020-0255(96)00153-

МЕТОД ВЫБОРА РАЦИОНАЛЬНОГО СОСТАВА СЛОЖНЫХ СИСТЕМ НА БАЗЕ МОДИФИЦИРОВАННОГО МЕТОДА TOPSIS

Александр Николаевич Косогов
Воинская часть А1906, Киев, Украина

В статье выделены специфические особенности задач выбора рационального состава сложной системы, в частности системы информационной безопасности, позволяющие идентифицировать их как задачи многокритериального анализа и принятия решений в нечеткой среде. Предложена обобщенная концептуальная модель принятия решений в задачах выбора альтернативных вариантов состава системы, а также модификацию метода TOPSIS. Эта модификация заключается в интегрировании с алгоритмом принятия решений дополнительной компоненты, которая обеспечивает расчет на основе метода анализа иерархий коэффициентов компетенции экспертов, а также сведения иерархической структуры критериев выбора, характеризующий альтернативы, к одноступенчатой иерархии

Ключевые слова: *управление, сложная система, принятия решений, нечеткая среда, интеллектуальные технологии, многокритериальная оптимизация.*

METHOD OF SELECTING THE RATIONAL COMPOSITION OF COMPLEX SYSTEMS ON THE BASIS OF THE MODIFIED METHOD OF TOPSIS

Oleksanr M. Kosogov

Military unit A1906, Kyiv, Ukraine

The article highlights specific features of the problems of choosing the rational composition of a complex system, in particular, the information security system, which makes it possible to identify them as tasks of multi-criteria analysis and decision-making in a fuzzy environment. A generalized conceptual model of decision making is proposed in the problems of selecting alternative variants of the system composition, as well as modification of the TOPSIS method. This modification consists in integrating with the decision algorithm of an additional component that provides calculation based on the method of analyzing hierarchies of expert competence coefficients, as well as information on the hierarchical structure of selection criteria that characterizes alternatives to a single-stage hierarchy

Keywords: *management, complex system, decision-making, fuzzy environment, intelligent technologies, multi-criteria optimization*

References

1. **Romanchenko, I. S.** Використання таксономічних метоів при проведенні досліджень у воєнній справі [Text] / I. S. Romanchenko, M. Zagorka // Zb. sciences. pr. ЦНДІ ЗС України. - К., 2007. - No. 3 (41). - P. 5-16. **2. Zagorka. O.M.** Elements of the attachment of the folding systems of the Visek confession. [Text] / OM Zagorka, SP Mosov, A.I. Sbitnev, P.I. Stužuk. - К .: NAUU, 2005. - 100 with. **3. Korneenko, V.P.** Methods of optimization: textbook [Text] / VP Korneenko. - M .: Higher education. shk., 2007. - 664 p. **4. Ahmadi, H**. Rading, M. Nilashi, O. Ibrahim, A. Almaee // Health Informatics - An International Journal . - 2013. - Vol. 2. - No. 4, November. - R. 19-32. **5. Saelee**, S. Biomass type selection for boilers using the TOPSIS multi-criteria model [S.T.] / S. Saelee, B. Paweewan, R. Tongpool, T. Witoon, J. Takada, K. Manusboonpurmpool // International Journal of Environmental Science and Development. - 2014, April. - Vol. 5. - No. 2. - P. 181-186. **6. Baleželentis,** A. Multimoora-FG: a multi-objective decision making method for linguistic reasoning with an application for personnel selection [Text] / A. Baleželentis, T. Baleželentis, W. K. M. Brauers // Informatica. - 2012. - Vol. 23. - No. 2. - P. 173-190. **7. Potyomkin, M.M.** Technique of the designation of a rational warehouse for the folding systems of the Visek confession on the basis of the modified ELECTRE method [Text] / MM Potyomkin / Zb. sciences. pr. ЦНДІ ЗС України. - К., 2008. - No. 3 (45). - P. 62-68. **8. Koshetsov V.O.**, Telelim V.M., Lobanov A.A. Prior to the pittance otsinyuvannya efektivnosti functitsovanuvannya sistemi zabezpechennia voynnoi bezpeki power, / / Science and Defense. - 2010. - No. 3. - P. 8-12. **9. Kosogov O.M.** Methodical pidhid before rozrawnku pokaznikiv efektivnosti functiionuvannya sistemi informatsiynoї bezpeki Головного управління розвідки Ministry of Defense of Ukraine / O.M. Kosogov, A.O. Sirik, D.V. Kosarenko // Зб. sciences. prac. - К.: - НДІ ГУР МО України, 2015. - Vip. 41. - P. 51-60.

10. Romanchenko I.S. The TOPSIS-core method is that of yoga vicarities for bagatocritorial alternative portfolios / I.C.Romanchenko, M.M.Potomkin / / System of information boxes: zbirnik naukovyh prac. - X .: Харківський університет Повітряних Сил імені Івана Кожедуба, 2016. - Vip. 1 (138). - P. 103 - 106 **11. Hsu, H. M**. Fuzzy, H. Hsu, C. T. Chen // Information Sciences. - 1997. - Vol. 96, Issue 1-2. - P. 79-91. doi: 10.1016 / s0020-0255 (96) 00153-

УДК 355.6

Ігор Славович Левченко

Військова академія, Одеса, Україна

МЕТОД ЕКСПЕРТНОГО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТИЛОВОЇ РОЗВІДКИ

У статті йдеться про метод експертного оцінювання ефективності тилової розвідки. Запропонований метод отриманий завдяки використанню положень теорії математичної статистики та теорії тилового забезпечення і надає можливість визначити ймовірності виконання завдань групою тилової розвідки, як стосовно окремих завдань, так і щодо оцінювання ефективності тилової розвідки в цілому. Розглянуто основні завдання тилової розвідки, зокрема: вибір районів розташування частин і підрозділів тилу, місць посадкових майданчиків для вертольотів, шляхів підвезення й евакуації, джерел води та визначення потреби в силах і засобах для їх підготовки; визначення наявності місцевих ресурсів і можливостей їх використання для тилового забезпечення частин (підрозділів); визначення санітарно-епідемічного й санітарно-ветеринарного стану смуги (району) дій з'єднання (частини). Для оцінювання узгодженості отриманих експертних оцінок показано порядок розрахунку їх рангів та коефіцієнту конкордації.

Ключові слова: *ефективність, метод, тилова розвідка.*

Вступ

Постановка проблеми. З метою своєчасного забезпечення достовірною інформацією про територію, на якій знаходяться війська, навколишню інфраструктуру, для використання її в інтересах тилового забезпечення *мбр*, проводиться тилова розвідка [4].

Основними завданнями тилової розвідки є:

вибір районів розташування частин і підрозділів тилу, місць посадкових майданчиків для вертольотів, шляхів підвезення й евакуації, джерел води та визначення потреби в силах і засобах для їх підготовки;

визначення наявності місцевих ресурсів і можливостей їх використання для тилового забезпечення частин (підрозділів);

визначення санітарно-епідемічного й санітарно-ветеринарного стану смуги (району) дій з'єднання (частини).

Через важливість виконання зазначених завдань постає проблема щодо оцінювання ефективності тилової розвідки, яка практично не розв'язується із застосуванням детермінованих методів.

Аналіз останніх досліджень і публікацій. Завдання тилової розвідки є одним із таких, що вирішуються системою матеріально-технічного (тилового) забезпечення [1–3]. Водночас, публікації щодо методів експертного оцінювання ефективності тилової розвідки автору невідомі.

Метою статті є висвітлення розробленого автором методу експертного оцінювання ефективності тилової розвідки.

Виклад основного матеріалу дослідження

Тилова розвідка проводиться спеціально призначеними розвідувальними групами із складу частин і підрозділів тилу.

Тилова розвідка повинна проводитися безперервно, бути цілеспрямованою і мати конкретний характер. Безперервність розвідки полягає в тому, що вона проводиться постійно та в усіх видах бойових дій військ.

Основними об'єктами тилової розвідки є: місцевість із її рельєфом, гідрографією та рослинністю; дороги та дорожні споруди; населені пункти, їх воєнно-економічна база, санітарно-гігієнічний, ветеринарно-санітарний та епізоотичний стан; місцеві ресурси; джерела води.

Імовірність виявлення місцезнаходження об'єктів тилової розвідки групою тилової розвідки *мбр* може бути визначена методом експертного оцінювання.

Під час застосування методу експертного оцінювання [4] кожен з експертів визначав імовірність виявлення місцезнаходження об'єктів тилової розвідки $P_{TлP}$, вказуючи значення від 0 до 1 з точністю до сотих. При цьому враховувалося, що:

$$P_{TлP}=(1-P_{нв})=P_{підр}+P_{гтр}+P_{ОК}+P_{ін}\ ^{3}\ P_{TлP}^{вим} \qquad (1)$$

де $P_{підр}$ – імовірність виявлення об'єктів тилової розвідки підрозділами *мбр*, $P_{гтр}$ – імовірність виявлення об'єктів тилової розвідки групами тилової розвідки *мбр*, $P_{ОК}$ – імовірність виявлення об'єктів тилової розвідки групами тилової розвідки оперативного командування, $P_{ін}$ – імовірність виявлення об'єктів тилової розвідки сусідніми підрозділами з інших частин, $P_{нв}$ – імовірність того, що об'єкт тилової розвідки не буде виявлений, $P_{TлP}^{(вим)}$ – задана ймовірність виявлення місцезнаходження об'єктів тилової розвідки $P_{TлP.}$

Під час заповнення таблиці враховувалося, що у рядках сума значень ймовірності повинна дорівнювати одиниці. У загальному вигляді варіант прогнозу експертів показано у табл. 1.

Таблиця 1

Імовірність виявлення об'єктів силами й засобами тилової розвідки

Вид бойових дій *мбр*	Виявлення об'єктів тилової розвідки				
	$P_{ТлР}$				$P_{нв}$
	$P_{підр}$	$P_{стр}$	$P_{ОК}$	$P_{ін}$	
Оборона	P_1	P_2	P_3	P_4	P_5

Узагальнена оцінка експертів розраховувалася як середнє арифметичне визначених експертами ймовірностей (на прикладі ймовірності P_1) за формулою:

$$P_1 = \frac{P_1^{(1)} + P_1^{(2)} + ... + P_1^{(i)} + ... + P_1^{(q)}}{q}, \qquad (2)$$

де $P_1^{(1)}$, $P_1^{(2)}$,…, $P_1^{(i)}$, $P_1^{(q)}$ – оцінки, що отримані від i-их експертів; q – загальна кількість експертів, які брали участь в оцінюванні; $i = 1, 2, …, q$.

Аналогічно розраховані всі інші ймовірності з табл. 2.

Для оцінювання узгодженості отриманих експертних оцінок розраховувався *коефіцієнт конкордації* W [4].

Для цього кожній отриманій оцінці експерта ($s = \overline{1, s}$) привласнювалося натуральне число в межах $\overline{1, s}$, де s – найбільше натуральне число з можливих. При цьому 1 привласнювалося максимальній оцінці, а s – мінімальному значенню оцінки.

Визначення рангу оцінок i-го експерта показано в табл. 2. (на прикладі табл. 1).

Таблиця 2

Визначення рангу оцінок *i*-го експерта

Параметри, що оцінюються i-тим експетом	s_1	s_2	s_3	s_4
бали	P_{11}	P_{12}	P_{13}	P_{14}
числа натурального ряда	σ_1	σ_2	σ_3	σ_4
ранги	b_{is1}	b_{is2}	b_{is3}	b_{is4}

Ранг – вага оцінки s-го параметра, яка визначена i-им експертом.

Оскільки серед оцінок i-го експерта зустрічаються однакові, то цим (однаковим) оцінкам призначається однаковий ранг, який розраховується як середньоарифметичне відповідних натуральних чисел (на прикладі 3 та 4 параметрів):

$$b_{is3(4)} = (s_3 + s_4)/2 \qquad (3)$$

Кількість груп з однаковими рангами (оцінками), отриманих від i-го експерта під час розрахунків, позначили через L_i, t_l - кількість однакових рангів (оцінок) в l-ій групі відповідного i-го експерта.

Коефіцієнт конкордації за умови наявності однакових рангів розраховується за формулою:

$$W = \frac{12 \sum_{s=1}^{s} d_s^2}{q^2 (k^3 - k) - q \sum_{i=1}^{n} T_i}$$

де d_s – відхилення суми рангів a_s s-го параметра від середньоарифметичного сум рангів a_{cp} s-го параметра;

$$d_s = a_s - a_{cp}, \qquad (5)$$

$$a_s = \sum_{i=1}^{n} b_{is}, \qquad (6)$$

$$a_{cp} = \frac{a_s}{q}, \qquad (7)$$

де T_i – показник рівних (однакових) рангів

$$T_i = \sum_{l=1}^{L_i} (t_l^3 - t_l), \qquad (8)$$

де k – кількість параметрів.

Якщо W=0, то це означає повне неузгодження експертних оцінок (відсутність загальних поглядів експертів), якщо W = 1, то це повна узгодженість оцінок експертів.

Висновки й перспективи подальших досліджень

Описаний метод експертного оцінювання ефективності тилової розвідки розроблений з використанням положень теорії математичної статистики та теорії тилового забезпечення.

Перспективами подальшого дослідження є удосконалення методики оцінювання ефективності системи тилового забезпечення.

Література

1. Романченко І. С., Теоретичні основи аналізу, моделювання та синтезу системи матеріально-технічного забезпечення як просторово-розподіленої системи: монографія. Романченко І. С. та ін. – Київ: ЦНДІ ЗС України, 2013. – 221 с. **2. Голушко И. М.,** Варламов Н. В. Основы моделирования и автоматизации управления тылом / – М.: Воениздат, 1982. – 237 с. **3. Романченко І. С.,** Хазанович О. І., Трегубенко С. С. Моделювання системи матеріально-технічного забезпечення: монографія / – Львів: НАСВ ЗС України, 2015. – 156 с. **4. Абчук А. В,** Введение в теорию выработки решений: учебное пособие. Абчук А. В. и др.– М.: Воениздат, 1972. – 341 с.

МЕТОД ЭКСПЕРТНОЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ ТЫЛОВОЙ РАЗВЕДКИ

Ігорь Славович Левченко
Военная академия, Одесса, Украина

В статье рассмотрен метод экспертной оценки эффективности тыловой разведки. Предложенный метод разработан с использованием положений теории математической статистики и теории тылового обеспечения. Использование метода позволяет найти вероятности решения задач группой тыловой разведки, как в случае отдельных задач, так и для задачи оценки эффективности тыловой разведки в целом. Рассмотрено основные задания тыловой разведки, в частности: выбор районов размещения частей и подразделений тыла, мест посадочных площадок для вертолетов, путей подвоза и эвакуации, источников воды и определение необходимости в силах и средствах для их подготовки; определение местных ресурсов и возможностей их использования для тылового обеспечения частей (подразделений); определение санитарно-эпидемического и санитарно- ветеринарного состояния полосы (района) действий соединения (части). Для оценивания согласованности полученных экспертных оценок показан порядок расчета их рангов и коэффициента конкордации.

Ключевые слова: *эффективность, метод, тыловая разведка.*

METHOD OF EXPERT EVALUATE OF THE LOGISTIC INTELLIGENCE EFFECTIVENESS

Ihor Slavovych Levchenko
Military academy, Odessa, Ukraine

Method of expert evaluate of the logistic intelligence effectiveness is considered in this article. Offered method is developed by the theory of mathematical statistic and the theory of logistic regulations. The method allows to find probabilities of the task decision by the group of logistic intelligence, during conducting separate tasks and for the conducting the task of effectiveness evaluate of logistic intelligence. It is reviewed the main tasks of logistic reconnaissance especially: chosen of the region of location of the units and subunits, landing place for helicopter, transportation and evacuation routes, sources of water and determination of the needs of forces and means for their preparation; determining the availability of local resources and abilities to use them for units logistics (subunits); definition of sanitary and epidemiological and veterinary-sanitary condition of the band (district) action of formation (unit). To evaluate the consistency of received expert estimates it is showing the order of calculating of their ranks and concordance coefficient.

Key words: effectiveness, method, logistic intelligence

References

1. Romanchenko I.S. (2013), Theoretical basis of analyses, modulation and synthesis of supply system as the spatial-distributed system: monograph. Romanchenko I.S. and other–Kyiv: CCRI od AF of Ukraine, 221 p. **2. Holushko I.M.,** Varlamov N.V. (1982), Basis for modulation and automation of logistic direction/ – M.: Milproduc., 237 p. **3. Romanchenko I.S.,** Hazanovych O.I., Tregubenko S.S. (2015), Modulation of supply system: monograph / – Lviv: NALF of AF of UKraine, 156 p. **4. Abchuk A.V.** (1972), The theory of conducting the: manual. Abchuk A.V. and ather.– M.: Milproduc, 341 p.

УДК: 355.02

Андрій Дмитрович Наливайко *(канд. техн. наук, доцент.)*
Андрій Іванович Поляєв
Ігор Михайлович Сівоха

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ, Україна

ГЕНЕЗИС ТА РОЗВИТОК ОБОРОННОГО ПЛАНУВАННЯ В УКРАЇНІ

Стаття присвячена аналізу процесу генезису, становлення, сучасного стану та перспектив розвитку оборонного планування в Україні. В ній автори проаналізували в історичній послідовності формування та розвиток нормативно-правової бази оборонного планування в Збройних Силах України а також особливості організації та здійснення оборонного планування в державах-членах НАТО . Особлива увага була приділена активізації законотворчої та нормотворчої діяльності в оборонній галузі, запровадженню методики оборонного планування на основі спроможностей, використанню принципів та механізмів оборонного планування, які застосовуються в державах-членах НАТО. Запропоновано шляхи удосконалення законодавчого регулювання оборонного планування в Україні.

Ключові слова: *оборонне планування; стратегічне планування; оборонний огляд; сектор безпеки і оборони; сили оборони; спроможності.*

Вступ

Відповідно до основних положень Концепції розвитку сектору безпеки і оборони одним з основних шляхів її реалізації є, зокрема, і "удосконалення системи планування у секторі безпеки та оборони (СБО), забезпечення раціонального використання державних ресурсів".

Розвиток СБО України вимагає запровадження універсальних механізмів планування для всієї системи забезпечення національної безпеки, уніфікації та унормування процедур міжвідомчого планування, що дозволить синхронізувати та узгодити розвиток усіх складових СБО, узгодити розподіл функцій і завдань його суб'єктів , організувати ефективну взаємодію між ними та оптимізувати видатки державного бюджету.

Зазначений підхід вимагає відповідно і необхідності розвитку та удосконалення системи оборонного планування ЗС України, як складової планування у сфері національної безпеки, зокрема СБО.

Постановка проблеми. Виявлення та аналіз проблем системи оборонного планування на сучасному етапі розвитку Збройних сил України (ЗС України) є досить важливими. Актуальність їх зумовлюється тим, що ЗС України є однією із найвагоміших складових сил оборони, адже на них покладається оборона України, захист її суверенітету, територіальної цілісності й недоторканості. Тому з метою вирішення значимих проблем системи оборонного планування в ЗС України існує нагальна необхідність проведення аналізу його генезису, становлення, сучасного стану, недоліків та перспектив розвитку.

Аналіз останніх досліджень і публікацій. Аналіз сучасного стану оборонного планування в ЗС Україні виявив низку проблем у його організації та проведенні в умовах наявних та потенційних загроз. Найбільш суттєвими з них є недосконаліть процедур оборонного планування, їх слабка узгодженість з бюджетним процесом, недостатня ефективність механізмів управління оборонними ресурсам, низький рівень координації з іншими складовими сил оборони, недостатнє врахування передового досвіду зарубіжних країн.

Проблеми удосконалення ОП, а також його впровадження в складових сил оборони розглядалися в наукових публікаціях Р.І. Тимошенка, В.П. Бочарнікова, Г.М. Потапова, Н.Н. Дєнєжкіна, В.С. Корендовича, С.Ю. Полякова, Ф.В. Саганюка, М.М. Лобка, С.В. Свєшнікова, В.С. та інших [1,2]. Більшість з них зосереджувалася на розробленні підходів, методів, моделей та методик обґрунтування окремих елементів системи оборонного планування, механізму формування програм (планів) реформування та розвитку
ЗС України та оцінювання результатів їх виконання . Але при цьому недостатньо уваги приділялось питанням, пов'язаним з розвитком методу оборонного планування основаному на спроможностях та адаптацією системи оборонного планування ЗС України до аналогічних систем країн-членів НАТО.

Метою статті є дослідження генезису, становлення, сучасного стану та перспектив розвитку оборонного планування в Україні.

Виклад основного матеріалу дослідження.

Чинним законодавством України визначено, що оборонне планування (ОП) є складовою частиною стратегічного планування (СП) і здійснюється з метою забезпечення необхідного рівня обороноздатності держави у встановлені законом строки.

В 2004 році було ухвалено Закон України "Про організацію оборонного планування в

Україні" [3], в якому були визначені завдання, принципи, зміст і порядок планування в галузі оборони та координація дій органів державної влади в цій сфері. В зв'язку з цим, процес розвитку ЗС України набув певної системності, а заходи розвитку значною мірою кореспондувалися з ресурсними можливостями держави.

У 2003 – 2004 роках в Україні було започатковане проведення першого Оборонного огляду. Остаточним підсумком та висновком проведеного огляду став, затверджений 22 червня 2004 року Указом Президента України, Стратегічний оборонний бюлетень України (СОБУ) на період до 2015 року. В якості фінансової основи для розробки СОБУ були визначені, прийняті Кабінетом Міністрів України у лютому 2004 року, прогнозні показники видатків із загального фонду державного бюджету на потреби оборони. Виходячи із зазначених показників передбачалося фінансування потреб ЗС України в середньому на рівні 2 % ВВП. Бюлетень став основою для середньострокового оборонного планування та окреслив основні позиції політики України в оборонній сфері на довгострокову перспективу. Його можна вважати документом, на який опиралися при створенні програми розвитку ЗС України на 2006–2011 роки. Оборонний огляд 2004 року став першим подібним досвідом держави і показав як можна будувати оборонну стратегію за принципами прийнятими у державах лідерах оборонної сфери. Його результати та висновки привели до ряду реформ, які започаткували системну трансформацію ЗС України в 2005–2008 роках.

Тим не менш не всі результати огляду були реалізовані. Реалізації завадила низка об'єктивних обставин, зокрема для планування реформування ЗС України були спрогнозовані економічні показники держави, що були далекі від реальних, бюджетні видатки були значно нижчі від запланованих. Це призвело до того, що реальні реформи розгорнути повною мірою не вдалося, а деякі були виконані лише частково. В першу чергу не вдалося в повній мірі оснастити армію сучасною зброєю та технікою, не вистачало грошей на оснащення військових, що служили за контрактом, та на вирішення їх соціальних проблем. Крім цього, розробка реалістичної довгострокової стратегії оборонної сфери теж зіштовхнулася з проблемами фінансової нестабільності.

За 4 роки після проведення першого Оборонного огляду ситуація в країні зазнала кардинальних змін, як в політичному так і економічному плані. Через світову економічну кризу бюджет країни зазнав серйозних змін, політична система в країні змінювалась, відбулися значні зміни як у внутрішній так і у зовнішній політиці держави. Така ситуація вимагала перегляду державної військової політики для збереження актуальності механізмів воєнної безпеки. В 2008 році стало остаточно зрозуміло, що Україна не зможе в середньостроковій перспективі приєднатися до однієї з систем колективної безпеки, а тому має розраховувати виключно на власні сили та вести обережну зовнішню політику.

Другий Оборонний огляд відбувся в 2008-2010 роках в умовах глибокої кризи оборонної сфери, відомого наперед провалу чинної на той час державної програми реформування ЗС України (ДПР ЗС) та відсутності реальної перспективи на обґрунтовану і реалістичну програму реформування. У ньому МО України замахнулося на стратегію розвитку незрівнянно більш складної системи – сектору безпеки і оборони України (СБОУ). У результаті його підсумковий документ – СОБУ до 2015 року, затверджений Указам Президенту України в червні 2012 року, по багатьох аспектах не відповідав своєму призначенню .

Нині в Україні здійснюється, започаткована у 2014 році, оборонна реформа, і відповідно розпочався новий цикл ОП. Цей етап супроводжується розробкою та затвердженням нових нормативно-правових актів щодо модернізації оборонного планування.

Так, з метою вдосконалення наявної системи оборонного планування у Збройних Силах України, інших військових формуваннях складових сил оборони, правоохоронних органах спеціального призначення та в деяких інших органах, приведення періодів оборонного планування у відповідність з періодами планування економічного і соціального розвитку України, у Міністерстві оборони України розроблений Проект Закону України "Про внесення змін до Закону України "Про організацію оборонного планування", який був прийнятий Верховною Радою України 2 червня 2015 року в першому читанні.

В цьому законопроекті були уточнені завдання оборонного планування, повноваження об'єктів та суб'єктів оборонного планування; був розширений перелік і зміст документів оборонного планування, які розробляються на довго - , середньо - та короткострокову перспективу а також визначений взаємозв'язок з іншими видами планування, в тому числі з плануванням застосування та діяльності складових сектору безпеки і оборони; уточнені завдання оборонного огляду і організація його проведення.

Однак Президент України застосував право вето до цього Закону і повернув його до парламенту для повторного розгляду.

Він зазначив, що вказаний Закон не може бути підписаний оскільки: комплексний характер загроз для національної безпеки України, суттєві зміни в геополітичному безпековому просторі вимагають кардинального перегляду існуючих механізмів планування у секторі безпеки і оборони, які б передбачали поєднання політичних, цивільних та військових спроможностей для ефективного врегулювання наявних і потенційних криз та забезпечення

безпечного функціонування держави; редакція Закону України "Про внесення змін до Закону України "Про організацію оборонного планування" виглядає архаїчно, базується на чинному Законі і в частині визначення завдань, принципів та порядку здійснення оборонного планування не містить принципово нових підходів. Крім того, Президент висловив ще низку інших зауважень до Закону, які, на його думку, не дозволяють підписати прийнятий Закон.

Враховуючи зауваження та пропозиції Президента України, міжвідомчою робочою групою з удосконалення законодавства у сфері національної безпеки і оборони України при Апараті Ради національної безпеки і оборони України у 2015 році були розроблені: проект Закону України "Про планування в секторі безпеки і оборони України" (на базі проекту вищезазначеного Закону), а також нова редакція Закону України "Про основи національної безпеки". В подальшому в результаті законотворчої діяльності на початок 2017 року був розроблений проект комплексного Закону України "Про національну безпеку України", який ввібрав в себе нові трактування основних положень Законів України: «Про основи національної безпеки України», «Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави», «Про організацію оборонного планування».

В проекті нового Закону питання оборонного планування викладені у розділі V "Планування у сфері національної безпеки і оборони", метою якого визначено: розроблення стратегій, концепцій, програм, а також планів дій органів сектору безпеки і оборони та управління ресурсами, спрямованих на формування та реалізацію державної політики у сфері національної безпеки і оборони України.

В той же час керівництвом держави продовж 2015 - 2017 років прийняті нові редакції документів і документи з питань ОП в секторі безпеки і оборони України та їх складових, а саме: Стратегія національної безпеки України, Воєнна доктрина України, Стратегічний оборонний бюлетень України, Концепція розвитку сектора безпеки і оборони України, наказ МО України щодо затвердження "Положення про середньострокове та короткострокове оборонне планування в МО і ЗС України" та "Рекомендацій з оборонного планування на основі спроможностей в МО та ЗС України" [4-9].

Стратегічний оборонний бюлетень 2016 року став "останнім документом стратегічного значення" серед прийнятих раніше документів довгострокового планування і, як і очікувалося, був презентований на самміті НАТО у Варшаві.

На основі Стратегічного бюлетеня розроблені, затверджені та реалізуються Державна програма розвитку ЗС України до 2020 року та інші оборонні програми.

Бюлетень же спрямований на забезпечення практичної реалізації положень Воєнної доктрини України та Концепції розвитку сектору безпеки і оборони України, визначає стратегічні й оперативні цілі оборонної реформи та очікувані результати їх досягнення. Він зокрема визначає шляхи досягнення цілей оборонної реформи, кінцевим етапом якої є набуття повноправного членства в Організації Північноатлантичного договору.

Однією з оперативних цілей оборонної реформи в Україні визначено удосконалення системи ОП відповідно до євроатлантичних принципів та підходів. На виконання визначених цим документом завдань, МО України приступило до нового етапу удосконалення системи оборонного планування, в рамках зазначеної стратегічної цілі № 2, а саме – впровадження планування розвитку спроможностей ЗС України, у подальшому сил оборони; створення інтегрованої системи управління ризиками як складової системи оборонного планування; впровадження в бюджетну політику у сфері оборони євроатлантичних принципів та підходів щодо бюджетного планування [7].

Ключовою відмінністю цього процесу є те, що він дозволяє здійснювати постійну оцінку стану ЗС України, визначати спроможності яких бракує, обраховувати їх вартість та формувати відповідні цільові пакети розвитку спроможностей.

Головні зусилля у реалізації цього завдання зосереджено за такими напрямами:

практичні заходи, які мають закласти основу оборонного планування на основі спроможностей;

створення відповідної нормативно-правової бази (засад та керівних документів) з питань стратегічного й оборонного планування на основі спроможностей;

впровадження категорійно-понятійного апарату для забезпечення єдиного розуміння термінології і абревіатур, які застосовуватимуться в процесах оборонного, оперативного, бюджетного планування, планування підготовки військ, розвитку озброєння та військової техніки й будуть сумісними з відповідними формалізованими документами НАТО;

визначення базового переліку військових стандартів Альянсу, які містять загальні вимоги до бойових (оперативних) спроможностей військ (сил), системи управління, підготовки, критерії оцінювання, попередній огляд наявних спроможностей.

У рамках зазначеного, МО України підготовлено військово-політичні вказівки, у яких визначено:

порядок виконання основних заходів оборонної реформи у 2017 році;

перелік спроможностей ЗС України, які планується набути;

напрями спрямування міжнародного співробітництва, що здійснюється задля розвитку

спроможностей, а також завдання у рамках участі в Процесі планування та оцінки НАТО.

На найближчу перспективу передбачається [10]:

закласти основи розвитку спроможностей шляхом опрацювання законодавчих, нормативно-правових актів відповідно до стандартів і досвіду країн-членів Альянсу та забезпечити належне функціонування постійно діючих колегіальних органів (робочих груп), зокрема:

внести на розгляд Верховної Ради України проект Закону України "Про національну безпеку України";

розробити тимчасове положення про організацію оборонного планування на основі спроможностей;

здійснити попередню оцінку (аудит) наявних спроможностей ЗС України відповідно до Каталогу спроможностей НАТО;

сформувати каталоги спроможностей видів та родів військ (сил) ЗС України з описами вимог до кожної з наведених типових спроможностей;

розробити Каталог спроможностей ЗС України та сформувати Єдиний перелік спроможностей МО України та ЗС України.

У подальшому планується здійснити оцінку нового процесу, його впливу на підвищення здатності ЗС України виконувати завдання за призначенням, провести його удосконалення та поширити на інші складові сектору безпеки і оборони.

В контексті вирішення питань впровадження нового процесу планування вже протягом 2017 року передбачається:

організувати профільну підготовку персоналу (на базі Національного університету оборони України імені Івана Черняховського та відповідних курсів закордонних військових навчальних закладів);

виконати науково-дослідні роботи з за профільною тематикою наступних тематик [10]:

"Обґрунтування пропозицій щодо удосконалення оборонного планування в силах оборони, основаного на спроможностях", шифр "Планувальник";

"Раціональний розподіл фінансових оборонних ресурсів для ефективного розвитку спроможностей сил оборони", шифр "Розподіл";

"Розвиток основ стратегічного планування в секторі безпеки і оборони України", шифр "Консолідація";

залучити допомогу іноземних експертів до розробки (внесення змін до) документів з питань організації оборонного планування.

Очікуваним результатом запропонованих заходів є перехід до гнучкого, адаптивного планування, що здійснюється за визначених економічних умов з метою формування комплексних оперативних спроможностей ЗС України для гарантованого виконання ними визначених завдань.

Кінцевим результатом цієї роботи має стати підвищення здатності ЗС України в цілому, а в сфері оборонного планування - розроблення Комплексного документа розвитку спроможностей ЗС України на середньострокову перспективу, який буде основою для відпрацювання планів утримання та розвитку ЗС України, а також започаткування циклічного процесу огляду (оцінки) спроможностей та формування відповідних пропозицій керівництву МО України.

Зазначений процес є системозмінюючим. Він має безпосередній вплив на створення нової культури планування розвитку ЗС України, започатковує практику здійснення регулярного аналізу загроз та оцінки спроможностей, а також поширює стандарти Альянсу на інші сфери їх діяльності, такі як бюджетне планування, підготовка та оцінка військ.

Запровадження нової методики оборонного планування на основі спроможностей потребує глибокого переосмислення всіма його учасниками комплексності процесу в цілому та вирішення низки проблемних питань, зокрема [11]:

визначення самого поняття "спроможність" з метою його узгодження з іншими термінами, які визначають здатність до виконання завдань ("боєздатність", "бойова готовність", "бойовий потенціал" тощо);

запровадження нових, специфічних елементів циклу оборонного планування на основі спроможностей: оцінки (огляду) спроможностей і оцінки ризиків, пов'язаних з вибором того чи іншого варіанту розвитку спроможностей Збройних Сил України в залежності від фінансового ресурсу;

опрацювання методики переведення спроможностей у кількісно-якісні показники для формування відповідних організаційно-штатних структур;

уточнення (перерозподіл) функцій та завдань, а також відповідальних за їх виконання у МО України та ГШ ЗС України.

Впровадження нової методики дозволить більш якісно здійснювати середньострокове планування розвитку ЗС України, гармонізувати оборонне та бюджетне планування, відійти від ручного, ситуативного планування, та врешті - решт отримати бюджет розвитку.

Висновки й перспективи подальших досліджень

В цілому прийняті останнім часом в України законодавчі та нормативно-правові акти з питань реформування і розвитку ЗС України сприяли в певній мірі удосконаленню системи ОП.

Разом з тим до цього часу законодавчо не внормовано створення, функціонування та розвиток таких структур як сектор безпеки і оборони України, сил оборони, сил безпеки; відсутнє нормативне врегулювання процесу ОП у ЗС України та інших складових сил оборони, основаного на спроможностях; потребує уточнення категорійно-понятійний апарат, що застосовується у сфері стратегічного та оборонного планування. Разом з цим будь-які законодавчі зміни повинні бути глибоко

осмисленими та ґрунтуватися на позитивних результатах вітчизняного та зарубіжного досвіду, передових досягненнях науки з урегулювання оборонних питань, питань безпеки, питань воєнної сфери. Перспективи подальших пошуків авторів у цьому науковому напрямі будуть спрямовані на поглиблення дослідження питань у сфері оборонного планування.

Література

1. Саганюк В.Ф. Сектор безпеки і оборони: стратегічне планування / В.Ф.Саганюк, М.М.Лобко, О.В. Устименко, А.К. Павліковський // за ред. Р.І.Тимошенка. – К.: Майстер книг, 2016. – 148 с.

2. Дєнєжкін М.М., Наливайко А.Д. Аналіз систем оборонного планування Збройних Сил України та країн-членів НАТО. Збірник тез доповідей науково-практичного семінару "Впровадження процесу оборонного планування у сфері оборони відповідно до євроатлантичних принципів та підходів" 15 червня. 2017 р., НУОУ.-К.,2017.-С. 74-77.

3. Закон України "Про організацію оборонного планування в Україні" від 18 листопада 2004 р. № 2198 // Відомості Верховної Ради України. – 2005. – № 4. – Ст. 97.

4. Про рішення Ради національної безпеки і оборони України від 5 травня 2016 року "Про Стратегію національної безпеки України": Указ Президента України від 26 травня 2015 року № 287/2015 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua/laws/show/287/2015. 1. Указ Президента України від 26 травня 2015 року № 287/2015 "Про рішення Ради національної безпеки і оборони України від 5 травня 2016 року Про Стратегію національної безпеки України.

5. Указ Президента України від 24 вересня 2015 року № 555/2015 "Про рішення Ради національної безпеки і оборони України від 2 вересня 2016 року "Про нову редакцію воєнної доктрини України "

6. Указ Президента України від 14 березня 2016 року № 92/2016 "Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року "Про Концепцію розвитку сектору безпеки і оборони України".

7. Указ Президента України від 6 червня 2016 року № 240/2016 "Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про стратегічний оборонний бюлетень України".

8. Наказ Міністерства оборони України від 17.11.2016 р. № 610 " Про затвердження Положення про середньострокове та короткострокове оборонне планування в Міністерстві оборони України і Збройних Силах України".

9. Рекомендації з оборонного планування на основі спроможностей в МО та ЗС України, затверджені Міністром оборони України 13.06.2017 р. № 5789/з/3.

10. Рішення ТВО Міністра оборони України. Щодо впровадження нової системи оборонного планування на основі спроможностей від 04.01.2017 р. № 1773/у/146-2016.

11. Поляєв А.І., Наливайко А.Д. Збірник матеріалів круглого столу "Перспективи розвитку ЗС України з урахуванням завдань та тенденцій розвитку збройної боротьби" 30 травня 2017 р., ЦНДІ ЗСУ.-К., 2017.- С.93-96.,інв.№ 17718

ГЕНЕЗИС И РАЗВИТИЕ ОБОРОННОГО ПЛАНИРОВАНИЯ В УКРАИНЕ

Наливайко Андрей Дмитрович., к.т.н., доцент
Поляев Андрей Іванович
Сивоха Игоьр Михайлович

Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев, Україна

Статья посвящена анализу процесса генезиса, становления, современного состояния и перспектив развития оборонного планирования в Украине. В ней авторы в исторической последовательности проанализировали формирование и развитие нормативно-правовой базы оборонного планирования в Вооруженных Силах Украины. Особое внимание было уделено активизации законотворческой и нормотворческой деятельности в оборонной отрасли, внедрению новой методологии оборонного планирования на основе возможностей, использованию современных принципов и механизмов оборонного планирования, применяемых в государствах-членах НАТО. Предложены пути совершенствования законодательного регулирования оборонного планирования в Украине.

***Ключевые слова**: оборонное планирование, стратегическое планирование, оборонный обзор, сектор безопасности и обороны, силы обороны, способности.*

GENESIS AND DEVELOPMENT OF DEFENSE PLANNING IN UKRAINE

Andriy Dmitrovich Nalivayko Ph.D.
Andriy Ivanovich Polyayev
Igor Myhailovich Sivoha
Center for Military and Strategic Studies National Defence University of Ukraine named after Ivan Chernyhovsky, Kyiv, Ukraine

Resume. *The article is devoted to the analysis of the process of genesis, formation, the current state and*

prospects of the development of defense planning in Ukraine. In it, the authors analyzed in a historical sequence the formation and development of the normative and legal basis of defense planning in the Armed Forces of Ukraine. Particular attention was paid to the revitalization of law-making and rule-making in the defense industry, the introduction of a new capacity-based defense planning methodology, the use of modern principles and defense planning mechanisms that are applied in the member states of NATO. The ways of improving the legislative regulation of defense planning in Ukraine are proposed.

***Key words**: defense planning, strategic planning, defense review, security and defense sector, defense forces, capabilities. The article is devoted to the consideration of the initiation, formation and analysis of the current state of defense planning in Ukraine.*

References

1. Saganyuk V.F. Security and Defense Sector: Strategic Planning / VF Sahanyuk, MMLobko, O.V. Ustimenko, AK Pavlikovsky // ed. RI Tymoshenko. - K .: Master of Books, 2016. - 148 p.

2. Denejkin MM, Nalyvayko AD Analysis of defense planning systems of the Armed Forces of Ukraine and NATO member states. Collection of abstracts of reports of the scientific and practical seminar "Implementation of defense planning process in the field of defense in accordance with the Euro-Atlantic principles and approaches" June 15, 2017, NUO.-K, 2017.-p. 74-77.

3. Law of Ukraine "On the organization of defense planning in Ukraine" of November 18, 2004, No. 2198 // Bulletin of the Verkhovna Rada of Ukraine. - 2005. - No. 4. - Art. 97 ..

4. On the decision of the National Security and Defense Council of Ukraine dated May 5, 2016 "On the Strategy of National Security of Ukraine": Decree of the President of Ukraine dated May 26, 2015 No. 287/2015 [Electronic resource]. - Access mode: zakon.rada.gov.ua/laws/show/287/2015. 1. Decree of the President of Ukraine dated May 26, 2015, No. 287/2015 "On the decision of the National Security and Defense Council of Ukraine dated May 5, 2016, On the Strategy of National Security of Ukraine

5. Decree of the President of Ukraine dated September 24, 2015 № 555/2015 "On the decision of the National Security and Defense Council of Ukraine dated September 2, 2016" On the new edition of the military doctrine of Ukraine"

6. Decree of the President of Ukraine dated March 14, 2016, No. 92/2016 "On the decision of the National Security and Defense Council of Ukraine dated March 4, 2016" On the Concept of Development of the Security and Defense Sector of Ukraine ".

7. Decree of the President of Ukraine dated June 6, 2016, No. 240/2016 "On the decision of the National Security and Defense Council of Ukraine dated 20 May 2016" On the strategic defense bulletin of Ukraine "

8. Order of the Ministry of Defense of Ukraine dated November 17, 2016 No. 610 "On Approval of the Provision on Medium-Term and Short-Term Defense Planning in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine"

9. Recommendations on Defense Planning on the basis of capabilities in the Ministry of Defense and Armed Forces of Ukraine, approved by the Minister of Defense of Ukraine on June 13, 2017 No. 5789 / s / 3.

10. Decision of the TCO of the Minister of Defense of Ukraine. Concerning the introduction of a new system of defense planning on the basis of capabilities. From 01.04.2017, No. 1773 / u / 146-2016

11. Poliaev AI, Nalyvayko AD Collection of materials of the round table "Prospects for the development of the Armed Forces of Ukraine in light of tasks and trends in the development of armed struggle" May 30, 2017, Central Scientific Library of the Armed Forces. -K., 2017.- p.93-96., Inv. № 17718.

УДК 358.3:528

Михайло Віталійович Приймак
Сергій Валентинович Зотов
Віталій Володимирович Зуйко *(кандидат військових наук)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ЗАХОДІВ ТОПОГЕОДЕЗИЧНОГО ЗАБЕЗПЕЧЕННЯ ЗА ДОПОМОГОЮ РЕГРЕСІЙНОГО АНАЛІЗУ

У статті розглянутий підхід до підвищення оперативності виконання заходів з топогеодезичного забезпечення шляхом прогнозування значень робочого набору топогеодезичних даних що дає можливість скоротити час необхідний для постановки завдань на застосування сил топографічної служби. Визначення значень параметрів робочого набору даних на інтервалі прогнозу здійснюється шляхом знаходження функції тренду за часовим лагом (глибині передісторії значень) за допомогою регресійного аналізу. Таким чином за допомогою функції тренду можлива екстраполяція значень робочого набору топогеодезичних даних на потрібний момент прогнозу, що у свою чергу дозволяє підвищити оперативність визначення кількості заходів з топогеодезичного забезпечення.

Ключові слова: *топогеодезичне забезпечення, прогнозування, регресійний аналіз, оперативність, робочий набір даних.*

Вступ

Підготовка і ведення операцій угруповань військ (сил) потребує ретельного всебічного забезпечення у тому числі і топогеодезичного забезпечення (ТГЗ) як складової оперативного забезпечення. Топогеодезичне забезпечення в операції угруповання військ (сил) організовується та здійснюється з метою підготовки і своєчасного доведення до органів управління, військових частин та підрозділів топогеодезичної інформації, яка необхідна для вивчення та оцінки місцевості під час прийняття рішень та планування операції, організації управління, взаємодії, ефективного застосування наявних систем озброєння та військової техніки, створення для відповідних підрозділів сприятливих у топогеодезичному відношенні умов під час підготовки та у ході ведення операції [1]. Однією з головних умов досягнення мети топогеодезичного забезпечення військ (сил) в операції є застосування сил та засобів топографічної служби відповідного рівня підпорядкування та самих військ (сил) за визначеними завданнями ТГЗ, а саме:

забезпечення органів управління і військ топографічними картами;

забезпечення органів управління і військ цифровими (електронними) картами;

забезпечення органів управління і військ вихідними геодезичними даними;

забезпечення органів управління і військ спеціальними картами і фотодокументами про місцевість та постійне ведення топографічної розвідки [2].

Усі заходи з топогеодезичного забезпечення військ здійснюється за складних та швидкоплинних умов зміни обстановки. Основна увага приділяється виконанню завдань ТГЗ в інтересах частин, які діють на головному напрямку. Також необхідно передбачити виконання заходів з топогеодезичного забезпечення в інтересах дій військових частин Національної гвардії України, МВС, СБУ, ДПС, щодо виконання покладених на них завдань в операції та організувати взаємодію з вищезазначеними частинами і підрозділами.

Топогеодезичне забезпечення організовується начальником штабу через начальника топографічної служби відповідного рівня на основі існуючих принципів ТГЗ повсякденної діяльності військ (сил) та з урахуванням специфіки завдань, що виконуються частинами, яким необхідна топогеодезична інформація .

Досвід проведення антитерористичної операції на території Донецької та Луганської областей показав що необхідність скорочення термінів на виконання заходів з топогеодезичного забезпечення військ (сил), оновлення та підтримання в актуальному стані усіх складових топогеодезичної інформації вимагає обгрунтованих пропозицій щодо скорочення часу отримання інформації про місцевість штабами і військами всіх рівнів.

За умов великого обсягу завдань, що виконуються топографічною службою, постає питання підвищення оперативності виконання заходів з топогеодезичного забезпечення.

Постановка проблеми.

Одним з основних видів оперативного (бойового) забезпечення військ (сил) є топогеодезичне забезпечення. Частини і підрозділи топографічної служби, які організовують і здійснюють топогеодезичне забезпечення військ (сил), у відповідності до функціонального призначення [3].

Стрімкий розвиток інформаційних технологій висуває наступні сучасні вимоги до

топогеодезичного забезпечення. Їх характерними рисами сьогодні є:

широке використання супутникових навігаційних та високоточних автоматизованих геодезичних засобів для визначення місцеположення елементів бойових порядків військ (сил), розвитку геодезичних мереж спеціального призначення;

повний перехід до цифрових технологій створення картографічної інформації;

постійне використання геоінформаційних технологій для вирішення завдань аналізу місцевості та прийняття рішень;

впровадження у війська нових видів документів про місцевість, таких, як цифрові ортофотокарти, ортофотознімки, просторові моделі місцевості, карти умов спостереження тощо;

забезпечення швидкого поширення геопросторової інформації до зацікавлених санкціонованих користувачів засобами автоматизованих систем управління;

оперативне виготовлення в польових умовах необхідних видів документів про місцевість.

У зв'язку з цим, актуальною є наукова проблема прогнозування обстановки як фактору підвищення оперативності топогеодезичного забезпечення.

Аналіз останніх досліджень і публікацій.

Питанням добору та дослідженням методів прогнозування за допомогою регресійних моделей будь-якої складності, а також практичним аспектам їх застосування присвячені роботи [4,5]. За допомогою розроблених статистичних методів аналізу стало можливим встановлення кількісних взаємозв'язків між окремими параметрами. Крім того, регресійний аналіз дозволяє здійснювати згортку інформації за багатьма параметрами у вигляді єдиного поліноміального рівняння [5].

Вищезазначені праці висвітлили фундаментальні підходи до питань прогнозування, але в частині застосування методів регресійного аналізу під час виконання заходів топогеодезичного забезпечення дій військ (сил) розглянуті не були.

Мета статті полягає у підвищенні оперативності виконання заходів з топогеодезичного забезпечення шляхом прогнозування значень робочого набору топогеодезичних даних необхідних для підготовки і своєчасного доведення до органів управління, військових частин та підрозділів топогеодезичної інформації.

Виклад основного матеріалу дослідження

Робочій набір даних обстановки IS для розробки замислу і планування операції відповідає фактичній ситуації лише на момент збору інформації ($t = 0$). Але за час організаційного етапу управління на момент ($t = TO$) початку дій військ (сил) по виконанню планових бойових завдань їх актуальність значно знижується, бо фактична ситуація на цей момент вже істотно відрізняється від ситуації на момент збору даних обстановки. Це об'єктивно веде до втрати реальної бойової ефективності бойових систем через нерелевантність планових завдань військам (силам) на момент початку їх дій [6].

Тому виникає нова задача забезпечення управління – прогнозування значень робочого набору даних обстановки IS ($t = 0$) на момент ($t = TO$) і використання даного робочого набору IS ($t = TO$) в якості вихідних даних для подальшої розробки замислу і планування операції. Дана процедура повинна входити у функцію усіх систем збору інформації даних обстановки для систем управління бойових систем (у тому числі і системи топогеодезичного забезпечення).

Нехай робочій набір даних обстановки IS на момент його формування ($t = 0$) складає сукупність значень n параметрів – вектор

$$X(t=0) = \left\langle x_j(0),\ j = \overline{1,n} \right\rangle. \qquad (1)$$

Прогнозування значень параметрів на інтервалі прогнозу (момент TP) потребує визначення функції тренду $Y\{X(t)\}$ по часовому лагу (глибині передісторії значень), тобто для ($t > 0$) методами регресійного аналізу. Тоді за допомогою функції тренду можлива екстраполяція значень робочого набору $X(0)$ на потрібний момент прогнозу TP, тобто визначення з припустимою точністю прогнозу (похибкою ΔX) саме $X(TP)$. Але задача прогнозування завжди є компромісною, оскільки точність прогнозу знижується при зростанні інтервалу прогнозу. Розглянемо рисунок 1.

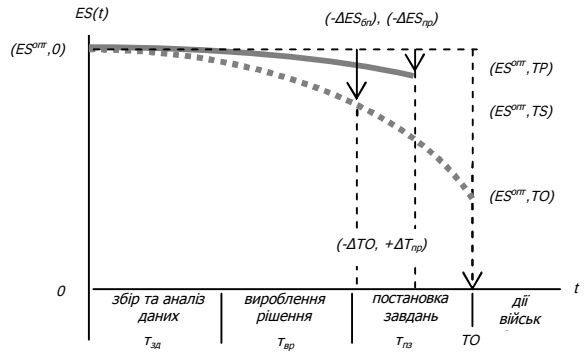


Рисунок 1 Залежність ефективності бойової системи від прогнозування обстановки

Пунктирною лінією показаний графік залежності ефективності БС від тривалості етапу оптимального організаційного управління, яка знижується до рівня ($ES^{\text{їїо}}, TO$). Заходи щодо підвищення оперативності (наукова організація) процесу етапу організаційного управління скорочують його тривалість на ($-\Delta TO$), що дає підвищення ефективності до рівня ($ES^{\text{їїо}}, TS$).

Неперервною лінією показаний графік залежності ефективності БС від тривалості оптимального процесу етапу ОУ при наявності прогнозування, яке збільшує тривалість процесу TS на додатковий час прогнозування $+\Delta T^{\text{їд}}$, але підвищує ефективність до рівня ($ES^{\text{їїо}}, TP$). Якщо при цьому зниження ефективності через зниження

актуальності даних обстановки при прогнозуванні ($-\Delta ES^{ïð}$) менше, а ніж без прогнозування ($-\Delta ES^{âï}$), то прогнозування завжди доцільне.

Визначення функції тренду $Y\{X(t)\}$ потребує попереднього (до моменту $t=0$) спостереження часового ряду m значень її аргументу –

$$X(-t_m),...,X(-t_1) \qquad (2)$$

та обчислення методами регресійного аналізу констант аналітичного виду функції. Після цього дана функція Y придатна для екстраполяції (на інтервал прогнозу) значень $X(TP)$.

Процедура прогнозування методом часового лагу складається з наступних етапів:

спостереження часового ряду значень аргументу $X(t)$ (на протязі лагу моментів часу $[-tm,-tl)]$);

обчислення параметрів аналітичної форми і оцінка імовірності функції регресії, як функції тренду для робочого набору даних обстановки $X(t)$;

прогнозування (екстраполяція), за допомогою функції тренду $Y\{X(t)\}$, значень параметрів обстановки в момент $X(t=0)$ на момент $X(t=TP)$ початку етапу оперативного управління діями сил в операції.

Таким чином, формування робочого набору даних обстановки з прогнозуванням потребує певної зміни, в порівнянні з існуючою, процедури формування, а саме – збір даних на протязі потрібного (для точності визначення функцій тренду) часового лагу (до початку операції або вже у процесі збору даних етапу організаційного управління, визначення функцій тренду даних робочого набору та прогнозування. Це приводе, з одного боку, до зростання тривалості етапу організаційного управління саме на ($+\Delta T^{ïð}$), а з другого боку – до зменшення втрати планової ефективності бойової системи.

Слід відмітити, що скорочення інтервалу прогнозу вдосконаленням процесу функціонування системи управління на етапі оперативного управління суттєво підвищує точність і імовірність прогнозування, що є додатковим фактором підвищення бойової ефективності бойової системи.

Для об'єктів, системні показники яких не мають сталого тренду (так звані динамічні системи), прогнозування можливе методом системної динаміки (по Дж. Форрестеру). Прогнозною інформацією є, як правило, чисельний стан різнорідних ресурсів об'єкту на протязі інтервалу прогнозу.

Математична модель об'єкта динамічна система надається повно зв'язним орієнтованим графом, вершинами якого є чисельні стани різнорідного ресурсу підсистем над-системи, а інцидентними до верши дугами – напрямки переходів різнорідних ресурсів між чисельними станами з відповідними темпами. Тоді граф-модель системи описується двома компонентами:

матриця чисельності станів підсистем за видами ресурсу

$$N_{m'z}(t)=\|n_{ik}(t)\|_{m'z}, \qquad (3)$$

де m – кількість чисельних станів (підсистем) системи, z – кількість видів різнорідних ресурсів системи;

матроїд (багатомірна матриця) темпів переходу різнорідного ресурсу між суміжними чисельними станами системи –

$$\Lambda_{m'm'z}(t)=\|\lambda_{ijk}(t)\|_{m'm'z}. \qquad (4)$$

Процес зміни чисельності станів підсистем у модельному часі (динаміка над-системи) описується матрицею диференційних рівнянь –

$$\dot{N}_{m'z}=\left\|\frac{dn_{ik}}{dt}=-\sum_{j=1\,j\neq i}^{m}\lambda_{ijk}(t)+\sum_{j=1\,j\neq i}^{m}\lambda_{jik}(t)\right\|_{m'z} \qquad (5)$$

Рішення системи диференційних рівнянь матриці при початкових умовах (для моменту модельного часу $t=0$) –

$$\begin{aligned} N_{m'z}(t=0)&=\|n_{ik}(t=0)\|_{m'z},\\ \Lambda_{m'm'z}(t=0)&=\|\lambda_{ijk}(t=0)\|_{m'm'z} \end{aligned} \qquad (6)$$

дає значення поточної чисельності станів на бажаний момент прогнозу ($t=T$) –

$$N_{m'z}(t=T)=\|n_{ik}(t=T)\|_{m'z} \qquad (7)$$

Якщо темпи $\Lambda_{m'm'z}=\|\lambda_{ijk}\|_{m'm'z}$ незмінні у часі, то в процесі переходів ресурсів між підсистемами через певний час ($t=T^{ñòàò}$) в системі встановлюється стаціонарний режим, коли чисельності станів досягають своїх асимптотичних значень, яки практично не змінюється, і саме вони є прогнозними значеннями на будь-який інтервал прогнозу $T>T^{ñòàò}$.

Якщо темпи $\Lambda_{m'm'z}(t)=\|\lambda_{ijk}(t)\|_{m'm'z}$ змінюються у часі (за дією випадкових або невизначених факторів, чи вони є керованими), то процес переходів не буде стаціонарним, що потребує імітаційного моделювання процесу до потрібного моменту прогнозу ($t=T$).

Комп'ютерна дослідницька імітаційна модель системної динаміки розроблена воєнними науковцями. Штабна модель для прогнозування повинна мати масиви достатньої розмірності (матрицю чисельності станів за видами ресурсу та матриоїд темпів потоків ресурсів за видами), які заповнюються конкретним робочим набором вихідних даних для моделювання, а також типову процедуру рішення системи диференційних рівнянь чисельними методами (наприклад, методом дотичних Ейлера).

Метод дотичних полягає у переході від похідних до співвідношення диференціалів (кінцевих різниць) у рівняннях (5)

$$\dot{N}_{m'z}\approx\left\|\frac{\Delta n_{ik}(t)}{\Delta t}\approx-\sum_{j=1\,j\neq i}^{m}\lambda_{ijk}(t)+\sum_{j=1\,j\neq i}^{m}\lambda_{jik}(t)=f_{ik}(t)\right\|_{m'z} \qquad (8)$$

Тепер можливо представити кінцеві різниці сусідніми у модельному часі значеннями, а саме –

$$\dot{N}_{m' z} \approx \left\| \frac{n_{ik}(t+\Delta t) - n_{ik}(t)}{\Delta t} \approx f_{ik}(t) \right\|_{m' z} \quad (9)$$

Звідси одержимо рекурентне рівняння для даної чисельності стану на кожний подальший момент часу $(t+\Delta t)$ в залежності від чисельності стану у поточний момент часу t –

$$N_{m' z}(t) = \left\| n_{ik}(t+\Delta t) \approx n_{ik}(t) + (f_{ik}' \Delta t) \right\|_{m' z} \quad (10)$$

Алгоритм моделювання системної динаміки наступний.

Початкові присвоювання:

ввід розмірності масивів *m,z*;

заповнення матроїда темпів Λ константами початкових значень;

заповнення матриці чисельних станів N початковими значеннями;

введення значення дискретності модельного часу Δt (одиниці часу);

введення значення модельного часу T (одиниці часу);

введення поточного значення циклу моделювання *k:=0*;

обчислення поточного значення (9) функції *f(k)*.

k-й цикл моделювання

1. Присвоювання номеру циклу (*k:=k*+1).

2. Присвоювання –

$$\left\| n_{ik}(k) \approx n_{ik}(k-1) + f_{ik}(k-1)' \Delta t) \right\|_{m' z} \quad (11)$$

3. Перевірка умови чи $(k \times \Delta t) \geq T$? Якщо так, то перехід на етап кінець процесу.

4. Перерахунок значень елементів матроїду (тільки для нестаціонарного процесу) на момент $(t=k \times \Delta t)$ –

$$\Lambda_{m' m' z}(k) = \left\| l_{ijk}(t) = l_{ijk}(k' \Delta t) \right\|_{m' m' z} \quad (12)$$

5. Обчислення поточного значення (8) функції *f(k)*.

6. Перехід до пункту 1 наступного циклу.

кінець процессу

Результати моделювання:

значення елементів масиву *N(k)* для останнього циклу моделювання (тобто на момент прогнозу *T*);

кількість циклів моделювання *k*.

Висновки й перспективи подальших досліджень

Таким чином, у статті запропоновано підхід підвищення оперативності виконання заходів з топогеодезичного забезпечення шляхом прогнозування значень робочого набору топогеодезичних даних необхідних для підготовки і своєчасного доведення до органів управління, військових частин та підрозділів топогеодезичної інформації за рахунок використання регресійного аналізу.

Література

1. Чорнокнижний О. А. Теоретичні основи застосування за призначенням частин та підрозділів топографічної служби. Вісник Київського національного університету імені Тараса Шевченка. Київ: №2 (35), 2016. С. 43–45. **2. Зотов С. В., Савчук Р. Г., Чорнокнижний О. А.** Аналіз забезпечення збройних сил провідних країн світу спеціальними картами та фотодокументами про місцевість у локальних війнах і збройних конфліктах останніх років. Науково-технічний журнал ЦНДІ ОВТ ЗСУ, №2 (6). Київ: ЦНДІ ОВТ ЗСУ, 2015. С. 43–47. **3. Положення** про частини топографічної служби Збройних Сил України. Київ: ВТУ ГШ ЗС України. 2000. **4. Астахов А. Д.** Пути создания модели оценки эффективности системы топогеодезического обеспечения войск. Москва: РИО ВТС. 1984. 185 с. **5. Норман Дрейпер, Гарри Смит** Прикладной регрессионный анализ. Москва: Диалектика. 2016. 912 с. **6. Смаль С. В., Чорнокнижний О. А.** Питання визначення раціонального способу виконання завдань навігаційного забезпечення. Труди академії. Національна академія оборони України. Київ: НАОУ. 2005. С. 136-139

ПОВЫШЕНИЕ ОПЕРАТИВНОСТИ МЕРОПРИЯТИЙ ТОПОГЕОДЕЗИЧЕСКОГО ОБЕСПЕЧЕНИЯ С ПОМОЩЬЮ РЕГРЕСИВНОГО АНАЛИЗА

Сергей Валентинович Зотов
Михаил Виталиевич Приймак
Виталий Владимирович Зуйко *(кандидат военных наук)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье рассмотренный поход повышения оперативности выполнения задач по топогеодезическому обеспечению путем прогнозирования значений рабочего набора топогеодезических данных, что дает возможность сократить время необходимое для постановки задач на применение сил топографической службы. Определение значений параметров рабочего набора данных на интервале прогноза осуществляется путем нахождения функции тренда по временному лагу (глубине предыстории значений) с помощью регрессионного анализа. Таким образом с помощью функции тренда возможна экстраполяция значений рабочего набора топогеодезических данных на необходимый момент прогноза, что в свою очередь позволяет повысить оперативность определения количества задач по топогеодезическому обеспечению.

Ключевые слова: *топогеодезическое обеспечение, прогнозирование, регрессионный анализ, оперативность, рабочий набор данных.*

Mikhailo V. Prvimak
Serhiy V. Zotov
Vitaliy V. Zuiko (Candidate of Military Sciences)

National Defence University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine

ENHANCING OPERATIONAL EFFICIENCY OF TOPOGEODEZIC SUPPORT WITH THE HELP OF REGRESSIONAL ANALYSIS

The article considers the approach to increase the efficiency of the task implementation of topogeodetic provision by forecasting the values of the working set of topogeodetic data, which makes it possible to reduce the time required to set tasks for the use of the forces of topographic service. Determining the values of the parameters of the working data set at the forecast interval is carried out by finding the trend function for the time lag (deep prehistory values) using regression analysis. Thus, using the trend function, the extrapolation of the values of the working set of topogeodetic data at the desired moment of forecast is possible, which in turn allows us to increase the efficiency of determining the number of actions for the topogeodetic maintenance.

***Key words**: topogeodesic support, forecasting, regression analysis, efficiency, working data set.*

References

1. Chernoknizhny A. A. Theoretical bases of use of the units and topographic service / Chernoknizhny A. A. // Bulletin of Kyiv national University named after Taras Shevchenko. K.: №2 (35), 2016. – P. 43 – 45 **2.** The position of the topographic service of the Armed Forces of Ukraine. Kiev. : WTU General staff of the armed forces of Ukraine, 2000. **3. Smal S. V.** the problem of determining the rational way of performing tasks, navigation / Sec.In. Smal, A. A. Chernoknizhny // Proceedings of the Academy / NAO Ukraine. - K., 2005. - S. 136-139 **4. Fedchenko A. P.** Application of a systematic approach in the study of improving the efficiency of the survey support the operational grouping of troops (forces) in operation and O. P. Fedchenko, G. Pisarenko, V. // Collection of scientific works. - K.: the MIKNU, 2011. - No 30 —S. 275-278.

УДК 355.02:327.56

Леонід Станіславович Голопатюк

Національний університет оборони України імені Івана Черняховського, Київ, Україна

УДОСКОНАЛЕНА МЕТОДИКА ОЦІНЮВАННЯ ІНТЕНСИВНОСТІ СУЧАСНИХ ВОЄННИХ КОНФЛІКТІВ

При визначенні заходів запобігання воєнним конфліктам є необхідність в проведенні оцінювання інтенсивності останніх на різних етапах розвитку. Оцінювання інтенсивності традиційних (конвенційних) воєнних конфліктів зазвичай здійснюється за обмеженою кількістю чітко визначених параметрів. Для оцінювання інтенсивності сучасних (не конвенційних) воєнних конфліктів необхідно врахування вже значної кількості параметрів, які мають нечіткий характер.

При удосконаленні методики оцінювання інтенсивності СВК запропоновано використовувати метод теорії нечітких множин. Сутність методу полягає в представленні СВК у вигляді розподілу функції приналежності, яка його повністю описує за вибраними параметрами. Застосування відомого алгоритму нечіткої контекстної кластеризації дозволяє виділити кластери (групи) схожих за рівнем інтенсивності СВК, виявити в кожній групі прототип, який описує всю групу. При появі нового конфлікту достатньо оцінити його приналежність до прототипів кластерів та визначити рівень інтенсивності для вибору заходів з запобігання.

Відмінність запропонованих методичних положень полягає у використанні математичних методів які враховують невизначеність інформації про СВК.

Ключові слова: *сучасний воєнний конфлікт, інтенсивність сучасного воєнного конфлікту, кластерний аналіз,заходи запобігання.*

Вступ

Початок третього тисячоліття характеризується глибокими змінами у визначальних сферах життєдіяльності суспільства. Закінчення холодної війни не наблизило світ до стабільності, він не став безпечнішим, а воєнна сила як і раніше розглядається як найефективніший фактор світової політики. Для України проблема забезпечення її воєнної безпеки лишається актуальною. Воєнні конфлікти нового типу, що виникли в різних районах земної кулі, особливо на теренах України, суттєво впливають на забезпечення її воєнної безпеки. Ситуація ускладнюється економічним становищем в країні, забезпеченням Збройних Сил, що потребує нових підходів до теоретичного обґрунтування і практичного вжиття заходів щодо належного реагування на виклики її воєнній безпеці.

Постановка проблеми.

Обґрунтування шляхів зміцнення колективної безпеки для запобігання сучасного воєнного конфлікту (СВК) безпосередньо пов'язано з оцінюванням його інтенсивності. Аналіз існуючих методичних підходів, методів і методик до оцінювання інтенсивності воєнних конфліктів показує, що вони мають ряд обмежень при оцінюванні інтенсивності СВК. Ці методики можуть бути використані для вирішення часткових задач оцінювання СВК тільки в одній із сфер протиборства і при обмеженій кількості параметрів, які мають чітко визначені значення. Тобто необхідно вдосконалення методики оцінювання інтенсивності СВК за всіма сферами і яка враховує їх відмінності від традиційних конвенційних конфліктів.

При проведенні оцінки інтенсивності СВК інститути колективної безпеки і національного сектору безпеки і оборони в основному мають справу з неповною та неточною інформацією. Прийняття рішення на запобігання сучасному воєнному конфлікту, розробка пропозицій до мандату і планування операції з підтримання миру і безпеки здійснюється в умовах невизначеності інформації про інтенсивність СВК. Тому методика оцінювання інтенсивності СВК повинна засновуватися на використанні методів, які дозволяють урахувати (понизити) невизначеність інформації щодо показників конфлікту.

Аналіз останніх досліджень і публікацій. Методичні положення з оцінки інтенсивності воєнних конфліктів, що містяться в останніх публікаціях достатньо повно розкривають порядок і послідовність оцінки інтенсивності воєнних конфліктів на різних етапах їх розвитку. Разом з цим в них не в повній мірі розкриті питання щодо урахування особливостей сучасних воєнних конфліктів, в першу чергу одночасне застосування протиборства в різних сфер протиборства, значне зростання кількості параметрів, які суттєво впливають на об'єктивність оцінки та нечіткий характер цих параметрів.

Мета статті. Удосконалити методичні положення оцінювання інтенсивності сучасних воєнних конфліктів на основі використання методу теорії нечітких множин.

Виклад основного матеріалу досліджень.

Початок XXI століття відзначився принципово новим, відмінним від конвенційного, типом воєнних конфліктів.

Воєнна доктрина України визначає дві наступні особливості СВК: асиметричне застосування воєнної сили не передбаченими законом збройними формуваннями; комплексне використання воєнних і невоєнних інструментів: економічних, політичних, інформаційно-психологічних.

Таким чином, традиційне розуміння воєнного конфлікту змінилося та вимагає корекції.

Визначимо сучасний воєнний конфлікт як дії, що здійснюються шляхом поєднання політичних, військових, економічних, інформаційних і міжнародно-правових сценаріїв ведення конфлікту з метою досягнення воєнно-стратегічних цілей.

До основних сфер протиборства у СВК віднесемо: зовнішньо і внутріполітична боротьба (політична сфера); традиційні і асиметричні воєнні дії (безпекова сфера); фінансово-економічна боротьба (економічна сфера); інформаційне протиборство (інформаційна сфера); міжнародно-правова сфера. В сукупності ці сфери визначають інтенсивність СВК.

За даними міжнародних інститутів з проблем безпеки новітні підходи щодо запобігання сучасним воєнним конфліктам, як важливої складової забезпечення воєнної безпеки будь якої держави, засновуються на практичному підтвердженні зниження ролі військових засобів, способів та методів у вирішенні кризових ситуацій, особливо в умовах, коли держава зазнає серйозних економічних, науково-технічних та демографічних проблем.

Тому, на теперішній час, на перше місце виходить не пошук універсальних способів забезпечення воєнної безпеки України, а проблема комплексного та узгодженого використання усіх наявних в державі та міжнародних безпекових організаціях механізмів, сил, засобів та способів для запобігання воєнного конфлікту, що триває.

Застосування запропонованої в [1] аналітико-логічної моделі дозволяє визначати вимоги до аналізу сучасних воєнних конфліктів, а алгоритм кластеризації – отримати групи (кластери) схожих конфліктів.

Однак для повної характеристики сучасних воєнних конфліктів необхідно визначення їх інтенсивності для подальшого вироблення заходів щодо їх запобігання з боку колективної безпеки.

Для цього пропонується удосконалена методика оцінювання інтенсивності сучасних воєнних конфліктів (рис. 1).

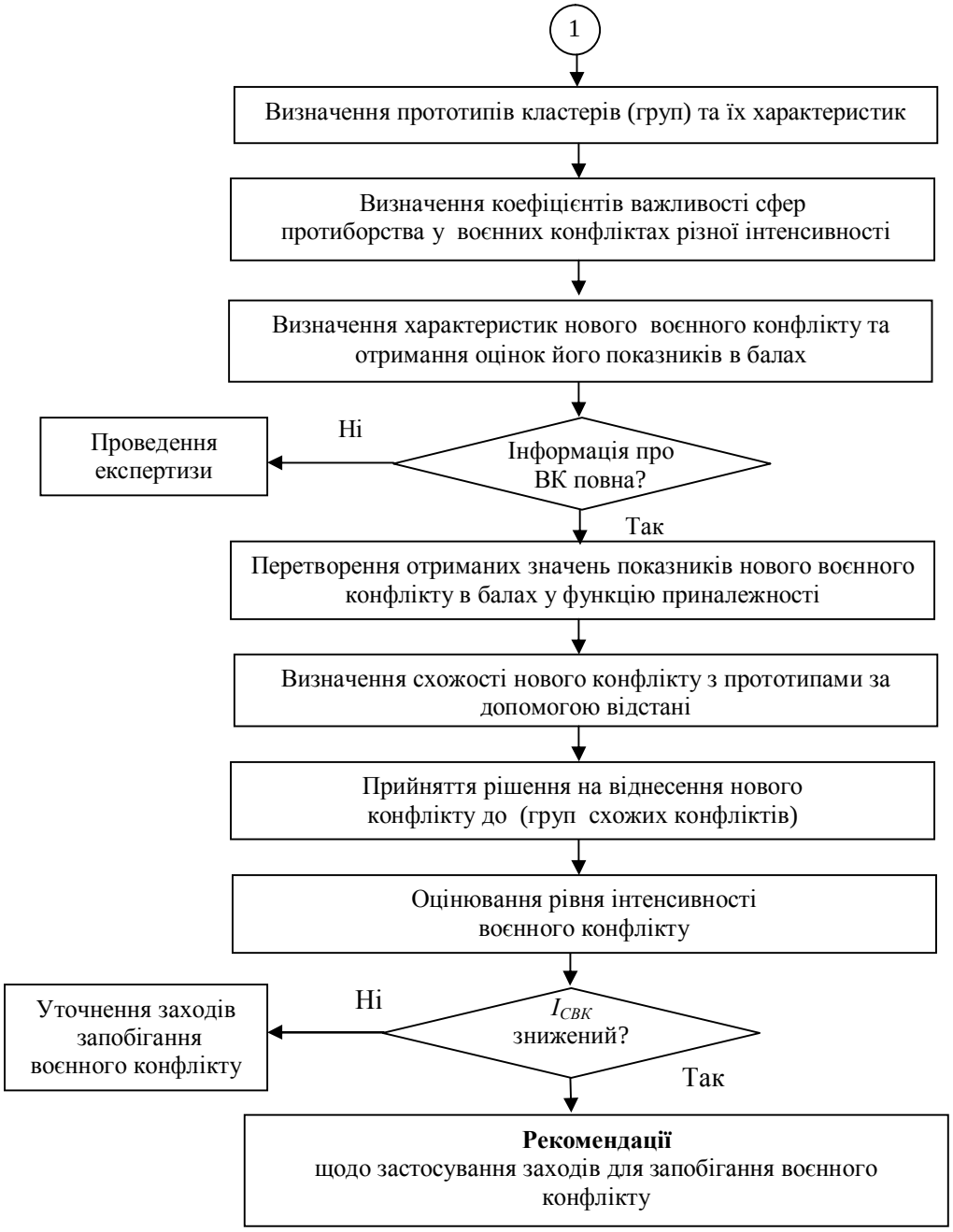


Рис. 1. Удосконалена методика оцінювання інтенсивності сучасного воєнного конфлікту

Удосконалена методика має 2 етапи.

За узагальнений показник в методиці прийнято показник, що характеризує рівень інтенсивності сучасного воєнного конфлікту ($I_{СВК}$).

Частковими є показники які характеризують СВК у п'яти сферах. У військовій: тривалість воєнного конфлікту; характер зіткнень між протиборчими силами; просторові межі воєнного конфлікту; кількість жертв серед мирного населення; кількість жертв серед військовослужбовців; озброєння яке використовується у воєнному конфлікті; військово-технічна допомога сторонам конфлікту. У політичній: характер воєнно-політичних відносин між сторонами конфлікту; міжнародно-політична підтримка сторін конфлікту. У економічній: економічні взаємовідносини між сторонами конфлікту; економічна допомога сторонам конфлікту. У інформаційній: інтенсивність дій в інформаційному просторі; міжнародна інформаційна підтримка сторін. У міжнародно-правовій: виконання норм міжнародного права сторонами конфлікту; ступінь участі міжнародних безпекових організацій у конфлікті.

Оцінювання кожного показника здійснюється за 5-ти бальною шкалою [1].

На першому етапі за даними міжнародних інститутів, університетів, центрів щодо конфліктів здійснюється оцінювання за частковими показниками сучасних воєнних конфліктів на предмет виявлення груп схожих та виявлення в кожній групі еталонного конфлікту який описує всю групу. Результатом є база даних прототипів кластерів. Для отримання схожості СВК використано аналітико-логічну модель, як поєднання часткових показників з позиції вибраного контексту порівняння. Результатом є множина нечітких функцій приналежності, які описують конфлікти. Отримання кластерів схожих СВК базується на використанні відомого алгоритму нечіткої контекстної кластеризації [2], результатом, якого є дендрограма розбиття СВК на кластери, вибір оптимального розбиття і визначення прототипу кластеру.

Найбільш важливою характеристикою самого кластеру є його прототип. Прототипом кластеру є найбільш типовий його об'єкт, який найближчий до центру кластеру, або віртуальний об'єкт який є центром ваги кластера. В нашому випадку будемо використовувати у якості прототипу центр ваги кластеру.

Тобто ми маємо множину прототипів для кожного кластеру СВК, яка є базою даних. Для кожного кластеру можна прив'язати множину заходів зі сторони колективної безпеки чи можливостей країни щодо його вирішення.

Далі визначаються коефіцієнти важливості сфер протиборства у воєнних конфліктах різної інтенсивності.

Цей етап Методики дозволяє уточнити поняття інтенсивності конфлікту за рахунок врахування інших сфер протиборства, описати його як протопит кластеру та визначити коефіцієнти важливості сфер протиборства у конфліктах різної інтенсивності.

Для сучасного воєнного конфлікту розподіл сфер за важністю в залежності від інтенсивності представлено в таблиці 1.

Таблиця 1

Сфери	Рівень інтенсивності		
	Низький	Середній	Високий
Військова	0,1	0,19	0,21
Політична	0,3	0,29	0,2
Економічна	0,15	0,14	0,2
Інформаційна	0,38	0,28	0,21
Міжнародно-правова	0,07	0,1	0,18

Другий етап починається з блоку "Визначення характеристик нового воєнного конфлікту та отримання оцінок його показників в балах"

На другому етапі за результатом моніторингу ситуації в зоні зародження конфлікту здійснюється порівняння нового конфлікту з базою даних отриманою на попередньому етапі. Результатом є віднесення нового конфлікту до конкретної групи конфліктів, визначення його інтенсивності, заходів запобігання і їх пріоритетності.

Для отримання рівня інтенсивності воєнного конфлікту (будемо виходити з того, що чим більш негативні характеристики прототипу кластеру тим вища інтенсивність воєнного конфлікту) будемо використовувати формулу, яка враховує значення показників СВК, отриманих раніше:

$$I_{СВК} = \frac{\sum_{i=1}^{C} k_i r_b^i}{C}$$

де r_b^i – відстань між новим воєнним конфліктом та протопипом;

k_i – коефіцієнт рівня негативності кластеру;

C – кількість отриманих кластерів.

Отримувані чисельні оцінки інтенсивності СВК змінюються в інтервалі [0,1], де оцінка тим негативніша, чим ближче її значення до 1. Для аналізу і оцінки рівнів інтенсивності використовується уніфікована кількісно-якісна шкала. Вона розроблена на основі додаткових досліджень у галузі аналізу ризиків, у тому числі рекомендацій міжнародних організацій відносно визначення світових політичних ризиків, з врахуванням особливостей теоретичного апарату, що використано при моделюванні. Шкала припускає використання якісних неоднозначних характеристик. У шкалі частковий перетин кількісних областей означає плавний перехід від одної якісної характеристики до іншої (див. рис. 2).

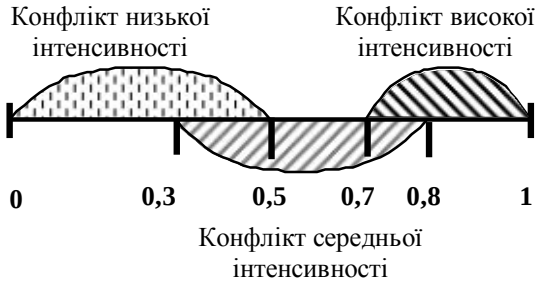


Рис. 2. Шкала оцінювання рівня інтенсивності СВК

Для оцінювання результативності заходів запобігання сучасному воєнному конфлікту будемо виходити з наступного: при виникненні конфлікту колективна безпека через свої інститути здійснює ряд заходів для його запобігання. Маркером того, що ці заходи результативні у загальному випадку є зниження

рівня інтенсивності воєнного конфлікту. Тобто маємо:

$$E = g(1 - I_{СВК})$$

де E – результативність заходів запобігання СВК;

g – коефіцієнт реалізації заходів запобігання конфлікту (вимірюється в інтервалі від 1 – всі заходи реалізовані; 0 – не реалізовані, що також враховує їх затрати);

$I_{СВК}$ – інтенсивність конфлікту.

Цей етап методики дозволяє визначити інтенсивність нового конфлікту та оцінити заходи з його запобігання. Результативністю заходів є зниження інтенсивності.

Висновки й перспективи подальших досліджень.

Приведена у статті удосконалена методика оцінювання інтенсивності СВК ґрунтується на використанні теорії нечітких множин та відомого алгоритму нечіткої контекстної кластеризації.

Сутність методики полягає у визначенні рівня інтенсивності конфлікту з урахуванням параметрів різних сфер протиборства. Параметри конфлікту при цьому мають нечіткий характер.

Удосконалена методика має 2 етапи.

На першому етапі здійснюється оцінювання за частковими показниками сучасних воєнних конфліктів на предмет виявлення груп схожих. Результатом є база даних прототипів кластерів.

На другому етапі здійснюється порівняння нового конфлікту з базою даних. Результатом є віднесення нового конфлікту до конкретної групи конфліктів та визначення його інтенсивності.

Відмінність запропонованої методики полягає у використанні математичних методів які враховують невизначеність інформації про конфлікти.

В подальших дослідженнях планується розширити запропоновану методику на вирішення проблеми прогнозування розвитку СВК.

Література

(ДСТУ ГОСТ 7.1:2006)

1. Голопатюк Л.С. Визначення типових сучасних воєнних конфліктів на основі алгоритму нечіткої кластеризації // Зб. наук. пр. ЦНДІ ЗС України. – К., 2017. – № 1(79) С. 120-126.

2. Бочарніков В. П., Возняк С. М., Алгоритм кластеризації воєнно-політичних сил в умовах невизначеності: Науково-технічний збірник. – Вип. 3. – К.: ННДЦ ОТ і ВБ України, 1999. – С. 35- 42.

УСОВЕРШЕНСТВОВАННАЯ МЕТОДИКА ОЦЕНКИ ИНТЕНСИВНОСТИ СОВРЕМЕННЫХ ВОЕННЫХ КОНФЛИКТОВ

Леонид Станиславович Голопатюк

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

При определении мер предупреждения военных конфликтов возникает необходимость в проведении оценки интенсивности последних на разных этапах развития. Оценка интенсивности традиционных (конвенционных) военных конфликтов обычно осуществляется с ограниченным количеством четко определенных параметров. Для оценки интенсивности современных (не конвенционных) военных конфликтов (СВК) необходимо учитывать значительное количество параметров, которые имеют нечеткий характер.

При совершенствовании методики оценки интенсивности СВК предложено использовать метод теории нечетких множеств. Сущность метода заключается в представлении СВК в виде распределения функции принадлежности, которая его полностью описывает по выбранным параметрам. Применение известного алгоритма нечеткой контекстной кластеризации позволяет выделить кластеры (группы) похожих по уровню интенсивности СВК, выявить в каждой группе прототип, который описывает всю группу. При появлении нового конфликта достаточно оценить его принадлежность к прототипам кластеров и определить уровень интенсивности для принятия мер по предупреждению.

Отличие предложенных методических положений заключается в использовании математических методов, учитывающих неопределенность информации о СВК.

Ключевые слова: *современный военный конфликт, интенсивность современного военного конфликта, кластерный анализ, меры предупреждения.*

A IMPROVED METHODOLOGY OF EVALUATION OF INTENSITY OF MODERN MILITARY CONFLICTS

Leonid S. Golopatyuk

National Defence University of Ukraine named after Ivan Chernyahovsky

In determining measures to prevent military conflicts, there is a need to assess the intensity of military conflicts at different stages of development. Estimation of the intensity of traditional (conventional) military conflicts is usually carried out with a limited number of well-defined parameters. To assess the intensity of modern (non-conventional) military conflicts (MMC), it is necessary to take into account already a considerable number of parameters that are fuzzy.

With the improvement of the methodology of estimating the intensity of the MMC, it is proposed to use the method of the theory of fuzzy sets. The essence of the method is the representation of the MMC in the form of a distribution of the function of belonging, which fully describes it according to the selected parameters. The application of the known fuzzy context-sensitive clustering algorithm allows the selection of clusters (groups) similar in intensity to the MMC, to find in each group a prototype that describes the entire group. In the event of a new conflict, it is enough to evaluate its affiliation with cluster prototypes and determine the level of intensity for choosing prevention measures.

The difference between the proposed methodological conditions is the use of mathematical methods that take into account the uncertainty of information about the MMC.

***Key words**: modern military conflict, intensity of modern military conflict, cluster analysis, preventive measures.*

Шановні колеги!

Запрошуємо до участі в науковому журналі
"Сучасні інформаційні технології у сфері безпеки та оборони",
Видавець: Національний університет оборони України імені Івана Черняховського
Наказом Міністерства освіти і науки України
від 29 грудня 2014 р. №1528 журнал включено до Переліку наукових фахових видань України в галузях "технічні науки" та "військові науки"
Наклад – 100 примірників, відкрите видання.

На сторінках журналу розглядаються такі питання:

1. Теоретичні основи та інструментальні засоби створення і використання інформаційних технологій у сфері безпеки та оборони.
2. Критерії оцінювання і методи забезпечення якості, надійності, живучості інформаційних технологій і систем.
3. Принципи оптимізації, моделі та методи прийняття рішень при створенні автоматизованих систем різноманітного призначення у сфері безпеки і оборони.
4. Дослідження закономірностей побудови інформаційних комунікацій та розроблення теоретичних засад побудови і впровадження інтелектуальних інформаційних технологій для створення новітніх систем накопичування, переробки, збереження інформації та систем управління у сфері безпеки та оборони.
5. Інтерактивні моделі розвитку науково-освітнього простору у сфері безпеки та оборони.
6. Збереження, розвиток і трансформація культурно-мовної спадщини в інтерактивному дискурсі у контексті інформаційної безпеки держави.
7. Глобалізація, полілогічність та інтерактивність як філософське підґрунтя розвитку інформаційних технологій у сфері безпеки та оборони.
8. Інтелектуальні освітні інформаційні технології у сфері безпеки та оборони. Проблеми сумісності і взаємодії технологій навчання.
9. Сучасні підходи до проектування розподілених інтелектуальних систем для освіти і науки.
10. Військово-теоретичні проблеми.

Схема оформлення статей

УДК (*Arial, кегль – **11** пт.*)

*¬ — 1 пустий рядок – **10** пт.*

[1]***Анатолій Анатолійович Іванов*** *(д-р техн. наук, професор)*
[2]***Іван Іванович Петров*** *(канд. техн. наук, доцент, доцент кафедри)*

*¬ — (кегль – **11** та **8** пт.)*

*¬ — 1 пустий рядок – **6** пт.*

[1]***Університет…, Київ, Україна***
[2]***Інститут…, Київ, Україна***

*¬ — (кегль – **11** пт.)*

*¬ — 1 пустий рядок – **10** пт.*

НАЗВА СТАТТІ (*Arial, кегль – **14** пт.; накреслення – "напівжирне", по правому краю)*

*¬ — 1 пустий рядок – **10** пт.*

Текст анотації мовою тексту статті (в даному випадку – українською). Зміст анотації має стисло і достатньо інформативно підсумовувати основні ідеї та отримані результати дослідження. Розмір анотації повинен становити 100–250 слів. Зверніть увагу на те, що дані про авторів, назва, ключові слова та анотація будуть використані як метадані для опису Вашої статті, тому вони повинні максимально чітко описувати її зміст. Для більш якісного пошуку даного контенту в мережі, будь ласка, уникайте занадто узагальнених та складних формулювань, використовуйте тільки загальновідомі абревіатури.

Ключові слова: *поняття1; поняття 2; поняття3.* (*кегль – **10** пт.*)

Вимоги до набору

Формат аркуша: А4 (21 × 29,7 см).

Параметри сторінки (відступи від краю): зліва – 3 см.; справа – 2 см.; зверху – 2 см.; знизу – 2 см.

Шрифт статті – *Times New Roman*; накреслення – пряме; кегль – 10 пт.; міжрядковий інтервал – одинарний.

Текст статті розташовується у два стовпчики однакової ширини – 7,75 см.; відстань між стовпчиками – 0,5 см.; відступ першого рядка абзацу – 0,5 см.; вирівнювання – за шириною.

Підзаголовок – кегль – 12 пт.; накреслення – напівжирне; відступів немає; вирівнювання – центроване.

Не використовуйте для форматування тексту пропуски, табуляцію тощо. Не встановлюйте ручне перенесення слів, не використовуйте колонтитули. Між значенням величини та одиницею її вимірювання ставте нерозривний пропуск (Ctrl + Shift + пропуск).

УВАГА! Остання сторінка статті заповнюється не менш, ніж на 3/4.

Набір формул: редактор формул *MS Equation.*

Забороняється використовувати для набору формул графічні об'єкти, кадри й таблиці.

В меню "*Размер ® Определить*" ввести такі розміри:
Обычный – 10 пт.; Крупный индекс – 8 пт.;
Мелкий индекс – 7 пт.; Крупный символ – 15 пт.;
Мелкий символ - 9 пт.

Стиль формул – "прямий", тобто в меню "*Стиль ® Определить*" поля "Формат символов" – пусті.

Табличний заголовок (10 пт.) – **обов'язковий**.

Рисунки **обов'язково** супроводжуються центрованими підрисунковими підписами (кегль – 10).

Не допускаються кольорові та фонові рисунки.

Допускається розташування великих рисунків, формул та таблиць в одну колонку (до 16 см.).

Список літератури виділяється підзаголовком "***Література***"та оформлюється згідно з міждержавним стандартом ДСТУ ГОСТ 7.1:2006 "(кегль – 9 пт.).

Структура рукопису

Відповідно до постанови ВАК України від 15.01.2003 № 7-05/1 текст статті повинен мати таку структуру: ***постановка проблеми*** *у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями*; ***аналіз останніх досліджень і публікацій***, *на які спирається автор*; ***формулювання мети статті*** (*постановка завдання*); ***виклад основного матеріалу*** *дослідження з повним обґрунтуванням отриманих наукових результатів*; ***висновки*** *з даного дослідження і перспективи подальших досліджень у даному напрямку.*

Текст статті розбивається на відповідні розділи з підзаголовками, які виділені напівжирним шрифтом.

Робочі мови – українська, російська, англійська.

На останньому аркуші статті після списку літератури наводяться: назва статті, прізвище, ім'я, по батькові, науковий ступінь та вчене звання автора (співавторів), назва організації, у якій працює автор (співавтори), анотація та ключові слова українською, російською та англійською мовами (крім основної мови статті) за нижченаведеним зразком (10 кегль (8 для наукового ступеня, звання, посади), міжрядковий інтервал – 1,0, вирівнювання – по центру). Обсяг анотації – 100-250 слів, англійською – 150-250 слів.

НАЗВАНИЕ СТАТЬИ

*[1]**Анатолий Анатолиевич Иванов** (д-р техн. наук, профессор)*
*[2]**Иван Иванович Петров** (канд. техн. наук, доцент, доцент кафедры)*

*[1]**Университет…, Киев, Украина***
*[2]**Институт…, Киев, Украина***

Перевод текста аннотации и ключевых слов

ARTICLE TITLE

*[1]**Anatolii A. Ivanov** (Doctor of Technical Sciences, Professor)*
*[2]**Ivan I. Petrov** (Candidate of Technical Sciences, Associate Professor)*

*[1]**University…, Kyiv, Ukraine***
*[2]**Institute…, Kyiv, Ukraine***

Translation of the abstract and keywords

Після цього наводиться список літератури англійською мовою за зразком (9 кегль):

References

1. Pukhov G.E. (1990), Differential spectrums and models. [*Dyferentsiini spektry ta modeli*], Kyiv, Naukova Dumka, 184 p. **2. Mikheenko L.A.**, Nechiporuk S.A. (2011), Energy model of digital camcorder. [*Enerhetychna model tsyfrovoi videokamery*], Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh, No. 1, pp. 150–157. **3. Voskresenskava E.V.** (2003), Legal regulation of valuation activities: dissertation. [*Pravovoe regulirovanie otsenochnoi deyatel'nosti: dis. kand. yurid. nauk*], St. Petersburg, 187 p. **4. Bezrodnaya V.F.** (2004), Features of civil society development in the process of politicalmodernization of Ukraine: Author's thesis. [*Osobennosti formirovaniya grazhdanskogo obshchestva v protsesse politicheskoi modernizatsii Ukrainy: avtoref. dis. kand. polit. nauk*], Odessa, 16 p. **5. Serdyuk T.V.,** Self-regulation in Ukraine: advantages and disadvantages in the current economic conditions. [*Samoregulirovanie v Ukraine: preimushchestva i nedostatki v sovremennykh ekonomicheskikh usloviyakh*], available at: http://economy.kpi.ua/ru/node/343.

A.A. Ivanov: iv@u.ua I.I. Petrov: petr@u.ua

Корисні посилання для здійснення транслітерації:

http://translit.kh.ua/?passport – автоматична транслітерація з української мови
http://translate.meta.ua/ua/translit/ – автоматична транслітерація з російської мови

Після цього наводяться відомості про рецензента та контактна інформація авторів.

Рецензент: д-р техн. наук, професор О. Ю. Пермяков, начальник інституту, Національний університет оборони України імені Івана Черняховського, Київ.

Автор*: Анатолій Анатолійович Іванов*
Роб. тел. – 333-33-33, дом. тел. – 777-77-77, E-mail – kim@ic.ua.

Подання матеріалів

Обсяг рукопису – від 3 до 10 аркушів українською, російською або англійською мовами.

Для публікації необхідно представити статтю у електронній формі з роздрукованим екземпляром, підписаним всіма авторами статті.

Комп'ютерна верстка: *М.В. Приймак*

Оформлення обкладинки: *О.В. Войтко*

Рукопис супроводжується ***експертним висновком, рецензією доктора наук (професора), витягом з протоколу засідання кафедри (відділу).***

Подані матеріали автору не повертаються.

Матеріали просимо подавати до інституту інформаційних технологій Національного університету оборони України імені Івана Черняховського за адресою: 03049, м. Київ, Повітрофлотський пр., 28, тел.: (044) 271-07-31, Войтку Олександру Володимировичу, каб. 2/309, тел.: 098-2734862, e-mail: sitnuou@ukr.net.

З питань оплати звертатись до редакції.

Редколегія залишає за собою право відмови у публікації статей, що не відповідають проблематиці журналу й умовам оформлення матеріалів.

Засновник і видавець Національний університет оборони України імені Івана Черняховського.
Св-во КВ № 20490-10290ПР. Адреса редакції: 03049, м. Київ, Повітрофлотський пр-т, 28. Тел. (044) 271-07-31.
Підписано до друку 25.09.2017. Формат 60×84 ⅛. Ум. друк. а. 20,25. Тираж 100 прим.
Надруковано у друкарні Національного університету оборони України імені Івана Черняховського.