# Концептуальні напрямки комплексного вирішення проблеми захисту від несанкціонованого доступу в складних системах спеціального призначення

Сергій Вдовенко
кафедра зв'язку та АСУ,
Національний університет оборони України
Київ, Україна
vsg64@ukr.net

Юрій Даник
Інститут інформаційних технологій,
Національний університет оборони України
Київ, Україна
zhvinau@ukr.net.

# Conceptual directions of the complex solution of the problem of protection against unauthorized access in complex systems of special purpose

Serhii Vdovenko
Communication and Information Systems Department,
National Defense University of Ukraine.
Kyiv, Ukraine.
vsg64@ukr.net

Yuriy Danyk
Information Technologies Institute,
National Defense University of Ukraine.
Kyiv, Ukraine.
zhvinau@ukr.net.

***Анотація* — Запропонована методика виявлення критичних елементів, вузлів та зв'язків системи на основі диференційного підходу до класифікації, розпізнання та визначення рівня загроз деструктивних впливів, що дозволяє обгрунтувати та створити комплексну організаційно-технічну підсистему захисту складних інформаційно-керуючих систем спеціального призначення, яка гарантовано забезпечить адекватне реагування на реальні та потенційні загрози.**

***Abstract* – The proposed method of detecting critical elements, nodes and connections of the system on the basis of a differentiated approach to the classification, recognition and determination of the level of threats of destructive influences, can justify and create a comprehensive organizational and technical subsystem for the protection of complex information-control systems of special purpose, which is guaranteed to provide an adequate response. on real and potential threats.**

***Ключові слова — Диференційний аналіз, загрози, комплексний захист систем, несанкціонований доступ, складні системи спеціального призначення.***

***Keywords – complex protection of systems, differentiated approach, complex special purpose systems, threats, unauthorized access.***

## I.Вступ

Результатом стрімкого науково-технічного прогресу у сфері інформаційних технологій стало значне посилення ролі складних автоматизованих систем управління, які застосовуються у багатьох галузях діяльності людини, зокрема у військовій сфері [1]. Процеси функціонування таких систем відбуваються у сформованому новому штучному просторі – кіберпросторі, який доповнив природні: сухопутний, морський, повітряний, космічний, та став сферою конфліктів і можливих бойових дій [2]. Зважаючи на сутність кібербезпеки, як безпеки перш за все управління, слід звернути особливу увагу на питання захисту від несанкціонованого доступу систем, які його забезпечують.

В класичних системах управління спеціального призначення замкнутого типу реалізуються такі основні функції: розпізнавання, ідентифікація, прогнозування, підтвердження (ухвалення) рішення, безпосередньо управління. Задача управління вирішується в умовах апріорної невизначеності, динамічної зміни зовнішніх і внутрішніх факторів впливу безпосередньо на системи управління, їх складові та процеси які реалізуються в них [1].

Зазвичай, особливо у військовій сфері, управління здійснюється в умовах кризових ситуацій та деструктивних впливів, що суттєво посилює вимоги до математичного й програмно-алгоритмічного забезпечення сучасних інформаційно-керуючих систем (ІКС), інженерно-технічної реалізації підсистем їх захисту, при цьому, не знижуючи рівня вимог до персоналу. Досвід їх застосування в кризових ситуаціях показує необхідність формування додаткових вимог щодо захисту ІКС від деструктивного комплексного кібервпливу. Причому, ускладнення систем, приводить до зростання їх вразливості та відповідно вимог щодо забезпечення їх захисту.

Тому, задача вироблення ефективних підходів щодо комплексного захисту складних систем, зокрема вирішення проблеми їх захисту від несанкціонованого доступу, є актуальною.

## II. Теоретичний базис захисту складних систем від НСД

Традиційні підходи для побудови моделі складних інформаційних систем для визначення їх структури і параметрів розглянуто в працях А.Д. Цвіркуна, І.В. Кузьміна, В.С. Черняка, В.В. Дружиніна, Д.С. Конторова та ін. Ці підходи грунтуються на використанні однокритерійних моделей та методів оптимізації.

Вони знижують адекватність кінцевих рішень, зокрема щодо визначення рівнів та характеру загроз, при зміні вимог до складної системи та умов її функціонування. Це вимагає розробки нових багатокритеійних підходів до структурного та параметричного синтезу складних інформаційних систем.

Найбільш перспективним для ідентифікації загроз ІКС є метод розпізнавання ситуацій, але він має досить слабке розвинення, як в теоретичному, так і у практичному плані.

Основу його складає розроблення гіпотез з відповідними їм імовірнісними характеристиками, які мають визначати не тільки можливість появи таких загроз, але й взаємозв’язок між ними. Це дає змогу визначити загальний можливий перебіг ситуацій.

Але, такий метод не є ефективним в умовах апріорної невизначеності обстановки тому-що вимагає ретельного відбору даних, їх тривалої обробки та детальної багаторазової перевірки.

При моделюванні загроз ІКС в кризових ситуаціях має місце суттєвий рівень апріорної невизначеності ряду умов, зокрема таких як: якість та повнота вихідних даних; точність завдання функціональних взаємозв'язків між складовими моделі ІКС; значна динаміка змін обстановки; вплив зовнішніх факторів та множини імовірних загроз на процеси, що відбуваються у системі; часові параметри імовірних атак в умовах інформаційної надмірності; рівень оптимізації рішень; ступінь формалізації змодельованих процесів, тощо.

Тому, для комплексного захисту складних систем спеціального призначення запропоновано здійснювати:

декомпозицію загроз складним системам з точки зору їх вразливості і захищеності та формування диференційної моделі загроз їм;

SMART-захист складних систем на основі диференційного аналізу вразливості її складових та системи в цілому.

Складні системи управління з позиції загроз розглядаються з точки зору забезпечення їх захисту від НСД наступним чином (рис.1.):

Імовірні загрози складним системам Rj відносяться до випадкових сумісних подій

.


**Рис. 1. Диференційована схема загроз R складної системи.**

Розглянемо в цьому контексті формалізацію складних систем за ідентифікацією на основі самоорганізації [1]. У загальному вигляді задача формулюється наступним чином. Є множина об’єктів ідентифікації (ОІ) R={R1,R2…Rj}, j=1…n. В даному сенсі, як ОІ розглядаються різні ризики, загрози та конфліктні ситуації, в т.ч. загрози, пов’язані із цілеспрямованим або

ненавмисним втручанням персоналу; інформаційними, криптографічними або кібернетичними атаками, впливом систем протидії тощо (виключно фізичне знищення). Всі їх можна об'єднати в групу загроз "несанкціонований доступ" (НСД).

НСД-загрози різних рівнів та характеру можуть відрізнятися способами їх реалізації, але всі вони мають за мету нанесення збитків складній ІКС. В залежності від потенційних розмірів евентуальних збитків слід будувати системи захисту.

Умовно, враховуючи специфіку складних управлінських систем, будемо розглядати два основних класи методів захисту від загроз: організаційні (режимні);

інженерно-технічні (алгоритмічні, програмно-технічні, криптографічні тощо).

Організаційно-правова сторона цього питання полягає в регламентації та виконанні оперативно-розшукових, режимно-обмежувальних та інших спеціальних заходів, які забезпечують захист від НСД [3].

Визначення повної множини загроз Rj та вибору варіанту реалізації конкретних загроз, необхідно для формування найбільш раціонального варіанту реалізації комплексного захисту інформації в складній системі та в окремих її складових, відповідно до ситуації що складається в поточних умовах обстановки. Ускладнення цього завдання вимагає також й зміни підходів до захисту.

Диференційний підхід до забезпечення захисту інформації в складних системах спеціального призначення зводиться до (рис. 2):

визначення і класифікації множини загроз Rj

розподілу загроз за декількома (трьома) рівнями: зовнішньому (глобальному) $R_I$, загальносистемному (локальному) $R_{II}$, і внутрішньому (на рівні складових) $R_{III}$;

ідентифікації та класифікації загроз залежно від збитків, що можуть бути нанесені складній системі в цілому, її складовим, окремим елементам та (або) зв'язкам між ними.

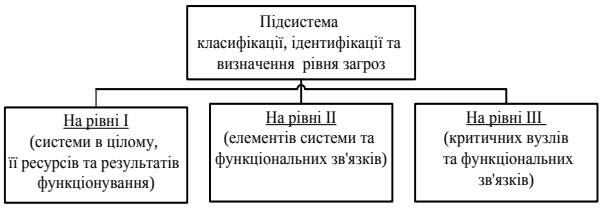


**Рис. 2. Модель підсистеми класифікації загроз .**

З метою протидії загрозам Rj, підсистеми захисту, зокрема від НСД, реалізовані в складних ІКС, мають вирішувати наступні організаційно-технічні завдання:

забезпечення безпеки санкціонованого доступу персоналу до системи та її складових;

запобігання цілеспрямованих злочинів та ненавмисних помилкових дій персоналу та сторонніх осіб, направлених на НСД до системи та її складових;

захист складної системи та її складових від деструктивного кібервпливу та інші.

Завдання ідентифікації загроз полягає у визначенні типу НСД, його властивостей та можливостей в умовах апріорної невизначеності про об'єкт, надмірності іншої зовнішньої інформації, в т.ч. й хибної, зовнішнього деструктивного впливу на складну ІКС, тощо [1].

Ідентифікація здійснюється на підставі отриманих даних (D), фактів (F), суджень (S). В спрощеному вигляді, це можна представити:

$$Rj = \sum \{Dj, Fj, Sj\}, \qquad (1.1)$$

Ефективний захист слід організовувати та здійснювати на підставі загальних законів суспільства та природи, тобто - суджень Sj щодо апріорно невідомих, але ймовірних, властивостей та спроможностей потенційних загроз Rj. Дані Dj та факти, Fj є допоміжними множинами, які за умов їх ідентифікації та визначеності, можуть призвести до оптимізації витрат на забезпечення захисту. Конкретна загроза системі R*i* об'єктивно містить в собі, або породжує унікальну комбінацію притаманних лише їй множин незалежних ознак: даних – $D_i\{d_{ij}\}$, фактів – $F_i\{f_{il}\}$, суджень – $S_i\{s_{ik}\}$.

Виходячи з цього, апріорну множину визначених ознак загроз представити формулою:

$$Ri = \{ Di\{d_{ij}\}, F\{f_{il}\}, S\{s_{ik}\} \}, \qquad (1.2)$$

Такий підхід дозволить побудувати систему захисту ІКС, що виконує завдання в умовах апріорної невизначеності, на принципах доцільності, раціональності та розумної достатності. В результаті декомпозиції складних систем управління, які виконують завдання в кризових умовах, з'ясовано, що для забезпечення функціональної стійкості складні системи мають створюватися з урахуванням наступних основних вимог [3, 4, 5, 6, 7]:

безперервність функціонування;

гнучкість та адаптивність до загроз (атак);

забезпечення захисту від загроз;

багаторівневість захисту відповідно до рівнів загроз;

комплексність (реалізація організаційних, організаційно-технічних й інженерно-технічних засобів та заходів);

уніфікація програмно-апаратних та алгоритмічних рішень систем захисту;

варіативність функціональної логіки (адаптивність підсистеми захисту ІКС до інших подібних складних систем);

автономність функціонування технічної компоненти системи захисту;

реалізація багаторівневої системи контролю безпеки та захисту від помилок персоналу;

гарантоване кореговане забезпечення обмежень кола службових осіб щодо виконання ними повноважних функцій;

дотримання розумного балансу між завданням швидкої обробки великих заданих обсягів інформації в ІКС за мінімальний наявний проміжок часу та необхідністю витрачання значного часового ресурсу на досягнення мети функціонування систем захисту.

В останній третині XX століття захист від НСД складних управлінських систем спеціального

призначення реалізовувався переважно за рахунок режимно-обмежувальних й організаційно-технічних заходів. Інженерно-технічні рішення, внаслідок низького рівня автоматизації процесів управління, використовувалися обмежено та переважно локально. До того ж, такі системи захисту були та залишаються вразливими через персонал. Крім того, симетричні криптографічні системи того часу були хоча й математично криптостійкими, але внаслідок специфіки своєї реалізації, не могли бути стовідсотково використані на всіх рівнях в складних системах управління.

Сучасні умови вимагають зміни пріоритетів, виводячи на перший план інженерно-технічні заходи, насамперед, криптографічні.

З розвитком інформаційних технологій, широким їх застосуванням в системах державного і військового управління, розвідки, модель загроз безпеці інформації змінилася в бік ускладнення (рис.3.). Якісні зміни загроз на всіх рівнях у вигляді зростання можливостей технічних видів розвідки (радіоелектронної, кібернетичної тощо) та криптоаналізу, вимагають збільшення довжини ключової послідовності реалізованого криптоалгоритму. Що обумовлює прагнення до збільшення часу на цикл реалізації завдань управління, що є не можливим. Навпаки, час циклу має стійку тенденцію до мінімізації.

Вирішення задачі можливе лише за рахунок оптимізації підходів до реалізації ІКС, в тому числі – до побудови систем комплексного захисту від НСД.

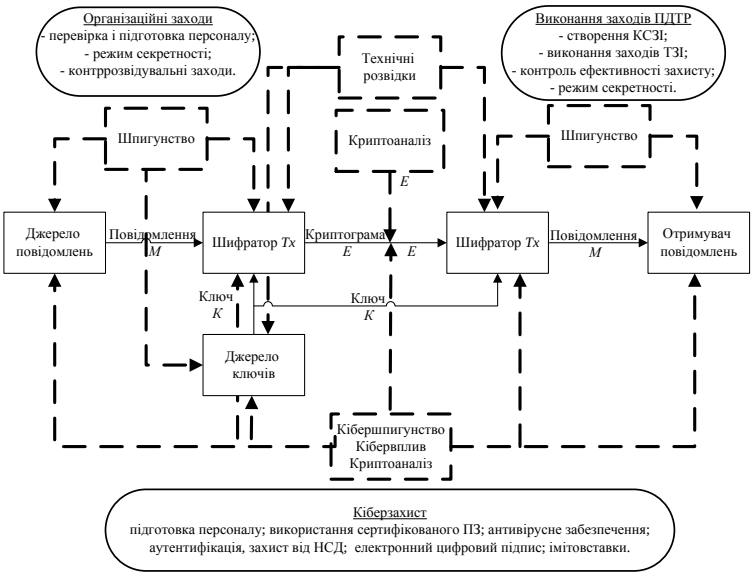


**Рис. 3. Схема потенційних загроз ІКС та варіанти заходів щодо запобігання їм (на прикладі системи КЗІ).**

## III. Висновки

В доповіді розглянуті напрями до вибору та реалізації раціональних підходів при вирішенні питання комплексного захисту від несанкціонованого доступу в складних системах спеціального призначення.

Запропоновані методика оцінки функціональної стійкості складних систем до деструктивних впливів та виявлення критичних елементів, вузлів та зв'язків системи, а також диференційний підхід до класифікації, розпізнання та визначення рівня загроз для складних ІКС, дозволяють обгрунтувати та створити комплексну організаційно-технічну підсистему захисту складних ІКС спеціального призначення, яка гарантовано забезпечить адекватне реагування на реальні та потенційні загрози, раціонально використовуючи наявні у держави можливості і ресурси [2, 3, 8].

## Література, References

[1] Ю.Г.Даник. Багатокритерійні математичні моделі ситуаційного управління та саморганізації у складних інформаційних системах. Монографія./ Ю.Г.Даник, О.О.Писарчук, В.І.Шестаков, К.О.Соколов, С.В. Чернишук, О.В.Лагодний, С.В.Тимощук, Житомир – 2016, с.129-143.

[2] Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

[3] Вдовенко С.Г. Даник Ю.Г., Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління Збройних сил / Сучасні інформаційні технології у сфері безпеки та оборони № 2(29), 2017, с. 98-106.

[4] В.М.Шлюкін, С.В.Малахов, О.Л.Гостєв, А.Г.Снісаренко, С.Г.Вдовенко, О.М.Присяжний, Загальносистемні питання санкціонування застосування ракетних комплексів Сухопутних військ / Системи озброєння і військова техніка № 2 (30), 2012, с. 95-103.

[5] 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.

[6] Вдовенко С.Г. Сучасні вимоги до охорони державної таємниці та захисту інформації з обмеженим доступом в особливий період / Імперативи розвитку цивілізації №2, Київ – 2015, с. 93-96.

[7] Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування. Монографія. Харків. Вид. 2-ге, перероблене й доповнене.

[8] Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.2016 № 92/2016.