DOI 10.31891/2307-5732-2020-281-1-105-109
УДК 004.056

А. В. ДУДАТЬЄВ, О. П. ВОЙТОВИЧ, В. В. МИРОНЮК
Вінницький національний технічний університет

# ІНФОРМАЦІЙНО-АНАЛІТИЧНІ ЦЕНТРИ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

*Запропоновано модель «інформаційного портрету» об'єкта захисту від локального до держави. Наведена схема інформаційного забезпечення інформаційно-аналітичного центру. На базі отриманих результатів запропонована методологія побудови трьохрівневої політики безпеки, спрямованої на державу, регіон та локальний об'єкт.*

***Ключові слова:*** *інформаційно-аналітичний центр, інформаційний портрет об'єкта захисту, політика безпеки, інформаційна безпека держави.*

A.V. DUDATYEV, O. P. VOITOVYCH, V. V. MIRONYUK
Vinnytsia National Technical University

## INFORMATION-ANALYTICAL CENTERS OF THE STATE INFORMATION SECURITY MANAGEMENT

*The methodological basis of the informational-analytic center creation for the state information security management is proposed. The analysis of the existing results upside of the informational-analytic center designing and information support definition in the state management system is carried out. The approach on practical realization of two main tasks, namely assessment and assurance of the information security certain level is proposed. Such approach allows to effectively implement the process of information security management, that is, to implement appropriate situational models, algorithms, rules, etc. Information-analytical work is impossible without effective information support. The analysis shows that the information security management of the state is a multilevel process. Today there is no single understanding of this process, however. The reason is the lack of a consistent methodology of the state information security management system. The methodology that enables effective information-analytical research to provide information support is solving the following tasks: the problem of forecasting and timely detection of information security threats, creating conditions for likelihood minimizing of threats implementation, creating conditions and mechanisms for responding to new threats, countermeasures organization of information-cybernetic and information-psychological operations, countermeasures effectiveness assessment carrying out. The approach to the construction of methodological bases for the information-analytical centers (services) creation in the system of the state information security management is proposed, namely: the model of information profile of the protected object, which allows to formalize the task by the "object - group of objects (region) – state" level; the structural model of the information-analytical center, which includes models of the protected object profile; the method of providing comprehensive information security at the "object - object group (region) – state" level using the proposed models and structures.*

***Keywords:*** *informational-analytic center, protected object information profile, security policy, state information security.*

## Вступ

Процес оцінювання та забезпечення заданого рівня інформаційної безпеки держави (ІБД) супроводжується роботою з великою кількістю різноманітної інформації, серед якої доцільно виділити інформацію щодо множини загроз, потенційних порушників, власне самого об'єкту захисту, середовищ, що оточують об'єкт захисту тощо. Необхідно також враховувати залежність рівня ІБД від рівня інформаційної безпеки на локальних об'єктах захисту – окремих підприємствах, установах, організаціях, в першу чергу критичних інфраструктур, порушення інформаційної безпеки яких може призвести до глобальних змін у стані держави в цілому. В напряму управління інформаційною безпекою підвищився обсяг інформації та динаміка її змін, тому загострюється необхідність оперативного і адекватного реагування на ситуацію, що формується у реальному часі. Необхідність ефективного рішення задачі оцінювання і забезпечення рівня інформаційної безпеки підвищується під час проведення інформаційного протиборства, зокрема проведення спеціальних інформаційно-психологічних операцій (ІПО) проти соціальної складової соціотехнічних систем (СТС), яке може відбуватися як на рівні окремих підприємств, групи підприємств, так і держави в цілому.

Актуальність створення інформаційно-аналітичного центру обумовлено багатьма факторами, зокрема: необхідністю реалізації комплексного підходу щодо управління ІБД, розв'язання задач прогнозування рівня ІБД, необхідністю реалізації багаторівневої системи управління ІБД. Тому забезпечення процесу управління інформаційною безпекою держави потребує системного підходу до оцінювання рівня загроз, ймовірних порушників, аналізу інформаційних ризиків на всіх рівнях управління інформаційною безпекою.

**Метою роботи** є розробка методологічних засад для побудови інформаційно-аналітичного центру управління інформаційною безпекою держави.

Задачами дослідження є:

- розробка інформаційного портрету об'єкта захисту;
- розробка структурної моделі інформаційно-аналітичного центру;
- розробка методу забезпечення комплексної інформаційної безпеки.

## Аналіз досліджень та публікацій

Відповідно до наказу президента України № 415/2019 від 19.06.2019 був створений національний координаційний центр кібербезпеки, який почав функціонувати при Раді національної безпеки і оборони України. Перед центром поставлено багато складних наукоємних завдань, зокрема: здійснення аналізу стану

кібербезпеки, участь у розробленні галузевих індикаторів стану кібербезпеки, прогнозування та виявлення потенційних та реальних загроз у сфері кібербезпеки України, удосконалення нормативно-правової бази у сфері забезпечення кібербезпеки України, зокрема правового регулювання у сфері відповідальності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України, механізмів взаємодії між ними, оперативне інформаційно-аналітичне забезпечення Ради національної безпеки і оборони України з питань кібербезпеки тощо. У роботі [1] запропоновано теоретичний підхід до інформаційного забезпечення в системі державного управління у воєнній сфері. У роботі [2] пропонується модель підтримки рішень управління інформаційною безпекою, також структурна модель багаторівневого інформаційно-аналітичного центру, діяльність якого спрямовується саме на розв'язок аналогічних задач. Метод виявлення вразливостей об'єкта захисту представлений у роботі [3]. У роботі [4] наведено моделі оцінки стану підприємства від витоку інформації, але в наведених роботах не запропоновано загальний методологічний підхід щодо створення ІАЦ, забезпечення його відповідними інформаційними ресурсами та його подальшого функціонування.

**Основна частина**

Для створення ефективної структурної моделі ІАЦ необхідно розширити методологічну базу, яка включає теоретичні та методологічні основи проведення інформаційної взаємодії різного типу. Фактично, функціонально ІАЦ має забезпечити комплексний захист від різного роду деструктивних інформаційних впливів. Комплексність тут передбачає забезпечення, по-перше, багаторівневості захисту і, по-друге, реалізацію захисту як від ІПО, так і від інформаційно-кібернетичних атак (ІКО).

Оскільки кінцевою метою створення ІАЦ є розв'язання складної інтегрованої задачі, яка полягає у організації і реалізації комплексного захисту від деструктивних інформаційних атак різного типу, які можуть проводитись на різних рівнях управління, а також прогнозування рівня захищеності, то для формалізації процесу рішення сформульованих задач використаємо метод декомпозиції. Такий підхід дозволить дещо спростити і узагальнити створення концептуальної моделі багаторівневої структури ІАЦ. Запропонований підхід передбачає виконання декількох етапів. Перший етап передбачає розробку так званих «інформаційних портретів» відповідних рівнів управління ІБ. Другий етап, після створення «інформаційних портретів», передбачає розробку ефективної політики безпеки відповідного об'єкта захисту – локального об'єкта, групи об'єктів або регіону і держави в цілому. Третій етап, ґрунтуючись на результатах двох попередніх етапів, дозволяє організаційно і технічно реалізувати отримані політики безпеки, використовуючи ті чи інші механізми захисту.

**Перший етап**

*Визначення 1.* Інформаційний портрет локального об'єкта складається з даних, які характеризують моделі загроз, моделі порушника та середовища, що оточують об'єкт захисту, зокрема інформаційне середовище, фізичне середовище та середовище користувачів, а також результатів аналізу ризиків.

*Визначення 2.* Інформаційний портрет регіону складається з розподілених у просторі інформаційних портретів локальних об'єктів.

*Визначення 3.* Інформаційний портрет держави складається з розподілених у просторі інформаційних портретів регіонів.

Використовуючи наведені визначення, формально інформаційний портрет локального об'єкта можна подати так:

$$IP_L = F(Z,PR,PHS,IS,SK,KR,R),$$

де Z – модель загроз; PR – модель порушника; PHS – фізичне середовище; IS – інформаційне середовище; SK – середовище користувачів; KR – критичність об'єкта; R – ризики.

Інформаційний портрет регіону можна подати так:

$$IP_{Reg}=F(IP_{L1},IP_{L2},\ldots\ldots,IP_{Ln}),$$

де $IP_{Li}$,(i = 1-n) – інформаційні портрети локальних об'єктів; n – кількість локальних об'єктів.

Відповідно інформаційний портрет держави формально можна подати так:

$$IP_D=F(IP_{Reg1},IP_{Reg2,}\ldots..,IP_{Regk}),$$

де $IP_{Regi}$, (i=1-k) – інформаційні портрети регіонів, k – кількість регіонів.

**Другий етап**

Отримані інформаційні портрети дозволяють інформаційно та аналітично забезпечити розробку трьохрівневої політики безпеки рівня (об'єкт – група об'єктів (регіон) – держава).

На цьому етапі використовують результати аналізу об'єкта захисту, розроблені моделі загроз та моделі потенційних порушників, результати аналізу середовищ, що оточують об'єкт захисту, а також результати аналізу інформаційних ризиків. У практичній площині на цьому етапі відбувається вибір основних рішень і формулювання базових правил з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій тощо, які регламентують використання спеціальних організаційних заходів, інженерно-технічних рішень щодо захисту інформаційних ресурсів на всіх рівнях управління інформаційної безпеки.

На третьому етапі створюється розподілена система захисту, яка забезпечує розроблену багаторівневу політику безпеки. Синтез оптимальної системи захисту інформаційних ресурсів розглянутий у

багатьох роботах, зокрема [5].

Реалізація трьох вищенаведених етапів дозволяє запропонувати метод забезпечення заданого рівня комплексної інформаційної безпеки держави. Структурна модель запропонованого метода показана на рис. 1.

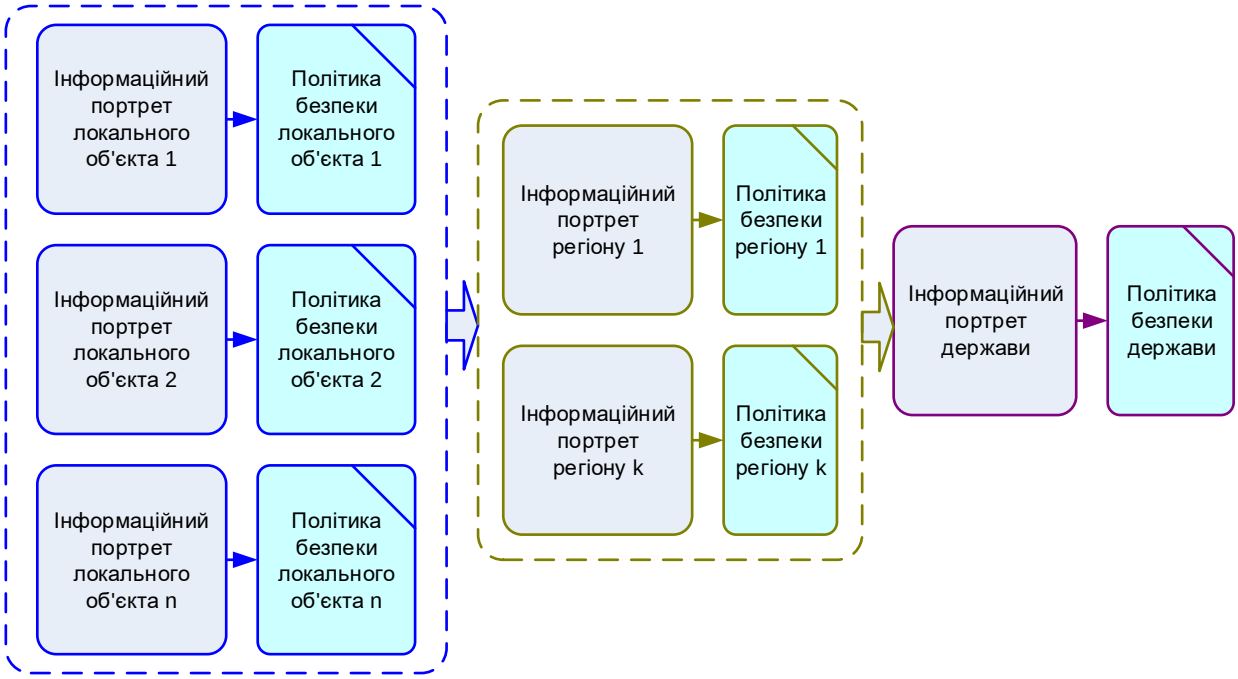


**Рис. 1. Структурна модель методу забезпечення комплексної інформаційної безпеки**

Інформаційно-аналітична робота неможлива без ефективного інформаційного забезпечення. Аналіз показує, що управління ІБД є багаторівневим процесом. Проте на сьогодні немає єдиного розуміння цього процесу. Причиною цього може бути відсутність сталої методології системи управління ІБД. Методика, що надає можливість ефективно проводити інформаційно-аналітичну роботу щодо забезпечення інформаційно-аналітичної роботи передбачає вирішення таких завдань: вирішення задачі прогнозування і своєчасне виявлення загроз інформаційній безпеці; створення умов для мінімізації ймовірності реалізації загроз; створення умов і механізмів реагування на виникнення нових загроз; організація заходів захисту та протидії ІКО та ІПО; оцінка ефективності контрзаходам.

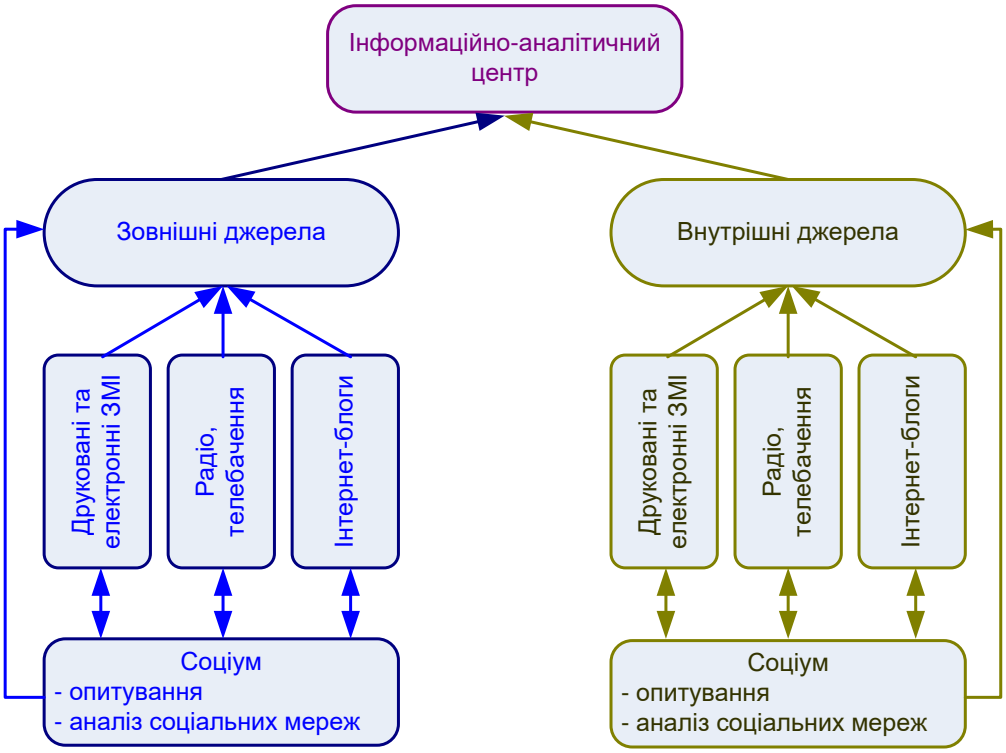


**Рис. 2. Схема інформаційного забезпечення інформаційно-аналітичного центру**

Метою інформаційного забезпечення є організація і реалізація інформаційно-аналітичної роботи для управління інформаційною безпекою. Реалізація цієї мети досягається через розв'язання низки задач, серед яких основними є такі:

- реалізація моніторингу щодо загроз (внутрішніх так і зовнішніх) інформаційному простору;
- проведення оперативної роботи з метою виявлення і нейтралізації діючих і потенційних джерел виникнення загроз;
- нейтралізація ІКО та ІПО, що спрямовані на кібернетичний та інформаційний простори держави;
- використання різноманітних ЗМІ (електронних, друкованих) для реалізації протидії деструктивним інформаційним впливам.

На підставі сутності державного управління інформаційною безпекою та з урахуванням представленого методу забезпечення ІБ побудовано схему інформаційного забезпечення ІАЦ (рис. 2).

Аналіз наведеної схеми інформаційного забезпечення ІАЦ фактично описує реалізацію процесу моніторингу різноманітних, як внутрішніх так і зовнішніх інформаційних ресурсів та ймовірних джерел впливу.

Роль інформаційного забезпечення в системі управління ІБД полягає в створенні необхідних умов для реалізації специфічних функцій підготовки та прийняття рішень щодо інформаційної безпеки на підставі своєчасної та достовірної інформації, а його місце визначається відповідним рівнем всього циклу управління інформаційною безпекою.

Виходячи з наведеного структурна модель управління ІБД наведена на рис. 3.


**Рис. 3. Структурна модель управління інформаційною безпекою держави**

Задачу моніторингу вирішує Головний ситуаційний центр України, створений відповідно до рішення РНБО України від 25.01.2015 р. Головною задачею центра є збір, накопичення і обробка інформації, для підготовки та прийняття рішень у сфері національної безпеки і оборони для забезпечення інформаційно-аналітичного супроводу роботи РНБО.

РНБО є дорадчим органом, який аналізує отриману інформацію і готує систематизовану інформацію для прийняття рішення. У статті 4 закону України "Про основи національної безпеки України" визначені суб'єкти, що забезпечують інформаційну безпеку держави. Відповідно під органом, що приймає рішення будемо розуміти інтегровану систему таких суб'єктів, яку очолює Президент держави і яка діє інтегровано і незалежно від зовнішніх і внутрішніх деструктивних впливів.

**Висновки**

Запропоновано підхід до побудови методологічних засад щодо створення інформаційно-аналітичних центрів (служб) в системі державного управління інформаційною безпекою, а саме:

- побудовано модель інформаційного портрету об'єкта захисту, що дозволяє формалізувати задачу за рівнями: об'єкт – група об'єктів (регіон) – держава;
- розроблено структурної моделі інформаційно-аналітичного центру, що включає в себе моделі портрету об'єкта захисту;
- розроблено метод забезпечення комплексної інформаційної безпеки на рівні об'єкт – група об'єктів (регіон) – держава, використовуючи запропоновані моделі та структури.

Подальші дослідження доцільно спрямувати на формалізацію процесу інформаційного забезпечення інформаційно-аналітичних центрів.

**Література**

1. Саричев Ю. О. Теоретичний підхід до інформаційного забезпечення в системі державного

управління у воєнній сфері / Ю. О. Саричев // Вісник НАДУ при Президенті України. Серія "Державне Управління". – 2016. – № 4. – С. 153–160.

2. Дудатьєв А. В. Моделі інформаційної підтримки управління комплексною інформаційною безпекою / А. В. Дудатьєв, О. П. Войтович // Радіоелектроніка, інформатика, управління. – 2017. – № 1. – С. 107–114.

3. Дудатьев А. В. Метод оцінювання безпеки інформаційних ресурсів підприємства на основі аналізу вразливостей / А. В. Дудатьєв, Ю. В. Баришев // Вісник Хмельницького національного університету. – 2008. – № 4. – С. 78–83.

4. Колесник І. С. Оцінка впливу витоку інформації на стан підприємства / І. С. Колесник, А.В. Дудатьєв, О. П. Войтович // Системи обробки інформації. – 2010. – № 5. – С. 224–229.

5. Дудатьєв А. В. Розробка уніфікованих моделей системного проектування оптимальних систем захисту інформаційних ресурсів / А .В. Дудатьєв // Вісник Черкаського технологічного університету. – 2008. – № 1. – С. 3–8.

**References**

1. Sarychev Yu. O. Teoretychnyi pidkhid do informatsiinoho zabezpechennia v systemi derzhavnoho upravlinnia u voiennii sferi / Yu. O. Sarychev // Visnyk NADU pry Prezydenti Ukrainy. Seriia "Derzhavne Upravlinnia". – 2016. – № 4. – S. 153–160.

2. Dudatiev A. V. Modeli informatsiinoi pidtrymky upravlinnia kompleksnoiu informatsiinoiu bezpekoiu / A. V. Dudatiev, O. P. Voitovych // Radioelektronika, informatyka, upravlinnia. – 2017. – № 1. – S. 107–114.

3. Dudatev A. V. Metod otsiniuvannia bezpeky informatsiinykh resursiv pidpryiemstva na osnovi analizu vrazlyvostei / A. V. Dudatiev, Yu. V. Baryshev // Herald of Khmelnytskyi National University. – 2008. – № 4. – S. 78–83.

4. Kolesnyk I. S. Otsinka vplyvu vytoku informatsii na stan pidpryiemstva / I. S. Kolesnyk, A. V. Dudatiev, O. P. Voitovych // Systemy obrobky informatsii. – 2010. – № 5. – S. 224–229.

5. Dudatiev A. V. Rozrobka unifikovanykh modelei systemnoho proektuvannia optymalnykh system zakhystu informatsiinykh resursiv / A .V. Dudatiev // Visnyk Cherkaskoho tekhnolohichnoho universytetu. – 2008. – № 1. – S. 3–8.

Рецензія/Peer review : 24.1.2020 р. Надрукована/Printed : 14.2.2020 р.
Стаття рецензована редакційною колегією