Класифікація інформаційно-аналітичних центрів з управління комплексною інформаційною безпекою

Коротаєв Д.О.[1], Дудатьєв А.В.[2]

[1]Аспірант кафедри захисту інформації, Вінницький національний технічний університет
вул. Хмельницьке шосе 95, м. Вінниця, Україна, dmitriy.mymail5@gmail.com
[2]К.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет
вул. Хмельницьке шосе 95, м. Вінниця, Україна, dudatyev.av@gmail.com

***Анотація* — На даний момент інформаційно-аналітичні центри є мало дослідженим, але досить важливим аспектом управління інформаційною безпекою. У даній доповіді представлено класифікацію інформаційно аналітичних центрів з урахуванням задач управління комплексною інформаційною безпекою.**

Ключові слова: засоби оцінки, комп'ютеризовані критичні системи управління, інформаційно-аналітичні центри.

Classification of information –analytical centers the management of complex information security

Korotayev D.O.[1], Dudatyev A.V.[2],

[1]PhD Student, Information Security Department, Vinnytsia National Technical University
Khmelnytske shosse str., 95, Vinnytsia, Ukraine, dmitriy.mymail5@gmail.com
[2]Ph.D., associate professor of Information Security Department,Vinnytsia National Technical University
Khmelnytske shosse str., 95, Vinnytsia, Ukraine, dudatyev.av@gmail.com

***Abstract* — Currently information analytical centers is unexplored, but very important aspect of information security management. Data presented in the report classificates information based on task management of integrated information security.**

Keywords: assessmen ttools, computer critical control systems, information analysis centers.

Вступ

В умовах стрімкого зростання інформаційних потоків, високої динамічності, складності, багатоаспектності, суттєвим зростанням ступеня невизначеності задач управління, браку часу для ухвалення управлінських рішень, критично важливим стає створення для керівників різного рівня сучасного науково-технологічного середовища. Це середовище повинно сприяти оперативному інформаційно-аналітичному забезпеченню керівництва в різних ситуаціях та забезпечувати прийняття ефективних управлінських рішень, зокрема рішень з управління інформаційною безпекою.

Метою даної роботи є виявлення класифікаційних ознак інформаційно-аналітичних центрів (ІАЦ) з урахуванням задачі управління комплексною інформаційною безпекою.

Актуальність даної теми полягає в тому, що питання управління інформаційною безпекою, є важливим для всіх об'єктів захисту, особливу остроту це питання викликає у так званих критичних об'єктів, які можуть знаходитись під впливом спеціальних інформаційних операцій. З плином часу ми спостерігаємо дуже стрімкий розвиток інформаційних технологій, відповідно збільшується і кількість спроб зламу та спроб несанкціоновано заволодіти певною критично важливою інформацією. Все це супроводжується виникненням нових загроз для інформаційної безпеки, про що свідчить зростання кількості інцидентів, пов'язаних із кіберзлочинністю та захистом інформації [1]. Данна проблема на сьогоднішній день є дуже важливою, оскільки зловмисники можуть отримати можливість перехоплювати паролі, окремі файли, звіти, контролювати бездротові мережі, веб-камери, системи управління автомобільними та залізничними шляхами, системи керування транспортом та ін. Все це може призвести до досить глобальних наслідків, в тому числі й державного рівня.

Інформаційно-аналітичним центрам із забезпечення комплексної інформаційної безпеки присвячено праці [1-5] та ін. Проте питання щодо особливостей класифікації та задач інформаційно-аналітичних центрів забезпечення комплексної інформаційної безпеки висвітлено ще недостатньо. Тому метою роботи є виявлення класифікаційних ознак інформаційно аналітичних центрів з урахуванням задачі управління комплексною інформаційною безпекою [1,2,5].

КЛАСИФІКАЦІЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ЦЕНТРІВ

На даний момент зараз в Україні не існує певної загальноприйнятої класифікації ІАЦ та конкретної дієвої його структури. Саме тому автори пропонують класифікацію ІАЦ, що представлена на рис.1..

Для початку розглянемо інформаційно аналітичні центри з точки зору вирішування поставлених задач. У роботі запропоновано розділити ІАЦ на такі рівні:

- Рівень особистості
- Рівень суспільства
- Рівень держави

Інформаційна безпека з нижнього рівня до найвищого – взаємозалежна. Саме тому потрібно організувати структуру управління комплексною інформаційну безпекою, яка гарантує достатній рівень безпеки.

Рівень держави аналізує дані з регіонів та областей і розробляє перспективні рішення щодо

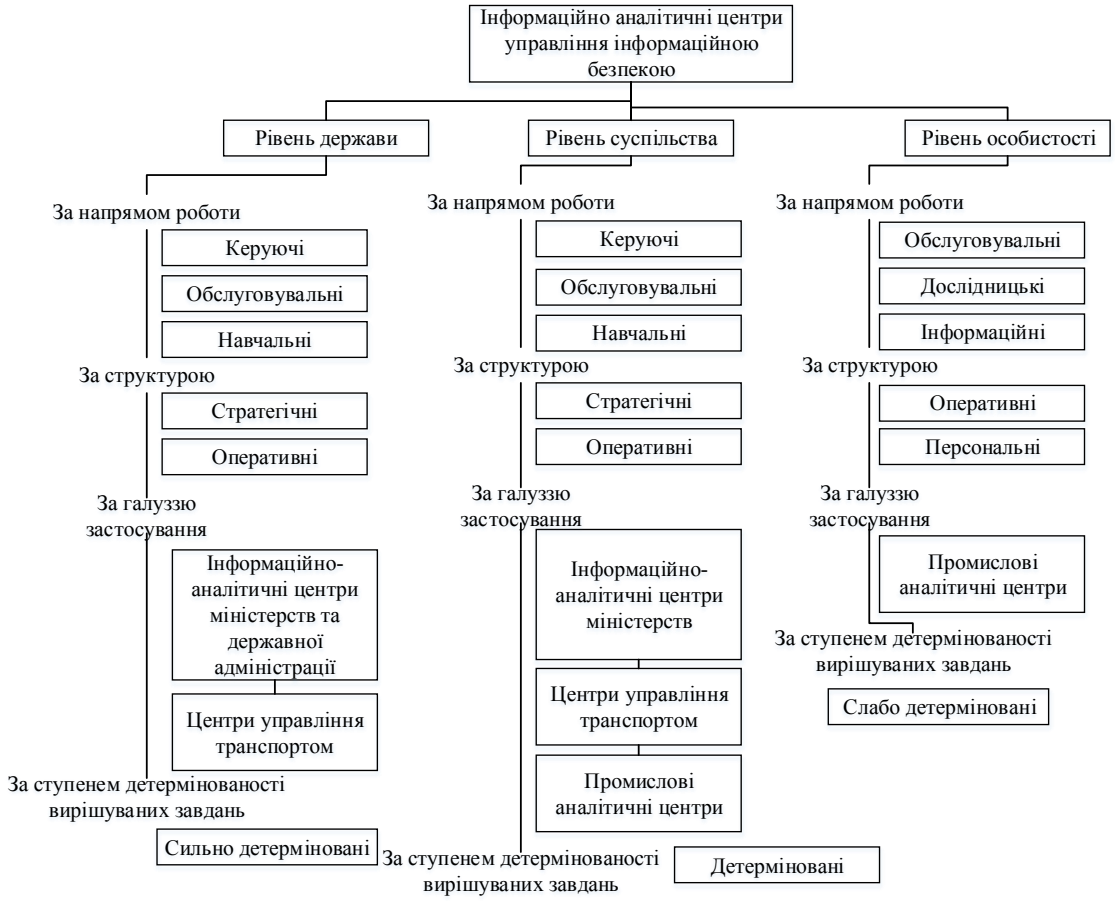

Рисунок 1. Класифікація ІАЦ

інформаційної безпеки. Пізніше дані рішення передаються на рівні нижче для відповідного опрацювання та впровадження. Даному рівню підпорядковуються усі рівні нижче.

Основне завдання керуючих центрів - управління певним складним технічним комплексом. Цільове призначення керуючих систем полягає у забезпеченні роботи складних технічних комплексів, управління ними, та підтримки безвідмовної роботи у заданому режимі і протягом установленого часу [3].

Функціонування ІАЦ відбувається відповідно до складності ситуації та поставленої задачі. Якщо певний рівень не може впоратися з ситуацією, він звертається за допомогою до іншого рівня, якому, в свою чергу, підпорядковується. Відповідно до розробленої структури, на рівні суспільства працюють фахівці, які будуть в основному збирати інформацію з рівня особистості, вдосконалювати

певні аспекти інформаційної безпеки та впроваджувати певні рішення розроблені рівнем суспільства та держави.

Обслуговувальні центри, це центри, в яких людина слідкує та здійснює необхідні дії щодо керування та обслуговування певних систем, проводить її ремонт, налаштування тощо.

Центри обслуговування використовуються для отримання інформації про наявність об'єктів у визначених зонах повітряного і водного середовища. Головними критичними завданнями є виявлення об'єктів, їх впізнання і нагляд за переміщенням їх у певному середовищі.

До навчальних центрів належать технічні засоби моделювання, імітатація загроз і т. ін. На

сьогоднішній день, такі центри не досягли особливого розвитку, їх заміняють імітаційні моделі, які використовуються на відповідних підприємствах.

Інформаційні аналітичні центри забезпечують пошук і накопичення необхідної інформації (системи зв'язку, телевізійні, радіолокаційні, документальні системи тощо), в той час як дослідницькі - використовуються у вивченні різних явищ, пошуку нової інформації та закономірностей (яскравим прикладом подібних систем є гідрометцентри). В цілому їх можна віднести до систем диспетчерського типу. Інформаційно аналітичні центри диспетчерського типу використовуються при управлінні транспортними засобами, розподілі енергії тощо. Основне їх призначення полягає в обслуговуванні, забезпеченні цілісності та надійності інформації та своечасному реагуванні на можливі небезпечні ситуації. Саме тому основними завданнями є: приймання оперативних рішень, контроль завантаження і виконання команд [4].

За структурою:

Стратегічний центр вирішує складні, масштабні, відповідальні завдання, спрямовані на структурну і функціональну перебудову.

Оперативний центр вирішує завдання автоматичної згортки оперативної інформації в ситуаційну модель, що дає першій особі можливість оперувати "Модулями" свого бізнесу в реальному масштабі часу.

Персональний центр вирішує завдання експрес-оцінки ситуації, оперативного доступу до керованого об'єкту і підтримує можливість першого керівника завжди "бути в курсі" незалежно від часу, місця і стану керуючого суб'єкта.

Окрім цього, критичні системи управління прийнято класифікувати ще й за ступенем детермінованості вирішуваних завдань:

- Слабо детерміновані. Детермінованість визначається ступенем хаотичності ситуації, закінченістю постановки задачі, інформаційною відкритістю проблеми, стереотипністю навчальних прикладів і іншими факторами;
- Детерміновані. До даного класу можна віднести завдання всеосяжного управлінського обліку в системах корпоративного або державного операційного контролінгу;
- Сильно детерміновані. До даного класу можна віднести деякі завдання управління рухом ракетою або регулювання розподілу електроенергії.

За галуззю використання інформаційні аналітичні центри класифікують наступним чином:

• Інформаційно-аналітичні центри міністерств та державної адміністрації

Основне призначення подібних центрів полягає в запобіганні кризи за рахунок своєчасного надання особам, які приймають рішення, вичерпної інформації щодо поточного стану контрольованих об'єктів і прогнозів можливих сценаріїв розвитку подій. У випадку ж якщо кризи уникнути не вдалося, такі ситуаційні центри стають, по суті, оперативними штабами з управління процесами локалізації наслідків кризи.

• Центри управління транспортом

Оперативно-диспетчерські центри, що вирішують в реальному часі завдання оперативного управління складними організаційно-технологічними процесами з численними інформаційними потоками. Спочатку в центрах цього класу основна увага приділялася презентаційній компоненті, з розвитком засобів обчислювальної техніки в них не тільки стали з'являтися сучасні засоби відображення інформації колективного користування, але і все більшу роль почало відігравати аналітичне інформаційно-програмне забезпечення прийняття рішень

• Промислові аналітичні центри

По суті їх характеристика збігається з центрами управління транспортом, але промислові аналітичні центри орієнтовані на прийняття не тільки оперативних, але і стратегічних рішень. До них відносяться багато із створених останнім часом інформаційно аналітичних центрів для найрізноманітніших застосувань, це можуть бути інформаційно-аналітичні центри управління ТЄС, ГЄС, АЄС тощо.

ВИСНОВКИ

Отже, в даній доповіді буловиявлено класифікаційні ознакиінформаційно аналітичних центрів з урахуванням задачі управління комплексною інформаційною безпекою.

Запропонована класифікація може стати корисною при подальшій розробці структури інформаційно-аналітичних центрів з управління комплексною інформаційною безпекою.

ЛІТЕРАТУРА REFERENCES

[1] Ильин Н. И. Ситуационные центры. Опыт, состояние, тенденции [Электронный ресурс] / Н. И. Ильин, Н. Н. Демидов, Е. В. Новикова. - М. : Медиа Пресс, 2011. - 336 с.

[2] Райков А. Ситуационная комната для поддержки корпоративных решений [Электронный ресурс] / А. Райков // Открытые системы. - 1999. - №9 7. - Режим доступу : http://www.osp.ru.

[3] Султанова Ж. Д. Обзор мирового опыта по использованию систем поддержки принятия решений (ситуационных комнат) для создания единого информационного пространства органов государственной власти / Ж. Д. Султанова, С. К. Сагнаева // Вестник ЕНУ им. Л. Н. Гумилева. - 2012. - №9 2. - С. 45-48.

[4] Ярочкин В.И. Корпоративная разведка / В.И. Ярочкин, Я.В. Бузанова.–М.: Ось – 89. 2004. – 288 с

[5] Марутян Р. Р. Ситуаційні центри як основа стратегічного управління в сфері національної безпеки [Електронний ресурс] / Р. Р. Марутян. – Режим доступу : http://www.dsaua.org/index.php?option=com_content&view=article&id=171:2012-10- 04-15-59-58&catid=51:2010-10-15-07-16-39&Itemid=89&lang=ru