УДК 004.056:004.621:004.738.5; 004.822:514

Н.Ф. Казакова

Одеський національний економічний університет, канд. техн. наук, доцент

НОРМАТИВНА РЕГЛАМЕНТАЦІЯ ТА ОБГРУНТУВАННЯ КОНЦЕПЦІЇ КОГНІТИВНОГО ЦЕНТРУ ОБРОБКИ ДАНИХ ДЛЯ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Показано доцільність розробки методології створення та функціонування єдиного когнітивного державного центру обробки даних та регіональних когнітивних центрів, як інформаційних систем для стратегічного прогнозування розвитку загальнодержавних та регіональних соціально-економічних систем з забезпеченням в них підвищеного рівня безпеки даних шляхом їх міграції у межах виділеної інформаційно-комунікаційної структури. Зазначено, що доцільним є розгляд проблеми міграції центру обробки даних у межах зазначеної структури у вигляді гібридного хмарного рішення.
Ключові слова: інформаційна безпека, міграція даних, міграція обчислювальних ресурсів, національна інформаційна інфраструктура, моніторинг, когнітивність, ЦОД.

Н.Ф. Казакова

НОРМАТИВНАЯ РЕГЛАМЕНТАЦИЯ И ОБОСНОВАНИЕ КОНЦЕПЦИИ КОГНИТИВНОГО ЦЕНТРА ОБРАБОТКИ ДАННЫХ ДЛЯ НАЦИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Показана целесообразность разработки методологии создания и функционирования единого когнитивного государственного центра обработки данных и региональных когнитивных центров, как информационных систем для стратегического прогнозирования развития общегосударственных и региональных социально-экономических систем с обеспечением в них повышенного уровня безопасности безопасности данных путем их миграции в пределах выделенной информационно-коммуникационной структуры. Отмечено, что целесообразным является рассмотрение проблемы миграции центра обработки данных в пределах указанной структуры в виде гибридного облачного решения.
Ключевые слова: информационная безопасность, миграция данных, миграция вычислительных ресурсов, национальная информационная инфраструктура, мониторинг, когнитивность, ЦОД.

N.F. Kazakova

LEGAL REGULATION AND RATIONALE OF THE CONCEPT OF COGNITIVE DATA CENTER TO THE NATIONAL INFORMATION INFRASTRUCTURE

The expediency of development of the methodology of creation and functioning of the single cognitive state of the data center. The necessity of the establishment of regional centers of cognition. The centers will be of strategic information systems for forecasting the development of national and regional socio-economic systems. Buddet systems to ensure data security. Data security is provided by their migration within the selected information and communication structure. An actual problem is the migration of the data center within said structure. The solution is expected in the form of a hybrid cloud solutions.
Keywords: information security, data migration, migration of computing resources, national information infrastructure, monitoring, cognitive, data processing center.

Постановка проблеми та її зв'язок з сучасними науковими та прикладними задачами

На сучасному етапі розвитку інформаційних технологій ефективним інструментом моніторингу інформаційної безпеки (ІБ) державних соціально-економічних систем, а також технічних систем (включаючи критично важливі сегменти та об'єкти (КВСО)) може бути єдиний державний центр обробки даних (ЦОД). Під терміном КВСО розумітемимо такі підсистеми та об'єкти національної інформаційної інфраструктури (НІІ), ураження яких може завдати істотної шкоди функціонуванню економіки, національної безпеки та національним інтересам країни.

У [1-3] розглянуто перспективи розвитку систем захисту інформації (СЗІ) щодо забезпечення ІБ державних та недержавних структур на основі моніторингу інформаційного простору для виявлення його найбільш безпечних та захищених сегментів з метою міграції до них обчислювальних ресурсів та даних, що забезпечить підвищення їх ступеню конфіденційності, цілісності та доступності. Такий підхід, при якому може виконуватися постійний динамічний процес моніторингу стану інформаційних процесів, що пов'язані з забезпеченням ІБ, включаючи відомості про внутрішній та зовнішній трафіки, з часом може стати невід'ємною частиною ідеології функціонування національної інформаційної інфраструктури. Аналіз міжнародної законодавчої та нормативної бази, а також вітчизняних джерел у зазначеному сенсі показав, що організація та функціональна діяльність ЦОД регламентовані недостатньо. Аналогічний висновок отримано у результаті проведення аналітичного огляду наукових публікацій, матеріалів, розміщених у мережі Інтернет, а також доступних баз патентів. Питання міграції самого ЦОД до безпечних сегментів інформаційного простору, який він контролює, не розглянуті зовсім. Виходячи з цього, ***метою статті*** є нормативна регламентація та обгрунтування концепції функціонування центру обробки даних для національної інформаційної інфраструктури. Зважаючи на це, встановлено, що реалізацію завдання створення єдиного ЦОД може бути обгрунтовано положеннями Указу Президента України від 12.02.2007 року №105/2007 «Про Стратегію національної безпеки України» (в редакції Указу Президента України від 8.06.2012 року). Так, згідно п. 4.3.8 Указу щодо забезпечення ІБ, існує необхідність:

– у стимулюванні впровадження новітніх інформаційних технологій та виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів захисту інформаційних ресурсів;

– у забезпеченні безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони і безпеки держави, кредитно-банківської та інших сфер економіки, систем управління КВСО;

– у розробці та впровадженні національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними стандартами держав – членів ЄС;

– у створенні національної системи кібербезпеки.

Нормативна регламентація та пошук технічних рішень щодо реалізації концепції єдиного ЦОД, можуть бути обгрунтовані у рамках виконання Указу Президента України від 8.07.2009 року №514/2009 «Про Доктрину інформаційної безпеки України», яка визначає принципи забезпечення ІБ в Україні, життєво важливі інтереси в інформаційній сфері напрями державної політики у сфері ІБ, а також реальні та потенційні загрози ІБ України.

Викладення основного матеріалу

Першим кроком Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ) щодо виконання окремих положень Указу Президента №105/2007, було створення CERT-UA (англ.: *Computer Emergency Response Team of Ukraine*, CERT-UA

– команда реагування на комп'ютерні надзвичайні події України). Визначено, що CERT-UA є спеціалізованим структурним підрозділом Державного центру захисту інформаційно-телекомунікаційних систем (ДЦЗ ІТС) ДССЗЗІ. Її функції, завдання та загальну структуру приведено у [4]. Згідно до них, з метою реалізації «Доктрини інформаційної безпеки України», CERT-UA розробила загальну структуру складових ІБ у такому вигляді, як це показано на рис. 1. Він визначає загальну структуру СЗІ у НІІ, а його технологічна складова – сегменти, які підлягають моніторингу зі сторони ЦОД.

ДССЗЗІ, регламентуючись Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 року №3475-IV, створила у своїй структурі три основні служби, а саме:

– Департамент спеціальних інформаційно-телекомунікаційних систем;

– Державний центр захисту інформаційно-телекомунікаційних систем;

– Державне підприємство «Українські спеціальні системи».

Встановлено, що їх функціями є:

1) оцінка стану захищеності державних інформаційних ресурсів;

2) координація роботи та управління CERT-UA;

3) забезпечення діяльності Центру антивірусного захисту інформації;

4) організація ведення реєстру інформаційно-телекомунікаційних систем органів виконавчої влади;

5) створення та підтримка функціонування єдиної точки доступу органів державної влади до мережі Інтернет.

У сукупності зазначене є Національною системою конфіденційного зв'язку. У ній, стосовно вище зазначених функцій, вже реалізовано або знаходяться на стадії розробки та впровадження, положення, які відзначені у пунктах 1-4, положення пункту 5 – на стадії досліджень.

Аналіз вище приведених матеріалів показав, що приведені технології організації функціонування та інформаційної взаємодії існуючих ЦОД, у сенсі діяльності ДССЗЗІ, мають ряд слабких сторін, а саме [5]:

– необхідність автоматизованого вибору та реалізації методів і засобів аналізу й обробки даних в умовах відомих джерел первинної інформації;

– необхідність орієнтації ЦОД на різні категорії користувачів;

– відсутність єдиного регламенту інформаційної взаємодії й обміну даними;

– підтримка прийняття рішень на основі ретроспективної інформації та звітних матеріалів;

– технологічна та організаційна різнорідність функціональних і інформаційних компонентів ЦОД;

– централізована архітектура інформаційних систем, які входять у сферу впливу ЦОД;

– децентралізована архітектура СЗІ в інформаційних системах, які входять у сферу впливу ЦОД;

– строго фіксоване територіальне розташування ЦОД.

Враховуючи результати аналізу літературних першоджерел, а також нормативної та законодавчої бази, відзначимо, що для створення єдиного ЦОД, наприклад, у складі існуючих структур ДССЗЗІ, метою якого буде виконання завдання інформаційного моніторингу ретроспективних станів СЗІ у підконтрольних йому інформаційних системах з метою виявлення безпечних сегментів та організації міграції до них даних та обчислювальних ресурсів, існують правові, нормативні, організаційні та технологічні можливості.

Обґрунтуємо структуру державного ЦОД, як гібридне хмарне рішення. Для цього встановимо, що функціонування єдиного ЦОД державного масштабу повинно відбуватися за рахунок залучення інформаційних ресурсів зацікавлених органів державної влади, державних наукових установ та інших державотворчих структур у рамках встановлених угод, які повинні бути однаковими для всіх учасників НІІ.

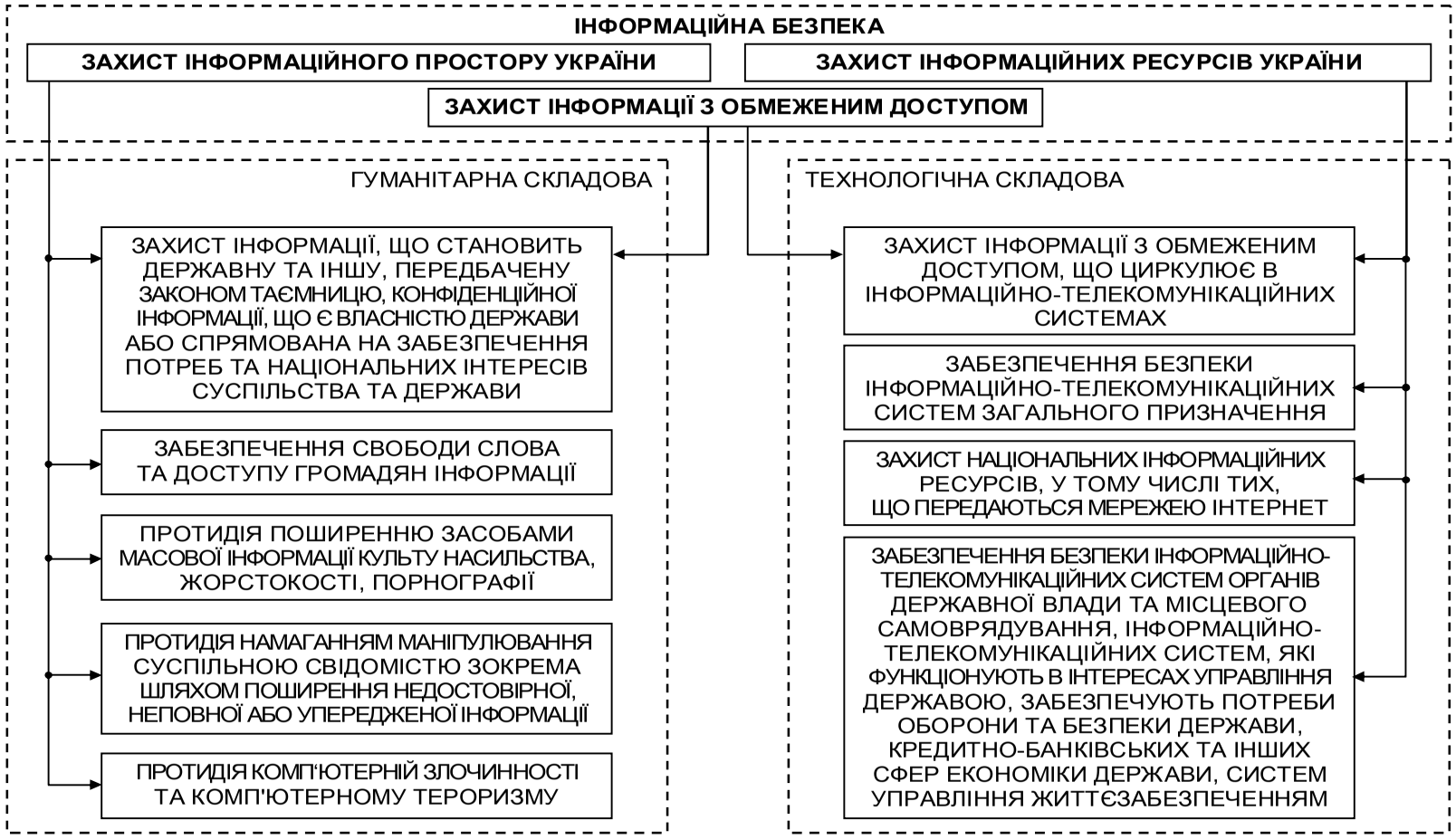

Рис. 1. Складові інформаційної безпеки за версією CERT-UA

Надалі такий ЦОД, який забезпечує ІБ НІІ, будемо позиціонувати, як *державний ЦОД*. У якості нового етапу розвитку забезпечення ним ІБ у НІІ, покладемо розробку методології автоматичної міграції обчислювальних ресурсів та даних до безпечних сегментів.

У сенсі наукових досліджень по усуненню раніше зазначених слабких сторін ЦОД, з врахуванням стану сучасних технологій побудови та організації роботи державного ЦОД, доцільною є розробка методології створення й використання єдиного когнітивного державного ЦОД і регіональних когнітивних центрів, як інформаційних систем для стратегічного прогнозування розвитку загальнодержавних та регіональних соціально-економічних систем (ЗД та РСЕС) [6] і забезпечення в них ІБ. Державний ЦОД, побудований у вигляді когнітивної структури, а також регіональні когнітивні центри, які можуть входити до його структури, забезпечать підтримку управління та функціонування СЗІ в складних децентралізованих системах, включаючи окремі регіони, території, стратегічні галузі й підприємства, КВСО, а також усілякі державні структури. В основу розробки технології функціонування державного ЦОД можуть бути покладені методи імітаційного й математичного моделювання, які мають на меті використання сучасних інформаційних технологій і прикладної математики для дослідження поведінки динамічних систем і процесів різної природи, що пов'язані із забезпеченням ІБ.

Звичайно, що середовищем функціонування когнітивного ЦОД є когнітивна мережа. Згідно до [7], когнітивна мережа – це тип мереж передавання даних, у яких забезпечується можливість для семантичної обробки поточного контексту операцій, аналізу, логічного висновку та планування дій. Це дозволяє приймати рішення та діяти відповідно до досягнутого рішенням з урахуванням попереднього досвіду. Когнітивні мережі мають здатність «думати», навчатися, запам'ятовувати та адаптуватися до мінливих умов для того, щоб досягти своїх цілей і завдань і, т.ч., володіют «самосвідомістю». Архітектура когнітивних мереж та, відповідно, ЦОД, який ними керує, базується на технологіях прийняття рішень і технологіях управління знаннями про предметну область. Когнітивні мережі та ЦОД, у перспективі, можуть бути використані для міжрівневої оптимізації мережі та управляти динамікою її дій, одночасно використовуючи параметри, що належать множинним рівням у стеку протоколів мережі. Такий підхід може забезпечити істотний ефект при рішенні завдань синтезу траєкторій ризикостійкого розвитку ЗД та РСЕС з врахуванням необхідності інтеграції, обробки та аналізу великого обсягу різнопланової інформації в галузі СЗІ. На основі цього підходу з'являється можливість формування мережі незалежних віртуальних когнітивних центрів (ВКЦ) управління ІБ ЗД та РСЕС. Як видно, підхід заснований на реалізації моделей неявного управління ІБ ЗД та РСЕС через створення адаптивного інтелектуального середовища її забезпечення в рамках віртуального простору країни та, при необхідності, окремих регіонів [8] або окремих КВСО.

Відповідно до [8], вважатимемо, що державний ЦОД у вигляді ВКЦ може являти собою комплекс, призначений для інтелектуальної підтримки прийняття рішень у сфері керування ІБ країни (регіону) у надзвичайних і кризових ситуаціях, а також ситуаціях, які можуть бути визнані такими, що містять загрози ІБ держави. Зважаючи на матеріали, які наведено у [9], основними завданнями ВКЦ і, відповідно, державного когнітивного ЦОД, є моделювання та прогнозування, стратегічне планування, синтез специфікацій взаємодії та моделей координації суб'єктів керування для розв'язку конкретних управлінських завдань у різних областях, у тому числі й у сфері інформаційної підтримки керування комплексною ІБ регіонів як складних соціально-економічних систем.

У якості технологічної основи для створення державного ЦОД, як випливає з [9], доцільно використовувати мультиагентні, хмарні та WEB-технології, а також засоби їх інтеграції [10]. Така концепція забезпечить можливість комплексної інформаційно-аналітичної підтримки прийняття управлінських рішень по забезпеченню встановленого рівня ІБ держави в кризових ситуаціях на оперативному, тактичному та стратегічному рівнях на базі віртуалізації й адаптивного моделювання проблемно-орієнтованої діяльності суб'єктів керування.

Позиціонування державного ЦОД, як гібридного хмарного рішення, робить його інструментарій доступним не тільки суб'єктам керування в області забезпечення ІБ різного рівня та експертам, але й усім зацікавленим державним і комерційним організаціям, що використовують у своїй практичній діяльності Інтернет-технології та засоби телекомунікацій.

У сенсі практичної реалізації когнітивного ЦОД, з [9] відомо, що на сьогоднішній день проведено ряд експериментів по програмній реалізації прототипу ЦОД у вигляді гібридної хмари, яку було побудовано на базі сервісної архітектури IaaS (англ.: *Infrastructure as a Service*, IaaS – Інфраструктура, як сервіс) [11]. Для цього було використано спеціально розроблене програмне забезпечення у вигляді гіпервізора Microsoft Hyper-V Server, хмарної платформи OpenNebula, WEB-сервера Apache, СУБД MySQL, операційної системи Ubuntu 12.04 LTS у якості ядра, що управляє обчислювальними процесам, і компонентів розподіленої агентної платформи [12]. Приведений перелік устаткування та зазначений програмний комплекс забезпечили виконання та підтримку функціонування мобільних програмних агентів, а також спеціалізованих WEB-сервісів, включаючи OpenMeetings, GeoServer, FreeBase, RedMine, Ushahidi, Sage nf ін. Вони були використані:

– для оперативної аналітичної обробки розподілених даних;

– для інтеграції різнорідних інформаційних ресурсів;

– для забезпечення колективної роботи користувачів у мережі Інтернет;

– для забезпечення ІБ користувачів.

З приведеного видно, що існує зацікавленість щодо створення когнітивних ЦОД, але лише для окремих структур у вигляді наборів існуючих програмно-технічних компонентів: єдиної методики з їх розробки не існує.

Як відзначено в [9], програмні агенти когнітивних ЦОД для різнотипних суб'єктів керування, включаючи агенти забезпечення ІБ, були розроблені на платформі JADE з використанням інструментальних засобів AgentBuilder і Cougaar мовою Java у відповідності зі стандартом FIPA та методологією проектування багатоагентних додатків GAIA. Інтеграція сервісів агентів, хмарних та WEB-сервісів у рамках ВКЦ дозволило дослідним суб'єктам керування використовувати сучасні когнітивні інформаційні технології та інструменти моделювання для синтезу погоджених стратегій і прийняття управлінських рішень у кризових ситуаціях в умовах невизначеності та ризику, включаючи ризики ІБ у КВСО. Це свідчить та підтверджує наявність технічних та програмно-інструментальних засобів у разі реалізації методології створення державного когнітивного ЦОД.

Основний інструментарій когнітивного ЦОД повинен включати [9]:

– засоби оперативного та різностороннього моніторингу й аналізу поточних процесів, які можуть існувати у системах забезпечення ІБ держави;

– засоби оперативного прогнозування та стратегічного планування для виконання завдань інформаційної підтримки керування загальною СЗІ у слабо структурованих кризових ситуаціях.

Крім того, як випливає з [9], до складу інструментарію будь-якого когнітивного ЦОД повинні входити технології підтримки колективної роботи експертів у режимі реального часу при наданні інформаційних послуг державним структурам і структурам різних галузей і сфер діяльності, які пов'язані з наданням засобів оперативної аналітичної обробки й проблемно-орієнтованого пошуку інформації для підтримки прийняття управлінських рішень по подоланню кризових і екстремальних ситуацій в області забезпечення ІБ.

Наведений перелік інструментарію державного когнітивного ЦОД повинен забезпечити розв'язок комплексу завдань формалізації, інтеграції, узгодження, обробки, аналізу та інтерактивної візуалізації колективних експертних знань для інформаційної підтримки прийняття управлінських рішень у сфері ІБ, а також моделювання поведінки суб'єктів керування в кризових ситуаціях при виникненні інцидентів у СЗІ державного рівня.

У [13] показано, що для підвищення ефективності взаємодії та задоволення інформаційних потреб суб'єктів керування, уже розроблено прототип віртуального інтеграційного майданчика BarentsNet. Його побудовано у вигляді соціальної когнітивної мережі, яка поєднує професійних експертів у різних соціальних, економічних і технічних областях, а також окремі бізнес-співтовариства та державні структури. Як випливає з зазначеної публікації, КВСО до складу майданчика включені не були. Метою об'єднання було співробітництво в області забезпечення загальної та ІБ з метою аналізу перспективних планів розвитку окремих регіонів. Відзначено, що Web-система BarentsNet інтегрована з інструментарієм когнітивного ЦОД для реалізації пошуку інформаційних і виконавчих ресурсів для рішення конкретних завдань керування, включаючи завдання керування ІБ.

Як результат проведення аналізу нормативної бази встановлено: факторами, що лімітують та впливають на впровадження когнітивних ЦОД, включаючи державний ЦОД, у практичну діяльність суб'єктів ІБ, є її недосконаліть та, як наслідок, складність позиціонування державного ЦОД у структурі державного управління як на регіональному, так і на державному рівнях. Крім того, та обмежена кількість вище розглянутих відомих технології побудови ЦОД передбачає лише фізичну прив'язку державного та регіональних ЦОД до певного місця. У кризових ситуаціях така технологія розміщення ЦОД може привести до його руйнування та до повної втрати функціонування, що веде до катастрофічних наслідків з управління державними та регіональними інформаційними структурами. Отже, враховуючи це, існує потреба у проведенні досліджень щодо розробки загальної моделі (методології) функціональної організації державного ЦОД для управління ІБ з використанням хмарних та агентних технологій з вирішенням проблеми автоматичного переміщення (міграції) державного та регіональних ЦОД, а також даних, які є предметом їх управління, до безпечних сегментів підконтрольного інформаційного простору. Створення подібної структури дозволить гармонійно та ефективно включитися до європейської та світової інфраструктури безпеки, забезпечити оперативну взаємодію в рамках європейських та світових програм протидії розповсюдженню вірусів та іншим протиправним діям. Першим кроком у напряму створення державного ЦОД можна вважати роботу захищеного вузла Інтернет-доступу у вигляді Державного центру безпеки, що функціонує в ДССЗЗІ. На сьогодні через вузол підключено до мережі Інтернет WEB – сайти Президента України та КМ України. Як свідчення ефективності роботи цього вузла Інтернет-доступу – фіксація та локалізація щотижня понад 100 атак.

У [14] зазначено, що одним з найважливіших досягнень у сфері ІБ нашої країни стало прийняття Закону України «Про Національну систему конфіденційного зв'язку України» (НСКЗ). Це створило правові основи для розгортання спеціальної телекомунікаційної системи, призначеної для обміну конфіденційною інформацією. Функціонування НСКЗ дасть змогу вирішити ряд загальнодержавних проблемних питань – передусім забезпечити надійний інформаційний обмін в інтересах органів державної влади та місцевого самоврядування на всій території України. Крім того цей проект є привабливим і з точки зору недержавних та комерційних структур. Необхідно врахувати, що на даний час, постійно поширюється коло недержавних структур, які заінтересовані в обміні конфіденційною інформацією. Окремо слід зазначити той факт, що НСКЗ створюється як система подвійного призначення, частина ресурсу якої може використовуватись у комерційних цілях, тобто участь недержавних структур, як інвесторів, на етапах створення, функціонування та розвитку НСКЗ носить і комерційну привабливість.

Висновки

Враховуючи необхідність постійного адекватного реагування на появу нових загроз для інформації, пов'язаних з лібералізацією суспільних і міждержавних відносин, впровадженням у всі сфери життя особи, суспільства і держави новітніх інформаційних технологій, автоматизованих систем, глобальних телекомунікаційних систем, застосу-

ванням все більш досконалих технічних засобів обробки інформації та зв'язку, розвитком і розповсюдженням технічних засобів несанкціонованого доступу до інформації та впливу на неї, розвиток і вдосконалення СЗІ та ІБ держави повинно бути безперервним у часі процесом. Одним з таких напрямків може бути створення єдиного когнітивного центру обробки даних для національної інформаційної інфраструктури. на нього може бути покладено вирішення всього комплексу важливих і актуальних для держави завдань, який вимагає підтримки та розуміння з боку всіх суб'єктів діяльності в інформаційній сфері, а також забезпечення скоординованого та динамічного розвитку взаємовідносин між цими суб'єктами.

Література

[1]. Казакова, Н. Ф. Моніторинг інформаційних ресурсів в захищених інформаційних мережах [Текст] // Н. Ф. Казакова / Світ інформації та телекомунікацій : VII міжнар. наук.-техн. конф. студентства та молоді, 15-16 квітня 2010 р. — ДУІКТ, Київ. — С. 165-168.

[2]. Казакова, Н. Ф. Розробка формальної моделі когнітивної мережі, яка забезпечує функціонування спеціалізованих екзофакторів моніторингу інцидентів інформаційної безпеки та процеси міграції даних до безпечних сегментів [Текст] // Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів [Звіт про НДР] : (проміжн.) / О. О. Скопа, О. В. Орлик, Н. Ф. Казакова [та ін.] ; кер. О. О. Скопа. — Одеса : ОНЕУ, 2014. — ДР № 0112U007713. — 527 с. — С. 433-454.

[3]. Выявление нарушений информационной безопасности по данным мониторинга информационно-телекоммуникационных сетей [Текст] : дис… канд. техн. наук: 05.13.19 / Ковалев Д. О. — М., 2011. — 170 с.

[4]. Computer Emergency Response Team of Ukraine : [Електронний ресурс] / Портал : cert-gov. — Режим доступу \www/ URL: http://cert.gov.ua/. — Заголовок з екрану, доступ вільний, 12.05.2013.

[5]. Шишаев, М. Г. Использование концепции «User as an expert» в разработке мультипредметных web-ресурсов, основанных на онтологиях [Текст] // М. Г. Шишаев, П. А. Ломов, В. В. Диковицкий / Труды Института системного анализа Российской академии наук. — 2012. — Т. 62. — № 3. — С. 40-47.

[6]. Десятов, И. В. Когнитивные центры как информационные системы для стратегического прогнозирования [Текст] // И. В. Десятов, Г. Г. Малинецкий, С. К. Маненков [и др.]. / Keldysh Institute preprints. — 2010. — № 50. — 28 с.

[7]. Гладун, А. Я. Когнитивные сети и онтологический анализ в повышении адаптивности и качества обслуживания в гетерогенной беспроводной среде [Текст] // А.Я. Гладун, Ю. В. Рогушина / Открытые семантические технологии проектирования интеллектуальных систем = Open Semantic Technologies for Intelligent Systems (OSTIS-2012) : матер. II междунар. научн.-техн. конф., 16-18 февраля 2012 г., Минск / В. В. Голенков (отв. ред.) – Минск : БГУИР, 2012. – С. 493-500.

[8]. Маслобоев, А. В. Мультиагентная информационно-аналитическая среда поддержки управления региональной безопасностью «Безопасный виртуальный регион» [Текст] // А. В. Маслобоев / Scientific and Technical Journal of Information Technologies, Mechanics and Optics. — 2013. — № 4(86). — С. 128-138.

[9]. Черненко, С. С. Применение мониторинга для обеспечения безопасности информационных систем [Електронний ресурс] // С. С. Черненко, А. С. Барабошин, Е. И. Лысенко, Л. С. Духнина / Портал : Современные проблемы науки и образования. — Режим доступу \www/ URL: http://www. science-education.ru/118-14171. — Заголовок з екрану, доступ вільний, 01.02.2015.

[10]. Маслобоев, А. В. Аркхитектура и технологии формирования интегрированной информационной среды поддержки управления безопасностью развития региона

[Текст] // А. В. Маслобоев, М. Г. Шишаев / Scientific and Technical Journal of Information Technologies, Mechanics and Optics. — 2011. — № 6(76). — С. 98-103.

[11]. Грибова, В. В. Проект IACPaaS. Комплекс для интеллектуальных систем на основе облачных вычислений [Текст] // В. В. Грибова, А. С. Клещев, Д. А. Крылов [и др.]. / Искусственный интеллект и принятие решений. — 2011. — № 1. — С. 27-35.

[12]. Маслобоев, А. В. Проблемно-ориентированная агентная платформа для создания полимодельных комплексов поддержки управления безопасностью региона [Текст] // А. В. Маслобоев, А. В. Горохов / Scientific and Technical Journal of Information Technologies, Mechanics and Optics. — 2012. — Т. 2(78). — С. 60-65.

[13]. Маслобоев, А. В. BarentsNet — виртуальная интеграционная площадка для информационной поддержки управления развитием арктических территорий [Текст] // А. В. Маслобоев / Развитие Севера и Арктики: проблем и перспективы : Труды Всероссийск. научн.-практ. конф., 2013 г. — С. 175-177.

[14]. Скриник, О. П. Безпека — необхідна складова сучасних інформаційно-телекомунікаційних систем [Текст] // О. П. Скриник / Computer World. — № 33(377) : [Електронний ресурс] / Портал : ДСТЗІ. — Режим доступу \www/ URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=44614&cat_id=38712&mustWords=%D0%A6%D0%B5%D0%BD%D1%82%D1%80+%D0%BE%D0%B1%D1%80%D0%BE%D0%B1%D0%BA%D0%B8+%D0%B4%D0%B0%D0%BD%D0%B8%D1%85&searchPublishing=1. — Заголовок з екрану, доступ вільний, 12.11.2014.