УДК 004.056:004.621:004.738.5; 004.822:514

Н.Ф. Казакова

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

ПЕРЕДУМОВИ ЩОДО ОРГАНІЗАЦІЇ МІГРАЦІЇ ДАНИХ ЯК МЕТОДУ ПІДВИЩЕННЯ РІВНЯ ЇХ БЕЗПЕКИ

Висвітлена політика держави щодо організації НІІ та сучасної методології забезпечення інфомаційної безпеки у ній, що може бути базою для впровадження нових методів організації безпеки даних та обчислювальних ресурсів. Показано існування проблеми, яка може бути достатньо актуальною з точки зору підвищення рівня захищеності даних та державних інформаційних ресурсів: знаходження найбільш безпечних секторів у межах НІІ та визначення їх технічних потужностей щодо переміщення до них великих обсягів інформації для приховування з метою підвищення рівня їх безпеки.
Ключові слова: *інформаційна безпека, міграція даних, міграція обчислювальних ресурсів, національна інформаційна інфраструктура, моніторинг.*

Н.Ф. Казакова

ПРЕДПОСЫЛКИ К ОРГАНИЗАЦИИ МИГРАЦИИ ДАННЫХ КАК МЕТОДА ПОВЫШЕНИЯ УРОВНЯ ИХ БЕЗОПАСНОСТИ

Освещена политика государства по организации НИИ и современной методологии обеспечения инфомацийний безопасности в ней, что может быть базой для внедрения новых методов организации безопасности данных и вычислительных ресурсов. Показано существование проблемы, которая может быть достаточно актуальной с точки зрения повышения уровня защищенности данных и государственных информационных ресурсов: нахождение наиболее безопасных секторов в пределах НИИ и определения их технических мощностей по перемещению к ним больших объемов информации для сокрытия с целью повышения уровня их безопасности.
Ключевые слова: *информационная безопасность, миграция данных, миграция вычислительных ресурсов, национальная информационная инфраструктура, мониторинг.*

N.F. Kazakova

BACKGROUND TO THE ORGANIZATION OF DATA MIGRATION AS A METHOD OF IMPROVING SAFETY

Illuminated state policy on the organization of a national information infrastructure. Briefly discussed the methodology infomatsiyny ensure security of national information infrastructure. It is noted that the methodology that exists, can be used to introduce new methods of organizing data security and computing resources. The existence of the problem, which may be quite relevant in terms of increasing the level of data protection and public information resources. The problem: finding the safest sectors in the national information infrastructure. The next stage of the problem: the definition of their technical capacity to relocate them large amounts of information to conceal. This will increase the level of their security.
Keywords: *information security, data migration, migration of computing resources, the national information infrastructure monitoring.*

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

Процеси глобальної інформатизації призвели до того, що сучасне суспільство поступове здобуває практично повну залежність від стану безпеки інформаційної інфраструктури. Уразливості національної інформаційної інфраструктури дозволяють недружнім державам, терористичним організаціям, кримінальним групам та окремим зловмисникам нанести країні збиток, порівнянний з впливом зброї масового ураження. Ця обставина вимагає розробки комплексу заходів щодо створення загальнонаціональної системи забезпечення безпеки критично важливих сегментів та об'єктів національної інформаційної інфраструктури (НІІ) на основі єдиного методологічного підходу до ідентифікації критично важливих сегментів і вибору методів та засобів підвищення їх захищеності. Аналіз документів, які є законодавчою та нормативною базою України та які спрямовані на забезпечення процесу розробки зазначених заходів, дозволив виявити невирішені проблеми та сконцентрувати на них увагу. Встановлено, що однією з проблем, яка може бути достатньо актуальною з точки зору підвищення рівня захищеності даних та державних інформаційних ресурсів, але яка, практично, не розглядалася у вітчизняній науковій літературі, це моніторинг найбільш безпечних секторів та їх потужностей у межах НІІ щодо переміщення до них для приховування великих обсягів інформації [1, 2]. Висвітлення передумов щодо вирішення цього питання є ***метою статті***.

Аналіз останніх досліджень і документів, у яких викладено підходи до вирішення проблеми

Численні літературні джерела свідчать, що *національною інформаційною інфраструктурою* є сукупність усіх приналежних країні (державі, її громадянам та юридичним особам) комп'ютерних систем, мереж зв'язку та інформаційних ресурсів, які зберігаються й обробляються в електронній формі, а також організацій, що забезпечують цілеспрямоване функціонування всіх складових інфраструктури.

Як зазначено у ст. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 року №537-16 [3], за умов швидкого розвитку глобального інформаційного суспільства, широкого використання інформаційно-комунікаційних технологій (ІКТ) в усіх сферах життя, особливого значення набувають проблеми інформаційної безпеки (ІБ). З метою визначення поняття про неї у ISO/IEC 13335-1:2004, ГСТУ СУІБ1.0/ISO/ IEC 27001:2010 встановлено терміни про: *цілісність* – властивість інформації, яка полягає в тому, що вона не може бути змінена випадково або навмисно неавторизованими користувачами та (або) процесами; про *доступність* – властивість інформації щодо доступності та використовуваності активів на вимогу авторизованого об'єкта; про *конфіденційність* – властивість інформації не ставати доступною та розкривною для неавторизованих осіб, об'єктів або процесів. Виходячи з цих термінів та згідно до [3], далі у статті *інформаційна безпека* розуміється, як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

– неповноту, невчасність та неймовірність інформації, що використовується;

– негативний інформаційний вплив;

– негативні наслідки застосування інформаційних технологій;

– несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

У [3] відмічено, що вирішення проблеми ІБ має здійснюватися шляхом:

– створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

– вдосконалення нормативно-правової бази щодо забезпечення ІБ, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

– розгортання та розвитку національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Саме зазначені шляхи дозволяють досягти поставленої мети щодо приховування великих обсягів інформації у найбільш безпечних сегментах НІІ.

Викладення основного матеріалу

Зважаючи на вище приведене визначення поняття про НІІ та шляхи вирішення проблеми ІБ, а також враховуючи аналогічні дані з [4], можна зробити висновок про те, що *інформаційна безпека держави* – це стан її захищеності, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам. Забезпечення інформаційної безпеки держави досягається у процесі свідомої цілеспрямованої діяльності органів державного управління по запобіганню можливостям порушення їх нормального функціонування в результаті дії загроз та небезпек, а метою забезпечення інформаційної безпеки держави є створення нормальних умов функціонування конкретного органу державного управління та їх сукупностей, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки [5].

Про необхідність підвищення рівня захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення ІБ держави свідчать положення Указу Президента України від 24 вересня 2001 р. №891/2001 «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних», в якому йдеться про порядок підключення органів виконавчої влади, інших державних органів до іноземних і міжнародних мереж передачі даних, у тому числі до мережі Інтернет; виконання вимог щодо захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах та забезпечення контролю за додержанням цього порядку. Тут же поставлено завдання перед компетентними суб'єктами розробити і внести на розгляд Верховної Ради України проекту Концепції національної інформаційної політики, яка визначатиме основні напрями, засади і принципи національної політики та механізми її реалізації, а також пріоритети розвитку інформаційної сфери, буде спрямована на створення умов для побудови в Україні розвинутого інформаційного суспільства, забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури, впровадження новітніх інформаційних технологій, захист національних моральних і культурних цінностей, забезпечення конституційних прав людини і громадянина на свободу слова та вільний доступ до інформації. Таку Концепцію було внесено на розгляд Верховної Ради 13 жовтня 2010 року та зареєстровано під №7251. Втім до поточного моменту вона не затверджена, так як має ряд суттєвих недоробок. Рішення, яке пропонуються далі, у певному ступені могло б сприяти їх усуненню.

Згідно [6], ІБ будь-якої держави забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері відповідно до прийнятих в установленому порядку взаємопов'язаних та незалежних множин доктрин, концепцій, стратегій і програм, системою заходів політичного, економічного, соціального, військового ха-

рактеру, які є адекватними існуючим та потенційним загрозам і викликам національним інтересам особи, суспільства та держави в інформаційній сфері, а також наявним можливостям держави здійснювати управління ними. Інструментом реалізації такої державної політики інформаційної безпеки є система забезпечення інформаційної безпеки, яка є похідною і детермінованою напрямами державної інформаційної політики. Це, у певній мірі, може бути складовою концепції ведення мережноцентричної війни, яка передбачає збільшення бойової потужності угруповання об‘єднаних сил за рахунок утворення інформаційно-комунікаційної мережі, що об‘єднує джерела інформації (розвідки), органи управління та засоби ураження (придушення). При цьому буде забезпечено доведення до учасників операцій достовірної та повної інформації про обстановку в реальному часі.

Існуючі на сучасному етапі українського державотворення загрози національним інтересам і національній безпеці України, визначені у ст. 7 Закону України «Про основи національної безпеки України», та чинники негативного впливу на стан їх забезпечення, зазначені у Стратегії національної безпеки України, яка затверджена Указом Президента України від 12 лютого 2007 р. №105/2007, потребують вжиття відповідних заходів реагування компетентними державними органами та установами, що визначені законодавцем у ст. 4 Закону України «Про основи національної безпеки України». Відповідно, під час формування державної системи забезпечення ІБ мають бути враховані національні інтереси в інформаційному середовищі, внутрішні та зовнішні загрози цим інтересам і передбачена система засобів виявлення та нейтралізації загроз. Вона обов’язково має включати механізм двостороннього зв’язку між суспільством, засобами масової інформації та державою. З огляду на це та враховуючи [6, 7], забезпечення ІБ передусім повинно здійснюватись шляхом проведення уповноваженими на це суб’єктами виваженої і збалансованої політики держави в інформаційній сфері, яка має три основні напрями:

1) захист інформаційних прав і свобод людини;

2) захист інтересів держави та суспільства в інформаційній сфері;

3) захист національного інформаційного ринку, економічних інтересів держави в інформаційній сфері, національних виробників інформаційної продукції.

Отже, структура системи забезпечення ІБ України (зокрема і структура системи суб’єктів, які її здійснюють) є похідною від тих пріоритетів та завдань, які ставить перед собою держава в інформаційній сфері. Тому саме державна інформаційна політика є визначальною для формування системи забезпечення ІБ, а остання є похідною від неї.

Т.ч., з огляду на наявність гострих проблем, явищ та чинників, що негативно впливають на реалізацію державної політики забезпечення національної безпеки в інформаційній сфері, чим породжують нові загрози національній безпеці та національним інтересам України в цій сфері та негативно впливають на розвиток вітчизняного громадянського суспільства й української держави та реалізацію її євроінтеграційних прагнень, РНБО України 21 березня 2008 року було прийняте рішення про доцільність вжиття невідкладних заходів щодо забезпечення інформаційної безпеки України. Це рішення було затверджене Указом Президента України «Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року «Про невідкладні заходи щодо забезпечення інформаційної безпеки України»» від 23 квітня 2008 року №377/2008. Воно, а також законодавчі та нормативні документи, які регламентують виконання зазначеного Указу, покладені в основу дослідження. Згідно до них, у багатьох пострадянських країнах, включаючи Україну, роботи з рішення проблеми підвищення ІБ НІІ ведуться недостатньо інтенсивно. Ці роботи проводяться різними відомствами, як правило, без загальної координації цієї діяльності з боку держави. У результаті неефективно витрачається велика кількість ресурсів та відсутній державний контроль над цією важливою сферою забезпечення національної безпеки.

Першим кроком до формування загальнодержавного підходу до вирішення проблем ІБ НІІ є розробка загальної методології вибору критично важливих сегментів НІІ і єдиного підходу до забезпечення їх ефективного захисту. До теперішнього часу у світі

сформувалася певна система поглядів на проблему забезпечення їх безпеки і розуміння того, що саме інфраструктурні галузі, і, насамперед, інформаційно-телекомунікаційна інфраструктура, стають найбільш уразливими областями національної безпеки. Під терміном «Критично важливі сегменти й об'єкти» (КВСО) далі будемо розуміти такі підсистеми й об'єкти НІІ, ураження яких може завдати істотної шкоди функціонуванню економіки, національної безпеки й національним інтересам країни. Як випливає з цього, на сьогоднішній день ІБ НІІ є стратегічним завданням державної важливості. Геополітичне й соціально-економічне положення країни, а також підвищення інтересу до її ресурсів з боку провідних світових держав ставлять проблему забезпечення її ІБ на перший план. При цьому вона позиціонується як самостійна проблема, яка вимагає всебічних наукових досліджень. Виходячи з цього, актуальним завданням є розробка нових і розвиток існуючих методів і засобів інформаційно-аналітичної підтримки управління ІБ як загальнодержавної, так і регіональних соціально-економічних систем (ЗД та РСЕС), які можуть зазнати впливу значної кількості різнорідних зовнішніх та внутрішніх деструктивних факторів.

На сьогодні є актуальною проблема, яка відома, як «міграція». Згідно до літературних першоджерел, її суттю є переміщення та адаптація даних та додатків на нову обчислювальну платформу. При цьому виконуються такі процедури, як:

– аналіз даних, консолідація і стандартизація даних з різних джерел;
– підготовка плану міграції;
– розробка інтеграційних шарів між інформаційними системами;
– інтеграція вихідної і цільової систем з метою безпечного перенесення даних;
– відновлення та завантаження даних в нову систему;
– відновлення даних, тестування продуктивності нової системи.

З приведеного переліку видно, що зазначені процедури не описують поняття міграції, а є лише засобами перенесення та адаптації обчислювальних ресурсів на нову програмну платформу. Суттю методу міграції, який мається на увазі, є повне перенесення даних та обчислювальних ресурсів до сегментів НІІ, які можуть бути визначені системами моніторингу, як безпечні у відповідності до встановлених критеріїв, без врахування програмно-технічних складових кінцевої інформаційної мережі. При цьому основою є використання процедур створення віртуальних машин, та збереження загальної технології підготовки міграції у тому вигляді, як це показано у вигляді вище приведеного переліку процедур.

Виходячи з проведеного аналізу законодавчих та нормативних документів, у рамках проблеми забезпечення ІБ НІІ шляхом міграції, перспективним напрямом наукових досліджень є дослідження когнітивних архітектур та розробка методів створення віртуальних проактивних систем, які можуть бути засновані на знаннях та мультиагентних технологіях, що забезпечить міграцію даних та обчислювальних ресурсів до безпечних сегментів інформаційного простору, який контролюється державою. Вони забезпечать фундамент для формування багатофункціональної інформаційної інфраструктури державної та регіональної безпеки на території країни. При цьому мається на увазі, що системи можуть бути такими, що масштабуються або розширюються у відповідності до встановленої множини динамічно мінливих вимог. Саме цій вимозі відповідає когнітивна архітектура, яка у своїй основі містить штучні обчислювальні процеси, що діють як окремі когнітивні системи, або діє по встановлених визначеннях, базуючись на отриманих знаннях про предмет діяльності. З цього витікає, що базою досліджень можуть бути елементи теорії когнітивізму (конструктивізму). Тоді когнітивною інформаційною мережею (структурою) доцільно вважати таку мережу, яка функціонує, базуючись на обробленій інформації, інтерпретуючи її відповідно до вже наявних у неї ретроспективних знань та представлень, а також враховує контекст, у якому отримані дані. У цьому сенсі термін «архітектура» передбачає підхід, який має на увазі моделювання не тільки поведінки об'єкта, а й структурні властивості модельованої системи: когнітивну архітектуру утворюють та визначають підмножини загальних архітектур агентів, що входять до неї. Ког-

нітивна архітектура є основою для роботи інтелектуальних агентів. Основою їх функціонування, в першу чергу, є моніторинг станів досліджуваного об‘єкту; по-друге – оцінка ризиків у залежності від поставлених умов; по-третє – синтез управляючих рішень для реалізації поставленої мети. Створення когнітивної архітектури дозволить так поєднати до цього часу розділені відомі засоби забезпечення ІБ, що показані на рис. 1-а, як це показано на рис. 1-б для когнітивної структури.

ЗАСОБИ ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ ЗАХИСТОМ		
ОЦІНКА СТАНІВ	ФОРМУВАННЯ ВАРІАНТІВ ВПЛИВУ	АДАПТАЦІЯ
ЗАСОБИ ПРОАКТИВНОГО ЗАХИСТУ		
АНАЛІЗ ЗАХИЩЕНОСТІ	ВИЯЛЕННЯ АТАК	ПРОТИДІЯ АТАКАМ
ТРАДИЦІЙНІ ЗАСОБИ ЗАХИСТУ		
ШИФРУВАННЯ	УПРАВЛІННЯ ДОСТУПОМ	КОНТРОЛЬ ЦІЛІСНОСТІ	РЕЄСТРАЦІЯ та ОБЛІК

а)

ЗАСОБИ ПРОАКТИВНОГО УПРАВЛІННЯ ЗАХИСТОМ, ЩО БАЗУЮТЬСЯ НА ЗНАННЯХ			
АНАЛІЗ ЗАХИЩЕНОСТІ	ОЦІНКА СТАНІВ	ФОРМУВАННЯ ВАРІАНТІВ ВПЛИВУ	АДАПТАЦІЯ
ТРАДИЦІЙНІ ЗАСОБИ ЗАХИСТУ			
ШИФРУВАННЯ	УПРАВЛІННЯ ДОСТУПОМ	КОНТРОЛЬ ЦІЛІСНОСТІ	РЕЄСТРАЦІЯ та ОБЛІК

б)

Рис. 1. Групування засобів забезпечення інформаційної безпеки: а – відоме; б – пропоноване до застосування у когнітивній структурі, яке об‘єднує засоби інтелектуального та проактивного управління

Висновки

1) Висвілена політика держави щодо організації НІІ та сучасної методології забезпечення інфомаційної безпеки у ній, що може бути базою для впровадження нових методів організації безпеки даних та обчислювальних ресурсів.

1) Показано існування проблеми, яка може бути достатньо актуальною з точки зору підвищення рівня захищеності даних та державних інформаційних ресурсів: знаходження найбільш безпечних секторів у межах НІІ та визначення їх технічних потужностей щодо переміщення до них великих обсягів інформації для приховування з метою підвищення рівня їх безпеки.

2) Показано, що існує відмінність між процесом міграції, який є засобом перенесення та адаптації обчислювальних ресурсів на нову програмну платформу, та процесом міграції, який забезпечує повне перенесення даних та обчислювальних ресурсів до сегментів НІІ, які можуть бути визначені системами моніторингу, як безпечні у відповідності до встановлених критеріїв, без врахування програмно-технічних складових кінцевої інформаційної мережі.

Література

1. Казакова, Н. Ф. Удосконалення методу моніторингу рівня інформаційної безпеки у спеціальних сегментах національної інформаційної інфраструктури [Текст] / Н. Ф. Казакова, Т. І. Соклакова // Бионика интеллекта. — 2015. — № 1(84). — С. 56-64.

2. Казакова, Н. Ф. Принципы мониторинга информационной инфраструктуры при обеспечении миграции данных в безопасные сегменты [Текст] // Информационные технологии и защита информации в информационно-коммуникационных системах : монография / Н. Ф. Казакова, А. А. Фразе-Фразенко [и др.] ; под ред. В. С. Пономаренко. — Х. : ТОВ «Щедра садиба плюс», 2015. — 486 с. (Русск. яз.).

3. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007—2015 роки» // Відомості Верховної Ради України (ВВР). — 2007. — № 12. — Ст. 102.

4. Нормативно-правове регулювання інформаційної безпеки України [Електронний ресурс] / Портал : pidruchniki. — Режим доступу \www/ URL: http://pidruchniki.com/1507041237027/politologiya/normativno-pravove_regulyuvannya_informatsiynoyi_bezpeki_ukrayini. — Заголовок з екрану, доступ вільний, 18.07.2014.

5. Система забезпечення інформаційної безпеки [Електронний ресурс] / Портал : pidruchniki. — Режим доступу \www/ URL: http:// pidruchniki.com/12631113/politologiya/sistema_zabezpechennya_informatsiynoyi_bezpeki#36. — Заголовок з екрану, доступ вільний, 18.07.2014.

6. Система державних суб'єктів забезпечення інформаційної безпеки України та шляхи її вдосконалення [Електронний ресурс] / Портал : pidruchniki. — Режим доступу \www/ URL: http://pidruchniki.com/1501092237031/politologiya/sistema_derzhavnih_subyektiv_zabezpechennya_informatsiynoyi_bezpeki_ukrayini_shlyahi_vdoskonalennya#11. — Заголовок з екрану, доступ вільний, 18.07.2014.

7. Petrov, A. Analiza stanu bezpieczeństwa ekonomicznego w sferze nowoczesnej ekonomii i biznesu [Текст] / Anton Petrov, Mikołaj Karpiński, Nadiya Kazakova // Zeszyty Naukowe Wyższej Szkoły Finansów i Prawa. — Bielsko-Biała : Wyższa Szkoła Finansów i Prawa. — 2013. — № 4. — S. 27-38.