Вдосконалення Методу Моніторингу Цифрових Слідів Інцидентів Інформаційної Безпеки у Сегментах Національної Інформаційної Інфраструктури

Надія Казакова
кафедра комп'ютерних та інформаційно-вимірювальних технологій
Одеська державна академія технічного регулювання і якості
Одеса, Україна
kaz2003@ukr.net

Олексій Фразе-Фразенко
кафедра комп'ютерних та інформаційно-вимірювальних технологій
Одеська державна академія технічного регулювання і якості
Одеса, Україна
frazenko@gmail.com

Monitoring Method Improvement of Information Security Incidents Digital Traces In National Information Infrastructure

Nadiia Kazakova
Department of computer, information and measurement technologies
Odesa State Academy of Technical Regulation and Quality
Odesa, Ukraine
kaz2003@ukr.net

Oleksii Fraze-Frazenko
Department of computer, information and measurement technologies
Odesa State Academy of Technical Regulation and Quality
Odesa, Ukraine
frazenko@gmail.com

***Анотація*—У межах вирішення проблеми виявлення найбільш захищених сегментів національної інформаційної інфраструктури засобами моніторингу сегментів інформаційного простору спеціального призначення, розглядається метод моніторингу стану безпеки заданих сегментів інфраструктури. Показано, що пропоновані удосконалення дозволяють забезпечити підвищення ймовірності оцінювання їх стану по відношенню до захищеності. Враховано, що характеристики сегментів містять велику кількість контрольованих параметрів, які з метою підвищення ефективності роботи систем моніторингу можуть бути об'єднані у відповідності до їх вагових внесків в окремих елементах, що підтримують функціонування різноманітних складових та процесів у системах забезпечення інформаційної безпеки.**

***Abstract*—Within solving the problem of the national information infrastructure most protected segments identifying by the tools of segment information space special purpose monitoring, the method of infrastructure safety monitoring of defined segments is considered. It is shown that the offered improvements allow to provide increase in probability of estimation of their state in relation to security. It is considered that characteristics of segments contain a large number of controlled parameters which for the purpose of increase in overall performance of monitoring systems can be integrated according to their weight contributions in separate elements which support functioning of different components and processes in systems of information security ensuring.**

Ключові слова—інформація; безпека; інформаційна інфраструктура; параметр; моніторинг; інформаційний простір

Keywords—information; security; information infrastructure; parameter; monitoring; information space

I. Вступ

Тривалий час застосування традиційних засобів захисту інформації, таких як системи розмежування прав доступу, використання міжмережевих екранів, антивірусного програмного забезпечення тощо, було стандартним методом забезпечення інформаційної безпеки (ІБ) будь-якої комунікаційної системи чи мережі. Відомості про їх роботу та ефективність можуть бути використані на новому етапі розвитку систем захисту інформації (СЗІ) щодо забезпечення ІБ, а саме – системами моніторингу інформаційного простору з метою виявлення його найбільш безпечних та захищених сегментів для переміщення (міграції) до них обчислювальних ресурсів та даних, що забезпечить підвищення ступеню їх конфіденційності, цілісності та доступності. Такий підхід передбачає постійний динамічний процес моніторингу стану інформаційних процесів, що пов‘язані з забезпеченням ІБ, і з часом може стати невід‘ємною частиною ідеології функціонування національної інформаційної інфраструктури (НІІ) [1, 2].

Застосування систем моніторингу НІІ з метою організації міграції даних суттєво підвищить ефективність наявних в інформаційній системі засобів забезпечення ІБ за рахунок синергетичного ефекту при обробці інформації

II. Метод моніторингу цифрових слідів інцидентів інформаційної безпеки

Методологія забезпечення ІБ державних ресурсів, яка передбачає їх міграцію до найбільш безпечних сегментів інформаційного простору, що може контролюватися єдиним центром обробки даних (ЦОД), вимагає використання різних засобів виявлення у них слідів мережевих атак, наявності та ефективності систем захисту від спаму, дієвості антивірусних засобів, ефективності міжмережевих екранів та сканерів безпеки, доступності, надійності та ефективності обчислювальних та інших технічних ресурсів [3]. При цьому розуміється, що доступ до відомостей, які характеризують зазначене, може бути забезпечений на основі відповідних угод між суб’єктами, які обслуговуються єдиним ЦОД.

Далі під загальним поняттям «ЦОД», який формуватиме управляючі впливи стосовно міграції даних, будемо розуміти комплексне організаційно-технічне рішення, метою функціонування якого є створення та підтримка високопродуктивної та відмовостійкої інформаційно-телекомунікаційної інфраструктури у межах виділеного інформаційного простору. Його загальним завданням буде ефективне консолідоване зберігання та обробка даних користувачів з одночасним наданням їм прикладних сервісів та підтримка функціонування корпоративних додатків. Обробка отриманих даних веде до зростання множини апаратно-програмних засобів забезпечення ІБ та суттєвого росту обсягів інформації, яка може бути необхідною для контролю мережевої безпеки. Відповідно, існує необхідність автоматизації зазначених процесів з метою підвищення продуктивності робіт з обробки даних, та рішення завдань щодо оперативності прийняття управляючих рішень для організації міграції даних та обчислювальних ресурсів. Це дозволить вирішити протиріччя між значним зростанням обсягів інформації, яка обробляється та аналізується для встановлення рівня безпеки визначених мережевих ресурсів, наявності загроз для них та їх ступенем, та оперативністю управління міграцією [4].

У межах вирішення проблеми виявлення безпечних сегментів НІІ на основі застосування систем моніторингу сегментів інформаційного простору спеціального призначення (СМСІПСП) [5, 6], розглянемо метод моніторингу стану безпеки заданих сегментів НІІ, який забезпечує підвищення ймовірності оцінювання їх стану по відношенню до захищеності [2, 7]. Враховуватимемо, що кожна з характеристик сегментів НІІ містить велику кількість контрольованих параметрів, які з метою підвищення ефективності роботи СМСІПСП можуть бути об‘єднані у відповідності до їх вагових внесків у окремих елементах, які забезпечують функціонування різноманітних складових та процесів у системах забезпечення ІБ [8]. Групування може виконуватися у тих випадках, коли є доцільним врахування динаміки керування часовими проміжками при ухваленні управляючих рішень щодо стану захищеності сегментів НІІ та врахування ступеню впливу груп контрольованих параметрів та величин відхилення їх значень від заданих.

Згідно до [7], існує метод, відповідно до якого моніторинг стану систем забезпечення ІБ в деякій системі, базується на попередньо заданій множині з $X > 2$ контрольованих параметрів безпеки. Крім того, метод передбачає, що $Y \geq X$ зразкових значень параметрів безпеки, які підлягають контролю, а також їх вагові коефіцієнти $k^{ваг}$, є заданими.

Маючи зазначені дані у якості вхідних параметрів, може бути виконаний аналіз, суть якого полягає у здійсненні наступних процедур:

- вимірювання значень контрольованих параметрів безпеки;
- порівняння їх зі зразками;
- формування звіту;
- формування управляючого рішення щодо стану систем забезпечення ІБ.

Згідно до [7], можливе додаткове формування $Z \geq 2$ груп параметрів, які підлягають контролю, з числа попередньо заданих контрольованих параметрів. Така процедура є необхідною у зв‘язку з тим, що кожна z-а група контрольованих параметрів, де $z = 1,2,...,Z$, є окремою характеристикою стану ІБ z-го структурного елемента або функціонального процесу, які відбуваються у системі, що контролюється засобами СМСІПСП. Вважається, що коефіцієнти важливості $k_z^{ваг}$ є незалежними та можуть бути задані для кожної z-ї групи. Для кожної такої групи параметрів повинно бути задано максимальне Δt_z^{max} та мінімальне Δt_z^{min} значення проміжків часу, протягом яких відбувається вимірювання

параметрів, що контролюються, а також момент часу $t_z^{звіт}$, який передбачає формування звіту про стан безпеки досліджуваної системи.

До процедури встановлення попередніх параметрів також може бути віднесено зазначення інтервалу часу вимірювань параметрів, що контролюються, наприклад, для z-ї групи, який дорівнює максимальному, тобто Δt_z^{max}. Після виконання процедури порівняння виміряних значень з заданими зразками, при їх співпадінні, цикл аналізу безпеки системи повинен бути повторений до настання моменту часу $t_z^{звіт}$ формування звіту про безпеку системи – у випадку, який розглядається, це досліджуваний сегмент НІІ. Якщо при порівнянні значення отриманих параметрів не співпадають зі встановленими зразками, то їх запам'ятовують або заносять до бази даних.

Після виконання процедури порівняння, необхідно внести корективи значень часових інтервалів вимірювань, $\Delta t_z^{кор} = \frac{\Delta t_z^{max}}{k_z^{ваг}}$. Далі необхідно отримане значення $\Delta t_z^{кор}$ порівняти з мінімальним Δt_z^{min}. Якщо $\Delta t_z^{кор} = \Delta t_z$, то цикл аналізу безпеки необхідно виконати повторно, а у протилежному випадку, коли $\Delta t_z^{кор} \le \Delta t_z^{\min}$, формується повідомлення про вихід контрольованих параметрів в z-й групі за межі припустимих значень. Як наслідок, СМСІПСП реєструє наявність порушень у системі забезпечення ІБ у контрольованому сегменті.

Аналіз приведеного методу виявив, що для забезпечення достовірного знаходження слідів інцидентів ІБ у спеціальних сегментах НІІ, необхідно достатньо часто та з високою вірогідністю виконувати моніторинг та аналіз параметрів, які характеризують стан СЗІ у них. Окрема актуальна задача – вчасне формування звітів про стан ІБ та передавання його до вищого рівня ієрархії СМСІПСП з метою формування управляючого рішення. Процедура моніторингу параметрів, що визначають стан систем захисту досліджуваної системи, здійснюється на основі локального зчитування їх значень з оперативної пам'яті контрольованих елементів та порівняння зі зразками. Процедура виконується на основі протоколів мережної взаємодії. Таким чином, значення параметрів СМСІПСП отримуються з оперативної пам'яті, що унеможливлює використання процедури для отримання відомостей про ретроспективний стан систем забезпечення ІБ у контрольованому середовищі. Відповідно, необхідно виконати її удосконалення з метою отримання значень параметрів з журналів реєстрації інцидентів ІБ зі збереженням показників економічної ефективності.

III. Вдосконалення методу моніторингу цифрових слідів інцидентів інформаційної безпеки

Вважатимемо, що контрольовані сегменти НІІ є складними інформаційними технічними структурами та містять велику кількість елементів, які підтримують функціонування систем забезпечення ІБ. У загальному випадку для моніторингу ретроспективних станів безпеки інформаційної структури, значна частина ресурсів, наприклад, відомостей про пропускну здатність каналів зв'язку, що змінена внаслідок DDos-атаки, не можуть бути отримані без даних про те, як вона функціонувала у штатному режимі. Збільшення ж множини значень про сукупні контрольовані ресурси шляхом розгортання локальної системи моніторингу веде до значних економічних затрат. З метою вирішення питання використаємо узагальнену схему (рис. 1), яка пояснює групування параметрів структурних елементів досліджуваної системи.

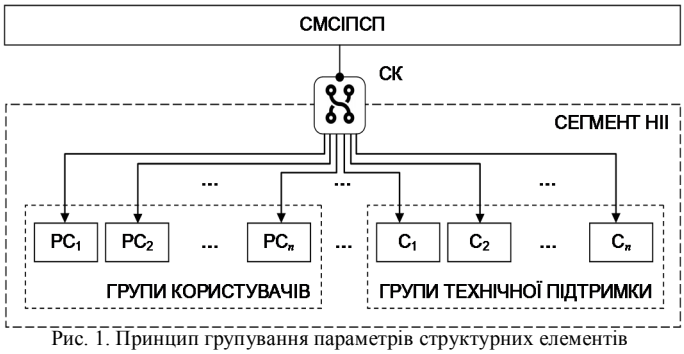


Рис. 1. Принцип групування параметрів структурних елементів досліджуваної системи, де: PCN – робочі станції, CN – сервери, комутатори та маршрутизатори, які програмно керуються; СК – системний комутатор, що управляється СМСІПСП

Організація системи моніторингу, яка приведена на рис. 1, дозволяє СМСІПСП визначати ті об'єкти у структурі сегменту НІІ, які задані завданням щодо визначення станів їх безпеки і, т.ч., управляти отриманням значень параметрів з журналів реєстрації інцидентів ІБ. При цьому підконтрольними СМСІПСП і, відповідно, державному ЦОД, будуть відомості про наступні дані, які мають відношення до інцидентів інформаційної безпеки:

- перелік активних логічних портів, які були задіяні у інцидентах (АЛП);
- про Ір-адреси, які були задіяні у створені інцидентів (ІР-адр);
- про вплив інцидентів на активність диспетчера підключень дистанційного доступу (АДПДД);
- про порушення вимог захисту даних у службах папок обміну даними (ЗДСПОД);
- про порушення локальних налаштувань сервера служби файлового обміну (ЛНССФО).
- про порушення локальних налаштувань захисту служб електронної пошти (ЛНЗСЕП);
- про порушення локальних налаштувань користувацького клієнта служб файлового обміну (ЛНККСФО);

У залежності від коефіцієнтів важливості $k_z^{ваг}$, відомості можуть бути об'єднані у групи, що підвищить ефективність роботи СМСІПСП. Відповідно до [7], доцільним є їх об'єднання у вигляді, наведеному на рис. 2, де також відзначено додаткові характеристики

структурних елементів контрольованого сегменту (відповідно до рис. 1).

Встановимо, що контрольований сегмент НІІ є множиною функціональних вузлів та телекомунікаційного обладнання. На рис. 1 наведено умовний досліджуваний сегмент, який керує з'єднаннями та управляється СМСІПСП. Ним, на основі використання закріплених ідентифікаторів, визначається множина технічних та програмних активів, які підлягають моніторингу. У якості ідентифікаторів найбільш доцільним є застосування мережних адрес з сімейства протоколів TCP/IP [7].

Для перевірки практичного застосування методу та окремих функцій з його удосконалення, встановимо, що множина функціональних вузлів та телекомунікаційного обладнання забезпечує: виконання функціональних процесів з контролю за обміном файлів, виконання функціональних процесів щодо контролю передавання електронної пошти, виконання функціональних процесів у межах мережної взаємодії.

Ці процеси є найбільш характерними при їх дослідженні з метою виявлення наслідків впливу інцидентів ІБ. При практичній перевірці журналів реєстрації інцидентів найбільш просто організувати доступ саме до них. В подальшому розумітимемо, що для СМСІПСП доступ до журналів забезпечується на основі відповідних договорів.

Записи у журналах активності, які підлягають моніторингу та аналізу, базуються на контролюванні функціональних процесів ІБ у точках входу до робочих додатків, які відповідають логічним портам на яких реалізується робочий процес. Кожна множина функціональних вузлів та телекомунікаційного обладнання, а також їх функціональні процеси, характеризуються деякою попередньо встановленою сукупністю параметрів, що описують стан їх ІБ і, т.ч., ці відомості реєструються у журналах та є досяжними для СМСІПСП. До них, як до елементів сегменту, що досліджується засобами СМСІПСП, віднесемо такі ж відомості, які наведено вище та згрупуємо (рис. 2).

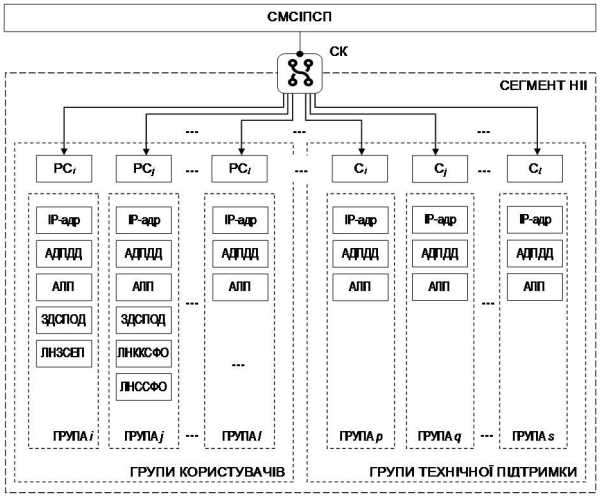
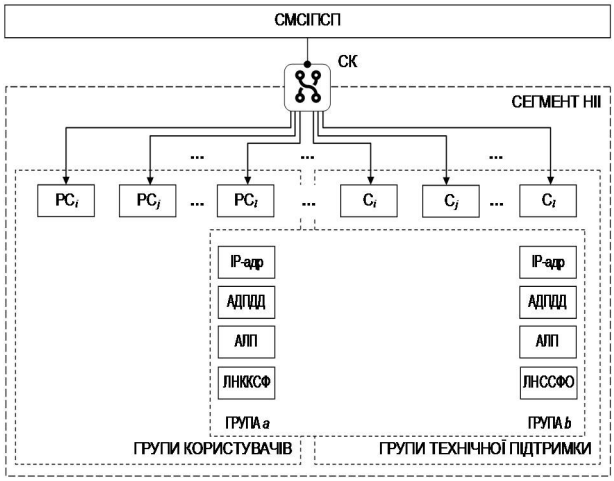
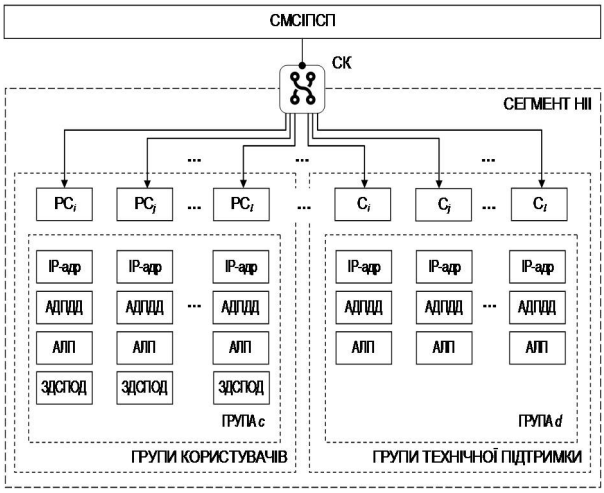


Рис. 2. Узагальнене групування додаткових характеристик структурних елементів контрольованого сегменту

Як видно з нього, взаємозв'язок параметрів контрольованих функціональних процесів ІБ у точках входу до робочих додатків, викликає необхідність їх додаткового групування. Це будуть 4 групи відомостей про інциденти ІБ у службах, що підтримують відповідно: a − обіг файлів; b − функціонування електронної пошти; c − функціонування папок обміну; d − мережевої взаємодії. Зазначені групи відображено на рис. 3.



а)



б)

Рис. 3. Додаткові групи відомостей про інциденти ІБ: a – відомості про загальне використання додатків користувачами та технічною підтримкою; б – відомості про розмежоване використання додатків користувачами та технічною підтримкою

Засоби контролю за інцидентами, які відносяться до приведених груп, внесуть записи до відповідних розділів журналів активності при їх виникненні. Це призведе до значного спрощення та пришвидшення роботи СМСІПСП. При цьому повинно враховуватися, що для кожної групи параметрів, що контролюються, та яка сформована у відповідності до приведеної схеми, попередньо задаються вагові коефіцієнти у відповідності до важливості групи, тобто у відповідності до ступеню порушення інцидентом ІБ гарантованого рівня конфіденційності, цілісності та доступності інформації у контрольованому сегменті.

Крім того, їх значення, а також зразкові величини (чи вимоги), повинні враховувати дані про важливість інформації та можливі потенційні вразливості контрольованих функціональних процесів ІБ. Для цього можуть бути використані методики, що базуються на достатньо відомих методах неформальної логіки та методах залучення експертів. При цьому, найбільш доцільним та ефективним для розрахунку надійності та достовірності отримання даних системами СМСІПСП є завдання значень параметрів у вигляді матриці. Пропонується, для ефективного рішення питання надійного та достовірного отримання даних про інциденти ІБ використання теорії псевдонапівзворотних матриць [14].

Як випливає з вище приведеного, врахування сукупності визначальних ознак веде до реалізації можливості комплексної оцінки стану параметрів у системах забезпечення ІБ з одночасною мінімізацією використовуваних ресурсів, а також використанням можливості адаптивного управління характеристиками процесу моніторингу. Це свідчить про те, що реалізація методу є можливою без доповнення контрольованих сегментів НІІ додатковими активними сенсорами, які виконують моніторинг стану СЗІ. Це, у свою чергу, веде до підвищення ймовірності оцінювання стану захищеності контрольованих сегментів з одночасним підвищенням економічної ефективності СМСІПСП у цілому. В основу роботи СМСІПСП, з незначними доробками, може бути покладено алгоритм, який наведено, наприклад, у [7]. Згідно до зазначеного джерела, алгоритм може забезпечити виявлення цифрових слідів інцидентів ІБ у контрольованих сегментах НІІ.

IV. Висновки

В процесі моніторингу слідів інцидентів ІБ у журналах записів, з високою ймовірністю можна виявити не тільки факт відмінності значень параметрів, що контролюються, від заданих, але й за рахунок їх групування по ваговому внеску підвищити ймовірності оцінювання стану захищеності контрольованого сегменту НІІ. Динамічне управління інтервалом часу прийняття управляючого рішення про ретроспективний стан безпеки сегменту НІІ забезпечує підвищення економічної ефективності СМСІПСП, що є додатковим обґрунтуванням актуальності викладеного.

Наведені дані можуть бути використані для подальшого розвитку теорії забезпечення ІБ у інформаційних структурах, а також для вирішення загальної науково-прикладної проблеми з розробки моделей та комплексних методів проактивного забезпечення ІБ в когнітивних мережах, у яких основою побудови та управління є SDN-технології. При цьому може бути враховано існування некоректних задач, пов’язаних з невизначеністю процесів у СМСІПСП [9], та деструктивних впливів [10], які порушують вимоги щодо конфіденційності, цілісності та доступності. Рішення зазначеної проблеми, в порівнянні з існуючими принципами функціонування комплексних СЗІ, дозволяє розробити концепцію безпечної міграції даних та обчислювальних ресурсів у межах хмарних структур, а також розширити теоретичні та практичні межі загальних принципів функціонування СЗІ у них, що веде до підвищення ступеня захисту інформаційних процесів, які володіють властивостями невизначеності [11]. Доцільними питаннями, які є перспективними щодо подальших досліджень у галузі забезпечення ІБ, є питання надійності та живучості СМСІПСП [12, 13].

Література References

[1] О. О. Скопа, Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем [Текст] / О. О. Скопа, Н. Ф. Казакова // Системи обробки інформації. — Харків : Харківський ун-т Повітряних Сил ім.І.Кожедуба. — 2009. — № 7(79). — 2009. — С. 48-54.

[2] Н. Ф. Казакова, 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.

[3] Н. Ф. Казакова, Оцінка живучості систем моніторингу інформаційного простору [Текст] / Н. Ф. Казакова // Восточно-европейский журнал передовых технологий. — Харьков : Технологический центр. — 2012. — № 4/2(58). — С. 12-15.

[4] Н. Ф. Казакова, Визначення показників для вирішення завдань прогностичного контролю мультисервісних телекомунікаційних мереж / Н. Ф. Казакова, О. О. Скопа // Сучасний захист інформації. — К. : ДУІКТ. — 2010. — Спецвипуск (4). — С. 55-61.

[5] Н. Ф. Казакова, Застосування програмно реалізованого прогностичного контролю для вирішення практичних завдань забезпечення якості надання послуг у захищених інформаційних мережах / Н. Ф. Казакова // Сучасна спеціальна техніка. — К. : Державний науково-дослідний інститут МВС України. — 2012. — № 2(29). — С. 86-95.

[6] О. О. Скопа, Проблематика якості послуг інтернет-провайдерів / О. О. Скопа, С. Л. Волков, К. Б. Айвазова // Збірник наукових праць Одеської державної академії технічного регулювання та якості. — 2013. – № 1(2). — С. 27-31.

[7] Спосіб моніторингу безпеки автоматизованих систем : пат. № 2355024 : МПК G06F15/00, G06F17/00 / О. С. Євстигнєєв К. М. , Зорін, М. О. Карпов [та ін.] ; заявник та патентообладач Військова академія зв‘язку ім. С. М. Будьонного ; заявл. 12.02.2007 ; опубл. 10.05.2009.

[8] С. Л. Волков, Оптимізація параметрів телекомунікаційної мережі методом статистичної регуляризації / С. Л. Волков, Н. Ф. Казакова // Сучасна спеціальна техніка. — К. : Державний науково-дослідний інститут МВС України. — 2012. — № 1(28). — С. 54-60.

[9] Н. Ф. Казакова, Некоректні задачі відновлення даних у системах моніторингу інформаційного простору / Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. — Луганськ : СНУ ім. В.Даля. — 2012. — № 8(179). — Т. 1. — С. 325-332.

[10] О. В. Грабовський, Регуляризація визначення показників якості функціонування ІВС з врахуванням нечіткості інформації / О. В. Грабовський, С. Л. Волков, О. О. Скопа // Вісник Національного технічного університету «ХПІ» : Нові рішення в сучасних технологіях. — 2013. — №26 (999). — С.169-174.

[11] О. О. Скопа, Інтелектуальні автономні системи: концептуальні положення створення та функціонування / О. О. Скопа, Є. В. Вавілов // Бионика интеллекта. — 2013. — №1(80). — С. 35-40.

[12] О. В. Грабовський, Скорочення випробувань надійності ІВС за рахунок її функціональної надмірності / О. В. Грабовський, Н. Ф. Казакова // Технологічний аудит та резерви виробництва. — 2013. — №2/1(10). — С. 24-27.

[13] О. О. Скопа, Концепція контрольних випробувань резервних систем на основі біноміальної схеми / О. О. Скопа, С. Л. Волков, А. В. Мінін // Інформаційна безпека. — 2011. — №2(6). — С.69-76.

[14] С. А. Петренко, Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. — М. : АйТи; ДМК Пресс, 2004. — 384 с.