УДК 004.738.5:681.14, 621.396:681.142:004.621

Н.Ф. Казакова[1], Т.І. Соклакова[2]
[1]ОНЕУ, м. Одеса, Україна, kaz2003@ukr.net
[2]ХНУРЕ, м. Харків, Україна, Tetiana_Soklakova@yahoo.com

УДОСКОНАЛЕННЯ МЕТОДУ МОНІТОРИНГУ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СПЕЦІАЛЬНИХ СЕГМЕНТАХ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

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.

ІНФОРМАЦІЯ, БЕЗПЕКА, ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА, ПАРАМЕТР, МОНІТОРИНГ, ІНФОРМАЦІЙНИЙ ПРОСТІР

Вступ

Ще у недалекому минулому застосування традиційних засобів захисту інформації було стандартним методом забезпечення інформаційної безпеки (ІБ) будь-якої комунікаційної системи чи мережі. Ними були та є на поточний момент системи розмежування прав доступу, використання міжмережевих екранів, антивірусного програмного забезпечення та ін. 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 їх ступеню конфіденційності, цілісності та доступності. Такий підхід, при якому виконуватиметься 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 (НІІ) [1, 2].

Застосування систем моніторингу НІІ з метою організації міграції даних у значному степені підвищить ефективність засобів забезпечення ІБ, які вже є в інформаційній системі, за рахунок синергетичного ефекту при обробці інформації.

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.

Вирішення питань, які пов'язані з науково-прикладною задачею, що винесена у заголовок, та проблемами, які корелюються з нею у сенсі розробки моделей та комплексних методів проактивного забезпечення інформаційної безпеки в когнітивних мережах, у яких основою побудови та управління є SDN-технології, з врахуванням існування некоректних задач, пов'язаних з невизначеністю процесів у системах моніторингу, а також відновленням даних у них, започатковано у працях достатньо обмеженої кількості членів наукової спільноти. Найбільш відомі серед вітчизняних вчених, це О. Корченко, А. Горбенко, В. Бурячок, Г. Гулак, М. Дивизинюк, В. Хорошко, О. Шумейко, В. Баранов, А. Засядько, С. Лєнков, М. Шелест, О. Голубенко, В. Харченко, Ю. Яремчук, О. Рибальський, Л. Пархуць, О. Скопа, О. Петров, В. Бабак, В. Кудінов, М. Корнійчук, В. Коваль, А. Гладун; серед зарубіжних – R. Whiteley, S. Prentice, G. Dewnarain, D. Vellante, J. Gantz, D. Reinsel, L. Hiebert, J. Feldhan. Результати, які ними отримано, свідчать про актуальність завдання, та доцільність подальших досліджень у зазначеній предметній області.

1. Передумови удосконалення методу моніторингу цифрових слідів інцидентів інформаційної безпеки

Вважатимемо, що далі під загальним поняттям «ЦОД», який формуватиме управляючі впливи стосовно міграції даних, вважатимемо комплексне організаційно-технічне рішення, метою функціонування якого є створення та підтримка високопродуктивної та відмовостійкої інформаційно-телекомунікаційної інфраструктури у межах виділеного обмеженого інформаційного простору. Нехай його загальним завданням буде ефективне

консолідоване зберігання та обробка даних користувачів з одночасним наданням їм прикладних сервісів та підтримка функціонування корпоративних додатків. У такому разі 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. З цього слідує висновок про те, що існує необхідність автоматизації зазначених процесів з метою підвищення продуктивності робіт з обробки даних, та до рішення завдань щодо оперативності при прийнятті 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 інформаційної безпеки [8]. Як показано у цьому джерелі, 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 інформаційної безпеки 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 $k^{\text{ваг}}$, 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 інформаційної безпеки.

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 інформаційної безпеки z-го структурного елемента або функціонального процесу, які відбуваються у системі, що контролюється засобами СМСІПСП. Вважається, що коефіцієнти важливості $k_z^{\text{ваг}}$ є незалежними та можуть бути задані для кожної z-ї групи. Для кожної такої групи параметрів повинно бути задано максимальне $\Delta t_z^{\max}$ та мінімальне $\Delta t_z^{\min}$ значення проміжків часу, протягом яких відбувається вимірювання параметрів, що контролюються, а також момент часу $t_z^{\text{звіт}}$, 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 $\Delta t_z^{\max}$. Після виконання процедури порівняння виміряних значень з заданими зразками, при їх співпадінні, цикл аналізу безпеки системи повинен бути повторений до настання моменту часу $t_z^{\text{звіт}}$ формування звіту про безпеку системи – у випадку, який розглядається, це досліджуваний сегмент НІІ. Якщо при порівнянні виявляється, 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, а саме:

$$\Delta t_z^{\text{кор}} = \frac{\Delta t_z^{\max}}{k_z^{\text{ваг}}}. \qquad (1)$$

Далі необхідно отримане значення $\Delta t_z^{\text{кор}}$ порівняти з мінімальним $\Delta t_z^{\min}$. Якщо $\Delta t_z^{\text{кор}} = \Delta t_z$, то цикл аналізу безпеки необхідно виконати повторно, а у протилежному випадку, коли $\Delta t_z^{\text{кор}} \leq \Delta t_z^{\min}$, формується повідомлення про вихід контрольованих параметрів в z-й групі за межі припустимих значень. Як наслідок, СМСІПСП реєструє наявність порушень у системі забезпечення інформаційної безпеки у контрольованому сегменті.

Аналіз приведеного методу виявив, що для забезпечення достовірного знаходження слідів інцидентів інформаційної безпеки у спеціальних сегментах НІІ, необхідно достатньо часто та з високою ймовірністю виконувати моніторинг та аналіз параметрів, які характеризують стан систем захисту інформації у них. Окрема актуальна задача – вчасне формування звітів про стан інформаційної безпеки 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. Про-

цедура виконується на основі протоколів мережної взаємодії. Як видно з цього, значення параметрів СМСІПСП отримуються з оперативної пам'яті, що унеможливлює її використання для отримання відомостей про ретроспективний стан систем забезпечення інформаційної безпеки у контрольованому середовищі. Відповідно, необхідно виконати її удосконалення з метою отримання значень параметрів з журналів реєстрації інцидентів інформаційної безпеки зі збереженням показників економічної ефективності.

2. Рішення щодо впровадження 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.

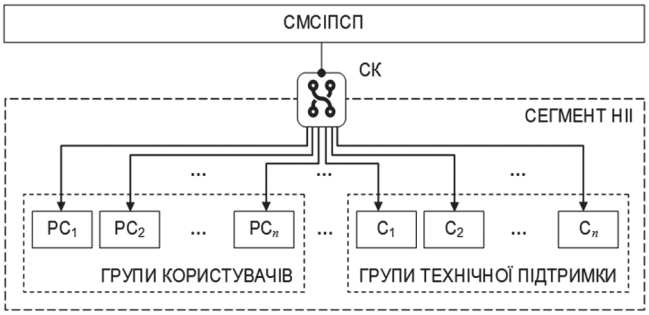


Рис. 1. Принцип групування параметрів структурних елементів досліджуваної системи, де: PC_N – робочі станції, C_N – сервери, комутатори та маршрутизатори, які програмно керуються; СК – системний комутатор, що управляється СМСІПСП

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 (АЛП), які були задіяні у інцидентах;

– про IP-адреси, які були задіяні у створені інцидентів (IP-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 настроювання сервера служби файлового обміну (ЛНССФО).

– про порушення локальних настроювань захисту служб електронної пошти (ЛНЗСЕП);

– про порушення локальних настроювань користувацького клієнта служб файлового обміну (ЛНККСФО);

У залежності від коефіцієнтів важливості $k_z^{\text{ваг}}$, відомості можуть бути об'єднані у групи, що підвищить ефективність роботи СМСІПСП. Так, у [7] зазначено, що доцільним є їх об'єднання у такому вигляді, як це показано на рис. 2, де також приведено додаткові характеристики структурних елементів контрольованого сегменту (відповідно до рис. 1).

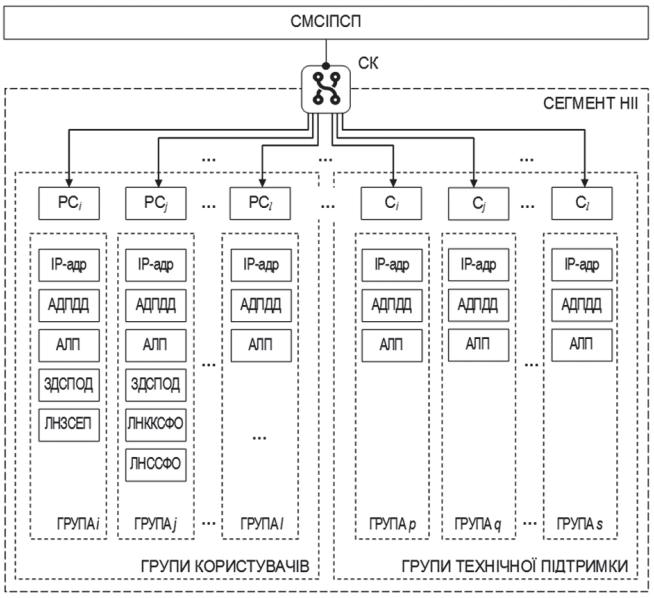


Рис. 2. Узагальнене групування додаткових характеристик структурних елементів контрольованого сегменту

Встановимо, що контрольований сегмент НІІ є множиною функціональних вузлів та телекомунікаційного обладнання. Їх зв'язок забезпечується фізичними засобами у вигляді ліній зв'язку з різноманітною реалізацією. Умовно це показано на рис. 1, де приведено умовний досліджуваний сегмент у вигляді множин робочих станцій, серверів, комутаторів та програмно-керованих маршрутизаторів, а також системного комутатора, 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 є найбільш доцільним застосування мережних адрес з сімейства протоколів TCP/IP [7], що використано далі.

З метою спрощення опису та 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 інформаційної безпеки у точках входу до робочих додатків. Точки 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 приведено вище у попередньому списку, та згрупуємо їх так, як показано на рис. 2. 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:

– група *a*: у службах, що підтримують обіг файлів;

– група *b*: у службах, що підтримують функціонування електронної пошти;

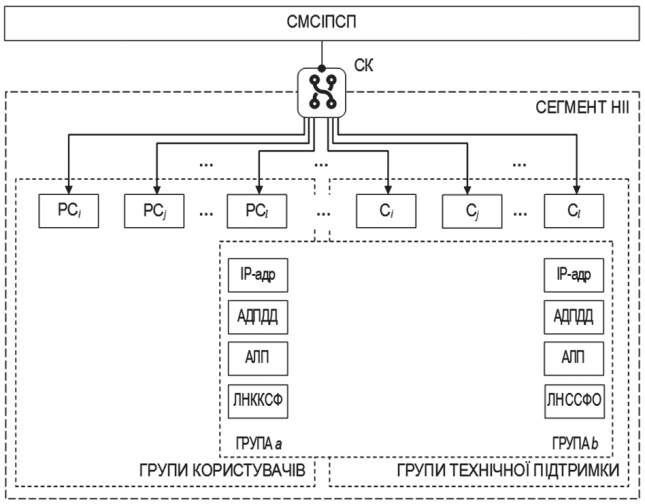
– група *c*: у службах, що підтримують функціонування папок обміну;

– група *d*: у службах, що підтримують функціонування мережевої взаємодії.

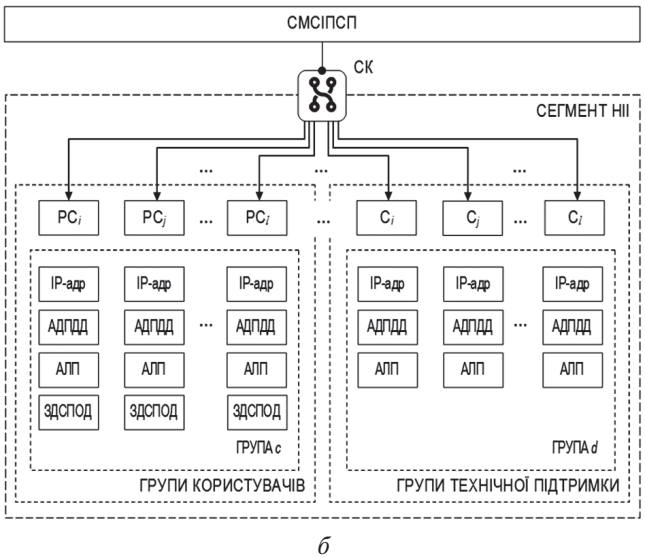
Зазначені групи відображено на рис. 3.

Засоби контролю за інцидентами, які відносяться до приведених груп, внесуть записи до відповідних розділів журналів активності при їх виникненні. Це приведе 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 $k_z^{\text{ваг}}$, де $z = 1,2,...,Z$, 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, як відмічено у [14], найбільш доцільним та ефективним для розрахунку надійності та достовірності отримання даних системами СМСІПСП є завдання значень параметрів у вигляді матриці. Ефективне рішення питання надійного отримання даних про інциденти ІБ, базою якого є пропонована теорія псевдонапівзворотних матриць, приведено у одному з наступних розділів дисертаційного дослідження.



а



б

Рис. 3. Додаткові групи відомостей про інциденти інформаційної безпеки: *а* – відомості про загальне використання додатків користувачами та технічною підтримкою; *б* – відомості про розмежоване використання додатків користувачами та технічною підтримкою

Як випливає з вище приведеного, врахування сукупності визначальних ознак, веде до реалізації

можливості комплексної оцінки стану параметрів у системах забезпечення інформаційної безпеки 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 приведено, наприклад, у [7]. Згідно до зазначеного джерела, алгоритм може забезпечити виявлення цифрових слідів інцидентів ІБ у контрольованих сегментах НІІ.

Відомостей щодо аналогічних рішень щодо моніторингу стану систем забезпечення ІБ в інформаційних системах будь-якого призначення, не виявлено.

3. Практична перевірка рішення задачі пошуку слідів порушення інформаційної безпеки у спеціальних сегментах НІІ

З метою практичної перевірки рішення задачі пошуку слідів порушення ІБ у спеціальних сегментах НІІ, у відповідності до вище викладеного та даних, отриманих з [7], перелік параметрів, які підлягають контролю, а також їх значення, що використані у якості зразкових, та довільно обрані коефіцієнти важливості груп, приведемо у вигляді табл. 1. Під поняттям «вимір» будемо розуміти результат роботи процедури отримання даних з журналів реєстрації інцидентів ІБ.

У табл. 1 темне поле означає, що контрольований параметр відноситься до вказаної групи. Значенням параметру може бути логічна «1» (ввімкнено), або логічний «0» (не ввімкнено). Зразковим значенням всіх параметрів, крім IP-адреси, є логічна одиниця.

У табл. 1 незатемнене поле означає, що засобами СМСІПСП в даній групі значення параметрів не отримуються.

У рядках табл. 1, що відповідають «IP-адр», містяться ідентифікатори контрольованих функціональних процесів ІБ. IP-адреси, які закінчуються цифрою «1», у контрольованому сегменті Одеського національного економічного університету, присвоєні серверам. Отримані результати порівнювалися з даними з [7] на предмет відповідності відомим даним.

$t_z^{\text{звіт}}$ та $\Delta t_z^{\max}$, які відповідають мінімальним та максимальним значення інтервалів часу виміру значень параметрів, що контролювалися, а також $t_z^{\text{звіт}}$, тобто момент формування звіту про стан безпеки контрольованого сегменту, були задані довільно, але з врахуванням важливості інформації, яка була наявною у сегменті, а також потенційної уразливості контрольованих функціональних процесів та елементів цього ж сегменту.

Мінімальне значення інтервалів часу вимірів $t_z^{\text{звіт}}$ значень параметрів, які контролювалися, для кожної z -ї групи було встановлено таким, що

Таблиця 1

Порівняння контрольованих параметрів, їх зразкові значення та коефіцієнти важливості груп

Параметри	Елементи сегменту, який контролюється						Групи параметрів, які контролюються							
	PC_i		PC_j		C_l		Служби файлового обміну		Служби електронної пошти		Служби папок обміну		Служби мережевої взаємодії	
	Отримано з [7]	Задано	Отримано з [7]	Задано	Отримано з [7]	Задано	Отримано з [7]	Задано	Отримано з [7]	Задано	Отримано з [7]	Задано	Отримано з [7]	Задано
	$k_z^{\text{ваг}}$ груп контрольованих параметрів													
	1	1	1	1	2	2	1	1	2	1	3	2	3	3
IP-адр	19168.77.1	19168.205.2 19168.205.3	19168.77.2	19168.205.3	19168.77.3	19168.205.1	19168.77.2 19168.77.3	19168.206.1	19168.77.1 19168.77.2	19168.207.1	19168.77.1 19168.77.2 19168.77.3	19168.208.1	19168.77.1 19168.77.2 19168.77.3	19168.209.1
АДПДД	■	■	■	■	■	■	■	■	■	■	■	■	■	■
АЛП	■	■	■	■	■	■	■	■	■	■	■	■	■	■
ЛНЗСЕП	■	■							■	■				
ЗДСПОД	■	■	■	■							■	■		
ЛНККСФО					■	■			■	■				
ЛНССФО					■	■	■	■						

нижче нього процедура моніторингу була або неповною, або призводила до порушень нормального функціонування досліджуваного сегмента (аналог DDos-атаки). Один з прикладів з завданням часових характеристик моніторингу, відображено у табл. 2.

На рис. 4 приведено результат візуалізації даних для табл. 2.

Як видно з рис. 4, не зважаючи на значення часових характеристик, де дані, які задавались при проведенні досліджень, відрізняються від даних з [7], їх тренди для обох випадків практично збігаються, що свідчить про їх тотожність.

Наступний крок – завдання інтервалу часу виміру параметрів, які отримуються, для кожної z-ї групи (табл. 3, дані округлено).

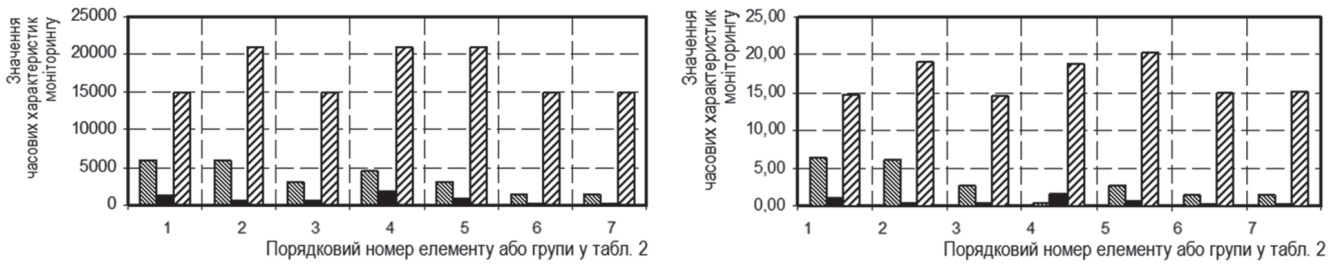
Як видно з табл. 3, інтервал часу виміру параметрів встановлювався таким, що дорівнює максимальному, тобто $\Delta t_z^{\max}$. Відповідно до цього перший вимір параметрів виконувався для груп з коефіцієнтом важливості $k_z^{\text{ваг}} = 3$ через довільний час, який, як рекомендовано у [7], дорівнював 25 хвилин, а для $k_z^{\text{ваг}} = 2 - 50$. Аналогічно завдавалися інші значення, які приведені у табл. 3. Темне поле у таблиці означає, що запити від СМСІПСП призвели до блокування роботи контрольованого елементу або до неможливості отримання даних про групу параметрів; знак «×» – кінець процедури моніторингу та формування звіту.

Згідно до [7], де описано алгоритм роботи СМСІПСП, у моменту часу $\Delta t_z^{\max}$ послідовно визначається значення параметрів у кожній із груп. Визначені значення порівнюються з їх попередньо встановленими зразковими значеннями. Якщо значення співпадають, то цикл моніторингу записів у журналах інцидентів інформаційної безпеки повторюється до тих пір, поки настане час формування звіту $t_z^{\text{звіт}}$. Так, як видно з табл. 3, на перших

Таблиця 2

Приклад результатів, отриманих для інтервалів часу вимірів значень параметрів, які контролювалися

Часові характеристики моніторингу	Елементи сегменту, який контролюється						Групи параметрів, які контролюються							
	PC_i		PC_j		C_l		Служби файлового обміну		Служби електронної пошти		Служби папок обміну		Служби мережевої взаємодії	
	Порядковий номер контрольованого елементу або групи параметрів													
	1		2		3		4		5		6		7	
	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено
	$k_z^{\text{ваг}}$ груп контрольованих параметрів													
	1	1	1	1	2	2	1	1	2	1	3	2	3	3
	IP-адреси													
	19168.77.1	19168.205.2 19168.205.3	19168.77.2	19168.205.3	19168.77.3	19168.205.1	19168.77.2 19168.77.3	19168.206.1	19168.77.1 19168.77.2	19168.207.1	19168.77.1 19168.77.2 19168.77.3	19168.208.1	19168.77.1 19168.77.2 19168.77.3	19168.209.1
$\Delta t_z^{\max}$, сек	6000	6,30	6000	6,24	3000	2,64	4500	4,20	3000	2,76	1500	1,38	1500	1,38
$\Delta t_z^{\min}$, сек	1200	1,08	600	0,48	600	0,36	1800	1,62	900	0,66	300	0,30	300	0.30
$t_z^{\text{звіт}}$, сек	15000	14,70	21000	19,08	15000	14,46	21000	18,78	21000	20,22	15000	15,06	15000	15,12



а *б*

$\rightarrow \Delta t_z^{\max}$; $\rightarrow \Delta t_z^{\min}$; $\rightarrow t_z^{\text{звіт}}$

Рис. 4. Візуалізація даних табл. 2: *а* – задання даних відповідно до [7]; *б* – задання даних при проведенні досліджень

чотирьох кроках моніторингу ті значення, які вимірювалися, збіглися з еталонними (табл. 1, табл. 2). У таких випадках корекція інтервалів часу вимірів не проводилася. Тоді, коли вимірювані значення параметрів не співпадали з еталонними (у межах допусків, крок 5), то вони заносилися до пам'яті або до бази даних. Після цього проводилося корегування інтервалу часу вимірів згідно до формули (1). З табл. 3 видно, на п'ятому кроці виявлена розбіжність між заданими значеннями та тими, що отримані – 6 та 7 групи параметрів. Відповідно, значення інтервалів часу вимірів було піддано корегуванню, а саме:

$$\Delta t_6^{\text{кор}} = \frac{\Delta t_6^{\max}}{k_6^{\text{ваг}}} \text{ та } \Delta t_7^{\text{кор}} = \frac{\Delta t_7^{\max}}{k_7^{\text{ваг}}}.$$

Отримані значення відображено у тому рядку таблиці, який відповідає 5-му кроку. Як наслідок, зміна інтервалу часу вимірів веде до того, що моніторинг 6 та 7 груп параметрів виконуватиметься частіше, починаючи з кроку 6. Це значить, що інтервал моніторингу скоротився та не є кратним 25 хв.

Далі необхідно порівняти відкориговане значення $\Delta t_z^{\text{кор}}$ з мінімальним $t_z^{\text{звіт}}$ і, так як у даному випадку $\Delta t_z^{\text{кор}} = \Delta t_z^{\max}\ (8 > 5)$, то цикл аналізу необхідно повторити, переходячи до наступного кроку. Якщо на цьому кроці значення параметрів, які контролюються, в 6 та 7 групах знову не будуть відповідати зразковим, то значення інтервалу часу вимірів коректується повторно.

Так як значення умови $\Delta t_z^{\text{кор}} \le \Delta t_z^{\min}$ для 6 та 7 груп є позитивним, (3<5), то це свідчить про наявність слідів, залишених інцидентом ІБ, що призвело до виходу параметрів, які контролюються у 6

Таблиця 3

Інтервали часу виміру параметрів, які отримуються, для досліджуваних груп

Номер кроку моніторингу	Час моніторингу	Елементи сегменту, який контролюється						Групи параметрів, які контролюються							
		PC_i		PC_j		C_l		Служби файлового обміну		Служби електронної пошти		Служби папок обміну		Служби мережевої взаємодії	
		Порядковий номер контрольованого елементу або групи параметрів													
		1		2		3		4		5		6		7	
		Отримано з [7]	Встановлено	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено	Отримано з [7]	Встановлено
		$k_z^{\text{ваг}}$ групи контрольованих параметрів													
		1	1	1	1	2	2	1	1	2	1	3	2	3	3
		IP-адреси													
		19168.77.1	19168.205.2 19168.205.3	19168.77.2	19168.205.3	19168.77.3	19168.205.1	19168.77.2 19168.77.3	19168.206.1	19168.77.1 19168.77.2	19168.207.1	19168.77.1 19168.77.2 19168.77.3	19168.208.1	19168.77.1 19168.77.2 19168.77.3	19168.209.1
		$\Delta t_z^{\text{кор}}$ для груп контрольованих параметрів													
1	25	–	–	–	–	–	–	–	–	–	–	25	25	25	25
2	50	–	–	–	–	50	55	–	–	50	50	25	25	25	25
3	75	–	–	–	–	–	–	75	75	–	60	25	25	25	25
4	100	100	100	100	100	50	50	–	80	50	50	25	25	25	25
5	125	–	110	–	110	–	55	–	–	–	60	8	8	8	8
6	133	–	–	–	–	–	–	–	–	–	–	3	3	3	3
7	150	–	–	–	–	25	25	75	75	50	50		–		–
8	175	–	–	–	–	12	15	–	80	–	60				–
9	187	–	–	–	–	6	6	–	–	–	–				
10	200	100	100	100	100		–	–	–	50	50				
11	225	–	120		120		–	75	75	–	60				
12	250	×	–	–	–			–	80	50	50				
13	275	–	–	–	–			–	–	–	60				
14	300	–	–	100	100			75	75	50	50				
15	325	–	–	–	120			–	80	–	60				
16	350	–	–	×	–			×	–	×	–				

та 7 групах за межі встановлених значень. Моніторинг інших груп параметрів продовжується до часу $t_z^{звіт}$ (8...16 кроки моніторингу). Після ухвалення рішення про відсутність слідів інцидентів ІБ, про це складається відповідний звіт.

Висновки

В процесі моніторингу щодо знайдення слідів інцидентів інформаційної безпеки 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, що веде підвищення 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.

Приведені дані можуть бути використані для подальшого розвитку теорії забезпечення інформаційної безпеки у інформаційних структурах, а також для вирішення загальної науково-прикладної проблеми з розробки моделей та комплексних методів проактивного забезпечення інформаційної безпеки 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 інформаційної безпеки, є питання надійності та живучості СМСІПСП [12, 13].

Список літератури: 1. *Скопа, О. О.* 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.** *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. **3.** *Казакова, Н. Ф.* 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.** *Казакова, Н. Ф.* Визначення показників для вирішення завдань прогностичного контролю мультисервісних телекомунікаційних мереж [Текст] / Н. Ф. Казакова, О. О. Скопа // Сучасний захист інформації. – К. : ДУІКТ. – 2010. – Спецвипуск (4). – С. 55-61. **5.** *Казакова, Н. Ф.* Застосування програмно реалізованого прогностичного контролю для вирішення практичних завдань забезпечення якості надання послуг у захищених інформаційних мережах [Текст] / Н. Ф. Казакова // Сучасна спеціальна техніка. – К. : Державний науково-дослідний інститут МВС України. – 2012. – № 2(29). – С. 86-95. **6.** *Скопа, О. О.* Проблематика якості послуг Інтернет-провайдерів [Текст] / 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 [Текст] : пат. № 2355024 : МПК G06F15/00, G06F17/00 / Євстигнєєв О. С., Зорін К. М., Карпов М. О. [та ін.] ; заявник та патентообладач Військова академія зв'зку ім. С. М. Будьонного ; заявл. 12.02.2007 ; опубл. 10.05.2009. **8.** *Волков, С. Л.* Оптимізація параметрів телекомунікаційної мережі методом статистичної регуляризації [Текст] / С. Л. Волков, Н. Ф. Казакова // Сучасна спеціальна техніка. – К. : Державний науково-дослідний інститут МВС України. – 2012. – № 1(28). – С. 54-60. **9.** *Казакова, Н. Ф.* Некоректні задачі відновлення даних у системах моніторингу інформаційного простору [Текст] / Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ : СНУ ім. В.Даля. – 2012. – № 8(179). – Т. 1. – С. 325-332. **10.** *Грабовський, О. В.* Регуляризація визначення показників якості функціонування ІВС з врахуванням нечіткості інформації [Текст] / 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.** *Скопа, О. О.* Інтелектуальні автономні системи: концептуальні положення створення та функціонування [Текст] / О. О. Скопа, Є. В. Вавілов // Бионика интеллекта. – 2013. – №1(80). – С. 35-40. **12.** *Грабовський, О. В.* Скорочення випробувань надійності ІВС за рахунок її функціональної надмірності [Текст] / О. В. Грабовський, Н. Ф. Казакова // Технологічний аудит та резерви виробництва. – 2013. – №2/1(10). – С. 24-27. **13.** *Скопа, О. О.* Концепція контрольних випробувань резервних систем на основі біноміальної схеми [Текст] / О. О. Скопа, С. Л. Волков, А. В. Мінін // Інформаційна безпека. – 2011. – №2(6). – С.69-76. **14.** *Петренко, С. А.* Управление информационными рисками. Экономически оправданная безопасность [Текст] / С. А. Петренко, С. В. Симонов. – М. : АйТи; ДМК Пресс, 2004. – 384 с.

Надійшла до редколегії 18.02.2015

УДК 004.738.5:681.14, 621.396:681.142:004.621

Совершенствование метода мониторинга уровня информационной безопасности в специальных сегментах национальной информационной инфраструктуры / Н. Ф. Казакова, Т. И. Соклакова // Бионика интеллекта: научн.-техн. журнал. – 2015. – № 1 (84). – С. 56–64.

Приведены результаты усовершенствования метода мониторинга следов инцидентов информационной безопасности в ограниченной информационной структуре.

Показано, что при мониторинге следов инцидентов информационной безопасности в журналах записей есть возможность продемонстрировать факт отличия значений параметров, которые контролируются, от заданных. Отмечено, что за счет их группирования по весовому коэффициенту появляется возможность повышения вероятности оценивания состояния защищенности контролируемого сегмента. Также показано, что динамическое управление интервалом времени принятия управляющего решения о ретроспективном состоянии безопасности сегмента обеспечивает повышение экономической эффективности системы мониторинга. Полученные результаты могут быть использованы для дальнейшего развития теории обеспечения информационной безопасности в информационных структурах. Они также могут быть применены для решения общей научно-прикладной проблемы по разработке моделей и комплексных методов проактивного обеспечения информационной безопасности в когнитивных сетях в которых основой построения и управления являются Sdn-технологии. Полученные результаты не противоречат принципам решения некорректных задач, которые связаны с неопределенностью процессов в системах мониторинга. Полученные решения, в сравнении с существующими принципами функционирования комплексных систем защиты информации, могут быть одной из составляющих концепции безопасной миграции данных и вычислительных ресурсов в пределах облачных структур. Они позволяют расширить теоретические и практические границы общих принципов функционирования систем защиты информации, что ведет к повышению степени защиты информационных процессов, которые владеют свойствами неопределенности.

Ил. 4. Библиогр.: 14 назв.

UDK 004.738.5:681.14, 621.396:681.142:004.621

Perfection of a method of monitoring the level of information security in a special segment of the national information infrastructure / N. F. Kazakova, T. I. Soklakova // Bionics of Intelligense: Sci. Mag. – 2015. – №1 (84). – P. 56–64.

The results of monitoring should be to improve the method of information security incidents in the restricted information structure. It is shown that the monitoring of trace information security incidents in the logs have an opportunity to demonstrate the fact of differences between the values of the parameters that are monitored on the specified. It is noted that due to their grouping on the weighting factor it is possible to increase the probability estimation state security monitored segment. It is shown that the dynamic time control manager making decisions about the security status of a retrospective segment enhances the economic efficiency of the monitoring system. The results can be used for further development of the theory of information security in the information structures. The results can be used to solve the problem of modeling and complex methods of proactive information security in cognitive networks in which the basis for building and managing are the SDN-technology. The results do not contradict the principles of solving ill-posed problems that are associated with the uncertainty of process monitoring systems. These solutions, in comparison with the existing principles of the functioning of complex information security systems, can be a component of the concept of safe migration of data and computing resources within the cloud structures. They allow you to extend the theoretical and practical limits of the general principles of functioning of information security systems, which leads to an increase in the degree of protection of information processes, which own properties uncertainty.

Fig. 4. Ref.: 14 items.