УДК 004.056:004.621:004.738.5

Н.Ф. Казакова

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

ВИЗНАЧЕННЯ ПРИНЦИПІВ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ З МЕТОЮ ОРГАНІЗАЦІЇ МІГРАЦІЇ ДАНИХ ДО ЇЇ БЕЗПЕЧНИХСЕГМЕНТІВ

Розглянуто перспективи розвитку систем захисту інформації щодо забезпечення інформаційної безпеки 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 виконуватиметься постійний динамічний процес моніторингу стану інформаційних процесів, що пов‘язані з забезпеченням інформаційної безпеки, включаючи відомості про внутрішній та зовнішній трафіки, з часом може стати невід‘ємною частиною ідеології функціонування національної інформаційної інфраструктури.
Ключові слова: інформаційна безпека, міграція даних, міграція обчислювальних ресурсів, національна інформаційна інфраструктура, моніторинг, центр обробки даних, системи захисту інформації.

Н.Ф. Казакова

ОПРЕДЕЛЕНИЕ ПРИНЦИПОВ МОНИТОРИНГА ИНФОРМАЦОННОЙ ИНФРАСТРУКТУРЫ С ЦЕЛЬЮ ОРГАНИЗАЦИИ МИГРАЦИИ ДАННЫХ В ЕЕ БЕЗОПАСНЫЕ СЕГМЕНТЫ

Рассмотрены перспективы развития систем защиты информации по обеспечению информационной безопасности государственных и негосударственных структур на основе мониторинга информационного пространства с целью выявления его наиболее безопасных и защищенных сегментов для миграции вычислительных ресурсов и данных, что обеспечит повышение их степени конфиденциальности, целостности и доступности. Такой подход, при котором будет выполняться постоянный динамический процесс мониторинга состояния информационных процессов, связанных с обеспечением информационной безопасности, включая сведения о внутреннем и внешнем трафике, со временем может стать неотъемлемой частью идеологии функционирования национальной информационной инфраструктуры.
Ключевые слова: информационная безопасность, миграция данных, миграция вычислительных ресурсов, национальная информационная инфраструктура, мониторинг, центр обработки данных, системы защиты информации.

N.F. Kazakova

FINDING THE PRINCIPLES MONITORING OF IT-INFRASTRUCTURE TO ORGANIZE THE DATA MIGRATION OF ITS SAFETY SEGMENTS

We consider the development of information security systems. The systems of information protection, providing information security of state and non-state actors. The basis is the monitoring of the information space. The monitoring system should find safe clusters. The data center has to organize the migration of computing resources and data from unprotected to protected clusters of clusters. Such a procedure will improve the degree of confidentiality, integrity and availability of data. Implementation of permanent monitoring of the state of the dynamic process of information processes that ensure information security, has the potential to become part of the ideology of the national information infrastructure.
Keywords: information security, data migration, migration of computing resources, national information infrastructure, monitoring, data processing center, information security systems

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

Методологія забезпечення інформаційної безпеки (ІБ) державних ресурсів на основі застосування методів міграції даних та обчислювальних ресурсів до найбільш безпечних сегментів національної інформаційної інфраструтури (НІІ), яка контролюється 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 і т.д. При цьому розуміється, що доступ до відомостей, які характеризують зазначене, може бути забезпечений на основі відповідних угод між суб'єктами, які обслуговуються єдиним ЦОД. Якщо вважати, що далі під загальним поняттям «ЦОД» розумітемимо комплексне організаційно-технічне рішення, метою функціонування якого є створення та підтримка високопродуктивної та відмовостійкої інформаційно-телекомунікаційної інфраструктури у межах виділеного обмеженого інформаційного простору, то його загальними завданнями буде таке:

– ефективне консолідоване зберігання та обробка даних користувачів;

– надання прикладних сервісів;

– 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. З цього слідує висновок про те, що існує необхідність автоматизації зазначених процесів з метою підвищення продуктивності робіт з оброблення даних, та до 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. Висвітлення зазначеного є ***метою статті***.

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

Численні літературні першоджерела свідчать, що з погляду ІБ НІІ, під ***загрозою*** інформаційній безпеці, у більшості випадків, розуміється сукупність умов та факторів, які приводять до порушення функціонування інформаційної мережі в цілому. Це відмічено, наприклад, у [1-5]. Зважаючи на постановку завдання, яке винесено у заголовок, ЦОД необхідно виявити найбільш безпечні сегменти НІІ, які є її складовими. Відповідно до цього будемо вважати, що розглянуте поняття про загрозу розповсюджується не тільки на інформаційну мережу в цілому, а й на підконтрольні ЦОД її окремі активи та, в межах його компетентності, на окремих користувачів. Виявленню підлягають як сліди навмисних загроз, так і природних. Про це йде мова у [6], де наведено їх опис та характеристики.

Технологічні процеси виявлення слідів порушення безпеки інформаційного простору, який підконтрольний єдиному ЦОД, апріорі вимагають врахування дії всієї множини можливих видів загроз. У цьому сенсі дослідники відзначають, що природні загрози у плані врахування ризиків, легко формалізуються, а технології захисту від них можуть бути описані достатньо лінійними залежностями. Відповідно, виявлення слідів впливу таких загроз не є достатньо складною проблемою, так як вони автоматично реєструються системами безпеки [4, 7-9].

На відміну від виявлення слідів природних загроз, сліди загроз, причинами яких є людський фактор, вимагають особливої уваги. До цього фактору у літературних перншоджерелах віднесено не тільки організаційні заходи та їх навмисне чи ненавмисне порушення, не тільки непередбачуваність дій персоналу, а й навмисну розробку та використання всіляких технічних та програмних засобів, принципом функціонування яких є отримання доступу до інформації, що має відповідні грифи обмеження доступу, з метою порушення вимог щодо конфіденційності, цілісності та доступності. До цієї ж категорії загроз віднесено загрози, які аналогічні зазначеним, але мають ознаки відсутності наміру заподіяння шкоди. Найбільш повно про це мова йде у [10]. Виявлення таких ситуацій засобами ЦОД може свідчити про недостатній контроль зі сторони керівництва за діяльністю співробітників, які обслуговують відповідну ділянку НІІ, що призведе виключення її зі списку безпечних сегментів підконтрольної інформаційної структури [11].

Ідеологія функціонування єдиного ЦОД у сенсі знаходження безпечних сегментів, передбачає виявлення слідів десятків, а той сотень тисяч подій, які можуть мати відношення до ІБ НІІ. При цьому ЦОД повинен враховувати, що переважна більшість з них, це сліди нормального функціонування інформаційної інфраструктури – тільки деякі з них є сигналами про те, що могли відбутися або відбулися інциденти фактичного порушення ІБ [2-5, 7-9].

Виходячи зі сказаного, актуальним завдання для єдиного ЦОД є моніторинг стану підконтрольного інформаційного простору та його окремих сегментів, що дозволить відслідковувати не тільки поточний стан систем забезпечення його ІБ, але й їх ретроспективні динамічні зміни.

Викладення основного матеріалу

Під загальним поняття «моніторинг» розуміють систематичний збір та обробку інформації, яка може бути використана для поліпшення процесу прийняття рішення, а також, побічно, як інструмент зворотного зв’язку з метою здійснення проектів, оцінки програм або вироблення політики. Він несе одну або більше з трьох організаційних функцій [2-5, 7-9]:

1) виявляє стан критичних або таких, що перебувають у критичному стані, змін явищ довкілля щодо яких існує вироблений курс дій на майбутнє;

2) встановлює стосунки зі своїм оточенням, забезпечуючи зворотний зв’язок з метою корегування попередніх успіхів або невдач певної політики або програм;

3) встановлює відповідності правилам та контрактним зобов’язанням.

У цілому, моніторинг інформаційного простору, який є підконтрольним зі сторони єдиного ЦОД з метою визначення безпечних сегментів НІІ, можна визначити [12, 13]:

– як постійне спостереження за результатами дій об’єктів та факторів, які в ретроспективі впливали на функціонування їх систем забезпечення ІБ та на загальний стан їх функціонування;

– як аналіз результатів спостереження, включаючи зберігання та узагальнення відповідної інформації.

Доцільним є проведення досліджень щодо вирішення питання моніторингу у сенсі, як це викладено вище, з розробкою методу превентивного моніторингу ІБ складових НІІ, які є предметом управління єдиного ЦОД. Метод повинен виявляти результати дії деструктивних впливів або їх сліди у роботі складових НІІ, які можуть бути наслідками як технічних збоїв, так і несанкціонованих впливів. Для цього необхідно передбачити можливості знаходження слідів деструктивних впливів довільних типів, що призвели до порушень роботи систем забезпечення ІБ, як по прямих, так і по непрямих ознаках, пролонгованих у часі [14]. Важливість цього відмічена у [15].

Для виявлення слідів деструктивних впливів, як зазначено у [13], є доцільним застосування автоматичного моніторингу записів у журналах подій, які відбулися у системах захисту інформації (СЗІ) та були виявлені існуючою множиною спеціалізованих систем: аналізаторами мережевих протоколів, системи мережевого моніторингу, антивіру-

сними засобами, міжмережевими екранами, криптографічними засобами захисту інформації, системами виявлення атак та ін. Втім, зважаючи на те, що зазначені засоби у СЗІ застосовуються періодично, мають несистемний характер та у якості інструмента використовуються для розв'язків вже виниклих проблем, а для профілактики – лише зрідка, базуючись на суб'єктивних рішеннях адміністраторів, то виникає необхідність застосування активного компонента – системи навантажувального тестування. Така система надасть можливості виявити порушення у СЗІ та на основі цього синтезувати відповідні управляючі рішення. При цьому при розробці системи навантажувального тестування необхідно врахувати застосування не тільки методів аналізу підконтрольного єдиному ЦОД інформаційного простору, що спрямовані на виявлення заздалегідь відомих загроз, а й тих, які містять ознаки їх модифікації та ознаки новизни, що значно підвищить достовірність даних стосовно стану ІБ окремих сегментів НІІ.

Процедура моніторингу передбачає створення у складі єдиного ЦОД об'єднаної системи управління всіма активами інформаційного простору. Така система буде відігравати координаційну роль при розгортанні системи моніторингу. Це дасть право єдиному ЦОД виконувати:

– постійний динамічний контроль стану ІБ активів підконтрольного простору в реальному часі;

– отримувати та накопичувати статистику про інциденти ІБ, що вже відбулися у підконтрольному інформаційному просторі, з метою використання отриманих відомостей для прогнозування ситуацій, які можуть вплинути на прийняття управляючого рішення стосовно міграції даних та обчислювальних ресурсів.

До компонентів системи моніторингу, завданням якої є виявлення безпечних сегментів НІІ, та яка є підконтрольною єдиному ЦОД, включимо:

– автоматичну систему управління моніторингом, яка дозволить приймати управляючі рішення в реальному масштабі часу;

– систему збору інформації, що знаходиться в журналах усіх наявних засобів забезпечення ІБ;

– базу даних для зберігання інформації про результати аналізу ретроспективних інцидентів ІБ або про події, які мали відношення до безпеки підконтрольних сегментів;

– технічні засоби, що виконують централізовану обробку інформації про ретроспективні інциденти ІБ або про події, які мали відношення до безпеки підконтрольних сегментів.

Встановимо, що напрямом, який забезпечить отримання системою моніторингу інформації про ретроспективний стан контрольованих сегментів НІІ, є аналіз записів у системних журналах серверів корпоративних мереж про:

– відомості щодо виявлення уразливостей корпоративних систем та мереж, що є складовими НІІ;

– відомості щодо виявлення недосконалості методів забезпечення ІБ, що застосовувалися для підтримки цілісності, доступності та конфіденційності інформації;

– відомості щодо відновлення працездатності систем, якщо це було пов'язано з інцидентами ІБ чи фізичними причинами;

– відомості щодо забезпечення, виконання та підтримки політик ІБ у корпоративних мережах, що є складовими НІІ;

– відомості щодо стану та вмісту мережевих пакетів для випадків, коли системою забезпечення ІБ певної мережі були зафіксовані факти її порушення або спроби цього;

– результати моніторингу роботи операційних систем та програмних додатків;

– результати моніторингу фізичного стану кабельних та інших систем, що забезпечують з'єднання всередині контрольованих сегментів НІІ та між ними;

– результати моніторингу функціонування активного мережевого устаткування;

– результати моніторингу функціонування серверів та робочих станцій з розділенням їх по ступеню важливості з погляду ІБ.

Обґрунтуванням отримання та зберігання приведеної множини даних є положення про те, що вони надалі будуть використовуватися для прийняття управляючих рішень щодо забезпечення безпеки методами міграції даних та обчислювальних ресурсів. При цьому, зважаючи на великі обсяги даних, а також на їх різнорідний характер, завдання їх врахування є достатньо складною проблемою, яка потребує розробки методик, які б дозволили їх класифікувати та аналізувати у режимі реального часу [13]. Розуміється, що для цього між єдиним ЦОД та складовими НІІ, які йому підконтрольні, повинно бути організовано передавання даних з достатньою швидкістю та якістю. Відповідно, необхідна розробка методики, яка б дозволяла виконувати ефективні розрахунки пропускної здатності каналів захищеного передавання даних та зробити оцінку надійності комунікаційної системи. Ця ж методика може бути використана при реалізації управляючих рішень щодо міграції даних та обчислювальних ресурсів, що дозволить оцінити час переміщення та її ефективність у критичних ситуаціях.

Як зазначалося вище, різноплановість даних, отриманих засобами моніторингу єдиного ЦОД в реальному часі, є однією з головних проблем, яка потребує свого вирішення. Аналіз численних літературних першоджерел свідчить про те, що найбільш доцільним методом її вирішення є обчислення консолідованої оцінки результатів моніторингу по певних параметрах, які повинні бути встановлені заздалегідь. При такому підході вся множина різнопланових даних, що відслідковуються системами моніторингу, може бути зведена до значимих показників. На основі їх аналізу можуть бути синтезовані управляючі рішення, які будуть використані для прийняття оперативних впливів на виконавчі системи. Втім, візьмемо до уваги, що при такому підході частина показників, які пов‘язані з інцидентами ІБ, але мають незначущий рівень щодо встановлених параметрів, можуть бути не враховані. Відповідно, вимоги до них повинні бути ретельно обґрунтовані для їх врахування засобами формування консолідованих показників та, на цій основі, системами моніторингу. Як слідує з [16], такий принцип синтезу консолідованої оцінки дозволяє виявити приблизно на 25% більше інцидентів ІБ, збільшивши тим самим обсяги баз даних, які будуть доступними для аналізу системами моніторингу.

Динамічний характер системи моніторингу, метою якої є виявлення слідів порушень ІБ у межах компетенції єдиного ЦОД, пов‘язаний з питаннями адаптивного динамічного управління процесами зміни всієї множини станів СЗІ у всій НІІ. Це призводить до того, що журнали фіксації інцидентів ІБ постійно (динамічно) оновлюються і відомості з них повинні бути динамічно враховані системою моніторингу. Виникнення множини є очевидним фактом, так як сукупність систем захисту забезпечує запобігання виходу НІІ не з одного фіксованого положення, а з діапазону таких, які у достатньому ступені задовольняють вимогам, що повинні враховуватися при формуванні консолідованої оцінки [17]. Неприпустимим є створення такої системи моніторингу слідів інцидентів ІБ, яка б враховувала факти збереження інформаційною структурою якогось безпечного стану протягом певного часу та, враховуючи їх відсутність, з метою оптимізації своєї роботи не проводила б її перевірку.

Використання консолідованих оцінок щодо ретроспективної роботи систем забезпечення ІБ для прийняття управляючих рішень про міграцію залежить від безлічі факторів. Враховуючи це та вище приведені факти, їх застосування повинне обумовлюватися лише крайньою необхідністю. Але навіть у таких випадках вони повинні враховувати практично всю множину критеріїв реєстрації інцидентів ІБ та велику кількість обмежень, які до них не відносяться. Як результат, система моніторингу, як система, що приймає управляюче рішення, не повинна використовувати спрощені методики аналізу і, т.ч., доцільним є синтез методів, які б забезпечили швидкість обробки даних та швидкість їх транспортування без шкоди для якості функціонування. Звідси випливає необхідність розробки системи підтримки прийняття рішень, яка зазначені функції розрахунку виконувала б автоматично, базуючись на нових ефективних алгоритмах, фіксуючи при цьому всі випадки щодо порушень ІБ НІІ.

Необхідною та обов‘язковою умовою прийняття рішень системою моніторингу, повинен бути аналіз журналів реєстрації інцидентів ІБ у яких повинні фіксуватися такі параметри:

– визначення факту інциденту, включаючи його класифікацію відповідно до розробленої системи вимог;

– наявність тенденцій поширення збоїв інформаційної системи внаслідок деструктивних впливів, тобто наявність засобів локалізації події СЗІ;

– список активів по категоріях, які зазнали впливів від інциденту ІБ;

– список користувачів, які зазнали збоїв у роботі інформаційної системи внаслідок деструктивних впливів з врахуванням їх рівнів доступу та інших параметрів систем забезпечення ІБ;

– відомості про вплив збоїв у роботі СЗІ на функціонування та ресурси НІІ в цілому;

– відомості про наявність в базі інформаційної мережі, яка підлягає аналізу, засобів протидії деструктивним впливам та відомості про їх ефективність.

У [18] показано, що складне завдання аналізу даних про інциденти ІБ системами моніторингу може бути вирішене на основі застосування нейронних мереж. Алгоритми аналізу даних та подій, які застосовуються в них, не використовують методи аналітичного програмування і, відповідно, дозволяють досягти необхідних результатів з достатньою оперативністю. При цьому нейронні мережі здатні до самонавчання, що дає додаткові переваги: збої інформаційних систем, які викликані інцидентами ІБ, можуть проявлятися у вигляді нелінійних залежностей між контрольованими параметрами та параметрами, що не завжди безпосередньо зв’язані ними. Цей факт дуже складно виявити аналітично. Існуючий варіант виявлення зазначених нелінійностей – використання мережі Хопфілда, тобто повнозв‘язаної тришарової мережі з симетричною матрицею зв’язків, яка прагне до досягнення рівноваги, параметри якої задаються як оптимізація процесів у мережі [19].

Рішення на базі нейронних мереж є доцільним для застосування у тих випадках, які потребують розробки технологій саме захисту інформаційних ресурсів, а не ретроспективного моніторингу інцидентів ІБ. Це пояснюється тим, що суттю роботи мережі Хопфілда є відновлення всіх зв‘язків у інформаційній мережі, які виникли у результаті дії деструктивного впливу. Воно є неприйнятним для вирішення задач дослідження, які не передбачають дій з відновлення мережі. Крім того, оперативність прийняття рішення мережею Хопфілда про факт порушення у СЗІ є надзвичайно низькою: мережа є системою, яка заснована на самонавчанні і, т.ч., час, який буде затрачено на таку процедуру, є достатньо великим, а записи у журналах обліку інцидентів можуть бути сформовані у терміни, що не відповідають вимогам, які сформовані системами моніторингу. Відповідно, цей факт підтверджує необхідність розробки нового ефективного методу моніторингу стану ІБ певних сегментів НІІ з метою міграції до них даних та обчислювальних ресурсів.

З [20] слідує, що перспективним напрямом удосконалення безпеки інформації в роботі систем моніторингу, а також в її передаванні, є розмежування потоків даних по кількох напрямах. Зазначено, що передавання інформації у вигляді одного потоку підвищує вразливість мережі на чверть. Інтеграція систем контролю мережевої безпеки, моніторингу та розмежування потоків даних усуває цей недолік. Невирішеним питанням є проблема швидкого розрахунку системами прийняття рішень пропускної здатності каналів, які можуть бути використані для переміщення даних та відомостей, що є предметом дослідження у системах моніторингу. Основою для вирішення можуть бути типові стандартні рішення, які, втім, не передбачають механізм адаптації систем безпеки до різних конфігурацій мережі [20]. Такі рішення призводять до того, що можливості організації ефективного використання незадіяних активів практично не використовуються через відсутність розроблених методів та алгоритмів адаптації. Як результат, часто спостерігається конкуренція за обчислювальні ресурси між засобами забезпечення ІБ та додат-

ками, які працюють в ті же моменти часу і, т.ч., це є додатковим аргументом поділу інформаційних потоків у реальному часі з метою оптимізації роботи інформаційної структури. Це надасть можливостей скорочення часу опитування серверів, що здійснюється системою моніторингу. У результаті може бути організований динамічний багатопоточний збір інформації системою моніторингу НІІ [21].

Виходячи зі сказаного та з результатів аналізу вище зазначених першоджерел, система моніторингу НІІ, до основної функції якої відноситься виявлення найбільш безпечних сегментів у межах компетенції єдиного ЦОД, та синтез управляючого рішення щодо міграції до них даних та обчислювальних ресурсів, повинна здійснювати два стратегічні види контролю:

1. Моніторинг цілісності досліджуваної системи, тобто стану сегменту НІІ, при якому вона функціонує як логічно єдина система апаратних та програмних засобів, які повноцінно підтримують роботу механізмів забезпечення ІБ, логіку їх коректної роботи та встановлені норми функціонування щодо нейтралізації загроз безпеці. Задачею системи моніторингу цілісності є постійне та динамічне відстеження змін щодо розподіленої конфігурації НІІ, та реагування на дії СЗІ та систем забезпечення ІБ при несанкціонованій модифікації потоків даних між вузлами НІІ.

2. Моніторинг захищеності досліджуваної системи, тобто реєстрація інцидентів ІБ, які виникли внаслідок спроб її власника виявити вразливості у захисті мережі та інші недоліки. Особливо актуальним це питання є при встановленні нового програмного забезпечення та у випадках зміни співробітників, які працюють з критично значущими вузлами інформаційної системи. Відомості про це повинні заноситися до баз даних у порядку, який повинен бути передбачений для всіх учасників НІІ.

Як витікає зі сказаного, система моніторингу повинна бути обов‘язковою складовою частиною загального забезпечення ІБ НІІ. Ефективність забезпечення ІБ, яка буде напряму залежати від неї, визначатиметься тим, наскільки однозначно будуть сформульовані вимоги до оперативних, тактичних та стратегічних завдань щодо функціонування НІІ, і наскільки цілісно при цьому буде забезпечений їх взаємозв’язок [22]. Така система моніторингу, як частина системи ІБ держави, забезпечить розв’язок оперативних та частково тактичних завдань, сприяючи досягненню стратегічної мети щодо ІБ НІІ.

Принцип роботи системи моніторингу інцидентів ІБ (СМІІБ) у НІІ повинен враховувати той факт, що різні корпоративні мережі, які входитимуть до неї, можуть бути побудовані за різними стандартами, включаючи міжнародні [23]. Також слід врахувати, що існуючі вітчизняні стандарти побудови корпоративних мереж, а тим більше – вимоги стандартів щодо побудови НІІ, далеко не завжди відповідають набору компетенцій [24] та вимогам стандартів та нормативних документів з безпеки [25]. Особливо це питання є актуальним для специфіки побудови систем критичного використання, спеціальних відомчих та технологічних інформаційних систем щодо яких передбачається процедура включення до загальної НІІ.

Динамічний системний моніторинг інцидентів ІБ у НІІ буде вимагати постійного двостороннього контакту фахівців з ІБ з боку замовника, тобто держави, з виконавцем робіт з розробки та впровадження систем моніторингу для своєчасного внесення виправлень та коректувань відповідно до принципів менеджменту якості [26]. Така вимога потребує вирішення питання постійної адаптації систем моніторингу та управління конфіденційністю, цілісністю та доступністю інформацією в умовах постійно мінливих завдань [27]. Як зазначено у [28], це повинно бути обов’язковою метою забезпечення ІБ при побудові НІІ.

З часом усе більша кількість державних структур, предметом діяльності яких є забезпечення ІБ держави, починають застосовувати системи моніторингу та аудиту стану інформаційних та комунікаційних мереж спеціального та критичного використання. Це веде до росту ефективності процесу виявлення загроз у них та їх нештатного функціонування, а також до зменшення часу реагування на інциденти ІБ при одночасному зростанні якості прийнятих управляючих рішень. На сьогодні позитивні результати досяг-

нуті за рахунок введення достатньо обмеженої кількості методів з автоматизації збору та аналізу даних про процеси, які відбуваються в окремих інформаційних мережах. Ті обмежені відомості, які є у відкритих літературних першоджерелах, свідчать про те, що дані автоматично реєструються саме системами моніторингу. У загальному вигляді об‘єкти моніторингу для НІІ стосовно державних ресурсів, приведено на рис. 1.

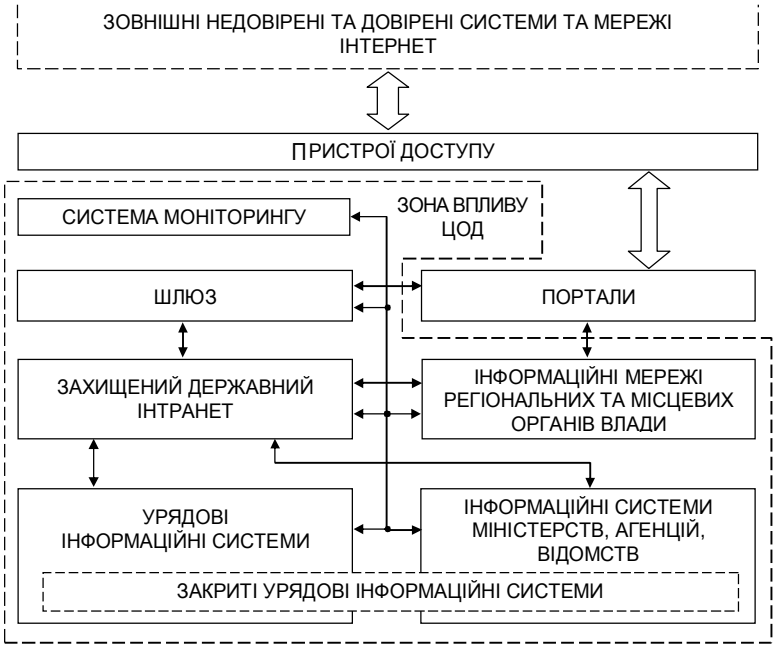

Рис. 1. Державні інформаційні ресурси, які є предметом моніторингу ретроспективного стану їх інформаційної безпеки

Висновок

Відзначимо, що ще у недалекому минулому застосування традиційних засобів захисту інформації було стандартним методом забезпечення ІБ будь-якої комунікаційної системи чи мережі. Ними були та є на поточний момент, застосування систем розмежування прав доступу, використання міжмережевих екранів, антивірусного програмного забезпечення та ін. Відомості про їх роботу та ефективність можуть бути використані на новому етапі розвитку СЗІ щодо забезпечення ІБ, а саме – системами моніторингу інформаційного простору з метою виявлення його найбільш безпечних та захищених сегментів з метою міграції до них державних 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 НІІ.

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

Література

1. Chirillo J. Hack Attack Testing: How to Conduct Your Own Security Audit. — Wiley Publishing, 2003. — P. 576.

2. Казакова Н. Ф. Відновлення та оптимізація інформації в системах прийняття рішень [Текст] : підручник / Баранов В. Л., Браіловський М. М., Засядько А. А. [та ін.] ; за ред. В. О. Хорошко. — К. : ДУІКТ, 2009. — 134 с.

3. Казакова, Н. Ф. Автоматизація процесу адаптації інформаційних систем до інцидентів інформаційної безпеки [Текст] / Н. Ф. Казакова, Є. В. Вавілов // Інформаційна безпека. — 2013. — №4(12). — С. 49-56.

4. 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. Йона, О. О. Світові тенденції боротьби з кіберзлочинністю [Текст] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2013. — № 15(204). — Т. 1. — С. 59-62.

5. Скопа, А. А. Политика предупреждения угроз информационной безопасности в практической деятельности Одесского филиала ОАО «Укртелеком» [Текст] / А. А. Скопа, Н. Ф. Казакова, С. Т. Сорока // Вісник Національного технічного університету «ХПІ» : Нові рішення в сучасних технологіях. — 2012. — № 17. — С. 42-47.

6. Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак [Текст] : дис… канд. техн. наук: 05.13.11, 05.13.19 / Степашкин М. В. — СПб., 2007. — 149 с.

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

8. 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.

9. 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.

10. Черненко, С. С. Робототехника и ее перспективы в социо-культурном аспекте [Текст] // С. С. Черненко, М. А. Назаренко / Успехи современного естествознания. — 2014. — № 5-2. — С. 194-195.

11. Казакова, Н. Ф. Принципи побудови захищених інтелектуальних мереж [Текст] / Н. Ф. Казакова // Вісник ДУІКТ. — 2009. — № 4. — Т. 7. — С. 381-388.

[12]. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления безопасностью. — М. : Стандартинформ, 2006. — С. 62.

13. 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.

14. Анализ и моделирование трафика в корпоративных компьютерных сетях [Текст] : дис… канд. техн. наук: 05.13.01 / Репин Д. С. — М., 2008. — 143 с.

15. Разработка методов и программных средств выявления аномальных состояний компьютерной сети [Текст] : дис… канд. техн. наук: 05.13.13, 05.13.11 / Дружинин Е. Л. — М., 2005. — 202 с.

16. 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.

17. Адаптивное управление безопасностью информационных систем на основе логического моделирования [Текст] : дис… докт. техн. наук: 05.13.19 / Калинин М.О. — СПб., 2010. — 310 с.

18. Назаренко, М. А. Разработка учебно-методических материалов для обучения персонала в соответствии со стратегией развития организации [Текст] // М. А. Назаренко, А. Ю. Котенцов, Е. А. Аверьянов, Г. С. Сергеев / Международный журнал прикладных и фундаментальных исследований. — 2014. — № 7. — С. 140.

19. Хайкин С. Нейронные сети: полный курс [Текст] : монографія. — М. : Вильямс, 2006. — 2-е изд. — 1104 С.

20. Контроль сетевой политики безопасности и разграничение потоков данных в компьютерных сетях научных организаций [Текст] : дис… канд. техн. наук: 05.13.19 / Козачок А. В. — Орёл, 2010. — 162 с.

21. Методы и алгоритмы для систем мониторинга локальных сетей [Текст] : дис… канд. техн. наук: 05.13.13 / Сторожук Д. О. — М., 2008. — 121 с.

22. Carter, E., Hogue, J. Intrusion Prevention Fundamentals. — Indianapolis, IN: Cisco Press, 2006. — P. 312.

23. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты [Текст] : монография . — М. : Книжный мир, 2009. — 352 с.

24. Назаренко, М. А. Программа развития образования в Московской области и особенности вступившего в действие законодательства [Текст] // М. А. Назаренко / Современные проблемы науки и образования. — 2014. — № 1. — С. 64.

25. Назаренко, М. А. Вычислительные комплексы и системы — терминальные системы в рамках ФГОС ВПО [Текст] // М. А. Назаренко, А. И. Белолаптикова, Е. И. Лысенко / Успехи современного естествознания. — 2013. — № 6. — С. 158-159.

26. Назаренко, М. А. Принципы менеджмента качества и системы доработки или внесения изменений во внедренное программное обеспечение [Текст] // М. А. Назаренко, А. О. Адаменко, Н. В. Киреева / Успехи современного естествознания. — 2013. — № 7. — С.177-178.

27. Акимова, Т. И. Применение принципа постоянного улучшения систем менеджмента качества в учебном процессе [Текст] // Т. И. Акимова, Д. Г. Мельников, М. А. Назаренко / Международный журнал прикладных и фундаментальных исследований. — 2014. — № 3. — С. 126-128.

28. Назаренко, М. А. Межпредметные связи теории организаций, организаци-онной культуры и кадрового аудита [Текст] // М. А. Назаренко / Международный журнал прикладных и фундаментальных исследований. — 2013. — № 10-3. — С. 518-519.