УДК 004.78+65.012.8

О. О. Гудзовата

ІНФОРМАЦІЙНА БЕЗПЕКА ХМАРНИХ СЕРВІСІВ

У статті охарактеризовано технологію хмарних сервісів, проаналізовано основні задачі і принципи її інформаційної безпеки, визначено перспективи розвитку як самої технології, так і параметрів безпеки.

Ключові слова*: хмарні сервіси (обчислення), інформаційна безпека, технологія, інфраструктура.*

Постановка проблеми. Інтенсифікація інноваційних процесів, розвиток інформаційних технологій, їх проникнення в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем. Проблеми захисту інформації потребують комплексного підходу, тобто створення системи інформаційної безпеки (ІБ).

Сучасні підприємства знаходяться під постійним впливом факторів, пов'язаних із розвитком технологій, які, з одного боку, спрощують роботу з великими обсягами інформації, проте, з іншого – зумовлюють проблеми, пов'язані насамперед з інформаційною безпекою.

Однією із таких технологій є хмарні сервіси (хмарні обчислення), що з'явилися в 2006 році, коли Amazon's Elastic Computing Cloud побудували свої дата-центри. Багато підприємств, які займалися інформаційними технологіями, створювали підґрунтя для власних хмарних обчислень. 2007 року Dell випускає свою версію хмарних сервісів, IBM запускає програмний продукт Blue Cloud. Пізніше з'являються такі продукти, як Google's MapReduce, Microsoftware's Windows Azure, iCloud, Amazon CloudDrive тощо.

Нині завершується ранній етап розвитку хмарних технологій, які характеризуються новаторськими експериментами, нестійкістю бізнес-моделей, невирішеними питаннями їх інформаційної безпеки.

Стан дослідження. Проблеми безпеки діяльності, фінансової та інформаційної безпеки є актуальними і набули широкого висвітлення у вітчизняній і зарубіжній науці. Питанням інформаційної безпеки присвячені дослідження таких вітчизняних науковців: Г. С. Гриджука, Б. А. Кормича, В. Л. Гевко, а також російських учених, таких як Е. Б. Белов, В. П.Лось, Р. В. Мещеряков, А. А. Шелупанов.

Слід зазначити, що дослідження теоретичних і практичних засад функціонування хмарних сервісів у вітчизняній науці ще не набули

достатнього поширення. Серед російських дослідників можна відзначити Е. Гребнева, А. Федорова, Д. Мартинова.

Інформаційна безпека хмарних сервісів є мало дослідженою сферою, особливо у вітчизняній практиці.

Метою статті є аналіз і теоретичних, і практичних аспектів інформаційної безпеки технології хмарних обчислень, визначення їх принципів і перспектив.

Виклад основних положень. Інформаційна безпека підприємства – це захист інформації, якою володіє підприємство від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок під час надходження. Крім того, під інформаційною безпекою розуміють захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може бути нанесення шкоди самій інформації, її власникам або підтримуючій інфраструктурі [1; 9].

Архітектура ІБ охоплює процеси, людей, технології, різні типи інформації, адаптуючись до них, враховує складність і мінливість сучасного підприємства. Іншими словами, вона описує бажану структуру інфраструктури безпеки організації й інших, пов'язаних з інформаційною безпекою, компонентів та інтерфейсів.

Метою системи безпеки є:

- захист прав підприємства (установи), його структурних підрозділів і співробітників;
- збереження й ефективне використання інформаційних, матеріальних і фінансових ресурсів;
- підвищення іміджу системи за рахунок забезпечення якості послуг щодо інформаційної безпеки.

Поява хмарних технологій спровокувала розгортання великомасштабних розподілених систем для постачальників програмного забезпечення. Хмарні системи забезпечують просту й уніфіковану взаємодію між постачальником і користувачем і включають програмне забезпечення, тобто сервісну підсистему, та базу даних із багаторазовим доступом. Ці системи динамічно розподіляють обчислювальні ресурси у відповідь на запити про резервування ресурсу користувачем і, відповідно, до певних стандартів якості обслуговування користувачів.

Хмарні обчислення (англ. *cloud computing*) – це технологія розподіленої обробки даних, в якій комп'ютерні ресурси та потужності надаються користувачам як Інтернет-сервіс [2].

Хмарний сервіс є особливою клієнт-серверною технологією, яка передбачає використання клієнтом ресурсів (процесорного часу,

оперативної пам'яті, дискового простору, мережевих каналів, спеціалізованих контролерів, програмного забезпечення тощо) групи серверів у мережі, які взаємодіють так:

• для клієнта вся група виглядає як єдиний віртуальний сервер;

• клієнт може прозоро та гнучко змінювати обсяги споживання ресурсів у разі зміни своїх потреб (збільшувати/зменшувати потужність сервера з відповідною зміною оплати).

В такому разі наявність декількох джерел ресурсів, які використовуються, з одного боку, дозволяє підвищувати доступність системи клієнт-сервер за рахунок можливості масштабування у разі підвищення навантаження, а з іншого – знижує ризик втрати працездатності віртуального сервера під час виходу з ладу будь-якого із серверів, що обслуговують клієнта, оскільки можливе автоматичне перепід'єднання віртуального сервера до ресурсів іншого (резервного) сервера.

За допомогою провайдерів хмарних рішень можна орендувати через Інтернет обчислювальні потужності та дисковий простір. Переваги такого підходу – доступність (користувач платить за ті ресурси, які йому потрібні) і можливість гнучкого масштабування. Клієнти позбавляються від необхідності створювати та підтримувати власну обчислювальну інфраструктуру.

Під час використання хмарних технологій програмне та технічне забезпечення надається користувачеві як Інтернет-сервіс. Користувач має доступ до власних даних, але не може управляти і не повинен піклуватися про інфраструктуру, операційну систему і програмне забезпечення, з якими він працює. «Хмарою» називають Інтернет, який приховує усі технічні деталі.

Хмарні сервіси змінюють підхід користувача до роботи з інформацією та програмами. Хмарні системи дозволяють мати доступ до інформації та серверів з будь-якого місця світу, звільнивши користувачів від необхідності мати стаціонарний комп'ютер та зробивши доступнішою спільну роботу багатьох людей, які можуть знаходитися в різних місцях.

Першою компанією, яка повною мірою усвідомила комерційну перспективу технологій віртуалізації, стала Amazon [8]. Якщо до 2006 року віртуалізацію розуміли як можливість розвернути потрібну кількість віртуальних серверів на власному обладнанні, то завдяки Amazon's Elastic Computing Cloud в практику впровадилась ідея оренди віртуальних серверів на чужому обладнанні. Саме в цьому полягає суть хмарних пропозицій класу «інфраструктура як сервіс» (Infrastructure as a Service – IaaS).

Найбільш авторитетне дослідження хмарних обчислень належить Національному інституту стандартів і технологій США (National Institute of Standards and Technology – NIST), який сформулював такі характеристики технології хмарних обчислень [6]:

- Самообслуговування на вимогу – споживач самостійно визначає і змінює обчислювальні потреби, такі як серверний час, швидкість доступу та обробки даних, обсяг збережених даних без взаємодії з представником постачальника послуг.
- Універсальний доступ мережею – послуги доступні споживачам через мережу передавання даних незалежно від термінального пристрою.
- Об'єднання ресурсів – постачальник послуг об'єднує ресурси для обслуговування великої кількості споживачів для динамічного перерозподілу потужностей між споживачами в умовах постійної зміни попиту на потужності.
- Еластичність – послуги можуть бути надані, розширені, звужені в будь-який момент часу без додаткових витрат на взаємодію із постачальником.
- Облік споживання – постачальник послуг автоматично обчислює спожиті ресурси на певному рівні абстракції (наприклад, обсяг збережених даних, пропускна здатність, кількість користувачів, кількість транзакцій) і на основі цих даних оцінює обсяг наданих споживачам послуг.

Виокремлюють основні моделі надання послуг за допомогою «хмар» (табл. 1).

Таблиця 1

Основні моделі хмарних сервісів

Послуга	Приклади
Програмне забезпечення (SaaS)	Сервіси Gmail та Google docs
Платформа (PaaS)	Google Apps надає додатки для бізнесу в режимі онлайн; ПЗ і дані зберігаються на серверах Google
Інфраструктура (IaaS)	Надання провайдером клієнтові різноманітної комп'ютерної інфраструктури: серверів, систем зберігання даних, мережевого обладнання, ПЗ для керування цими ресурсами

Аналіз хмарних технологій, як і будь-якої технології, що швидко розвивається, повинен враховувати як переваги, так і недоліки (табл. 2).

Таблиця 2

Переваги та недоліки хмарних сервісів

Переваги	Недоліки
• Не потрібен сучасний потужний комп'ютер для виконання складної обробки інформації • Комп'ютери в обчислювальній системі «хмари» завантажуються та працюють швидше, оскільки вони містять менше програм і процесів, інтегрованих у пам'ять • Збільшення обчислювальних потужностей за потребою • Менші витрати на ІТ інфраструктуру за рахунок використання обчислювальних ресурсів «хмари» для доповнення або заміни внутрішніх комп'ютерних ресурсів • Менші витрати на ПЗ; найсучасніші версії ПЗ • «Хмара» пропонує віртуально необмежений простір для зберігання інформації • Відсутність належності до одного комп'ютера чи мережі; документи та програми залишаються однаковими незалежно від того, за яким комп'ютером працює користувач • Надійність збереження даних, комп'ютерний збій у «хмарі» не призведе до втрати даних • У «хмарі» не має значення, якою операційною системою користується користувач • Хмарні сервіси значно скорочують апаратне та програмне обслуговування для підприємств усіх розмірів • Можливість багатьох користувачів легко організовувати спільну роботу над документами і проектами • Покращена сумісність форматів документів; не існує жодних форматних несумісностей, коли всі користувачі та документи знаходяться у хмарі • «Хмара» завжди має останню версію документа	• Технологія є вимогливою щодо доступу до Інтернету, його безперебійності та швидкодії; бувають випадки, коли сервер може бути недоступний, і тоді ця послуга стає неможливою • Аспекти безпеки даних; Закон України «Про захист персональних даних» не передбачає використання хмарних сервісів • Малоефективна робота у разі низької швидкості каналу зв'язку • Велика кількість ризиків втрати інформаційних даних, серед яких найголовнішими є: ризик захоплення даних на шляху від компанії до сервера, витік інформації з центрів обробки даних, де розташовані хмари

У разі виникнення ризиків у роботі проблема інформаційної безпеки в системі хмарних обчислень перетворюється в критичний елемент системи. Розглянемо деякі аспекти інформаційної безпеки «хмар».

Управління проблемами безпеки за допомогою віртуальної пам'яті

І для IBM Blue Cloud, і Microsoft Windows Azure технології віртуальних машин розглядаються як платформа основних компонентів хмарних обчислень, а різниця між Cloud Blue і Windows Azure полягає в тому, що віртуальна машина працює на операційній системі Linux або Microsoft Windows. Технологія віртуальних машин демонструє очевидні переваги, вона сприяє роботі сервера, який залежить не від фізичного пристрою, а від віртуальних серверів. У віртуальних машинах зміна фізичних параметрів або їх переміщення не впливають на надані постачальником послуги. Якщо користувачеві необхідно більше послуг, постачальник може задовольнити потреби користувачів без втручань в устаткування.

Традиційний центр обробки та забезпечення безпеки даних співвідноситься із межами апаратної платформи, тоді як хмарні обчислення можуть належати серверу з числа віртуальних серверів; віртуальний сервер може приєднуватися до різних груп логічних серверів. Тому існує можливість взаємної атаки, що веде до загрози захисту віртуальних серверів.

Аутентифікація користувачів та параметрів доступу

Хмарне середовище – це динамічний простір, в якому дані користувача передаються з центру обробки даних до клієнта-користувача. Для системи дані користувача змінюються постійно.

Можливість читання та запису даних залежить від ідентичності аутентифікації користувачів та параметрів доступу. У віртуальній машині можуть знаходитися різні дані користувача, які повинні підлягати чіткому контролю.

У хмарних обчисленнях є актуальною схема єдиного входу і корпоративної безпеки. В такому разі система звертається до сервісу контролю доступу для аутентифікації запиту до веб-сервісу. Веб-сервіс не реалізує власної схеми аутентифікації, а делегує цю задачу зовнішньому серверу. Отримавши підтвердження достовірності, веб-сервіс взаємодіє зі сховищем даних для надання інформації.

Концепція хмарних обчислень побудована на новій конфігурації

Нова конфігурація складається із розмаїття нових технологій, таких як Hadoop (програмний каркас), Hbase (один із видів нереляційних баз даних) сімейства Apache, що підвищує продуктивність системи

хмарних обчислень, але водночас може призвести до ризику. У середовищі хмарних обчислень користувачі створюють багато динамічних віртуальних організацій, які насамперед ґрунтуються на довірі між цими організаціями. Ризики часто виникають на інтерактивних вузлах між віртуальними машинами і є динамічним, непередбачуваним процесом. Середовище хмарних обчислень дає користувачеві можливість «купити» повний доступ до ресурсів, що також збільшує ризик загрози безпеці.

Вимоги до безпеки на основі аналізу HDFS

HDFS (HadoopDistributed File System) є відомою поширеною технологією хмарних обчислень, яка використовується у великомасштабних хмарних обчисленнях у типовій конфігурації розподіленої файлової системи. HDFS схожа на існуючу розподілену файлову систему, таку як GFS (Google File System); вони мають ідентичні цілі, продуктивність, доступність і стабільність. HDFS спочатку використовувалася в мережевій пошуковій системі Apache Nutch і стала основою проекту Apache Hadoop.

Аналізуючи HDFS, вимоги безпеки до хмарних обчислень можна поділити на такі групи:

- Перевірка достовірності *Логіна клієнта*: більшість хмарних обчислень перевіряють браузер клієнта і проводять ідентифікацію користувача згідно із запитом програм хмарних обчислень для первинної потреби.
- Присутність одиничної помилки з *Вузлом імені*: якщо Вузол імені атакують або зламують, це може призвести до катастрофічних наслідків у системі. Тому ефективність Вузла імені в хмарних обчисленнях і його дієвість – це ключ до успіху в інформаційній безпеці. Посилення захисту Вузла імені є критично важливим.
- Швидке відновлення блоків даних і контроль за правом читання/запису: *Вузол даних* (DataNode) – це вузол накопичення даних, де можливі проблеми та труднощі з доступом до даних.

Також необхідно враховувати й інші можливості, а саме: контроль доступу, шифрування файлів тощо.

Принципи захисту даних

Уся процедура захисту даних побудована на *конфіденційності*, *цілісності* та *доступності*. Конфіденційність належить до так званої прихованої функції фактичних даних або інформації і є однією із найжорсткіших вимог інформаційної безпеки. У випадку хмарних обчислень дані накопичуються в центрах обробки даних, де безпека та конфіденційність даних ще важливіші. Цілісність даних у будь-якому вигляді не відіграє значної ролі для гарантії несанкціонованого вида-

лення, зміни або пошкодження. Доступність даних означає, що користувачі можуть використовувати дані за рахунок використання потенціальних можливостей хмарних технологій.

Модель захисту даних

У моделі використовується тришарова захисна структура системи, кожен шар якої виконує свої власні завдання для забезпечення захисту даних на всіх рівнях «хмари».

- Перший шар відповідає за аутентифікацію користувачів цифрових сертифікатів, виданих відповідними органами; управляє кодами доступу користувачів.
- Другий шар відповідальний за шифрування даних користувача, а також захист конфіденційності користувачів у певний спосіб.
- Третій шар – використання даних користувача для швидкого відновлення.

Захист усієї системи – це останній рівень даних користувача. За допомогою трирівневої структури аутентифікація користувача використовується для забезпечення цілісності даних. Якщо в системі аутентифікації користувача відбулося нелегальне втручання і небезпечний користувач входить в систему, шифрування файлів і захист конфіденційності можуть забезпечити цей рівень захисту. На цьому рівні дані користувача зашифровуються у випадку, якщо ключ доступу був введений нелегально. Через функцію захисту конфіденційності небезпечний користувач не зможе отримати повного доступу до інформації, що дуже важливо для захисту комерційних таємниць ділових користувачів у середовищі хмарних обчислень. Нарешті, швидке відновлення шару файлів за допомогою алгоритму відновлення надає можливість даним користувача швидко відновлюватися навіть у разі великих пошкоджень.

Надійність

Перехід до хмарних технологій вимагає значного підвищення вимог до якості надання послуг доступу до Інтернет, які стають критично важливими. Найбільше в цьому питанні розвинулись американські провайдери. В американській практиці прийнято публікувати у відкритому вигляді деталізовані зобов'язання з дотримання якості надання послуг, які прописані в угодах про рівень обслуговування (Service Level Agreements). У випадку, якщо оператор не виконує своїх зобов'язань, він несе за це фінансову відповідальність.

Перегляд законодавства

Інтернет став платформою для розподілених додатків: компанія може вести конфіденційний внутрішній документообіг на чужих потужностях, уклавши контракт зі стороннім SaaS-постачальником, який,

своєю чергою, буде обробляти отримані дані на обчислювальних потужностях інших постачальників послуг IaaS і/або PaaS. Існуюче законодавство (і зарубіжне, і вітчизняне) практично зовсім не передбачає таких ситуацій.

Регулювання відносин у галузі хмарних технологій – складне завдання ще й тому, що інтереси користувачів, зацікавлених у збереженні контролю над своїми даними, та інтереси постачальників хмарних послуг, зацікавлених у максимальній свободі під час експлуатації та розвитку своїх сервісів, розходяться у протилежних напрямах. Майбутнє хмарних технологій багато в чому залежатиме від розумного компромісу обох сторін.

У дослідженні «Економіка хмарних обчислень» (The Economics of the Cloud) фахівці з Microsoft висловлюють думку, що існуючі сьогодні правові проблеми типові для будь-якої нової технології і згодом юридичні перешкоди для хмарних обчислень перестануть існувати просто в силу природного розвитку ринку [8].

NIST запропонував набір із *десяти базових принципів безпеки* для хмарних обчислень (табл. 3).

Таблиця 3

Основні принципи безпеки для хмарних обчислень

№ з/п	Принципи	Коротка характеристика принципів
1.	Прозорість	Компанії-провайдери розкривають внутрішні правила обробки інформації, а також відомості про діяльність
2.	Обмеження за сферами використання	Компанії не претендують на володіння даними замовників і можуть використовувати їх лише в тих цілях, для яких вони були отримані від замовників
3.	Розкриття	Компанії розкривають дані замовників лише у випадку, якщо це потрібно самим замовникам або передбачено законом, і повинні в такому разі попередньо повідомляти замовників про розкриття даних на вимогу правоохоронних органів у тій частині, наскільки це дозволяє законодавство
4.	Система управління безпекою	Компанії володіють потужною системою захисту даних, що відповідає міжнародним стандартам (таким, як ISO 27002)
5.	Додаткові можливості у сфері безпеки	Компанії зобов'язуються пропонувати замовникам додаткові можливості щодо захисту їх даних

Продовження таблиці 3

6.	Розміщення даних	Компанії надають замовникам список країн, в яких розміщуються пов'язані з ними дані
7.	Повідомлення про витоки інформації	Компанії оперативно повідомляють замовників про всі відомі витоки, які ставлять під загрозу конфіденційність або цілісність даних
8.	Аудит	Компанії звертаються до послуг сторонніх аудиторів з метою перевірки того, наскільки їх система управління безпекою відповідає вимогам відповідних стандартів
9.	Переносимість даних	Компанії надають замовникам можливість вивантаження даних у стандартному форматі, придатному для передавання через Інтернет
10.	Звітність	Компанії співпрацюють із замовниками в адекватному розподілі обов'язків під час складання звітності «Про приватність і безпеку»

Незважаючи на те, що зазначені пропозиції не набули широкої підтримки з боку учасників галузі, найімовірніше, в майбутньому дискусія призведе до вироблення загальногалузевих правил – спочатку в США і Європі, пізніше, а, можливо й одночасно, в інших країнах. Це сприятиме регулюванню інтересів користувачів і постачальників хмарних послуг.

Українське законодавство поки що не надає хмарним технологіям особливої уваги. Насамперед немає розробленого договору двох сторін, який би врегульовував відносини між користувачем та провайдером, що надає хмарні потужності, водночас як у Європі процес оновлення законодавства в цьому напрямі досить активний.

Висновки. Ідея доступних комп'ютерних послуг стає реальністю. Можливості «хмар» дозволяють розв'язувати завдання бізнесу та надавати користувачам сервіси в коротші терміни. Центри обробки даних отримують можливість надавати свої послуги більшій кількості користувачів. Розробники можуть думати про нові генерації своїх продуктів.

Передбачають, що масової міграції комерційних структур у публічні «хмари» не буде, повної відмови від власних дата-центрів також не передбачається – хмарні сервіси прийдуть до гібридної моделі, де збережуться обидва елементи.

Програмні застосування майбутнього матимуть частину, що працює на комп'ютері користувача, та частину, що працює у «хмарі», причому хмарна частка повинна швидко розширюватись для роботи з тисячами серверів в разі потреби, а також зменшуватись до роботи

на одній віртуальній машині. Мають бути розроблені системи керування енергетичним забезпеченням, щоб зробити можливим переведення у режим енергозбереження сервери разом з усією пам'яттю та мережею. І це також є одним з елементів інформаційної безпеки.

Ще потрібно не просто розробити правову модель використання нової технології, а й розподілити відносини між користувачами та постачальниками, забезпечивши найбільш розумний баланс між їхніми інтересами.

Питання інформаційної безпеки технології хмарних сервісів потребують значного вдосконалення, а в багатьох аспектах – першочергових розробок і напрацювань.

1. Белов Е. Б. Основы информационной безопасности: учеб. пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия-Телеком, 2006. – 544 с.

2. Бондар Є. С. Хмарні обчислення та їх застосування / Є. С. Бондар, М. М. Глибовець, С. С. Гороховський // Вісник КНУ ім. Т. Шевченка. – Вип. № 1. – К.: КНУ, 2011. – С. 74–82.

3. Гриджук Г. С. Систематизація методів інформаційної безпеки підприємства / Г. С. Гриджук. [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf

4. Гудзовата О. О. Хмарні сервіси: можливості, безпека, перспективи: колективна монографія: у 4 т. / О. О. Гудзовата // Теоретичні та прикладні аспекти підвищення конкурентоспроможності підприємств. – Дніпропетровськ: «Герда», 2013. – Т. 1 – 352 с. (Розділ 1.12). – С. 102–110.

5. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посібник / Б. А. Кормич. – К.: Кондор, 2004. – 384 с.

6. Облачные сервисы. Взгляд из России / под ред. Е. Гребнева. – М.: CNews, 2011. – 282 с.

7. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко. [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

8. Федоров А. Г. Windows Azure: облачная платформа Microsoft / А. Г. Федоров, Д. Н. Мартынов. [Электронный ресурс]. – Режим доступа: http://kak.znate.ru/docs/index-61012.html

9. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М.: ФОРУМ, 2013. – 416 с.

Гудзовата О. О. Информационная безопасность облачных сервисов.

В статье охарактеризованы технологию облачных сервисов, проанализированы основные задачи и принципы ее информационной безопасности,

определены перспективы развития как самой технологии, так и параметров безопасности.

Ключевые слова*: облачные сервисы (вычисления), информационная безопасность, технология, инфраструктура.*

Gudzovata O. O. Informational safety of the cloud computing.

In this article the author describes the technology of cloud computing, analyses the main tasks and the principles of its informational safety, defines the perspective of the development of this technology and the safety's options.

Key words*: cloud computing, informational safety, technology, infrastructure.*

Стаття надійшла 18 жовтня 2013 р.

УДЕ 65.012.8(477)

З. Б. Живко

ЗАБЕЗПЕЧЕННЯ ЕКСПЕРТНОЇ ОЦІНКИ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В статті досліджено вибір і застосування методів математичного та імітаційного моделювання функціонування системи моніторингу та об'єктів спостереження. Для визначення відповідності потенційного експерта необхідним вимогам запропоновано використовувати анкетне опитування, самооцінку експерта та оцінювати компетенції експерта.

Ключові слова*: моніторинг, економічна безпека підприємства, компетенції експерта, анкетне опитування, самооцінка експерта, коефіцієнт конкордації.*

Постановка проблеми. Моніторинг системи економічної безпеки підприємства передбачає реалізацію широкого комплексу заходів організаційного, методологічного й управлінського характеру з метою визначення і вибору оптимального поєднання різноманітних форм і видів оцінки зовнішнього та внутрішнього середовища, дослідження стану окремих функціональних складових економічної безпеки з урахуванням особливостей кожної конкретної ситуації, що є дуже важливим та вимагає ретельного дослідження.

Стан дослідження. З історії менеджменту очевидно, що швидкість змін зовнішнього середовища безперервно зростає [1], а відтак сучасний менеджмент у разі неможливості функціонувати ізольовано найперше висуває проблеми адаптованості до змін зовнішнього