УДК 65.012.8

А.В. Бєгун, канд. екон. наук, доцент,
ДВНЗ «КНЕУ імені Вадима Гетьмана»

ТЕНДЕЦІЇ РОЗВИТКУ РИНКУ ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЕКОНОМІЦІ

АНОТАЦІЯ. Стаття присвячена аналізу ринку розвитку засобів інформаційної безпеки діяльності економічних систем. Основна увага приділяється безпеці хмарних технологій для корпоративних клієнтів. Цей процес повинен існувати в умовах збалансованого дійства: безпека — витрати.

ABSTRACT. The article is sanctified to the market of development of facilities of informative safety of activity of the economic systems analysis. Basic attention is sanctified to safety of cloudy technologies for corporate clients. This process must exist in the conditions of the balanced action: safety is charges.

КЛЮЧОВІ СЛОВА. Економічна система, безпека, ринок засобів безпеки, хмарні технології, гібридна модель, публічна хмара, оркестрування.

Вступ. Інформаційна безпека (ІБ) у сфері сучасних інформаційних технологій є невід'ємною складовою суб'єктів економічних відносин. У першу чергу це пов'язано з тим, що кількість інформаційних атак з кожним роком збільшується як в Україні, так і в усьому світі [1]. До основних факторів такого росту кількості впливів можна віднести наступні:

— з кожним роком збільшується кількість користувачів загальнодоступних мереж зв'язку, де в якості нових користувачів виступають як окремі клієнтські робочі станції, так і корпоративні мережі;

— збільшується кількість вразливих місць в існуючому системному і прикладному програмному забезпеченні;

— зростає кількість розроблених засобів реалізації атак на маршрутизатори, комутатори, міжмережеві екрани тощо;

— спрощуються методи реалізації інформаційних атак;

— збільшується кількість внутрішніх атак з боку користувачів.

Для багатьох компаній важливо не тільки захистити свої локальні мережі та інформаційні ресурси від проникнення ззовні, але і організувати надійні, безпечні системи взаємодії з підрозділами через Інтернет. Свого рішення чекають також задачі електронної комерції, де без вживання особливих засобів з інформаційної безпеки й конфіденційності транзакцій неможливе їх широкомасштабне використання [2, 3]. За результатами дослідження, прове-

деного серед 1 700 організацій в усьому світі, 72 % респондентів прогнозують підвищення рівня ризику внаслідок зростання зовнішніх загроз. Проте лише близько третини респондентів переглянули стратегію інформаційної безпеки за останні 12 місяців [7].

Виклад основного матеріалу. Підвищені вимоги регулюючих органів до рівню безпеки і особливо до збереження конфіденційних даних ініціювали появу на ринку не лише самих засобів захисту, але і систем управління цими засобами: побудова процесів управління інцидентами, конфігураціями і засобами їх автоматизації. Водночас світовий бізнес почав ставити підвищені вимоги до візуалізації засобів аналізу, моніторингу і створення єдиного центру управління інформаційною безпекою в кожній компанії. За таких умов проявилися деякі загальні тенденції розвитку ринку засобів безпеки. По-перше, бізнес має інтерес не тільки з приводу дотримання законодавства у сфері ІБ, а і з приводу того, що дає ІБ бізнесу. Іншою загальносвітовою тенденцією є галузева стандартизація у сфері ІБ. Наприклад, постанова НБУ від 28.10.2010 року № 474, за якою банки повинні впровадити систему управління інформаційною безпекою (СУІБ) у відповідності до стандартів НБУ і розробити систему відповідальності за умов невиконання цього стандарту. Третім фактором, що визначає майбутнє ринку ІБ, є поява «хмарних обчислень» (cloud computing) — технології розподільної обробки даних, у якій інформаційні ресурси і потужності надаються користувачеві як інтернет-сервіс. У технології Cloud Computing ресурси Cloud-середовища швидко розгортаються й легко масштабуються, а ініціалізація усіх процесів, додатків і сервісів виконується за вимогами незалежно від місця знаходження користувача. Тут, безумовно, виникають питання безпеки, оскільки критично важливі сервіси надаються сторонньою організацією на умовах аутсорсингу. В цьому випадку об’єктами захисту стають гіпервізори, віртуальні машини і пристрої доступу до ІТ-сервісів. Але такий підхід порушує існуючу парадигму периметрового захисту ІТ-інфраструктури й підштовхує розробників до формування нових програмних продуктів з управління корпоративною ідентифікацією, доступом до документів і захисту баз даних.

При виборі рішень для побудови системи безпеки хмари важливим елементом є технологічний фактор. Підхід до побудови такого рішення не обмежується тільки управлінням «великої» віртуалізації (кількість віртуальних процесорів, віртуальної пам’яті) і полягає у цілісному управлінні усіма компонентами хмари: гі-

первізорами (у тому числі й сторонніми), апаратним забезпеченням, глибоким моніторингом критично важливих для бізнесу та інфраструктурних додатків, а також автоматичної оркестровки складових управління. Даний підхід реалізується різноманітними продуктами. В якості прикладу розглянемо стислий аналіз деяких рішень хмари з точки зору визначених його компонентів (табл. 1).

Таблиця 1

СИСТЕМИ УПРАВЛІННЯ ТА ОРКЕСТРУВАННЯ ВЕДУЧИХ КОМПАНІЙ [4,5]

	Microsoft	*VMware*
Гіпервізор	**Hyper-V** — Динамічна пам'ять — HA/Clustering — Live Migration — Quick Storage Migration	**ESXi/ESX 4.1** — Декілька технологій управління пам'яттю — HA — vMotion — Storage vMotion
Стек управління	**System Center** — Управління гіпервізорами — Управління фізичним і віртуальним середовищем — Управління додатками — Установка додатків всередині гостевих ОС за допомогою msdeploy, SQL DAC	**vCenter** — Обмежений управлінням тільки ESXi/ESX — Не управляє фізичним оточенням — Не може моніторити продуктивність і додатки в середині віртуальних машин
Автоматизація та оркестровка	**SystemCenterOpalis/Orchesrator** — Найкращий у своєму класі засіб створення процедур та оркестрування, інтеграція з SystemCenter і компонентами приватної хмари Microsoft — Просте оточення для створення нових процедур — Повна автоматизація ЦОД — Інтеграція із сторони рішень управління	**vCenter Orchesrator** — Відсутність інтеграції з vCloud Director — Складне створення процедур — Автоматизація тільки віртуалізованої частини ЦОД — Відсутність інтеграції із сторонніми рішеннями
Управління сервісами	**SC AppControles, SCVMM 2012** — Пули ресурсів (хмари в VMM 2012) — Логічні мережі в VMM 2012	**vCloud Director, vCenterChargeback, vShield** — Пули ресурсів (Resource Pools) — Логічні мережі (vCloud Director)

Закінчення табл. 1

	Microsoft	*VMware*
	— Управління сховищем — Множина ВМ — Сервісна модель з інтеграцією балансировників — Портал самообслуговування (AppController) — Управління додатками в VMM і Azure — Потужні партнерські рішення для Chargeback — Властивості безпеки в WS2R8 R2 і Forefront **— Встановлення політик та SLAs для додатків**	— Управління сховищем (vCenter) — Множина ВМ (vApp) — Портал самообслуговування (vCloud Director) — Відсутність інтеграції з PaaS; vCloud Director не може управляти додатками в GAPE або VMforce — Базовий chargeback без інтеграції з біллінгом vShield Edge, який включений до vCloud Director і не надає брандмауер DHCP, NAT і VPN **— Не можна встановлювати політики для додатків**

Відомо, що найбільш популярним хмарним сервісом серед економічних суб'єктів є електронна пошта; далі — хмарні системи зберігання даних — Dropbox, Microsoft SkyDrive, Google Drive; і, наприкінці, корпоративні портали, які забезпечують сумісну роботу над документами, заявками, угодами. До окремим структурам хмарних бізнес-додаткам належать CRM, HRM та інші.

Сучасний ринок «хмарних технологій» пропонує кілька структур: публічні, приватні та гібридні хмари. Кожна із запропонованих структур має свої особливості функціонування, які орієнтовані на відповідну галузь або предметну область застосування. Так, наприклад, відповідальність за підтримку безпеки сервісів або інфраструктури в приватній хмарі несе IT-підрозділ фірми, то в публічному — компанія-провайдер. Для середнього і великого бізнесу найбільш привабливою хмарою пропонується гібридна модель — симбіоз публічної та приватної. З точки зору безпеки така модель представляється найбільш надійною, так як забезпечує можливість зберігати особливо важливу інформацію і сервіси в середені компанії (приватна хмара), а решту в публічній хмарі (рис. 1).

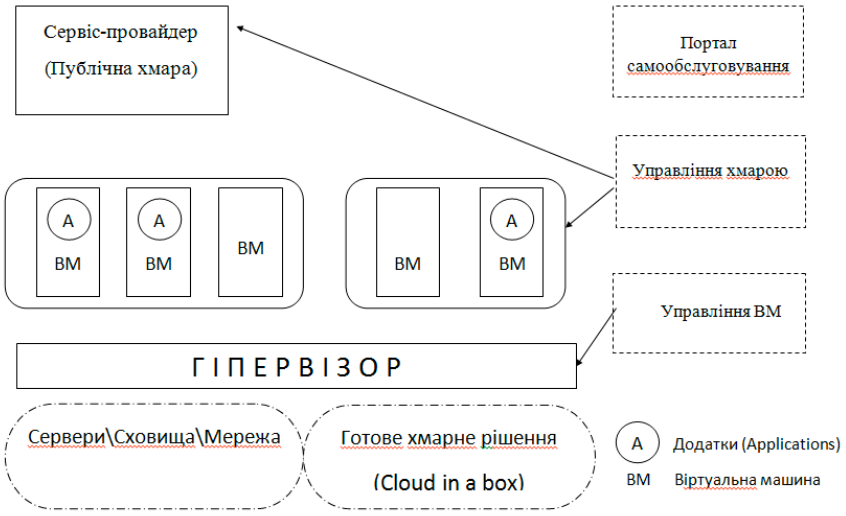

Рис. 1. Загальна схема гібридної хмари

Особливість формування безпеки гібридної моделі полягає у необхідності створення взаємодії між складовими приватної та публічної хмар; забезпечення управління усіма користувачами, контроль над сервісом і доступом інформації. При цьому усі дії повинні відбуватися в єдиному інформаційному просторі. Наприклад, користувачі електронної пошти, які повинні мати одне доменне ім'я, знаходяться як у публічній хмарі, так і в корпоративному Datacenter при єдиних стандартах безпеки і правилах користування. В таких умовах супроводження користувачів і сервісу виконує одна служба.

На ринку засобів безпеки клієнтів малого и середнього бізнесу перевага віддається моделі публічної хмари, а великі компанії — в силу їх внутрішньої політики конфіденційності, фінансової потужності та вимог регуляторних органів — здатні створювати приватні хмари. Ринок сервісів безпеки буде стрімко зростати з однієї простої причини — складна економічна ситуація не дозволяє нести великі витрати на побудову своїх власних хмар. В таких умовах багатьом компаніям в силу розвинутих технологій бізнесу простіше укладати угоду з деякою компанією-підрядником, яка буде надавати послуги захисту публічної хмари та її сервісів. Але для фінансових установ договірні відносини в сфері безпеки не завжди мають креативний зміст. По-перше, існування великої

кількості регуляторних політик у фінансовому середовищі забороняє виводити інформацію та обчислювальний потенціал за межі власної інформаційної системи. По-друге, фінансова діяльність накладає певні обмеження на розповсюдження власних даних і недовіру до зовнішніх постачальників знань. І, по-третє, враховуючи перші дві обставини діяльності фінансового середовища, більшість установ цієї сфери надає перевагу будівництву власних хмар. У той же час деякі функції (сервіси) агентів можна залучити до публічної хмари, яка використовує гібридну модель.

Застосування планшетних мобільних пристроїв і смартфонів займає важливе місце в списку найбільш серйозних проблем, з якими стикаються компанії при впровадженні нових технологій. При цьому більше половини респондентів розглядають дану проблему як складну або дуже складну. Зміни в політиці компанії і створення програм з підвищення обізнаності співробітників є двома основними заходами контролю ризиків, які виникають у зв'язку з появою нових мобільних технологій. Рівень застосування заходів безпеки та використання відповідного програмного забезпечення залишається низьким. Наприклад, криптографічні технології використовуються менш ніж у половині (47 %) організацій [7].

Тому одним із актуальних питань підтримки безпеки хмарних технологій в економічній сфері є розв'язання проблеми конфліктності платформ, пристроїв і провайдерів, які не дозволяють встановлювати конкретні стандарти безпеки, допомогти ІТ-службам у їх роботі. Наприклад, якщо компанія забезпечує можливість роботи з мобільними пристроями, то цей процес створює виклик усієї системи ІТ-безпеки. Ці пристрої є додатковим каналом витоку інформації; виникає критична необхідність розвертання у них додаткових сервісів, які забезпечують криптозахист, додаткову аутентифікацію користувачів, віддалений контроль пристроїв і жорсткий аудит доступу до інформації. І тут хмарні технології безумовно зможуть забезпечити оптимальний баланс між мобільністю та безпекою.

Висновки. Сучасний ринок засобів інформаційної безпеки потребує нових, більш надійних систем застосування, особливо в захисті мобільних ресурсів. Тут, безумовно, корисним буде залучення хмарних технологій із виведенням довіреного прикладного процесу в область функціонування гіпервізору, тобто за межу досяжності користувача й операційної системи як мобільного пристрою, так і віртуальної платформи (PaaS). Такий підхід, забезпечений відомими методами захисту, створює умови для повно-

цінної реалізації комплексної безпеки економічних об'єктів. Скорочення витрат в умовах покращення забезпечення сервісів — головне завдання хмарних моделей незалежно від того, які вони — приватні чи гібридні. Але цей процес повинен існувати в умовах збалансованого дійства: безпека — витрати.

Література

1. *Андрианов В. В*. Обеспечение информационной безопасности бизнеса / В.В. Андрианов, С.А. Зефиров, В.Б. Голованов, Н.А. Голдуев. — 2-е изд., перераб. и доп. — М.: ЦИПС и Р: Альшина Паблишерз, 2011. — 373 с.
2. *Бєгун А.В., Білошицький О.В*. Квазідинамічне моделювання аналізу віртуальних текстів // Зб. Культура народів Причорномор'я. — 2012. — № 238. — С. 15—19.
3. *Бєгун А.В*. Інформаційна парадигма безпеки економічної системи. — Зб. Моделювання та інформаційні технології в економіці. № 83. — 2011. — С. 144—151.
4. http://www.nist.gov/itl/cloud/
5. http://www.microsoft.com/virtualization/tn/us/solution-buisness-apps.aspx
6. http://www.gartner.com/technology/media-products/microsoft/vol2/article8a.html
7. http://www.ey.com/ua

Стаття надійшла до редакції 11.12.2012 р.

УДК 519.86+330.3:005.21

О.П. Суслов, д-р екон. наук, професор
професор кафедри інформаційного менеджменту,
Б.О. Тішков, старший викладач
кафедри інформаційних систем в економіці,
ДВНЗ «КНЕУ імені Вадима Гетьмана»

МОДЕЛЮВАННЯ СТРАТЕГІЇ РОЗВИТКУ ПІДПРИЄМСТВА

АНОТАЦІЯ. У статті здійснено моделювання стратегії екстенсивного та інтенсивного розвитку підприємства за рахунок прибутку від його основної діяльності.

КЛЮЧОВІ СЛОВА: моделювання, стратегія, продукція, інвестиції, інновації, прибуток, ефективність.