

- nkoO.pdf.–
16. Осовська Г.В. Основи менеджменту: Підручник / Г.В. Осовська – К.: Кондор, 2006. – 664 с.
 17. Markowitz Harry. Portfolio selection / H. Markowitz // J.Finance, 1952. – V.7. – P. 77– 91.
 18. Diamond D. Liquidity, Banks, and Markets / D. Diamond // Journal of Political Economy. – 1997. – # 105. – P: 928 – 956.
 19. Економічна теорія. Політекономія: підручник / В.Д. Базилевич, В.М. Попов, К. Базилевич, Н.І. Гражевська – К.: Знання– Прес, 2008. –719 с.
 20. Офіційний сайт Фондової біржі «Українська біржа» / [Електронний ресурс]. – Режим доступу: <http://www.ux.ua>.
 21. Масленніков Є.І. Методологічні та практичні засади дослідження системи управління фінансовою стійкістю промислового підприємства [моногр.] / Є.І. Масленніков. – Одеса : Прес-кур'єр, 2015. – 316 с.

РОЗДІЛ 23

ІННОВАЦІЙНО-ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНТЕЛЕКТУАЛЬНО-КАДРОВОЇ СКЛАДОВОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

*к.е.н., доцент,
доцент кафедри обліку, аналізу і аудиту
Одеський національний політехнічний університет
Башинська І.О.*

В сучасних умовах активного розвитку інформаційного суспільства та формування економіки знань особливого значення набуває інноваційна сфера діяльності, з якою пов'язане стійке економічне зростання будь-якої держави. Справді, як свідчить міжнародний досвід, національна економічна безпека будь-якої держави усе більше залежить не від її військового чи природно-ресурсного потенціалу, а від розвитку інноваційної сфери, яка, проникаючи в різні галузі національної економіки, зумовлює їх постійну модернізацію і перехід до нових моделей розвитку.

В умовах ринку ефективний розвиток національної економіки значною мірою залежить від забезпеченості її економічної безпеки. Створення сприятливих умов для розвитку бізнесу та реалізації права на підприємництво є невід'ємною складовою розвитку та економічної безпеки України, пріоритетною функцією уряду. Належний рівень бізнесу економічної безпеки є ключем до соціально-економічного розвитку, так як ринок, в якому конкуренція є основним компонентом, що загрожує.

У вітчизняній літературі, категорію «безпека» майже не розроблено, тому що в нашій країні безпека була монопольною, дуже

закритою сферою вищих політичних лідерів і вчені у вирішення цих проблем не заохочувались. Однак природний розвиток суспільства викликав неминучу еволюцію у ставленні і підходах до вивчення цієї концепції, еволюцію категорії.

Серед існуючих в економічній науці підходів до дослідження безпеки можна виділити дві групи. Перша – це вузько спеціалізований підхід, який передбачає аналіз окремих сторін безпеки суб'єктів або окремих видів безпеки у відокремленні від інших, наприклад безпека праці, екологічна, та ін., тобто спрощене тлумачення безпеки, розгляд її тільки в якомусь одному аспекті. Автори, досліджуючи вибраний тип безпеки, дають часто суперечливі думки, не узгоджуються між собою щодо визначення даного поняття, вибудовуються лише на підставі авторської позиції. Друга – розширювальне трактування, розвиваються межі поняття. Економічна безпека розглядається, по-перше, як діяльність певних соціальних суб'єктів, як сфера відносин, що виникають між ними, і сфера, в якій функціонує і розвивається суспільне, групове та індивідуальне свідомість, по-друге, як предмет теоретичного і емпіричного пізнання і, по-третє, як об'єкт аналізу з позицій політики, права, моралі.

Так, під *економічною безпекою* пропонуємо розуміти стан економічної системи, що характеризується наявністю конкурентних переваг, які досягаються ефективним використанням існуючих власних та залучених ресурсів, своєчасним впровадженням комплексу заходів з метою підтримання нормальних умов працездатності системи для максимального досягнення поставлених цілей у короткостроковому та довгостроковому періоді в умовах постійної зміни навколишнього середовища [1].

Суть економічної безпеки підприємства полягає у такому стані його економічної системи, який може бути охарактеризовано збалансованістю, стабільністю і стійкістю до негативного впливу будь-яких загроз, її здатністю забезпечити на основі своїх власних економічних інтересів стійкий й ефективний розвиток.

Інтелектуально-кадрову складову (ІКС) економічної безпеки підприємств визначають як синтетичну категорію економічної теорії, теорії управління персоналом, економіки праці, соціології, політології.

ІКС економічної безпеки є уніфікованою категорією, яка виявляється на всіх рівнях від окремо взятого підприємства до національної економіки і відіграє домінуючу роль у системі безпеки підприємства, оскільки ІКС первинна для інших її складових в будь-якій організації. Інтелектуально-кадрова складова охоплює безпеку життєдіяльності, соціально-мотиваційну безпеку, кар'єрну, професійну, адміністративну безпеку та розглядається як механізм запобігання негативним впливам на економічну безпеку підприємств через ризики і погрози, пов'язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами [2].

В умовах жорсткої конкуренції діяльність суб'єктів господарювання вимагає від керівників різних рівнів уміння ефективно управляти не тільки фінансово-господарськими процесами, а й ризиками шахрайства і маніпуляцій як всередині підприємства так і зловживаннями ззовні. Велика кількість різноманітних показників системи забезпечення, що відображають стан окремих її елементів, можуть бути об'єктами економічних злочинів. Тому запровадження модернізації забезпечення інформаційних потреб економічної безпеки підприємства на основі новітніх інформаційних технологій дуже актуальне.

Інформаційні технології (ІТ) – це системно організована для вирішення завдань управління сукупність методів і засобів реалізації операцій збирання, реєстрації, передачі, накопичення, пошуку, обробки і захисту інформації на базі застосування розвинутого програмного забезпечення, використання засобів обчислювальної техніки і зв'язку, а також способів, за допомогою яких інформація надається тим, хто її потребує [3].

Інформаційні технології наразі можна класифікувати за рядом ознак, зокрема: способом реалізації в інформаційній системі, ступенем охоплення завдань управління, класами здійснюваних технологічних операцій, типом призначеного для користувача інтерфейсу, варіантами використаня мережі ЕОМ тощо.

Управління пов'язане з обміном інформацією між компонентами системи, а також системи з навколишнім середовищем. В процесі управління одержують відомості про стан системи в кожен момент

часу, про досягнення (або не досягнення) заданої мети з тим, щоб впливати на систему і забезпечити виконання управлінських рішень.

Автоматизована інформаційна система є сукупністю інформації, економіко-математичних методів і моделей, технічних, програмних, технологічних засобів і фахівців, призначена для обробки інформації і прийняття управлінських рішень.

З кожним роком збільшується залежність організацій від використовуваних в них інформаційних систем та інформаційних технологій. Характерна риса нових (сучасних, перспективних, інноваційних) інформаційних технологій полягає в активному залученні кінцевих користувачів – непрофесіоналів у сфері обчислювальної техніки в процес підготовки управлінських рішень завдяки встановленню на їхніх робочих місцях сучасних комп'ютерів [4].

Використання нових інформаційних технологій суб'єктами господарювання можна розглядати в кількох напрямках: використання прикладних програмних рішень для вирішення конкретних управлінських задач; створення електронних та віртуальних офісів з використанням роботи працівників «вдома»; застосування «хмарних» сервісів; сховища даних; функціонування «інтелектуальних» споруд тощо.

Під *інноваційно-інформаційнимі технологіями (ИИТ)* пропонуємо розуміти методи та способи збору, зберігання, передачі та обробки інформації, що засновані на використанні новітніх технічних засобів та програми суттєво поліпшують різні сфери діяльності людства.

Забезпечення сучасного бізнес-середовища потребує, щоб усі одиниці підприємства працювали як єдиний і злагоджений механізм. Цьому процесу сприяють сучасні ERP (Enterprise Resource Planning) системи, які автоматизують бухгалтерський, фінансовий, управлінський, логістичний, виробничий, складський, кадровий та інші види обліку. ERP системи надають керівництву інформацію для аналізу поточного стану організації і прийняття обґрунтованих управлінських рішень; забезпечують прозорість і контроль діяльності підприємства на всіх рівнях. Такі системи уможливають побудову ефективної взаємодії з контрагентами і клієнтами; знижують

трудомісткість процесу бюджетування і ведення бюджетного контролю витрат; скорочують обсяг ручної і рутинної роботи працівників, знижують адміністративні витрати. Вибір ERP платформи залежить від типу підприємства, структури його бізнес-процесів і перспектив подальшого розвитку. Лідерами комплексної автоматизації підприємств є Microsoft, SAP, Oracle, «Галактика ERP». Об'єднання в єдиний інформаційний простір стає найбільш ефективним у тому разі, якщо працівники в будь-який момент мають доступ до корпоративної системи і можуть виконувати свої обов'язки, незалежно від свого місцезнаходження («мобільні робочі місця»). Потенційними замовниками продукту «Мобільне робоче місце» є малий і середній бізнес. Використовуються віртуальні офіси. В середньому, кількість працівників, які працюють у віддаленому режимі, складає 20% загального штату. При цьому «віртуальні робочі місця», які передбачають, що працівник працює без фізичної присутності в офісі, існують у 80% компаній [5].

Останнім часом підприємства залучаються до «хмарних» обчислень, використовуючи канали Інтернет для того, щоб отримати доступ до ресурсів віртуального центру обробки (ЦО), який має необхідну процесорну потужність, оперативну пам'ять і дисковий простір [6]; орендують програмне забезпечення тощо.

Для розвитку і процвітання бізнесу потрібно чітко і швидко визначати категорію показників, на підставі яких слід приймати рішення, проводити аналіз показників з різним ступенем деталізації з урахуванням усіх параметрів, які на них впливають. Якісна віртуалізація даних, орієнтованих на різні групи працівників і відділів – одна із основних задач, які вирішуються за допомогою сховища даних (Data Warehouse) – центру, в якому збирається вся необхідна інформація із різних підрозділів підприємства [7].

Новітні технології пропонують так звані «інтелектуальні будівлі». Досвід експлуатації показує, що в спорудах, старших за 40 років, основна маса (до 90 % витрат) – це переплата за водопостачання, енергоресурси, а також на ремонт обладнання і оплату праці інженерів. Будівлі зі штучним інтелектом скорочують витрати на управління і експлуатацію. Сучасна система телекомунікації (супутниковий зв'язок,

ЛОМ, Інтернет і телебачення) дозволяють проводити відеоконференції, наради, дискусії (навіть у інших містах), тобто зекономити час і витрати підприємства на поїздки і відрядження [8].

Активний обмін великими обсягами інформації зумовлює високі вимоги до продуктивності, безпеки і відмовостійкості ІТ-інфраструктури підприємства. Якісне функціонування ІТ-інфраструктури офісів, їх інтеграція в єдиний інформаційний простір і подальший розвиток ІТ-інфраструктури безпосередньо впливають на основний бізнес підприємства. Тому аудит інформаційної системи допомагає отримати об'єктивну оцінку її поточного стану, процесів і подій, пов'язаних з її функціонуванням.

Отже, постійне зростання обсягів і надалі ускладнюватиме пошук корисної і необхідної інформації. Очікуються радикальні зміни і в області взаємодії людини з технікою. Ми будемо дедалі частіше зустрічатися з «віртуальними людьми», автоматичними емоціями, жестами, реакціями. З'являться нові інтерфейси для прямої взаємодії між комп'ютером і людським мозком [9].

Хмарні Технології

Питання спрощення обігу та зберігання інформації стає дедалі більш актуальним. А враховуючи значну кількість незручностей під час користування, наприклад, паперовим документообігом, з якими стикаються не тільки українці, популярність отримують різноманітні технологічні рішення, покликані оптимізувати процеси з обробки та зберігання інформації.

Чи не найбільш вдалим рішенням цієї проблеми є використання хмарних технологій. Йдеться про сервер або мережі, де зберігаються дані і програми і які є доступними за умови під'єднання до мережі Інтернет. Крім того, хмарні технології дозволяють використовувати програми без встановлення, вести значно більш ефективне управління, наприклад, підприємством, завдяки тому, що вся управлінська і облікова інформація буде централізованою. Простим прикладом хмарних технологій є сервіси електронної пошти, наприклад Gmail, коли користувачеві потрібно тільки підключення до Інтернету, щоб відправити лист з необмеженим розміром прикріплених документів.

За одностайними прогнозами провідних консалтингових

компаній світу, швидке вдосконалення та поширення хмарних технологій (cloud computing) зараз є одним з тих ключових трендів, що в найближчі 5-8 років помітно вплинуть на глобальний розвиток не лише ІТ-індустрії, але й бізнесу, фінансів, державного управління, медицини, освіти і багатьох інших сфер людського життя [10; 11; 12; 13]. В умовах випереджувального розвитку ІКТ і чергового спаду світової економіки технологія, яка, наприклад, дає змогу організаціям та іншим суб'єктам відмовитись від значних витрат на власну ІТ-інфраструктуру на користь отримання всіх необхідних ІТ-ресурсів онлайн, розглядається як перспективний та рентабельний модернізаційний вибір, оптимальна інвестиція в майбутнє. Достатньо сказати, що, за підрахунками авторитетної International Data Corporation (IDC), вже у 2015 році до 60 % всіх даних людства зберігатиметься у хмарах [14]. У найрозвиненіших регіонах світу вже прийняті стратегічні рішення та плани дій щодо системного та комплексного розвитку хмарних сервісів, розгорнута відповідна робота. Інтерес українців до хмарних технологій за останній рік значно зріс. Так, за даними компанії IDC, обсяг продажів хмарних послуг IaaS / SaaS в Україні в 2014 році виріс, у порівнянні з 2013 роком, на 47% до \$ 8,5 млн.

Бізнес всіх рівнів, прагнучи скоротити витрати, дедалі частіше «йдуть у хмари» для вирішення виробничих завдань. Це, у свою чергу, стимулює зростання надання подібних послуг. Експерти відзначають, що вже 47% великих підприємств, 83% середніх і 17% малих оцінили переваги хмарних технологій.

Активізували інтерес бізнесу до хмарних технологій також події в країні. Зокрема, тимчасова втрата частини території, економічний спад стимулюють підприємців шукати шляхи мінімізації ризиків для функціонування свого бізнесу.

Відповідно, хмарні технології стають зручним інструментом і в плані скорочення витрат, і мінімізації фінансових та інших ризиків. Таким чином, серед основних переваг хмари: доступність, мобільність, економічність, надійність роботи та ін.

Зважаючи на зростаючу цікавість підприємців до хмарних технологій, ринку пропонуються нові хмарні рішення, конкурентні як

в плані технологій, так і фінансових умов.

Хмарні обчислення — зберігання, обробка та використання даних на дистанційно розташованих комп'ютерах шляхом отримання доступу через Інтернет [15; 16].

Дослідження хмарних технологій проводить і Національний Інститут стандартів та технологій (США), коротко NIST (The National Institute of Standards and Technology). Зазначена структура відповідає за розробку стандартів та положень, що включають мінімальні технічні вимоги для забезпечення адекватної інформаційної безпеки інформаційних активів державних структур США. У свою чергу, NIST дає таке визначення хмарним обчисленням: «Хмарні обчислення – модель надання широкого і зручного мережевого доступу до загального пулу керованих обчислювальних ресурсів та їх послуг (наприклад, мереж, серверів, систем зберігання, додатків і сервісів), які можуть бути швидко надані або звільнені з мінімальними зусиллями з системи управління при необхідності забезпечення взаємодії з провайдером послуг (сервіс-провайдером)» [17].

За документації IEEE, хмарні технології – це «парадигма, яка постійно зберігає для користувача інформацію на інтернет-серверах і лише тимчасово кешується на стороні користувача». Це можуть бути не тільки стаціонарні комп'ютерні системи, а й ноутбуки, планшети, смартфони тощо.

Ідея того, що зараз називається хмарними обчисленнями, вперше була озвучена Джозефом Карлом Робнеттом Ліклайдера (JCR Licklider) в 1970 році, коли він був відповідальним за розробку ARPANET (Advanced Research Projects Agency Network). Ідея Ліклайдера полягала в тому, що кожна людина буде підключений до мережі, з якої він буде отримувати не тільки дані, але і програми. Інший вчений Джон Маккарті (John McCarthy) говорив про те, що обчислювальні потужності будуть надаватися користувачам як послуга (сервіс). На цьому розвиток хмарних технологій було призупинено до 90-х років. Її розвитку посприяли ряд факторів:

– стрімкий розвиток мережі Інтернет, а саме пропускної здатності. Хоча на початку 90-х глобальних проривів в області хмарних технологій не відбулося, сам факт «прискорення» інтернету

дав поштовх до якнайшвидшому розвитку технології;

– у 1999 році з'явилася компанія Salesforce.com, яка надала доступ до свого додатку через сайт. Вона стала першою компанією, що надала своє програмне забезпечення за принципом «програмне забезпечення як сервіс» (SaaS);

– у 2002 році Amazon запустила свій хмарний сервіс, де користувачі могли зберігати інформацію і проводити необхідні обчислення;

– у 2006 році Amazon запустила сервіс Elastic Compute cloud (EC2), де користувачі могли запускати свої власні додатки. Таким чином, сервіси Amazon EC2 і Amazon S3 стали першими сервісами хмарних обчислень;

– свій внесок у розвиток хмарних обчислень внесла компанія Google зі своєю платформою Google Apps для веб-додатків в бізнес секторі;

– розвиток апаратного забезпечення (а саме створення багатоядерних процесорів і збільшення ємності накопичувачів інформації) і технологій віртуалізації (зокрема програмного забезпечення для створення віртуальної інфраструктури, наприклад, Хеп-віртуалізація) сприяло не тільки розвитку, але й більшій доступності хмарних технологій.

Для хмарних технологій найголовнішою особливістю є нерівномірність запиту Інтернет-ресурсів з боку користувачів. Щоб згладити дану нерівномірність і застосовується ще один проміжний шар – віртуалізація сервера. Таким чином, навантаження розподіляється між віртуальними серверами і комп'ютерами.

Як і у всіх інших областях комп'ютерних технологій, хмарні обчислення також мають і переваги, і недоліки:

Переваги:

– не потрібні великі обчислювальні потужності ПК – по суті, будь-який смартфон, планшет тощо, при відкритті вікна браузера отримує величезні потенціал;

– відмово стійкість;

– висока швидкість обробки даних;

– економія на покупці софту – всі необхідні програми вже є в

сервісі, де працюватимуть;

- ваш власний вінчестер не наповнюється – всі дані зберігаються в мережі;

- доступність – хмари доступні всім, з будь-якої точки, де є Інтернет, з будь-якого комп'ютера, де є браузер;

- безпека – «хмарні» сервіси мають достатньо високу безпеку при належному її забезпеченні, однак при недбалому ставленні ефект може бути повністю протилежним;

- надійність – надійність «хмар», особливо що знаходяться в спеціально обладнаних ЦОД (Центр Обробки Даних), дуже висока, оскільки такі ЦОД мають резервні джерела живлення, охорону, професійних працівників, регулярне резервування даних, високу пропускну здатність інтернет-каналу, висока стійкість до DDOS-атакам;

Недоліки:

- хмарна послуга надається завжди якоюсь компанією, відповідно, збереження даних користувача залежить від цієї компанії;

- поява хмарних монополістів;

- необхідність бути завжди в мережі для роботи;

- дороге обладнання – для побудови власного «хмари» компанії необхідно виділити значні матеріальні ресурси, що може бути вигідно тільки великим підприємствам.

Національним інститутом стандартів зафіксовані такі обов'язкові характеристики хмарних обчислень:

- самообслуговування на вимогу (self service on demand), споживач самостійно визначає і змінює обчислювальні потреби, такі як серверний час, швидкості доступу та обробки даних, обсяг збережених даних без взаємодії з представником постачальника послуг;

- універсальний доступ по мережі, послуги доступні споживачам по мережі передачі даних незалежно від використовуваного термінального пристрою;

- об'єднання ресурсів (resource pooling), постачальник послуг об'єднує ресурси для обслуговування великої кількості споживачів в єдиний пул для динамічного перерозподілу потужностей між споживачами в умовах постійної зміни попиту на потужності; при

цьому споживачі контролюють тільки основні параметри послуги (наприклад, обсяг даних, швидкість доступу), але фактичний розподіл ресурсів, що надаються споживачеві, здійснює постачальник (у деяких випадках споживачі все-таки можуть управляти деякими фізичними параметрами перерозподілу, наприклад, вказувати бажаний центр обробки даних з міркувань географічної близькості);

- еластичність, послуги можуть бути надані, розширені, звужені в будь-який момент часу, без додаткових витрат на взаємодію з постачальником, як правило, в автоматичному режимі;

- облік споживання, постачальник послуг автоматично обчислює спожиті ресурси на певному рівні абстракції (наприклад, обсяг збережених даних, пропускну спроможність, кількість користувачів, кількість транзакцій), і на основі цих даних оцінює обсяг наданих споживачам послуг.

З погляду постачальника, завдяки об'єднанню ресурсів і непостійному характером споживання з боку споживачів, хмарні обчислення дозволяють економити на масштабах, використовуючи менші апаратні ресурси, ніж потрібні б при виділених апаратних потужностях для кожного споживача, а за рахунок автоматизації процедур модифікації виділення ресурсів істотно знижуються витрати на абонентське обслуговування.

З точки зору споживача, ці характеристики дають змогу отримати послуги з високим рівнем доступності і низькими ризиками непрацездатності, забезпечити швидке масштабування обчислювальної системи завдяки еластичності без необхідності створення, обслуговування і модернізації власної апаратної інфраструктури.

Зручність і універсальність доступу забезпечується широкою доступністю послуг і підтримкою різного класу термінальних пристроїв (персональних комп'ютерів, мобільних телефонів, інтернет-планшетів).

Існують такі моделі розгортання хмарних технологій:

- приватна хмара – інфраструктура, призначена для використання однією організацією, що включає кілька споживачів (наприклад, підрозділів однієї організації), можливо також клієнтами та підрядниками даної організації. Приватне хмара може перебувати у

власності, управлінні та експлуатації як самої організації, так і третьої сторони (або будь-якої їх комбінації), і воно може фізично існувати як всередині, так і поза юрисдикцією власника;

- публічна хмара – інфраструктура, призначена для вільного використання широкою публікою. Публічне хмара може перебувати у власності, управлінні та експлуатації комерційних, наукових та урядових організацій (або будь-якої їх комбінації). Публічне хмара фізично існує в юрисдикції власника – постачальника послуг;

- громадська хмара – вид інфраструктури, призначений для використання конкретним спільнотою споживачів з організацій, що мають спільні завдання (наприклад, місії, вимог безпеки, політики, та відповідності різним вимогам). Громадське хмара може перебувати в кооперативній (сумісній) власності, управлінні та експлуатації однієї чи більше з організацій співтовариства або третьої сторони (або будь-якої їх комбінації), і воно може фізично існувати як всередині, так і поза юрисдикцією власника;

- гібридна хмара – це комбінація з двох або більше різних хмарних інфраструктур (приватних, публічних або громадських), що залишаються унікальними об'єктами, але пов'язаних між собою стандартизованими або приватними технологіями передачі даних і додатків (наприклад, короткочасне використання ресурсів публічних хмар для балансування навантаження між хмарами).

Хмарні технології можуть дуже допомогти в бізнесі. По-перше, користувачеві не потрібно піклуватися про продуктивність свого ПК, не потрібно переживати про вільне місце на дисковому просторі. З хмарними технологіями це питання автоматично знімається відразу ж, на перших етапах.

По-друге, користувачеві не потрібно витрачатися повністю на весь потрібний йому продукт. Тим більше що в подальшому більша його частина може і не знадобитися йому взагалі. Він платить тільки за послугу, надані можливості і тільки за конкретні функції.

По-третє, хмарні технології допомагають бізнесу в сезонному сенсі. Наприклад, якщо підприємство продає подарунки до міжнародного жіночого дня, який як всі знають тільки раз на рік, в решту часу (взимку, влітку, восени) її послуги нікому будуть не

потрібні. І саме в цей час підприємство не буде нести витрати на обслуговування того величезного функціоналу, який потрібен їй тільки в піковий період.

Основні категорії:

- програмне забезпечення як послуга (SaaS) По моделі SaaS постачається апаратна інфраструктура і ПЗ, також розробник забезпечує взаємодію з користувачем через інтерфейсний портал. SaaS на даний момент є досить широким ринком. За SaaS можуть надаватись самі різноманітні послуги, від веб-пошти, до управління запасами, обробки БД. Перевагою такої моделі є те, що кінцевий користувач може вільно користуватись послугою з будь-якої точки світу;

- платформа-як-сервіс (PaaS) PaaS в хмарі визначається як набір програмних продуктів та засобів розробки, що розміщені на інфраструктурі провайдера. Розробники можуть створювати програми на платформі провайдера через Інтернет. PaaS провайдери можуть використовувати API, сайт-портали, шлюзи, або програмне забезпечення встановлене на комп'ютері клієнта;

- інфраструктура як послуга (IaaS) IaaS являє собою віртуальний сервер instanceAPI для запуску, зупинки, доступу, налаштування своїх віртуальних серверів та систем збереження. IaaS дає змогу компанії платити саме за стільки потужностей, скільки їй необхідно. Дану модель іноді називають «комунальні обчислення».

Розглянемо основні «хмарні сховища даних»:

- Google Drive – безкоштовне хмарне сховище даних, що дає змогу користувачам зберігати свої дані на серверах в хмарі і ділитися ними з іншими користувачами в Інтернеті. Після активації замінює собою Google Docs. По суті, узяли Google Docs для роботи з документами, трансформували його в хмарний сервіс і додали 5 ГБ безкоштовного простору. У новому сервісі можна зберігати не лише документи, але і фотографії, музику, відео і багато інших файлів – всього 30 типів. Але взагалі все дуже зручно і звично для користувачів Google-сервісів. Кожному користувачеві Google Drive надається безкоштовно 15gb просторів (цією пропозицією Google перевершує стандартні умови Dropbox, але програє Яндекс.Диску). Якщо

виділеного об'єму недостатньо, можна придбати додатково до 16 ТБ;

– Dropbox – хмарне сховище даних, що дає змогу користувачам зберігати свої дані на серверах в хмарі і розділяти їх з іншими користувачами в Інтернеті. Його робота побудована на синхронізації даних. Dropbox надає три тарифні плани, у тому числі і безкоштовний;

– Mega – (MEGA Encrypted Global Access) – амбітний новачок, хмарний файлообмінник Ким Доткома (Kim Dotcom), засновника легендарного Megaupload. Фішка Mega: шифрує увесь контент прямо у браузері за допомогою алгоритму AES; користувачі можуть передавати один одному файли в зашифрованому виді, при цьому усі дані зберігаються в «хмарі»; ключі доступу до файлів не публікуються у відкритому доступі, а поширюються за схемою Friend-to-Friend, між користувачами, що довіряють один одному. Примітне те, що Mega відразу стартував з безкоштовними 50 Гбайтами, крім того, є можливість значно розширитися в платних пакетах;

– Яндекс.Диск – безкоштовний хмарний сервіс від Яндекса, що дає змогу користувачам зберігати свої дані на серверах в хмарі і передавати їх іншим користувачам в Інтернеті. Робота побудована на синхронізації даних між різними пристроями. Нині реєстрація користувачів доступна усім. Раніше, до запуску Яндекс. Диска, функції зберігання призначених для користувача файлів на Яндексі виконував сервіс Яндекс;

– Bitcasa – хмарне сховище даних, яке дає змогу зберігати необмежену кількість вашої інформації. Довгожданий реліз вийшов із стадії бета в 2013 році. Bitcasa була заснована колишніми співробітниками Mastercard, VeriSign, Classmates.com і Mozy. А це означає, що творці сервісу не з чуток знайомі з рішеннями для резервного копіювання даних онлайн, а також із засобами, що забезпечують безпеку зберігання призначених для користувача файлів;

– SugarSync – хмарне сховище даних, яке зберігає документи, файли, фотографії і музику. Ціни починаються від \$ 7,49 в місяць. Щоб оцінити переваги SugarSync, існує 30-денна безкоштовна тріал-версія для всіх платних пакетів. Для взаємодії з сервісом використовується зручна програма-клієнт, версії якої існують не лише для Windows і Mac, але і для Android, iPhone, Symbian. Кількість пристроїв, що

синхронізуються, не обмежена;

– OneDrive – перейменований в лютому 2014 Microsoft SkyDrive, що базується на хмарній організації Інтернет-сервіс зберігання файлів з функціями файлообміну. До речі, SkyDrive створений в серпні 2007 року компанією Microsoft. Сервіс OneDrive інтегрований з Microsoft Office. Безпосередньо з додатка можна зберігати файли Excel, OneNote, PowerPoint і Word в службі Windows Live OneDrive. Сервіс OneDrive дає змогу зберігати спочатку безкоштовні 7 Гбайт інформації у впорядкованому за допомогою стандартних тек виді. Для зображень передбачений попередній перегляд у вигляді ескізів, а також можливість їх перегляду у вигляді слайдів;

– OpenDrive обіцяє стандартний набір можливостей з 5 Гбайт простору для безкоштовного користувача (з обмеженням в 100 Мбайт на файл), але увагу привертає одна особливість: можливість встановлення користувачем ціни на викладені їм файли. Хочеш викачати – плати. Цікава опція, в деяких випадках може виявитися цілком корисною;

– Syncplcity – програмний комплекс для синхронізації даних в кроссплатформених середовищах. Безкоштовно надається 2 Гбайта дискової квоти для 1 користувача і двох комп'ютерів. Платні пакети стартують від 15 ум. од. на місяць. Одно з переваг Syncplcity в тому, що немає необхідності постійно тримати включеними обидва комп'ютери, синхронізація відбувається після включення. Недоліком програми є відсутність українського (російського) інтерфейсу і довідки;

– iDrive є ідеальним інструментом для онлайнного резервного копіювання з високим рівнем приватності. Якщо ви хочете зберегти копію важливих документів на хмарному сервері, то iDrive те, що ви шукаєте. Використати його просто: викачати iDrive програмне забезпечення, запустити додаток і вибрати теки для синхронізації. Безкоштовно надається 5 Гб дискової квоти зберігання.

Кожне підприємство самостійно обирає, які «хмарні технології» використовувати в залежності від поставлених цілей та рівня економічної безпеки.

Відповідно, можна дістати висновку, що успішне впровадження DLP-системи на підприємстві може виявляти канали витоку інформації, знаходити порушників, виявляти і коригувати небезпечні бізнес-процеси, отримувати підтвердження згідно зі стандартами безпеки, бачити статистику щодо зменшення кількості інцидентів. Також забезпечення інформаційної безпеки має здійснюватися одночасно із впровадженням чи використанням інформаційних технологій, проте українське законодавство поки що не приділяє хмарним технологіям особливої уваги, нормативно-правова база «відстає» від темпів розвитку ІТ-сфери.

Таким чином, «хмарні технології» – це підготовчий крок у забезпеченні інтелектуально-кадрової складової економічної безпеки підприємства. Одним з найбільш важливих аспектів функціонування ІКС є система моніторингу внутрішніх та зовнішніх загроз, ідентифікація ризиків в системі управління персоналом та розробка превентивних заходів щодо їх нейтралізації. Основним джерелом внутрішніх загроз, пов'язаних із персоналом підприємства, є насамперед відсутність ІКС в системі економічної безпеки підприємств та її окремих компонентів, зокрема визначеної стратегії кадрової політики, мотивації персоналу, його професійного розвитку тощо.

До зовнішніх загроз безпеки управління персоналом слід віднести кращий мотиваційний план або активні дії конкурентів спрямовані на переманювання кваліфікованих працівників, зовнішній тиск, втягнення співробітників у різні види залежності. Тому *механізми забезпечення кадрової складової* в системі економічної безпеки підприємств повинні реалізуватися за рахунок розробки стратегії управління персоналом, спрямованої на підвищення адаптивної стійкості підприємства в умовах мінливого зовнішнього середовища, зокрема за рахунок впровадження системи ключових показників результативності та цільового управління, які включають визначення кадрових потреб, планування розвитку потенціалу і показники ефективного використання персоналу як основи ефективності та стабільності функціонування підприємства, профільні функції кадрової складової – постійний моніторинг та контролінг,

внутрішній маркетинг персоналу із метою розробки системи заохочення працівників та забезпечення конкурентоспроможності підприємства на ринку праці, якісне організаційне забезпечення процедур управління персоналом.

Одним з механізмів вдосконалення кадрової складової системи економічної безпеки організацій є її правове та інформаційне забезпечення: вирішення правових питань трудових відносин, підготовка нормативних документів, що їх регулюють, забезпечення необхідною інформацією всіх підрозділів управління персоналом, що скоріше є функціями кадрової безпеки або її задачами [18].

Для ідентифікації «слабких місць» кадрової складової необхідно проаналізувати найпоширеніші види порушень: афери з боку провідних спеціалістів (топ-менеджерів і керівників напрямків середньої ланки); несанкціоноване використання власності підприємства із корисливою метою; підробка документації підприємства за допомогою електронної техніки та Інтернету; несанкціоновані операції з цінними паперами, матеріальними й нематеріальними активами підприємства; фальсифікація звітів про використання коштів, виділених на відрядження, «представницькі видатки», на інші потреби підприємства [19].

Для оптимізації ідентифікації ключових ризиків кадрової складової економічної безпеки та визначення механізмів вдосконалення процесів пропонуємо розподілити процеси управління персоналом на 3 стадії: робота з персоналом на вході в організацію; робота з персоналом всередині організації; робота з персоналом на виході із організації (рис. 1.). Відповідно до цього можна ідентифікувати та систематизувати ризики кадрової складової, розробити методи їх нейтралізації.

При роботі з персоналом на вході в організацію основними ризиками ІКС виступають: ризик неправильного вибору джерела пошуку кандидатів (досвід, сфера діяльності, стать, соціальний статус); ризик нечіткого формування вимог до кандидата на вакантну посаду; ризик неправильної оцінки кандидата на етапі підбору (недостатня кваліфікація, психологічна несумісність із колективом тощо).



Рисунок 1 – Механізм забезпечення кадрової безпеки (авторська розробка)

Основні механізми нейтралізації даних ризиків полягають у здійсненні ретельного моніторингу стану ринку праці та реалізації процедур скринінгу; налагодженні ефективної взаємодії лінійних менеджерів із працівниками служби персоналу (що забезпечить чітке формулювання вимог до кандидата із боку менеджера та їх розуміння із боку працівника служби управління персоналом); застосуванні різноманітних оцінних технологій (як професійної так і психологічної оцінки) при підборі кандидатів, у т.ч. методики Assessment Center для ключових посад; організації ретельної перевірки рекомендацій кандидата відповідними фахівцями.

Всередині організації основними загрозами ІКС виступають ризики втрати працівниками мотивації та стимулів до ефективної праці, ризик відходу провідних працівників до конкурентів та ризик припинення розвитку і втрати кадрового потенціалу працівниками підприємства. Основний спосіб нейтралізації даної групи ризиків – вдосконалення мотиваційних процесів матеріального і нематеріального стимулювання працівників, планування ділової кар’єри працівників та створення системи динамічного розвитку і навчання персоналу на підставі оцінки та атестації працівників.

В процесі роботи із персоналом на виході організації один із ключових ризиків – ризик формування негативного іміджу підприємства як роботодавця через розповсюдження негативної інформації про нього працівниками. Засобами вдосконалення процесів з нейтралізації цього ризику є інформаційно-консультаційна підтримка звільнюваних працівників про стан ринку праці, допомога в складанні резюме, рекомендації тощо.

Одним із ключових механізмів забезпечення кадрової складової є процес розвитку персоналу підприємств, який визначає необхідність системного і систематичного моніторингу відповідності ринковим вимогам трудового потенціалу співробітників, підрозділів, підприємства в цілому.

Як видно з запропонованого механізму, за роботу на всіх трьох стадіях відповідає служба безпеки підприємства. Для полегшення виконання її роботи та особливо через розвиненість інформаційних технологій та їхнього використання на будь-яких етапах господарської діяльності підприємства, пропонуємо використання програмних продуктів.

Для комплексного вирішення проблем були представлені деякі програмні продукти, які можуть вирішити поточні проблеми підприємства та забезпечити моніторинг ризиків на всіх стадіях запропонованого механізму для уникнення інших у майбутньому (табл. 2).

Таблиця 2 – Основні проблеми і варіанти їх вирішення [20]

Проблема	Рішення
Витік документів підприємства від співробітників, інсайдерів.	FileControl надає наступні можливості: моніторинг виходу в Інтернет з веденням журналу відвідування сайтів і ресурсів, листування в мережах і програмах месенджерів; контроль підключених до комп'ютера пристроїв і роботи з файлами; відео- і аудіо фіксація дій користувача; контроль друку документів. StanffCop Standard – контрольне всі дії співробітників за робочими комп'ютерами і дає змогу отримувати дані про роботу кожного з них як в режимі online, так і у вигляді наочних звітів за будь-який період часу. Дані зашифровані на всіх рівнях – на рівні бази даних, додатків, диска, папки або файлу. Даний функціонал дає змогу надійно захистити офісну мережу від будь-яких витоків інформації.
Винос конфіденційної інформації на носіях пам'яті, для особистого використання, втрата носія інформації з конфіденційними даними	FileControl зручно контролювати підключення всіх USB та інших зовнішніх пристроїв. Системний адміністратор бачить повний список пристроїв і приймає рішення про блокування або підключенні, в залежності від ситуації. Наприклад, можна заблокувати підключення фотоапаратів, смартфонів, але дозволити USB диски. Щоб запобігти витоку інформації ви можете заборонити всі пристрої і дозволити одну конкретну флешку, на яку можна буде зробити копіювання. Тоді ви зможете прицільно відстежити яку інформацію на неї скопіювали і винесли за межі офісу StaffCop Standard розпізнає всі операції з файлами та папками на комп'ютері користувачів. Ви з легкістю можете налаштувати, які файли вам необхідно контролювати і, таким чином, отримувати тільки необхідну вам інформацію. Наприклад, можна отримувати інформацію про доступ до Word або Excel файлів. Всі типи операцій такі, як копіювання, редагування, читання, видалення, успішно реєструються програмою.
Запис розмов співробітника, для запобігання витоку інформації через Skype	У FileControl реалізована функція прихованого перехоплення розмов і листування Skype. Програма записує голосові дзвінки у форматі MP3 і всі повідомлення автоматично. Ви можете прослухати переговори за допомогою вбудованого плеєра або завантажити файл для його подальшого вивчення службою безпеки.
Розкрадання у роботодавця та схильність до хабарництва і шахрайство	Кадрова система перевірки персоналу К-Фактор (HR1) дає змогу в автоматичному режимі протестувати співробітників підприємства або претендентів на роботу і на підставі аналізу істинності (хибності) відомостей, повідомлених тестованим, визначити наявність факторів ризику в його поведінці і дати прогноз їх можливого прояву в майбутньому.

Важливим елементом забезпечення економічної безпеки підприємства є інформаційно-аналітична підсистема управління економічною безпекою підприємства, яка має містити наступні дані: якісні і кількісні значення індикаторів фінансової безпеки, наявність або потенційність ризиків і загроз, формалізовані фінансові інтереси і стан їхньої реалізації, стратегічний план (стратегія) забезпечення фінансової безпеки підприємства, фінансовий план (бюджет).

Системи інформаційно-аналітичного забезпечення формуються на базі: даних бухгалтерського, управлінського, оперативного та статистичного обліку і звітності; галузевих показників діяльності підприємств-аналогів; звітів та планів і прогнозів, оцінки загроз фінансовій безпеці підприємницької діяльності тощо.

Таким чином, в основі механізму забезпечення економічної безпеки, знаходиться системне поєднання певних інструментів, методів, важелів та інформаційно-аналітичного забезпечення, створюваних на базі принципів забезпечення економічної безпеки, що об'єктивно існують як економічні закономірності, а також виробляються суб'єктами управління економічної безпеки підприємства для досягнення і захисту фінансових інтересів підприємства.

Експерти сходяться на думці, що людина розголошує конфіденційну інформацію від 0-6 місяців після звільнення. Саме тому важливо відстежувати контакти звільненого персоналу в цей термін. Звичайно, відстежувати варто тільки тих працівників, які володіють інформацією, розголошення якої може завдати істотних матеріальних збитків підприємству (технологи, топ-менеджери, керівний склад інші). Одним з найбільш ефективних інструментів для вирішення цієї проблеми є метод розпізнавання мови, який дає змогу виявити небезпеку навіть у момент ведення переговорів. Розпізнавання мови в реальному часі за допомогою сучасних методів вимагає великих обчислювальних ресурсів, обсяг яких часто буває обмежений. Неможливість широкого застосування багатьох алгоритмів сьогодні, наприклад, в мобільних пристроях, змушує дослідників шукати більш ефективні і оптимізовані методи.

Існує безліч методів розпізнавання мови:

– розпізнавання за зразком. Цей метод передбачає розпізнавання тексту або фрази по вже заготовленому користувачем шаблоном, тобто ви просто вимовляєте потрібну фразу, а пристрій сам знаходить її. Цей метод належить до диктатор залежності, оскільки створена вами команда реагує тільки на ваш голос (це властивість відносять до мінусів цього методу).

– виділення лексичних елементів, тобто з тексту виділяють окремі слова (конструкції).

– попередня обробка звукових сигналів, тобто мається на увазі, що будуть видалені сторонні звуки (шуми). Цю дію можна зробити за допомогою цифрових фільтрів.

– рівні розпізнавання зливої промови – це виділення їх тексту лексичних елементів, складів, слів, фраз.

Ось тільки частина методів розпізнавання мови, насправді їх дуже багато і кожен метод має свою функцію і послідовність виконання дій.

Розпізнавання за зразком

Якщо у вас є сучасний мобільний телефон, то, швидше за все, одна з систем розпізнавання мови вже лежить у кишені. Така система призначена для прискореного вибору абонентів із записника мобільного телефону за допомогою голосу.

При додаванні нового контакту в записну книжку надається можливість ввести голосову позначку, що ідентифікує цей контакт, наприклад, вимовити в телефон ім'я або прізвище абонента. Можливо, доведеться зробити це два або три рази.

Тепер, щоб зателефонувати абоненту, досить натиснути одну з кнопок, розташованих на корпусі мобільного телефону, і промовити голосову позначку. Номер абонента буде обраний із записника, після чого мобільний телефон спробує встановити зв'язок з абонентом.

Крім мобільного телефону, існують і інші пристрої з подібним голосовим управлінням, наприклад, комп'ютерні клавіатури. Такі клавіатури обладнуються вбудованим мікрофоном і дозволяють призначити голосові мітки певним клавішам, комбінаціям клавіш або послідовностям клавіш. Розробники клавіатур з голосовим інтерфейсом стверджують, що з його допомогою можна прискорити

введення інформації, однак якість розпізнавання голосових міток залежить, наприклад, від загального рівня шуму в кімнаті.

Технологія розпізнавання фрагментів за заздалегідь записаним зразком застосовується і в багатьох програмах, що дозволяють підключити голосове управління до операційної системи Microsoft Windows та її додатків. При використанні цих програм можна запускати додатки, перемикаючи між ними, вибирати рядки з меню і клацати кнопки діалогових вікон, віддаючи голосові команди і не доторкаючись руками до клавіатури або миші. Можливо, такі програми і не набагато прискорять роботу з додатками для звичайних людей, але вони частково допоможуть інвалідам, нездатним використовувати стандартні засоби спілкування з комп'ютером.

Ця технологія працює досить добре, якщо телефоном користується тільки одна людина, а загальна кількість голосових міток не перевищує десятків-других. Якщо «навчити» свій телефон (або клавіатуру з голосовим інтерфейсом) реагувати на голос, то тільки і зможе користуватися мовними мітками. Таким чином, ці системи відносяться до класу систем, залежних від диктора. Втім, цей недолік є і у багатьох більш досконалих систем розпізнавання мови, заснованих на виділенні з промови лексичних елементів.

Виділення лексичних елементів

Далі зосередимо свою увагу на підході до створення систем розпізнавання мови, заснованому на виділенні з промови лексичних елементів, таких як фонемі і Алофон.

Неможливо виділити з промови фонемі і Алофон, аналізуючи тільки форму обвідної звукового сигналу. Як зазначено, не можна обмежитися складанням бази даних із записів звукових сигналів всіх фонем, алофонів та інших лексичних елементів для подальшого порівняння форми сигналів в процесі розпізнавання. Тут потрібні більш складні методи.

Попередня обробка звукових сигналів

Перед тим як робити спроби розпізнавання мови, потрібно виконати попередню обробку мовного сигналу. Під час цієї обробки слід видалити шуми і сторонні сигнали, частотний спектр яких знаходиться поза спектра людської мови. Таку обробку можна

виконати за допомогою аналогових або цифрових смугових фільтрів, розглянутих нами у 2 розділі цієї книги.

Відфільтрований звуковий сигнал потрібно цифрувати, виконавши аналого-цифрове перетворення. Цей етап обробки ми теж вже обговорювали раніше.

Всю попередню обробку звукового сигналу можна зробити за допомогою стандартного звукового адаптера, встановленого в комп'ютері. Додаткова цифрова обробка звукового сигналу (наприклад, частотна фільтрація) може виконуватися центральним процесором комп'ютера. Таким чином, при використанні сучасних персональних комп'ютерів системи розпізнавання мови не вимагають для своєї роботи будь-якого спеціального апаратного забезпечення.

Важливим етапом попередньої обробки вхідного сигналу є нормалізація рівня сигналу. Це дає змогу зменшити похибки розпізнавання, пов'язані з тим, що диктор може вимовляти слова з різним рівнем гучності.

Зауважимо, що якщо вхідний звуковий сигнал має занадто малий рівень гучності, то після нормалізації може з'явитися шум. Тому для успішної роботи системи розпізнавання мови необхідно відрегулювати оптимальним чином чутливість мікрофона. Надмірна чутливість може привести до нелінійних спотворень сигналу і, як наслідок, до збільшення похибки розпізнавання мови.

Виділення інформативних ознак мовного сигналу

Залежно від різних обставин форма обвідної мовного сигналу може змінюватися в широких межах, що ускладнює задачу розпізнавання.

Для розв'язання задачі розпізнавання необхідно виділити первинні ознаки мови, які будуть використані на наступних етапах процесу розпізнавання. Первинні ознаки виділяються за допомогою аналізу спектральних і динамічних характеристик мовного сигналу.

Методи й алгоритми, які використовувалися дотепер, можуть бути розділені на чотири більші класи: методи дискримінантного аналізу, засновані на Байєсовській дискримінації; приховані моделі Маркова; динамічне програмування – часові динамічні алгоритми (DTW); нейронні мережі.

Алгоритм DTW обчислює оптимальну послідовність трансформації (деформації) часу між двома часовими рядами. Алгоритм обчислює обидва значення деформації між двома рядами й відстанню між ними.

Припустимо, що є дві числові послідовності (a_1, a_2, \dots, a_n) та (b_1, b_2, \dots, b_m) . Як видно, довжина двох послідовностей може бути різною. Алгоритм починається з розрахунків локальних відхилень між елементами двох послідовностей, що використовують різні типи відхилень. Найпоширеніший спосіб для обчислення відхилень – метод, що розраховує абсолютне відхилення між значеннями двох елементів (евклідова відстань). У результаті отримаємо матрицю відхилень, що має n рядків і m стовпців загальних членів: $d_{ij} = |a_i - b_j|$, $i = \overline{1, n}$, $j = \overline{1, m}$.

Мінімальна відстань у матриці між послідовностями визначається за допомогою алгоритму динамічного програмування та наступного критерію оптимізації: $a_{ij} = d_{ij} + \min(a_{i-1, j-1}, a_{i-1, j}, a_{i, j-1})$, де: a_{ij} – мінімальна відстань між послідовностями (a_1, a_2, \dots, a_n) та (b_1, b_2, \dots, b_m) . Шлях деформації – це мінімальна відстань у матриці між елементами a_{11} та a_{nm} , що складаються із тих a_{ij} елементів, які виражають відстань до a_{nm} .

Глобальні деформації складаються із двох послідовностей і визначаються по формулі: $GC = \frac{1}{p} \sum_{l=1}^p w_l$, де: w_l – елементи, які відносяться шляху деформації; p – їх кількість.

Існує три умови, що забезпечують роботу DTW відповідно до алгоритму забезпечення швидкої конвергенції:

Монотонність – шлях ніколи не повертається назад і не повторюється, тобто індекс i та j , які використовуються, ніколи не зменшуються.

Безперервність – послідовність просувається поступово: за один крок індекси i та j збільшуються не більше ніж на 1.

Граничність – послідовність починається в лівому нижньому куті й закінчується в правому верхньому.

Оскільки для визначення основи послідовності в динамічному програмуванні оптимальним є використання методу зворотного

програмування, необхідно використовувати певний динамічний тип структури, який називається «стек». Як і будь-який динамічний алгоритм програмування, DWT має поліноміальну складність. Коли ми маємо справу з більшими послідовностями, виникають дві незручності: запам'ятовування більших числових матриць; виконання великої кількості розрахунків відхилень.

Висновки: Одною з найголовніших складових економічної безпеки підприємства вважається інтелектуально-кадрова безпека. Це пов'язано з тим, що основні ризики підприємства зазвичай генеруються її власним кадрами. Співробітники впливають на всі аспекти життєдіяльності підприємства, вони невід'ємно пов'язані з її ефективною діяльністю. За даними статистичних досліджень близько 51% випадків економічних злочинів здійснюють співробітники підприємства [21], а уникнути збитків фірми, пов'язаних із людським фактором, можливо лише за рахунок виключення суб'єктивного фактору, тобто інноваційно-інформаційних технологій, які треба застосовувати системно та періодично переглядати адже інформаційний світ змінюється швидше за інші сфери зовнішнього впливу на діяльність підприємства.

Література

1. Башинська І.О. Розділ 3.2. Уточнення визначення дефініції та економічного змісту категорії «економічна безпека підприємства» (С. 14-20) у кол. монографії Економічна безпека в умовах глобалізації світової економіки : [колективна монографія у 2т.]. – Дніпропетровськ: «ФОП Дробязко С.І.», 2014. – Т. 2. – 349 с.
2. Поскрипко Ю.А. Механізми вдосконалення інтелектуально-кадрової складової економічної безпеки підприємств / Наукові записки УНДІЗ. – 2012. – №2(22). – С. 118-120
3. Материалы компании РБК СОФТ. [Електронний ресурс]. – Режим доступу: <http://www.rbcsoft.ru/ru/services/corporate/>
4. Щедрина О.І. Нові інформаційні технології. Навч. посіб. — К.: КНЕУ, 2005. — 445 с.

5. Тим Кук: Мобильность – наше будущее / Издательство «Открытые системы» – 2015. [Електронний ресурс]. – Режим доступу: <http://www.osp.ru/>
6. Чернобровцев А. Облако над сетью. [Електронний ресурс]. – Режим доступу: <http://www.osp.ru/news/articles/2014/11/13040094/>
7. Штефман И. Хранилища данных: шаги от идеи до внедрения / CNews [Електронний ресурс]. – Режим доступу: <http://www.cnews.ru/>
8. Мужиченко Н. Умные офисы: стандарты комфорта. [Електронний ресурс]. – Режим доступу: <http://www.cnews.ru/reviews/>
9. Дэйв Эванс. Грядет «лави́на новых технологий». [Електронний ресурс]. – Режим доступу: <http://www.cybersecurity.ru/manuals/net/service/2610>
10. Гнатюк Л.С. Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики [Електронний ресурс]. Режим доступу: <http://www.niss.gov.ua/articles/1191/>
11. Symantec: Protecting a Cloudier Future. Market Report. November 2012. [Електронний ресурс]. – Режим доступу : http://www.symantec.com/content/en/us/enterprise/white_papers/esg-protecting-a-cloudier-future.en-us.pdf;
12. Symantec. Avoiding the Hidden Costs of the Cloud. 15.12.2013. [Електронний ресурс]. – Режим доступу : <http://www.symantec.com/connect/blogs/avoiding-hidden-costs-cloud>;
13. IDC Predictions 2013. Competing on the 3rd Platform: Opportunities at the Intersection of Mobile, Cloud, Social, and Big Data [Електронний ресурс]. – Режим доступу : <http://clck.ru/8aXZM>;
14. IDC Predictions 2013. Competing on the 3rd Platform: Opportunities at the Intersection of Mobile, Cloud, Social, and Big Data [Електронний ресурс]. – Режим доступу : <http://clck.ru/8aXZM>
15. Юдін О.К., Зюбіна Р.В. Нормативно-правові аспекти використання хмарних технологій //Наукоємні технології. – 2014. – № 3 (23). – С. 303-307
16. Kroes Neelie. Towards a European Cloud Computing Strategy /

- Neelie Kroes [Електронний ресурс]. – Режим доступу : <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50>
17. NIST SP 500-292 NIST Cloud Computing Reference Architecture. Recommendations of the National Institute of Standards and Technology. U.S. 2011.
 18. Грещак М.Г. Безпека підприємництва / М.Г. Грещак. – К. : вид-во КНЕУ, 2003. – 611 с.
 19. Бухвальд Е. Макроаспекты экономической безопасности: факторы, критерии и показатели / Е. Бухвальд, Н. Гловацкая, С. Лазуренко // Вопросы экономики. – 2007. – № 12. – С.25-35.
 20. Башинська І.О. Глава 2.1 Сучасні тенденції на ринку інформаційно-аналітичного забезпечення економічної безпеки підприємства (С. 158-163) у міжнародній колективній монографії Mechanism of Sustainable Development of Economic Systems Formation – Collective monograph – Vol. 1. Verlag SWG imex GmbH, Nürnberg, Deutschland, 2014. – 220 p.
 21. Томаневич Л. М. Кадрова безпека підприємства як об'єкт теоретичного дослідження [Електронний ресурс] / Л. М. Томаневич. — Режим доступу : www.nbuv.gov.ua/portal/soc_gum/Uproz/2011_4/u1104cha.pdf

РОЗДІЛ 24

СТРАТЕГІЯ ІННОВАЦІЙНОГО РОЗВИТКУ ПІДПРИЄМСТВ ХАРЧОВОЇ ГАЛУЗІ НА ПРИНЦИПАХ ВЕРТИКАЛЬНОЇ ІНТЕГРАЦІЇ

*д.е.н., доцент,
доцент кафедри менеджменту зовнішньоекономічної
та інноваційної діяльності
Одеський національний політехнічний університет
Коваленко О.М.,*

*к.е.н., доцент,
доцент кафедри менеджменту
Одеський національний політехнічний університет
Станіславик О.В.*

На початку ХХІ в. вітчизняна економіка опинилася перед обличчям довготривалих системних викликів, обумовлених існуванням зовнішніх і внутрішніх факторів-загроз. До першої групи таких детермінант, перш за все, слід віднести розвиток процесів глобалізації, посилення конкуренції, що охоплює світові ринки праці, товарів, капіталів, наукомістких технологій. Зовнішньо несприятливий вплив цих чинників посилюється існуванням серйозних внутрішніх проблем, пов'язаних з нестабільністю систем управління національною економікою, дистанціюванням держави від регулювання соціально-економічних процесів, розривом існуючих раніше стійких господарських зв'язків, недосконалістю чинного законодавства, значним податковим тягарем. Ці та інші чинники, взяті в комплексі, визначають жорсткі вимоги, які пред'являються до темпу і якості росту української економіки, необхідних для забезпечення стійкості її розвитку, збільшення питомої ваги у світовій системі господарювання,