

діяльності. Встановлено, що протягом 2008-2009 рр. негативний фінансовий результат діяльності торговельних підприємств обумовлений збитковістю як основної так і інших видів діяльності. У період 2010-2012 рр. збиток від іншої діяльності компенсований позитивним фінансовим результатом від основної діяльності.

#### **Література:**

1. Офіційний сайт Державної служби статистики України [Електронний ресурс]. ☒ Режим доступу : <http://www.ukrstat.gov.ua>.
2. Global Powers of Retailing 2013 Retail Beyond. [Електронний ресурс] – Режим доступу: [https://www.deloitte.com/view/en\\_GX/global/industries/consumerbusiness/retail/a336253eda30c310VgnVCM2000003356f70aRCRD.htm#.UhHd-uUl\\_Qc](https://www.deloitte.com/view/en_GX/global/industries/consumerbusiness/retail/a336253eda30c310VgnVCM2000003356f70aRCRD.htm#.UhHd-uUl_Qc).
3. Global Retailers: Cautiously Aggressive or Aggressively Cautious? [Electronic resource]. – Available at : [http://www.akearney.com/consumer-products-retail/global-retail-development-index/full-report/-asset\\_publisher/oPFRGkblkz0Q/content/2013-global-retail-development-index/10192#sthash.W9HeJodN.dpuf](http://www.akearney.com/consumer-products-retail/global-retail-development-index/full-report/-asset_publisher/oPFRGkblkz0Q/content/2013-global-retail-development-index/10192#sthash.W9HeJodN.dpuf).
4. Бразилія, Чили і Китай лідери в Global Retail Development Index 2013 [Електронний ресурс]. – Режим доступу : <http://www.retailstudio.org/trends/24213.htm>.
5. Суммарная выручка ТОП-250 мировых ритейлеров превысила 4 трлн. долл. США [Электронный ресурс].
6. Ринок роздрібної торгівлі України за 2012 рік [Електронний ресурс]. – Режим доступу : [http://www.credit-rating.ua/img/st\\_img/AS/2013/29.04.2013/Roznica\\_2012.pdf](http://www.credit-rating.ua/img/st_img/AS/2013/29.04.2013/Roznica_2012.pdf).

## **ГЛАВА 4.2. СУЧАСНІ ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ СКЛАДОВОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПРОМИСЛОВОГО ПІДПРИЄМСТВА**

### **Башинська І.О.**

к.е.н., старший викладач кафедри обліку, аналізу та аудиту  
*Одеський національний політехнічний університет*

На сьогоднішній день інформаційна сфера є ведучою в діяльності держави і чинить вплив на всі елементи функціонування промислових підприємств. Разом зі зростаючою залежністю від електронних технологій, пов'язаних з поширенням інформації, зростає і загроза кібератак, метою, яких, як правило, стають інформаційні ресурси та мережева інфраструктура [1]. Оцінка системи управління безпекою промислових об'єктів в Україні виявила гостру необхідність формування чіткого діючого механізму розвитку програмних і технічних засобів, яка призначена для вироблення та реалізації керуючої дії на технологічний об'єкт. Діяльність промислових підприємств потребує особової уваги щодо забезпечення охорони своїх об'єктів, персоналу та інтелектуальної власності. Все це робить питання посилення безпеки цифрових мереж та інфраструктур особливо актуальним.

Під *економічною безпекою* розуміють власне 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 [2].

Виходячи із завдань, що стоять перед службою економічної безпеки для забезпечення інформаційно-аналітичної безпеки підприємства, розглянемо засоби

комплексу охоронної системи, заснованих на передових інформаційних технологіях і обладнанні провідних світових виробників.

Основні сучасні засоби охоронних систем:

1. Охоронна сигналізація;
2. Системи відеоспостереження;
3. Системи контролю доступу;
4. Інтелектуальні відеоаналітичні системи;
5. Біометричні системи контролю доступу;
6. Доглядове устаткування;
7. Системи охорони периметра території [2, 3, 4, 5].

Розглянемо кожен інструмент докладніше:

1. *Система охоронної сигналізації (ОС)* призначена для виявлення несанкціонованого проникнення на об'єкт, що охороняється і реагування на проникнення.

ОС складається з охоронної панелі (централі), яка збирає і аналізує інформацію охоронних датчиків, і виконує запрограмовані в ній функції при спрацьовуванні датчиків. Пульст управління ОС відображає стан сигналізації, служить для її програмування, постановки та зняття об'єкта з охорони.

Найбільш поширені охоронні датчики – об'ємні інфрачервоні, магнітоконтактні, акустичні, вібраційні, ультразвукові, променеві, ємнісні. За допомогою ОС також можливий моніторинг електроживлення, температури, витоку газу, протікання води та ін.

Системи охоронної сигналізації (ОС) поділяють на: провідні, бездротові радіосигналізація. ОС також поділяють за типом передачі сигналу: автономну (звучить сирена) і пультову (сигнал надходить на стаціонарний пост охорони).

2. *Системи відеоспостереження* призначені для організації відеоконтролю на об'єктах, вони також можуть використовуватися: як лічильник суб'єктів (фізичних осіб, транспортних засобів), для аналізу певних подій, як стандартне охоронне відеоспостереження для фіксування фактів крадіжок і т. п.

Сучасні системи ІР-відеоспостереження, основою для яких є ІР-камери, не вимагають прокладки додаткових ліній зв'язку, передача даних відбувається по мережевій інфраструктурі, побудованої на протоколі ІР. ІР-відеоспостереження використовує при передачі даних шифрування і систему авторизації для повної конфіденційності. Контроль і адміністрування системи здійснюється з будь-якого комп'ютера, що має доступ в мережу і спеціальне програмне забезпечення. ІР-відеоспостереження інтегрується з системами пожежної сигналізації, охоронної сигналізації, системами контролю і управління доступом, а також на будь-які сучасні мобільні пристрої.

3. *Системи контролю та управління доступом (СКУД)* дозволяє фіксувати і обробляти інформацію про кожному проходженні через елемент обмеження доступу, а також захистити приміщення від несанкціонованого проникнення, регламентувати доступ. В якості суб'єкта можуть виступати як фізичні особи, так і транспортні засоби.

В якості ідентифікатора суб'єкта застосовуються як фізичні носії (ключ-«таблетка», безконтактна карта, брелок), так і коди, що вводяться з клавіатури, також для ідентифікації людини використовуються його біометричні ознаки (відбиток пальця, малюнок райдужної оболонки ока).

Структурно об'єкт, на якому встановлена СКУД, складається з точок, кожна з яких оснащується контролером, зчитувачами електронних перепусток, що перепиняють пристроєм (замок, турнікет, шлагбаум, приводи воріт і т.д.), датчиками положення дверей і фіксації факту проходу.

Для організації безпеки при в'їзді на територію, що можуть встановлюватися протитаранні болларди. Вони є найнадійнішим блокувальником і часто відносяться до класу антитерористичних перешкод.

Мережеві СКУД управляються через центральний комп'ютер і можуть створювати звіти про події, що відбулися, про проходження на територію співробітників, вести облік і контроль суб'єктів за заданими параметрами.

4. *Інтелектуальна відеоаналітична система* інтегрується з системою відеоспостереження і робить можливим:

- розпізнавання об'єктів (осіб, автомобільних номерів, залишених предметів, що надають потенційну загрозу і інших факторів),
- реєстрацію фактів порушення порядку,
- інтеграцію з базами даних фотографій, фотороботів, номерних знаків автомобілів для ідентифікації терористів, злочинців, правопорушників.

За допомогою цієї системи силові структури зможуть вирішувати завдання забезпечення безпеки на якісно новому рівні, завжди оперативно реагувати і вживати необхідних заходів.

5. *Біометрична система контролю доступу*. Для особливо важливих приміщень силових відомств рекомендується застосовувати системи контролю доступу з біометричними технологіями ідентифікації, які дозволяють розпізнавати особистість людини з високою ефективністю:

- по відбитку пальця,
- по зображенню особи,
- по райдужній оболонці ока.

Біометрична система контролю доступу дозволяє:

- ефективно розмежувати доступ співробітників і гостей по території відомства,
- значно зменшити ризик витоку конфіденційної інформації, розкрадань і несанкціонованого доступу.

Силові структури успішно застосовують біометричні технології у протидії тероризму, організованій та транскордонній злочинності, торгівлі наркотиками, нелегальної міграції, сучасним формам работоргівлі, організації доступу осіб до приміщень де зберігається, обробляється і циркулює інформація з обмеженим доступом та багато іншого.

6. *Доглядове устаткування*. Об'єкти особливого значення обов'язково повинні бути оснащені доглядовим обладнанням. За допомогою цього обладнання можна своєчасно виявити матеріали і предмети, що використовуються для здійснення терактів, для огляду поштової кореспонденції і ручної поклажі, для виявлення вибухових, наркотичних і отруйних речовин.

Металодетектор (металошукач) – один з найпоширеніших видів доглядового обладнання, які бувають в основному двох типів: ручні (для огляду конкретної поклажі, багажу) і аличні.

Ручні металодетектори компактні, зручні в зверненні. За допомогою них можна швидко перевірити будь-якої людини, його ручну поклажу на присутність металевих предметів (у тому числі і вогнепальної або холодної зброї, будь-яких металевих деталей).

Арочні стаціонарні металодетектори зазвичай використовують для контролю та перевірки кількості людей (до 3000 чоловік за годину). Залежно від конструкції, арочні металодетектори бувають багатозонні і однозонні.

7. *Системи охорони периметра території*. Периметральні системи захисту здійснюють контроль за зовнішнім периметром об'єкта, який є першим і найважливішим кордоном охорони, і будь-яке несанкціоноване проникнення повинно викликати сигнал тривоги із зазначенням точного місця вторгнення.

Система охорони периметра включається в загальну систему охоронної сигналізації і будується на основі радіо променевого, радіохвильового або ємнісного датчиків, вібраційно-чутливих сповіщувачів з сенсорними кабелями та / або дротово-натяжних системах захисту периметра.

#### Телекомунікаційні мережі та сервіси

Проектування, побудова та сервіс телекомунікаційних мереж:

- Волокно-оптичні лінії зв'язку
- Структуровані кабельні системи
- Бездротові мережі Wi-Fi
- Розподільні мережі телебачення

*Волокно-оптичні лінії зв'язку (ВОЛЗ)* – це вид зв'язку, при якому інформація передається по оптичних каналах, більш відомі під назвою «оптоволокно». На теперішній момент оптоволокно – одне з кращих просторів для передачі інформації завдяки ряду переваг, таких як велика пропускна здатність і дешевизна виробництва.

Системи зв'язку, побудовані на основі оптоволокна, стійкі до електромагнітних перешкод. Інформація, передана по оптичних каналах, є захищеною від несанкціонованого доступу. Без фізичного втручання в мережу неможливо перехопити передані дані, а втручання в мережу можна відстежувати методами моніторингу цілісності ліній.

*Структурована кабельна система (СКС)* – це універсальна телекомунікаційна інфраструктура, що забезпечує передачу сигналів всіх типів, включаючи мовні, інформаційні та відео, що є сукупність пасивного комунікаційного устаткування: оптичні і мідні кабелю, розетки, комутаційні панелі, комутаційні шнури.

Сьогодні СКС – це основа діяльності будь-якої організації чи підприємства. За допомогою СКС можливо:

- об'єднання мереж і сервісів різного призначення (комп'ютерні та телефонні мережі, системи відеоспостереження, пожежної та охоронної сигналізації);
- контроль за всіма службами будівлі (система централізованого управління);
- переміщення і створення нових робочих станцій користувачів всередині будівлі;
- управління та адміністрування мінімальною кількістю обслуговуючого персоналу;
- незалежність від змін технологій і постачальника обладнання;
- одночасне використання декількох різних мережевих протоколів;
- зміна і нарощування без заміни всієї існуючої мережі завдяки модульності.

Проект побудови СКС повинен відповідати прийнятим міжнародним і держстандартам, а також стандартам електромагнітної сумісності, заземленню, блискавкозахисту.

*Бездротові мережі Wi-Fi* – це технологія, що дозволяє створювати локальні обчислювальні мережі (ЛОМ), які повністю відповідають стандартам для звичайних провідних мереж, без використання кабельної проводки по радіоканалах.

Комп'ютер, підключений до Wi-Fi може перебувати в будь-якій точці приміщення, так як не прив'язаний до мережевих кабелів. Це означає, що створення бездротової мережі не вимагає спеціальної планування приміщення, розміщення мережевих розеток і кабелів.

Бездротова мережа передачі даних дуже часто виявляється більш гідним рішенням в порівнянні з рішенням провідної мережі там, де стоїть завдання передачі даних на відстанях більше 100 метрів. Сумісність з стандартами 802.11a/b/g дозволяє працювати з бездротовими мережами більшості мобільних пристроїв, які існують на ринку.

*Розподільна мережа телебачення* – це найважливіший елемент системи телебачення, від неї залежить якість зображення на всіх ТВ-приймачах і можливість розширення системи із збільшенням числа трансльованих каналів без повної або часткової її заміни.

Головне завдання розподільної мережі – доставка групового сигналу певного рівня до кожного абонентського ТВ-приймача з мінімальними спотвореннями і шумами і з максимально однаковим рівнем сигналу в будь-якій точці мережі.

Неправильний розрахунок кількості підсилювачів, які є невід'ємними елементами мережі, неякісний монтаж елементів мережі, невиконання норм і правил при прокладанні кабельних ліній та встановлення обладнання призводять до появи перешкод і шумів.

- відеопроєкційні системи;
- конференц-системи, конгрес-системи;
- системи синхронного перекладу;
- аудіовізуальні комплекси для навчальних аудиторій;
- відеостіни;
- рішення для ситуаційних та диспетчерських центрів.

*Відеопроєкційна система* складається з відеопроєкторів, моніторів, моторизованих екранів. Відеопроєктор приймає відеосигнал від джерела і формує відповідну картинку на проєкційному екрані. Сучасні відеопроєктори здатні коригувати геометричні спотворення зображення, викликані порушенням правил просторового розташування відеопроєктора і екрану.

*Конференц-система* – це комплект обладнання, яке дозволяє зручно і ефективно проводити спільні зустрічі, семінари, дискусії. У завдання конференц-системи входить посилення мови виступаючого, а також регламентування і керування обговоренням завдяки різноманітним режимам роботи.

У комплекс обладнання конференц-системи входять:

- центральні блоки;
- блоки розширення конференц-систем;
- мікрофони;
- пульти учасників конференції;
- передавачі сигналу на пульти учасників (для бездротових конференц-систем).

За допомогою центрального блоку можна, наприклад, встановлювати регламент виступу або керувати всіма мікрофонами в залі.

Додатково конференц-системи можуть підтримувати роботу з іншим обладнанням (або містити в собі таке обладнання), такі конференц-системи називаються конгрес-системами.

Як правило, це наступне обладнання:

- обладнання синхронного перекладу мови (центральні блоки, пульти перекладачів, приймачі учасників, передавачі сигналу на приймачі учасників);
- обладнання реєстрації учасників (приймальні пристрої, реєстраційні картки, блоки обробки інформації)
- обладнання голосування (пульти для голосування, блоки обробки інформації, пристрої виведення інформації);
- обладнання візуалізації імен і посад учасників конференції;
- обладнання системи відеокамер, які наводяться автоматично на виступаючого.

Система синхронного перекладу призначена для онлайн- перекладу тексту виступаючого на іноземну мову. Як правило, система синхронного перекладу входить до складу конференц -систем.

*Відеостіна* – це універсальне рішення для ситуаційних центрів, центрів управління та прийняття рішень, командних та диспетчерських пунктів.

Графічні відеостіни являють собою поліекранні системи, які будуються з окремих елементів – проєкційних модулів (відеокубів) або відеопанелей з тонкою рамкою. Кожен проєкційний модуль є повноцінним засобом відображення інформації. Невелика глибина дозволяє встановити відео стіну практично в будь-якому місці, а вузька екранна рамка забезпечує природне і чітке зображення при стикуванні декількох моніторів в відео стіну. Конструктивні особливості дозволяють створювати відеостіни будь-якого розміру плоскої або зігнутої форми.

Тип відображення графічної або відеоінформації на відеостіні підбирається залежно від сценарію. Управляти відеостіною і завантажувати на неї файли різних форматів можна в дистанційному режимі за допомогою Web -технології.

Можливість масштабувати зображення, максимально деталізувати і виводити велику кількість карт, діаграм, відеотрансляція в реальному часі – все це спрощує і підвищує швидкість сприйняття та обробки інформації, дає можливість колективного перегляду.

*Диспетчерський/ситуаційний центр* – це сукупність спеціальних інформаційних технологій та апаратно-програмних комплексів, в які входять системи зв'язку, збору інформації, аналізу ситуації та прийняття рішень, що працюють в цілодобовому режимі і призначених для зведення несприятливих наслідків до мінімуму в режимі нештатної ситуації.

Особливістю диспетчерських або ситуаційних центрів є величезна кількість інформації, що надходить, яку потрібно оперативно обробляти. Людське око не здатне охопити зі стандартного монітора всі дані, які з безлічі дрібних вікон, тому найбільш ефективною системою візуалізації інформації для таких центрів є відеостіна.

З перерахованого списку засобів забезпечення інформаційної складової промислового підприємства обирає найбільш необхідні для нього за критерієм ціна/забезпечення безпеки. Також варто відмітити, що синергетичний ефект значно зростає при використанні різних засобів, причому обирати слід засоби різного спрямування для забезпечення захищеності з усіх можливих сторін.

### **Література:**

1. Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: Монографія. – Львів: Арал, 2008. – 384 с.
2. 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.
3. Проскурович О.В. Інформаційно-аналітичне забезпечення процесу прийняття рішень в системі управління. – Вісник ХНУ №2, Т.3, 2011 – С.17-18.
  4. Погребенник В.Д., Політило Р.В. Принципи побудови систем охоронної сигналізації // Вісник Національного університету «Львівська політехніка». – Львів, 2008. – №608. – С. 93-99.
  5. Погребенник В.Д., Політило Р.В. Оцінювання похибок ультразвукового методу охорони важливих приміщень // Вісник Черкаського Державного технологічного університету. – Черкаси, 2010. – № 4. – С. 134-137.

### **ГЛАВА 4.3. НАУКОВО-МЕТОДИЧНІ ПІДХОДИ ДО АНАЛІЗУ ПОТЕНЦІАЛУ РОЗВИТКУ ПІДПРИЄМСТВА**

**Гречина І. В.**

к.е.н., доцент кафедри контролю і АГД

**Ващенко Л.О.**

к.е.н., доцент кафедри контролю і АГД

*Донецький національний університет економіки і торгівлі  
імені Михайла Туган-Барановського*

Стан економіки України, у такий складний економічний період, спонукає підприємства різних галузей до пошуку нових можливостей їх розвитку і удосконалення. Складність економічного стану країни підтверджується офіційними даними, оприлюдненими на сайті Міністерства економічного розвитку і економіки України, де говориться, що номінальний валовий внутрішній продукт за III квартал 2013 р. склав 392,6 млрд. грн., а реальний порівняно з III кварталом 2012р. скоротився на 1,3% . Скорочення валової доданої вартості у III кварталі 2013 р. порівняно з відповідним періодом 2012 року зафіксовано за такими видами економічної діяльності як: будівництво, переробна промисловість, сільське господарство та ін. Зростання виробництва валової доданої вартості відбулося у торгівлі, сфері операцій з нерухомим майном, оренди, інжинірингу, послуг підприємцям, діяльності транспорту та зв'язку, добувній промисловості, фінансовій діяльності та ін. [1]. Слід акцентувати увагу на такому факті, що якщо максимальне підвищення валової доданої вартості зафіксовано на рівні 3,4%, то максимальне зниження складає 11,7%. Вищевикладене робить актуальними питання дослідження основних науково-методичних підходів, спрямованих на аналіз потенціалу розвитку сучасних підприємств.

Загальні проблеми управління потенціалом підприємств досліджували такі зарубіжні вчені-економісти як: Р. Маккен, В. (Р. McCann) Крейдер (В. Kreider) , В.О. Мілс (W.O. Mills) , Б. Карлоф (В. Karlof) , С.А. Маркова (S. A. Marcova) та ін. Питання оцінки ефективності використання окремих видів ресурсів, формування та аналізу стратегічного, економічного та виробничого потенціалів підприємства розглядали: О.Ю. Амосов, Д.М. Васильківський, В.А. Винокуров, З.І. Галушка, В.Я. Заруба, С.І. Левик, Ю.Ю. Мороз, К.І. Редченко, Т.І. Світлична, О.М. Скібіцький, Л.М. Таранюк, В.А. Чичун, О.В. Чернієва та багато ін.

Формалізація підходів різних науковців дозволило всебічно розглянути існуючу проблему та зробити висновок, що ряд питань, спрямованих на аналіз потенціалу розвитку підприємства недостатньо розроблені і досліджені. Особливо