# Управління стратегічними знаннями підприємства в умовах цифрової економіки

# ПЕРЕЛІК ВИКОНАВЦІВ

| | | |
|---|---|---|
| Керівник НДР<br>д.е.н., проф. | _____<br>2023.09.30 | Ірина ОТЕНКО<br>(загальне керівництво<br>розділ 1 – 50%) |
| Старший науковий співробітник | _____<br>2023.09.30 | Ганна ІВАЩЕНКО<br>(розділ 2 – 50 %) |
| Відповідальний виконавець | _____<br>2023.09.30 | Михайло МАКАРЕНКО<br>(розділ 1 – 25 %) |
| Старший науковий співробітник | _____<br>2023.09.30 | Світлана НАЗАРОВА<br>(розділ 1 – 25 %) |
| Молодший науковий співробітник | _____<br>2023.09.30 | Тетяна АНДРЮЩЕНКО<br>(розділ 2 – 25 %) |
| Молодший науковий співробітник | _____<br>2023.09.30 | Альона РУДЕНКО<br>(розділ 2 – 25 %) |
| Старший науковий співробітник | _____<br>2023.09.30 | Вікторія ЛУГОВА<br>(розділ 3 – 50 %) |
| Молодший науковий співробітник | _____<br>2023.09.30 | Марина КОЙНАШ<br>(розділ 3 – 25 %) |
| Лаборант | _____<br>2023.09.30 | Іван УСАТИЙ<br>(розділ – 25 %) |

# РЕФЕРАТ

Звіт про НДР: 43 с., 1 ч., 10 табл., 12 рис., 39 джерел.

УПРАВЛІННЯ, СТРАТЕГІЧНІ ЗНАННЯ, ТЕНДЕНЦІЇ, ШТУЧНИЙ ІНТЕЛЕКТ, ЦИФРОВА ЕКОНОМІКА, ІНФОРМАЦІЙНА ПІДТРИМКА, МЕТОД, ОЦІНЮВАННЯ, АНАЛІЗ, РОЗВИТОК, ХМАРНІ ТЕХНОЛОГІЇ.

Об’єкт дослідження – інформаційно-аналітичне забезпечення управління стратегічними знаннями торговельної компанії.

Метою науково-дослідної роботи є теоретико-методичне забезпечення та надання практичних рекомендацій щодо управління стратегічними знаннями підприємства в умовах цифрової економіки.

Очікувані результати:

визначення основних категорій управління знаннями компанії;

проведення аналізу глобального ринку систем безпеки в умовах цифрової економіки;

визначення основних тенденцій на ринку систем безпеки;

визначення ключових трендів на ринку систем відеоспостереження;

визначення основних переваг використання штучного інтелекту в системах безпеки;

визначення переваг застосування хмарних рішень в системах безпеки;

розроблення основних рекомендацій для удосконалення інформаційної підтримки управління стратегічними знаннями на ДП «ЕКОВУДБУД».

Основним результатом проведеного дослідження є розробка методичних основ та надання практичних рекомендацій щодо управління стратегічними знаннями підприємства в умовах цифрової економіки.

ЗМІСТ

# ВСТУП

У сучасному світі паралельно відбуваються важливі процеси інтелектуалізації суспільства та розбудови цифрової економіки, основою яких є активне використання знань. Ці процеси суттєво розширюють простір використання й функціонування знань, і дуже важливими характеристиками у цьому плані стають так звані цифрові знання, соціальні та управлінські вміння, якісні розумові здібності та креативність. Інновації із застосуванням нових комбінацій уже існуючих та нових знань стають основним результатом процесу продукування знань сектором бізнесу.

Сьогодні науковий світ збагачується новими дослідженнями, зумовленими стрімкими викликами, новими різновекторними проблемами, на які треба реагувати і давати відповідь.

Динамічність процесів і цифрова трансформація вимагають прискореної адаптації до змін усіх сфер суспільства, зокрема тих інституцій, в яких здобуваються знання.

Стратегічне управління знаннями підприємства в умовах цифрової економіки є важливим завданням для забезпечення конкурентоспроможності та успішного розвитку організації. У цифровій економіці інформація та знання стають цінним активом, який може надати перевагу на ринку.

Основна мета стратегічного управління знаннями в умовах цифрової економіки – створення, управління та розподіл знань усередині підприємства таким чином, щоб вони могли бути використані для досягнення стратегічних цілей та підвищення ефективності бізнес-процесів.

Метою науково-дослідної роботи є теоретико-методичне забезпечення та надання практичних рекомендацій щодо управління стратегічними знаннями підприємства в умовах цифрової економіки.

Основними завданнями науково-дослідної роботи визначено:

визначення основних категорій управління знаннями компанії;

проведення аналізу глобального ринку систем безпеки в умовах цифрової економіки;

визначення основних тенденцій на ринку систем безпеки;

визначення ключових трендів на ринку систем відеоспостереження;

визначення основних переваг використання штучного інтелекту в системах безпеки;

визначення переваг застосування хмарних рішень в системах безпеки;

розроблення основних рекомендацій для удосконалення інформаційної підтримки управління стратегічними знаннями на ДП «ЕКОВУДБУД».

Практичною цінністю результатів науково-дослідної роботи є їх практична значущість для вітчизняних підприємств в сфері реалізації обладнання для систем безпеки.

Методами дослідження виступають статистичні методи дослідження, аналіз, порівняння показників та їх структури, значення та динаміки змін в діяльності торговельних компанії.

Основним результатом проведеного дослідження є розробка методичних основ та надання практичних рекомендацій щодо управління стратегічними знаннями підприємства в умовах цифрової економіки.

Особливістю проведеного дослідження є визначення основних тенденцій на ринку систем безпеки та розроблення основних рекомендацій для удосконалення інформаційної підтримки управління стратегічними знаннями на ДП «ЕКОВУДБУД».

# РОЗДІЛ 1
# ВИЗНАЧЕННЯ ТА ЗМІСТ ПОНЯТТЯ «УПРАВЛІННЯ СТРАТЕГІЧНИМИ ЗНАННЯМИ ПІДПРИЄМСТВА»

В умовах якісної зміни природи конкуренції одним з найважливіших факторів успіху економічних організацій різних типів і бізнес-профілів є раціональне використання ресурсів, причому не стільки матеріально-технічних і фінансових, скільки інтелектуальних. За яскравим виразом П. Друкера, більшість ресурсів перестають бути специфічними: «Самий головний ресурс, що відрізняє бізнес та забезпечує вирішальні конкурентні переваги, – це специфічні виробничі та управлінські знання, які використовуються при веденні бізнесу» [15].

Концепція менеджменту знань (від англ. Knowledge management) поступово набирає популярності. Причина цього очевидна: опинившись у принципово нових умовах господарювання підприємства та інші економічні організації просто примушені шукати нові моделі та управлінські технології забезпечення свого успішного довгострокового розвитку. Коли доступ до традиційних ресурсів стає відкритим, коли майже зникають границі між економічними регіонами та системами внаслідок активного застосування інформаційно-комунікаційних технологій, коли класичні підходи до забезпечення конкурентоспроможності не спрацьовують, об’єктивно виникають передумови для пошуку нових джерел конкурентних переваг, перш за все — «всередині» організації, що знаходить своє відображення в концепціях динамічних здібностей, організаційних компетенцій та менеджменту знань.

Управління знаннями як управлінська технологія, що забезпечує довгостроковий успішний розвиток підприємства, сьогодні має два основі аспекти вивчення.

Перший полягає у суто технологічному (або інформаційному) підході до відбору, структуризації, накопичення та організації доступу до інформації як джерела конкурентних переваг у межах створення відповідних інформаційних підсистем на підприємстві.

Другий аспект розкриває значення знань як інтелектуального капіталу сучасної організації, який не тільки сприяє формування нових конкурентних переваг, але й дозволяє підприємствам формувати стратегічні активи як такі, що є цінними для організації, не мають замінників, не підлягають копіюванню або відтворенню, рідкісні серед активів конкурентів [22].

Ключові аспекти управління знаннями компанії подано на рис. 1.1.

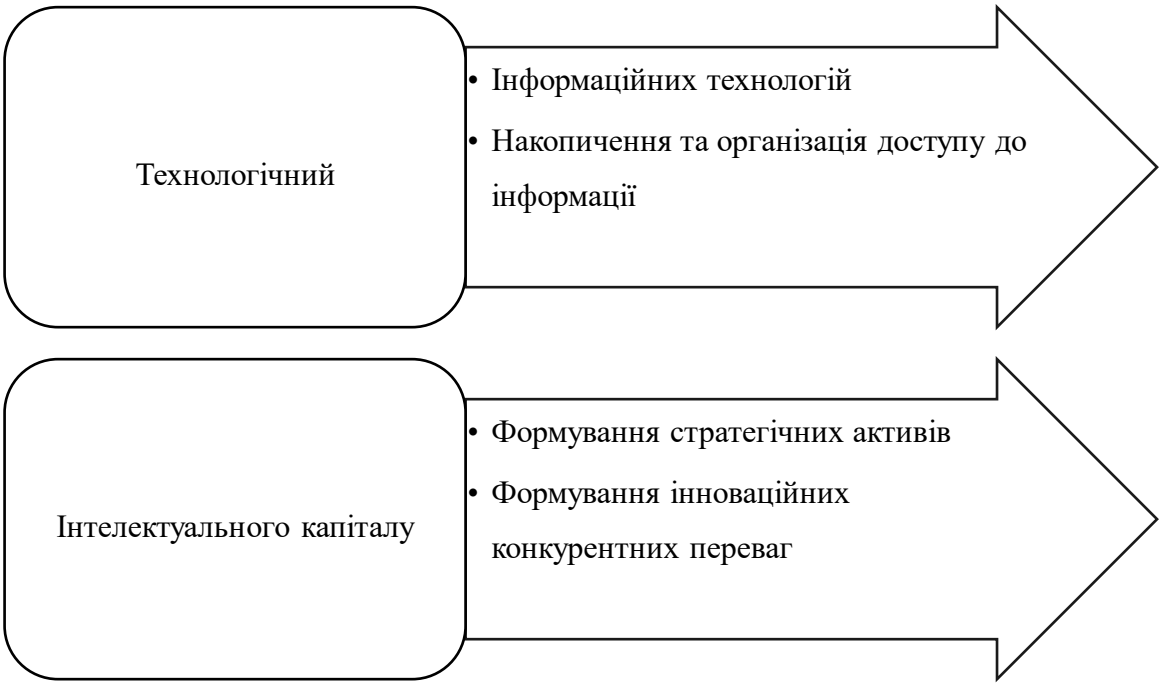


Рис. 1.1. Ключові аспекти управління знаннями компанії

Якщо основні засади IT-підходу до трактування основних засад менеджменту знань доволі ґрунтовно викладені в межах різноманітних теоретичних та прикладних концепцій інформаційних систем підприємства, то проблеми «стратегічного» пояснення природи та сутності знань організації як джерела неповторності та довготривалої успішності підприємства залишаються не достатньо дослідженими.

Сучасна концепція управління знаннями відноситься до неусталених в науковому та прикладному контекстах, про що свідчать намагання її ототожнювання з управлінням документообігом, інформаційними системами для бізнесу, засобами колективної праці (корпоративними порталами тощо). Проте сьогодні стає домінуючим розуміння того, що система управління

знаннями (СУЗ) – це не просто окремий (інформаційний, технологічний) продукт, а скоріше специфічна стратегія підприємства, спрямована на формування всередині організації культури знань та створення механізму підтримки «організаційної свідомості» [19], що поширюється за межами окремих організаційних одиниць з метою виявлення та перетворення на благо підприємства всієї інформації, досвіду та кваліфікації його працівників.

Управління знаннями – це організація управлінських дій на базі всіх інформаційних ресурсів фірми». Проте для використання цих ресурсів необхідний набір спеціалізованих продуктів і платформ.

Таким чином, система управління знаннями компанії є комплексним системним поняттям, що органічно поєднує інформаційну та управлінську складову задля реалізації стратегічних цілей підприємства.

Під управління знаннями потрібно розуміти цілеспрямовану та систематичну управлінську діяльність щодо забезпечення ефективного отримання, передачі та використання знань в компанії. Вона включає розробку методик, процедур, стандартів, визначення джерел, створення інструментів для пошуку, отримання, поширення, оцінки, зберігання, трансферу та перетворення знань, необхідних елементів інтелектуального капіталу [30].

Управління знаннями має базуватися, перш за все, на філософії, в тому числі: теорії М. Поланьї, квазіфізичному підході М. Мамардашвілі. Також прямо застосовна методологія вертикальної інтеграції знань І. Ханіна та М. Борматенко, яка дозволяє зв'язати філософію, науку та практику, тобто вносити глибинні зміни, починаючи зі світогляду людини.

Теоретичну базу управління знаннями формують: теорія підприємництва, фірми, конкурентоспроможності, інституціоналізм, мікроекономічна теорія управління знаннями, теорії перетворення знань, отримання нових знань, концепція організації, яка навчається, компанії, заснованої на знаннях, концепція «потрійної спіралі». Також використовуються загальнонаукові та спеціальні методи пізнання.

Для вдосконалення методології управління знаннями в компанії пропонується виокремлювати:

основні категорії УЗ (знання, процеси, нематеріальні активи, конкурентні переваги, інформаційні інструменти, інтелектуальні ресурси, інноваційний потенціал);

види управління (проактивне, адаптивне, системне, соціальне);

Основні категорії управління знаннями компанії надано на рис. 1.2.

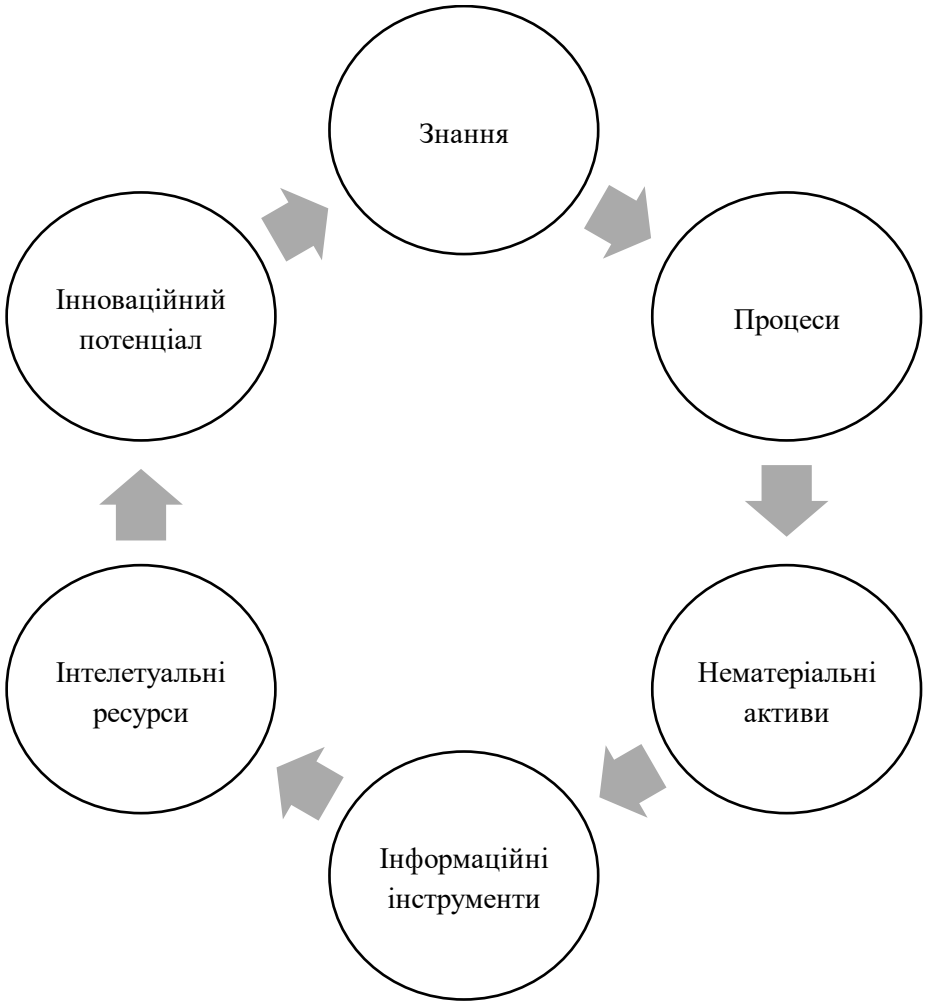


Рис. 1.2. Основні категорії управління знаннями компанії

принципи УЗ (свобода творчості; максимально вільна циркуляція знань; облік специфічних потреб людини; стратегічна спрямованість; облік нелінійності розвитку знань; різноманітність та гнучкість моделей; партисипативність та ін.);

базові підходи (з метою безпеки, з метою продуктивності, з метою лідерства та новаторства; суб'єктно-, об'єктно-, проблемно-, процесно-, ресурсно-орієнтований; централізоване та децентралізоване управління;

плановий, реакційний, компетентнісний, ринковий, інтуїтивний, заснований на лідерстві, конкурентний, консультативний, самоусунення та ін.);

кадрові (плани, інститути, процедури, методології та методики, оцінка знань, методи управління, інформаційні інструменти) та напрямки (управління НДДКР, вдосконалення інформаційних інструментів, управління інтелектуальними ресурсами, розвиток людського капіталу) УЗ;

ключові процеси, що проводяться на рівні дочірніх компаній та всієї корпорації, тобто на міжнародному рівні (генерування або покупка знань, передача, використання; організація робіт, координація, планування, моніторинг, аудит і контроль, мотивація, оцінка ефективності).

Головним об'єктом впливу в управління знаннями є людина, а саме окремі працівники та різні соціальні групи (колективи, відділи, спільноти). Також потрібно враховувати особливості різних видів знань, окремо розглядаючи знання для інноваційної діяльності, в тому числі фундаментальні наукові знання.

У діяльності компаній слід враховувати такі ознаки класифікації знань: важливість; період використання; спосіб, час і місце виникнення; захист власності; носій; рівень новизни.

В окрему категорію можна також виділити організаційні знання як сукупність уявлень про роботу компанії, її структуру, організацію, культуру, тобто знання, необхідні для інтерпретації внутрішньої інформації.

# РОЗДІЛ 2
# ОГЛЯД ГЛОБАЛЬНОГО РИНКУ СИСТЕМ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Обсяг глобального ринку систем безпеки для дому, який в 2021 році оцінювався в 53,6 мільярда доларів США, як очікується, досягне 78,9 мільярдів доларів США до 2025 року, при середньому темпі зростання 8,0% протягом прогнозованого періоду. Найбільшим світовим ринком продуктів і рішень для безпеки є США. Його в 2020 році оцінюють в 14,5 мільярдів доларів США. Очікується, що Китай, друга за величиною економіка світу, досягне прогнозованого розміру ринку в 15,5 мільярдів доларів США до 2027 року. Серед інших географічних ринків, які заслуговують на увагу, є Японія та Канада, де прогнозується зростання на 8,4% і 7,3% відповідно, в період 2021-2027 років. У Європі прогнозується зростання Німеччини приблизно на 7,3%.

Сьогодні клієнти віддають перевагу кільком рішенням в одному пакеті, щоб отримати доступ до найбільш бюджетного рішення. Наприклад, рішення яке забезпечує наскрізну безпеку в усіх аспектах будинку: захищає від зовнішньої загрози (крадіжки, проникнення), а також від будь-якої загрози безпеці, від пожежі, затоплення, витоку газу тощо.

Багато емпіричних даних свідчать про ефективність камер відеоспостереження в житловому секторі.

Зростання рівня злочинності та квартирних крадіжок є факторами, які вимагають нових рішень безпеки житла. Розробка ефективних і складних систем безпеки разом із зручним встановленням, що забезпечуються бездротовими технологіями, є ключовими факторами, які прискорять зростання ринку. Крім того, доступність віддаленого моніторингу за допомогою мобільних пристроїв буде стимулювати зростання ринку рішень для домашньої безпеки. Стрімке зростання швидкості і якості зв’язку забезпечене провайдерами телекомунікацій є факторами, які створюють великі можливості для зростання ринку безпеки. Однак, великі початкові інвестиції та вартість обслуговування обладнання, а

також недостатня обізнаність щодо переоцінки технологічних удосконалень, є факторами, які можуть стримувати зростання ринку.

Основні тенденції на ринку систем безпеки надано на рис. 2.1.

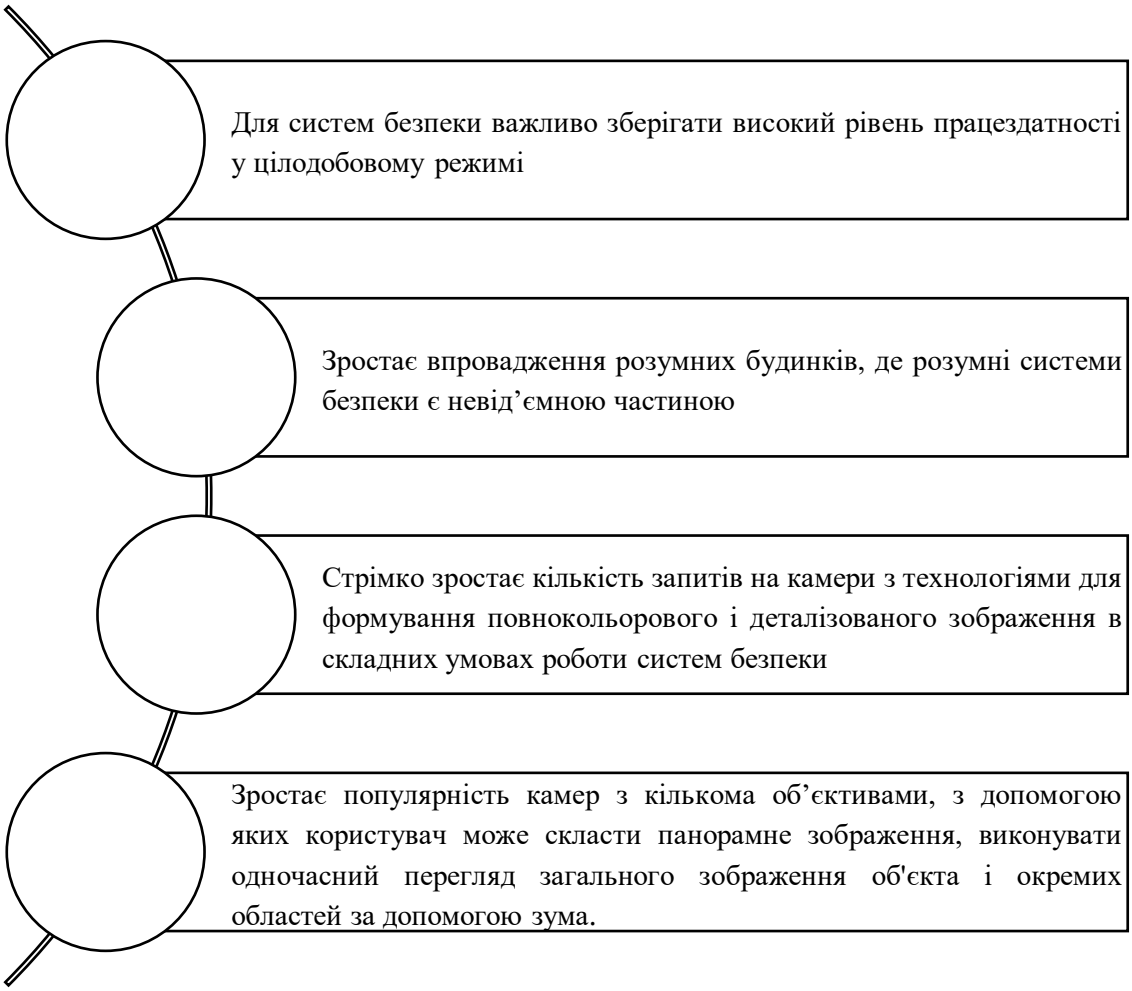


Рис. 2.1. Основні тенденції на ринку систем безпеки

Світовий ринок систем домашньої безпеки, зростає з надзвичайною швидкістю. З кожним роком з'являються нові тенденції та вдосконалюють старі технології, роблячи сектор безпеки будинку більш ефективним. Попит на системи домашньої безпеки, обумовлений зростаючим впровадженням розумних будинків, де розумні системи безпеки є невід'ємною частиною. Впровадження розумних будинків стало можливим завдяки розвитку таких технологій майбутнього, як Інтернет речей (IP, англ. Internet of Things, IoT) .

Інтернет речей (IP,англ.Internet of Things, IoT) – концепція мережі, що складається із взаємозв’язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп’ютерними системами в автоматичному режимі, за допомогою використання стандартних протоколів зв’язку.

Окрім давачів, мережа може мати виконавчі пристрої, вбудовані у фізичні об’єкти і пов’язані між собою через дротові чи бездротові мережі. Ці взаємопов’язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів.

Поява Інтернету речей призвело до розробки мініатюрних датчиків і виконавчих механізмів і малопотужних бездротових комунікаційних технологій. Крім того, зростаюче поширення Інтернету, планшетів і смартфонів відкриває шлях до впровадження IoT у домашню безпеку з використанням розумних додатків. Інтернет речей покращив якість продукції та узгодженість систем автоматизації. Мобільні пристрої та Інтернет виступають інтерфейсом для підключення систем безпеки до хмари; інтеграція систем безпеки будинку з хмарою допомагає у віддаленому моніторингу будинків або іншої інфраструктури. Нещодавні досягнення в області інтелектуальних пристроїв датчиків і керування, а також відповідних комунікаційних технологій, таких як Bluetooth Low Energy (BLE), ZigBee і ANT, полегшили інтеграцію IoT в домашні системи безпеки.

Успішна інтеграція мережі IoT, яка полегшує віддалений, у режимі реального часу й автоматизований моніторинг домашнього середовища, допомогла у розвитку розумних будинків. Таким чином, бездротові системи безпеки є одними з головних досягнень у сфері рішень для домашньої безпеки та Інтернету речей, яким власники будинків віддають перевагу для забезпечення ефективного захисту. Бездротовий доступ до кількох опцій безпеки, таких як контроль доступу та системи виявлення пожежі та газу, пропонує споживачам

гнучкість, зручність та впевненість. Бездротовий контроль над пристроями розумного дому збільшив ймовірність придбання цих пристроїв споживачами.

Ключові тренди на ринку систем відеоспостереження надано на рис. 2.2.


Рис. 2.2. Ключові тренди на ринку систем відеоспостереження

Для систем безпеки важливо зберігати високий рівень працездатності у цілодобовому режимі. Для камер охоронного відеоспостереження і військових потреб важливо зберігати високу якість зображення в будь-яких умовах, у тому числі при слабкому освітленні або при несприятливих погодних умовах.

Стрімко зростає кількість запитів на камери з технологіями для формування повнокольорового і деталізованого зображення в складних умовах роботи систем безпеки. Компанії з світовим досвідом бачать на ринку значне зростання запитів на високочутливі 4К-рішення. Причому все більше

розглядаються камери з роздільною здатністю більше 8 МП і навіть 8K, що вимагає розробки нових систем реєстрації, вузьким місцем яких залишаються процесори, мережі загального доступу і жорсткі диски.

Технології для повнокольорового спостереження в охоронних системах відеоспостереження сьогодні широко затребувані для аналогових і IP-камер. Причому якщо спочатку технології були розраховані тільки на камери з фіксованим об'єктивом, то за минулий рік у відповідь на запити ринку технології цілодобового кольорового зображення з'явилися і в лінійках камер з варіофокальним об'єктивом. В тому числі розвиваються спеціалізовані рішення, наприклад, PTZ-системи, до яких також у проектах починають прописувати вимоги про кольорові зображенні в режимі 24/7.

Говорячи про спеціалізовані системи, також варто підкреслити зростаючу популярність камер з кількома об'єктивами, з допомогою яких користувач може скласти панорамне зображення, виконувати одночасний перегляд загального зображення об'єкта і окремих областей за допомогою зума. Подібні рішення сьогодні також доповнюються високочутливими матрицями для більш якісної зйомки. Застосування таких систем знаходять на великих інфраструктурних об'єктах: аеропорти, залізничні вокзали та міські площі, стадіони та автомобільні стоянки, парки тощо.

Висока вартість, пов’язана з встановленням та обслуговуванням систем безпеки будинку, як очікується, буде ключовим фактором, що обмежує зростання ринку. Хоча клієнти все більше усвідомлюють переваги систем безпеки будинку; водночас вони скептично ставляться до інвестицій, оскільки ціни на системи безпеки все ще не доступні багатьом споживачам.

Вартість обладнання та експлуатації заважають розповсюдженню систем безпеки будинку. Більше того, вартість експлуатації буде ще вищою, оскільки включає в себе витрати на технічне обслуговування, передплату за моніторинг, вартість заміни деталей, а також витрати на встановлення.

Штучний інтелект (AI – artificial intelligence) може відігравати важливу роль у стимулюванні інновацій на ринку домашньої безпеки та моніторингу. Крім того, штучний інтелект у поєднанні з машинним навчанням може зменшити

ймовірність помилкових тривог, покращити виявлення аномальних дій і продуктивність відеоаналітики, а також запропонувати кращі можливості перевірки відео та спостереження. Впровадження цієї комбінації в системи безпеки та моніторингу може залучити більше споживачів.

Основні переваги використання штучного інтелекту в системі безпеки надано на рис. 2.3.

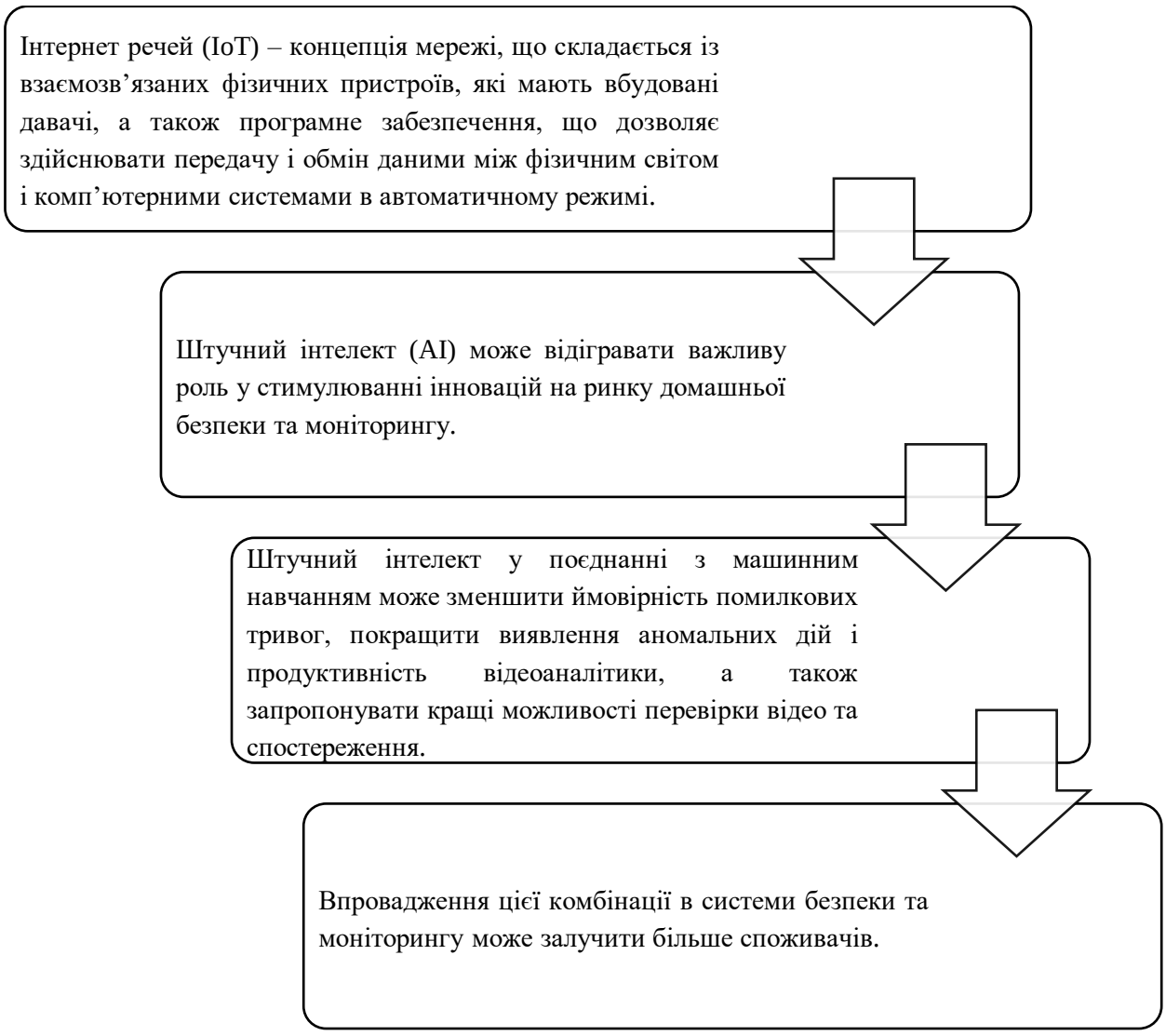


Рис. 2.3. Основні переваги використання штучного інтелекту в системах безпеки

Впровадження рішень безпеки на основі машинного навчання через аналіз даних і штучного інтелекту є тенденцією, що розвивається на ринку систем безпеки для дому.

Інтелектуальні віртуальні помічники (IVA), такі як Alexa і Google, вже інтегровані компаніями в різні системи безпеки будинку. Сьогодні камери спостереження використовують штучний інтелект і глибоке навчання, щоб зробити систему безпеку надійнішою та точнішою. Наприклад, компанія Hangzhou Hikvision Digital Technology (Китай) запустила серію камер DeepinView з функцією глибокого навчання для забезпечення точної та послідовної аналітики відеоконтенту (VCA). Ключові переваги цієї нової технології включають виявлення людського тіла, розпізнавання обличь, підрахунок людей та керування транспортними засобами. Глибоке навчання на основі штучного інтелекту та комп'ютерний зір передбачають вчинення злочину до фактичної події. Система на базі штучного інтелекту вивчає щоденний розпорядок сім'ї та може розпізнати власників будинку [32].

Америка має найбільша частка ринку у вартісному вираженні. Найбільший розмір ринку пояснюється раннім впровадженням систем безпеки будинку в цьому регіоні. Цей регіон є домом для великих компаній, які працюють на ринку, таких як Johnson Controls (США), Honeywell (США) та UCT (США); та відомі постачальники послуг безпеки моніторингу, такі як ADT (США), Vivint (США) і Protect America (США), більшість своїх доходів також отримують тут. Крім того, в економічно і технічно розвинених країнах, таких як США і Канада, є велика кількість домогосподарств з високим доходом. Впровадження IoT і розвиток розумних міст сприяли зростанню ринку систем безпеки будинку в регіоні [18].

Найбільшу частку ринку систем безпеки будинку займає відеоспостереження. Системи відеоспостереження, запроваджені вдома, мають різноманітні застосування, такі як моніторинг та контроль доступу, також оснащені функціями виявлення руху та нічного бачення. Очікується, що в умовах зростання рівня злочинності відеоспостереження відіграватиме значну роль у запобіганні злочинам, насамперед через загрозу бути ідентифікованим.

Розвиток технологій дозволив досягти значного прогресу у якості камер відеоспостереження, можливості запису та онлайн перегляду, разом із значним зниженням їх вартості. Камери відеоспостереження є центральним компонентом усіх систем безпеки. Одним з найпопулярніших видів відеокамер є IP-камери, які

широко використовуються як мережеві або інтернет-камери і забезпечують живе відео та аудіо з камери, до яких користувач може отримати віддалений доступ за допомогою інтернет-браузера або мобільного додатку [20].

Бездротові камери відеоспостереження отримали свою популярністю завдяки їх адаптивності, універсальності та простоті використання. Вони прості в установці, що значно знижує витрати на інсталяцію, оскільки для їх встановлення не потрібні довгі (і дорогі) кабелі або професіонали. Ця зручна функція дозволяє користувачам встановлювати камери в місцях, недоступних для звичайних камер відеоспостереження.

Більшість IP камер забезпечують безкоштовну трансляцію відео в реальному часі, та можливість запису на картку пам’яті або “хмару”. Використання хмарного сховища, вимагає від користувача щомісячної передплати за зберігання відео в хмарі. Користувач платить більше, якщо до сервісу підключено кілька камер. Оплата також залежить від того, як довго користувач хоче зберігати відеозаписи відеоспостереження [30].

Відеоаналітика покращує продуктивність систем відеоспостереження за рахунок виявлення подій у реальному часі, аналізу після подій та вилучення статистичних даних, заощаджуючи витрати на персонал і підвищуючи ефективність роботи системи спостереження.

Алгоритми відеоаналітики можуть бути реалізовані для аналізу записаного відео, що є складним і трудомістким завданням для людини-оператора, особливо у випадках, коли об’єм відеоданих, які потрібно видалити, величезний. Завдяки швидкому аналізу записаного відео, відеоаналітика може точно визначити подію в записаному відео та отримати відповідний сегмент відео із збереженого відео.

Новий ландшафт, викликаний глобальними потрясіннями та змінами за останні два роки, також породив нові типи викликів безпеки. Співробітники, клієнти та партнери все частіше працюють віддалено, обмінюючись даними та співпрацюючи через розрізнені онлайн-мережі, що може зробити дані вразливими для крадіжки. І оскільки об'єкти контролюються віддалено, нові правила громадської охорони здоров'я та безпеки регулюють роботу

підприємств. Нижче наведено попередній огляд деяких нових тенденцій, а також оцінка того, як вони вплинуть на галузь безпеки у 2022 році [15].

Системи безпеки та відеоспостереження все частіше включають вбудовану відеоаналітику для надання даних, які можуть забезпечити інтелектуальний захист та моніторинг. Роль бортової аналітики значно зростатиме у 2024 році і надалі, оскільки клієнти об'єднують периферійні обчислення та ШІ для підвищення ефективності моніторингу та пошуку.

В одному галузевому звіті прогнозується, що до 2028 року загальна глобальна інфраструктура периферійних обчислень коштуватиме понад 800 мільярдів доларів. До них відносяться виявлення та класифікація об'єктів, а також збір атрибутів у вигляді метаданих – і все це при одночасному зниженні вимог до затримки та пропускної спроможності системи відеоспостереження, а також забезпеченні збору даних у режимі поточного часу та ситуаційного моніторингу [25].

Штучний інтелект та периферійні обчислення продовжуватимуть підвищувати ефективність та результативність IP камер відеоспостереження, застосовуючи відеоаналітику (об'єкт, вештання, перетин віртуальної лінії та області, виявлення та інше) для моніторингу кожного типу області чи ситуації. Завдяки штучному інтелекту та периферійним обчисленням, які підтримуються камерами відеоспостереження, що використовуються у вертикальних секторах, користувачі можуть проводити «випереджувальне виявлення» і менше покладатися на моніторинг, який реагує, що підвищує безпеку і продуктивність.

Системи мережного відеоспостереження переходять від простих пристроїв моніторингу до комплексних рішень, які можна застосовувати у кожній вертикальній галузі та секторі ринку. Рушійною силою цього є технологія штучного інтелекту, інтегрована із системами на всіх рівнях, і очікується, що ця тенденція матиме безпрецедентне зростання. Справді, за оцінками галузевих аналітиків, світовий ринок відеоспостереження та безпеки на основі ШІ досягне 4,46 мільярда доларів вже до 2024 року [31].

Дані, що генеруються рішеннями штучного зору з використанням відеокамер штучного інтелекту як датчики технічного зору, створюють значну

бізнес-аналітику, що допомагає організаціям краще зрозуміти своїх клієнтів та їх операції. Тепловізійні камери, тепловізори та камери для визначення температури тіла на входах у громадські місця та вестибюлях використовують алгоритми штучного інтелекту на основі периферійних пристроїв для обходу нелюдських джерел тепла та зниження частоти помилкових спрацьовувань.

У хмарних рішеннях використовуються алгоритми підрахунку відвідувачів, щоб допомогти власникам магазинів оцінити продажі або стратегії дизайну статі, або теплова карта для вимірювання та запобігання довгим чергам на касі для підвищення задоволеності клієнтів. Аналогічні програми та переваги можуть бути застосовані до управління дорожнім рухом або систем інтелектуального паркування, логістики або охорони здоров'я для моніторингу критичних зон. Підприємства можуть автоматизувати свої методи забезпечення безпеки, при цьому відповідні заходи реагування вже заплановані та готові до розгортання [27].

"Відеоспостереження як послуга", "Контроль доступу як послуга" — всі ці терміни все частіше звучать в індустрії безпеки. Але що вони насправді означають і якими є переваги бізнес-моделі «як послуга»?

З розвитком та підвищенням зрілості хмарних сервісів виробники відеоспостереження тепер можуть трансформуватися у постачальників «рішення як послуги». Інсталятори та інтегратори комплектів відеоспостереження тепер можуть надавати рішення своїм клієнтам через хмарні платформи, а потім поширювати цю модель на всі сфери свого бізнесу [21].

У 2024 році світовий ринок загальнодоступних хмарних програм стане багатомільярдною галуззю. Компанії можуть реалізувати безліч переваг, об'єднавши програми, інфраструктуру та бізнес-процеси в комбіновану пропозицію «як послуга» або «aaS». Вони можуть швидко реагувати на ринкові умови, що швидко змінюються, швидше виходити на ринок з новими продуктами та послугами і максимально використовувати переваги розширеної відеоаналітики для покращення операцій за рахунок осмисленої інформації — все це допомагає створити унікальну конкурентну перевагу [17].

Переваги застосування хмарних рішень в системах безпеки наведено на рис. 2.4.

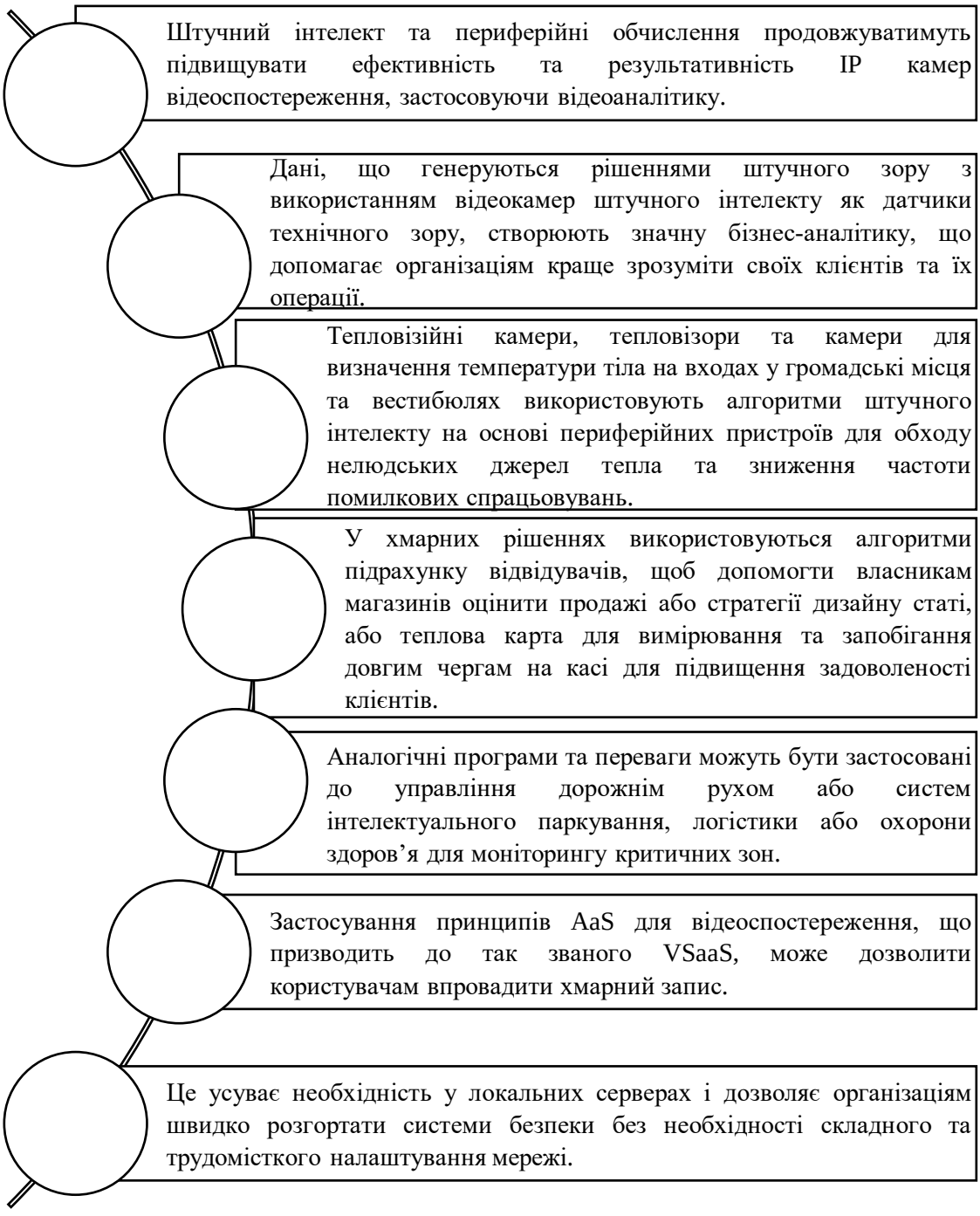


Рис. 2.4. Переваги застосування хмарних рішень в системах безпеки

Використовуючи ці моделі, організації можуть більш точно адаптувати рішення до своїх потреб замість того, щоб покладатися на готові пропозиції. Підхід AaS може забезпечити масштабованість та економічний зиск, скорочуючи

капітальні витрати за рахунок надання послуг у рамках операційних витрат, при цьому послуги надаються на основі підписки [10].

Застосування принципів AaS для відеоспостереження, що призводить до так званого VSaaS, може дозволити користувачам впровадити хмарний запис. Це усуває необхідність у локальних серверах і дозволяє організаціям швидко розгортати системи безпеки без необхідності складного та трудомісткого налаштування мережі. Камери відеоспостереження та всі пристрої можна контролювати централізовано, а багато мережевих та системних процесів можна автоматизувати.

У міру того, як організації впроваджували цифровізацію, можливість віддаленого управління операціями та отримання кращого розуміння за допомогою даних, що генеруються системами безпеки, приносила велику користь. Для багатьох підприємств це було нічим іншим, як трансформацією.

Проте, оскільки все більше їх операцій переноситься в онлайн, керуються віддалено і залежать від хмари, організації повинні впровадити надійні стратегії кібербезпеки для захисту даних, які виявилися для них цінними [27].

Оскільки під час пандемії різко зросла кількість кібератак, будь то фішинг, онлайн-шахрайство та шкідливі програми, такі як розподілена відмова в обслуговуванні (DDoS). В результаті організації все більше усвідомлюють свої обов'язки захисту даних відповідно до таких заходів, як Загальний регламент захисту даних (GDPR), і шукають постачальників і партнерів, які не тільки розуміють правила конфіденційності даних, пов'язаних з відеоспостереженням, але й можуть допомогти забезпечити їхню безпеку.

Попри те, що це ініціатива США, Закон про дозвіл на національну оборону (NDAA), як і раніше, важливий для багатьох європейських підприємств. Занепокоєння національною безпекою поширюється за межі США і уряди країн Європи демонструють явні ознаки посилення своєї позиції. Виходячи з цього, виробники, які змагаються за певні типи контрактів, особливо у державному секторі або пов'язані з міжнародною торгівлею, повинні будуть забезпечити дотримання вимог у всіх своїх операціях та лінійках продуктів, якщо вони розраховують отримати нові можливості для бізнесу.

Мережеві технології та Інтернет речей (IoT) вже набули широкого поширення, але вони продовжать руйнувати ринок камер відеоспостереження, відкриваючи нові можливості для потокової передачі HD-відео навіть на мобільних пристроях. Ці технології розширять потенційні програми для аудіо- та відеоаналітики та штучного інтелекту у світі, який стає все більш взаємопов'язаним. На ширшому рівні спостерігається масовий сплеск повсюдної цифрової трансформації, при цьому ключові технології, що рухають цією зміною, включають Інтернет речей, розумні будинки та мережі, а також хмарні обчислення, інтелектуальні дані та штучний інтелект [11].

Очікується, що на Інтернет речей позитивно вплинуть розробки в галузі мережевих технологій, особливо з точки зору пропускної спроможності та затримки. Додавання передових мережних технологій до відеокамер підтримує віддалене відеоспостереження в реальному часі, розширене використання мобільних програм та застаріле керування мережею. Штучний інтелект Інтернету речей (AIoT) може надати майже необмежений набір потенційних можливостей від відкритих та інтегрованих платформ до розширених можливостей підключення пристроїв.

У 2024 році буде продовжено розвиток таких технологій як штучний інтелект для забезпечення більшої цінності для користувачів, що, у свою чергу, створить нові можливості для бізнесу для установників та інтеграторів. І оскільки штучний інтелект дедалі частіше застосовується на периферії (на камері), його переваги охоплять набагато ширшу аудиторію та мають перетворити ринок безпеки [25].

# РОЗДІЛ 3
# УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ УПРАВЛІННЯ СТРАТЕГІЧНИМИ ЗНАННЯМИ НА ДП «ЕКОВУДБУД»

Управління знаннями є доволі складним процесом, який поєднує управлінський та технологічний аспекти для конвертації знань у вартість і перетворення їх на об’єкт економічних відносин.

До особливостей цифрової економіки, які безпосередньо впливають на всю систему управління знаннями, доцільно віднести:

формування технологічної свідомості;

зміну часово-вартісних аспектів менеджменту, оскільки ущільнюються час і простір;

динамічність усіх процесів і швидкий доступ до будь-якої інформації;

цифровізацію економічного й суспільного життя;

формування й нарощування цифрового ринку;

трансформацію культурних цінностей і формування культури віртуального середовища.

Вищеперераховані та інші особливості цифрової економіки тісно взаємопов’язані і відображають закономірності становлення й розвитку цифрової економіки та окреслюють нові тенденції в системі управління знаннями. Таким чином, управління знаннями ґрунтується на синергетичному зв’язку між технологічними складниками та поведінковими аспектами в менеджменті.

Основними рекомендаціями для удосконалення інформаційної підтримки управління стратегічними знаннями на ДП «ЕКОВУДБУД» є такі:

удосконалення сайту, зокрема, за рахунок додавання 3D-відео обладнання, яке пропонує компанія;

більш яскрава демонстрація можливостей обладнання для систем безпеки;

розширення функцій сайту;

додавання на сайт інформації щодо найбільших бізнес-партнерів;

розроблення реклами для потенційних клієнтів;

удосконалення сторінок в соціальних мережах;

розробка блогу для сайту.

Основними внутрішніми заходами, що стосуються покращення управління стратегічними знаннями є удосконалення організації роботи персоналу компанії. Такий комплекс заходів дозволить підвищити результативність діяльності спеціалістів відділу збуту ДП «ЕКОВУДБУД». Це можуть бути заходи, які стосуються як покарання, так і стимулювання працівників даного відділу.

Однією з пропозицій для ДП «ЕКОВУДБУД» є розробка Положення про порядок заохочення (або покарання) співробітників відділу збуту.

В якості основних критеріїв оцінки роботи працівників відділу збуту може бути закладена загальна сума зниження рівня запасів в цілому по всій групі товарів, яку веде менеджер, а також інші критерії. При цьому необхідно:

проводити оцінювання та аналіз змін в кінці кожного звітного періоду в порівнянні з попереднім сумарний рівень надлишкових запасів, зменшилася або збільшилася кількість дефіцитних позицій, по яких не були своєчасно оформлені заявки на чергові поставки;

доцільно визначити, хто конкретно із співробітників відділу збуту забезпечив наявність позитивних тенденцій, а хто – негативних.

Основні елементи удосконалення інформаційної підтримки управління стратегічними знаннями діяльності ДП «ЕКОВУДБУД» наведено на рис. 3.1.

Рис. 3.1. Основні елементи удосконалення інформаційної підтримки управління стратегічними знаннями ДП «ЕКОВУДБУД»

Тих співробітників, які своїми діями дозволили покращити збутову діяльність компанії, доцільно заохотити. Заохочення може бути матеріальним. Наприклад, премія чи певна доплата відсотку від прибутку. Також заохочення може бути моральним. Наприклад, вручення похвального листа, або певної моральної відзнаки такого співробітника.

Тих співробітників відділу, через непрофесійні дії яких підприємству завдано шкоди як матеріальної, так і репутаційної, повинні бути покарані. Покарання – це може бути зниження премії, або накладання штрафних санкцій.

Крім цього, рекомендується декілька основних заходів щодо удосконалення збутової діяльності компанії:

контролювати весь процес придбання обладнання для систем безпеки має одна відповідальна особа;

офіційний план придбання повинен бути затверджений і схвалений керівником компанії;

у випадку, коли є певні корегувальні показники такого плану, вони повинні бути зафіксовані;

передача повноважень із закупівлі обладнання для систем безпеки іншим співробітникам відділу закупівель повинна відбуватися тільки за умови чіткого позначення суми і переліку найменувань обладнання для систем безпеки, які заплановано.

Таким чином, для розробки заходів удосконалення управління стратегічними знаннями на ДП «ЕКОВУДБУД» рекомендується використовувати поєднання різних підходів до удосконалення інформаційного забезпечення управління стратегічними знаннями, та здійснювати заходи щодо удосконалення роботи персоналу відділів збуту та закупівель.

Рекомендується для покращення контролю робочого часу працівників відділу збуту, встановити спеціалізоване програмне забезпечення, яке

відслідковувало б робочий час співробітників. Наприклад, програмний продукт «Система обліку робочого часу «Бітрікс24».

Автоматичний облік робочого часу співробітників допоможе дізнатися, як проходить робочий день співробітників і скільки насправді часу працівники приділяють роботі.

Програмне забезпечення дозволить встановити:

час початку / закінчення роботи;

запізнення на роботу;

відсутності співробітників на робочих місцях;

фактично відпрацьовану кількість годин.

Також в даному програмному забезпеченні присутній моніторинг програм, додатків та сайтів й аналіз продуктивності роботи.

В базі даних даного програмного забезпечення існує більше 15000 тисяч програм і сайтів, кожен з яких має свою категорію продуктивності:

«Продуктивно» – ресурси, необхідні працівникові для роботи;

«Нейтрально» – додатки, які не потрібні для виконання робочих обов'язків, але періодично виникає необхідність в їх використанні;

«Непродуктивно» – ресурси, використання яких знижує ефективність роботи (соціальні мережі, чати, розважальні ресурси).

Програмне забезпечення для контролю за працівниками, використаним ними за призначенням робочим часом, яке пропонується встановити на ДП «ЕКОВУДБУД», вже існує на ринку України. Його вартість складає 200 грн за місяць на одного працівника. Але якщо порівняти скільки часу працівники на роботі використовують не в робочих цілях, то, звичайно, витрати на використання програмного продукту «Бітрікс 24» повинні дуже швидко окупитися.

Основні можливості програмного продукту «Система обліку робочого часу «Бітрікс24» наведено на рис. 3.2.

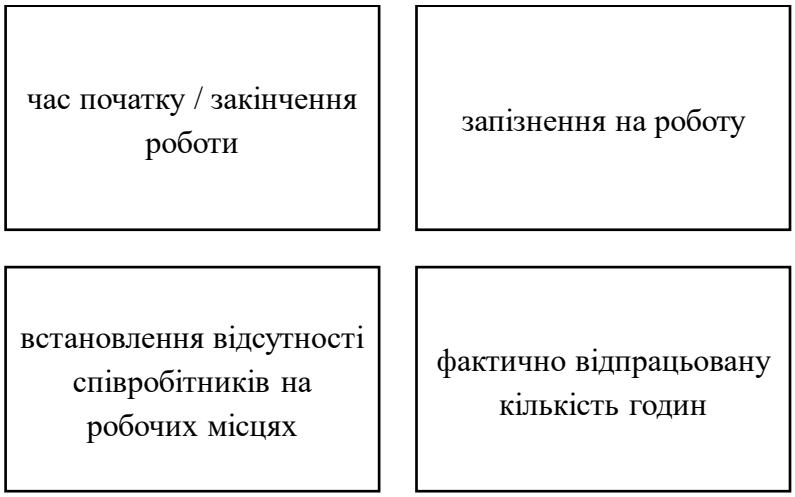


Рис. 3.2. Основні можливості програмного продукту «Система обліку робочого часу «Бітрікс24».

Програмне забезпечення фіксує, з якою програмою або сайтом працював співробітник і привласнює відповідну категорію продуктивності. При цьому одні й ті ж ресурси мають різну продуктивність для співробітників різних відділів.

Для покращення показників діяльності компанії та управління її стратегічними знаннями необхідно реалізувати наступні заходи:

відкриття додаткових ринків, поглиблення існуючих каналів комунікацій;

збільшення витрат на рекламу та на розвиток веб-сайту;

розширення ринків збуту обладнання для систем безпеки.

Питання безпеки комп'ютерних мереж зараз найбільш актуальне і важливе для сучасних корпоративних інфраструктур. Корпоративна інфраструктура повинна мати чітку політику безпеки, яка розробляється після аналізу ризиків, визначення критично важливих ресурсів і можливих загроз, які становлять найбільшу небезпеку. Найактуальнішими є такі загрози.

Маскарад – це використання інформаційних технологій, коли користувач видає себе за іншого, виникає вірогідність несанкціонованого доступу до важливих систем. Для зменшення ймовірності «маскараду» на ДП «Ековудбуд» необхідно використовувати механізмами ідентифікації та авторизації, тоді зменшиться ймовірність того, що користувач, з яким ви встановлюєте зв'язок, не є підставною особою.

Наступною загрозою кадровій безпеці, а також фінансово-економічній безпеці є крадіжка інформації при передачі. Дані можуть бути вкрадені під час передачі по незахищених каналах. Важливу інформацію слід шифрувати – це знизить вірогідність крадіжки конфіденційної інформації.

Ще однією загрозою кадровій безпеці є маніпулювання даними. Можлива зміна даних, які або зберігаються на будь-яких носіях, або передаються. Знову ж таки може допомогти шифрування даних, в деяких методах шифрування є технологія захисту цілісності даних, яка запобігає зміні конфіденційної інформації.

Суттєвою загрозою для сучасних підприємств визнано DoS атаки. Відмова від обслуговування (DoS) одна з різновидів хакерської атаки, в результаті якої важливі системи стають недоступними. Така атака проводиться шляхом переповнення системи непотрібним трафіком, внаслідок чого відбувається перевантаження пам'яті і процесора. Багато систем зараз мають засоби розпізнавання і захисту від DoS атак.

Основними елементами в політики в галузі безпеки є ідентифікація, активна перевірка і цілісність. Ідентифікація відвертає загрозу знеособлення і несанкціонованого доступу до ресурсів і даних. Цілісність захищає від крадіжки даних при передачі і зберігає незмінність переданої або що зберігається. Активна перевірка стежить за правильністю реалізації елементів політики безпеки і допомагає захиститися від хакерських атак і проникнень в мережу.

Для обмеження доступу персоналу до інформації комерційної таємниці керівник ДП «Ековудбуд» видав спеціальний наказ про введення до «Переліку відомостей, які вміщають комерційну таємницю підприємства», заходів щодо охорони цих відомостей, встановлює коло осіб, які мають доступ до неї, і правила роботи з документами ми, які мають гриф «Комерційна таємниця». Співробітники підприємства повинні під розписку ознайомитись із наказом та додатками до нього.

Приблизно перелік відомостей, що становлять комерційну таємницю підприємства: обсяги кредитів, які одержала або хоче одержати фірма; назви фірм-контрагентів; обсяги виробництва (місяць, квартал, рік); обсяги прибутку

(місяць, квартал, рік); розподіл прибутку; цілі, завдання, тактика переговорів з партнерами; умови комерційних контрактів, послуг; ступінь зацікавленості у придбанні товарів або послуг; заробітна плата працівників фірми; характер та репутація персоналу фірми; регіони збуту продукції; напрямки маркетингових досліджень фірми.

Зовнішні загрози, що сприяють витоку інформації представлено на рис. 3.3.

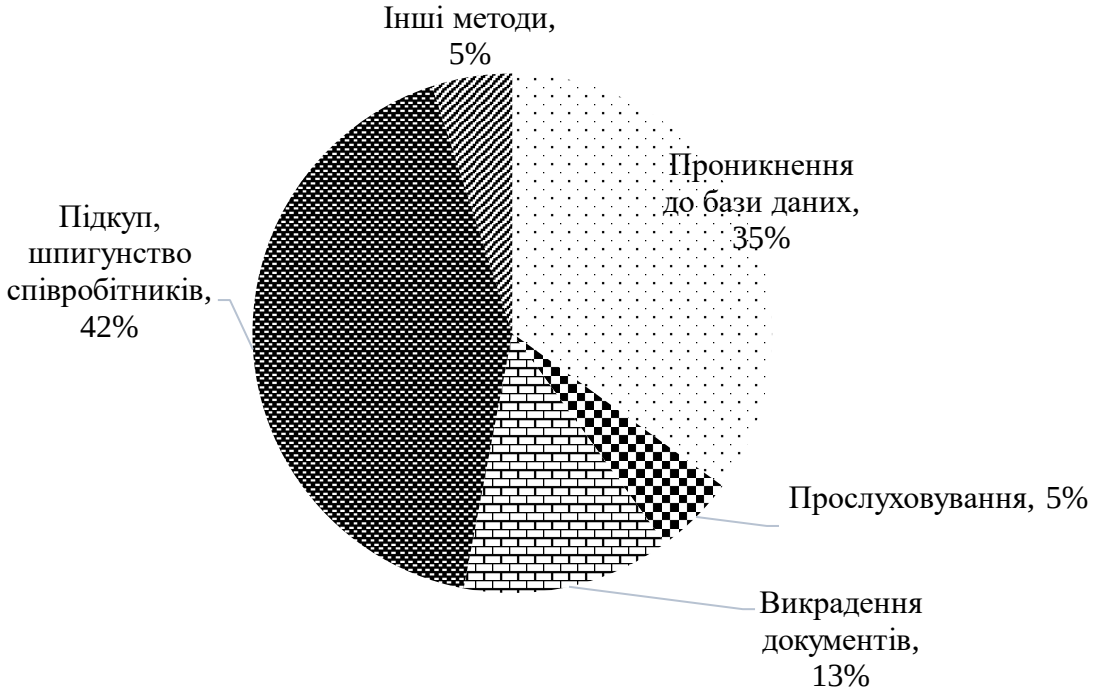


Рис. 3.3. Зовнішні загрози, що сприяють витоку інформації

Для будь-якого підприємства небажано присутність в колективі – на виробництві, в органах управління організації – працівників, які входять або потенційно можуть увійти до груп ризику. У загальному розумінні група ризику – це люди, що потрапили під вплив найбільш поширених видів залежності, внаслідок чого наявна девіатна поведінка. Ризик полягає в наступному:

можливість управління працівником, що входить до групи ризику;

постійні спроби залежності поширити вплив своїх згубних пристрастей, звичок на оточуючих;

задоволенні своїх залежностей за рахунок робочого часу;

схильність до злочинних дій і порушень.

Недобросовісна поведінка рядових працівників можна запобігти за допомогою безпосереднього спостерігача, використання технічних засобів контролю (відеокамери, спеціальне програмне забезпечення на комп'ютерах), на основі вимірювання показників праці, оцінки результативності. Внутрішні загрози, що сприяють витоку конфіденційної інформації надано на рис. 3.4.


Рис. 3.4. Внутрішні загрози, що сприяють витоку конфіденційної інформації

Найнадійніший спосіб захисту від недобросовісних керівників – обмежити відносини навколо перевірених партнерів, в надійності яких не виникає сумніву. Рекомендується для попередження загроз, що виходять від персоналу (а від керівників особливо) аналізувати як внутрішні показники ефективності діяльності підприємства, так і зовнішні – конкурентоспроможність продукції, репутація фірми.

Внутрішні показники засновані насамперед на показнику прибутку, а зовнішні виступають як ринкові індикатори, що відображають добробут

акціонерів – динаміка курсу акцій підприємства, розмір виплачуваних дивідендів. Маніпулювати цими показниками набагато складніше, оскільки оцінка діяльності підприємства дається ринком ззовні [5].

Система заходів, що забезпечують охорону комерційної таємниці, містить у собі:

облік і охорону деяких видів матеріалів і готових виробів (особливо дослідних зразків);

правильну постановку діловодства (циркуляції, обліку, зберігання, знищення документів);

контроль над засобами копіювання та розмноження документів;

захист інформації в засобах зв'язку та обчислювальній техніці;

охорону території підприємства або його основних будинків і споруджень;

нагляд за відвідуванням підприємства сторонніми особами. Контроль над комп'ютерною обробкою інформації [27].

Особливо необхідно підкреслити актуальність захисту інформації, що циркулює в комп'ютерних мережах. За оцінками західних експертів, щорічні втрати від незахищеності інформації в банківських і комерційних інформаційних технологіях у США й країнах ЄС сягають 120-140 млрд дол. США.

Для організації ефективного захисту комерційно цінної економічної інформації необхідно, щоб економічно важливі відомості мали статус комерційної таємниці, тобто потрібно належним чином їх оформити: обумовити існування комерційної таємниці в установчих документах; виключити з переліку інформацію, яка є державною таємницею, та ту, що не є КТ; згрупувати та класифікувати конфіденційну інформацію, яка належить до комерційної таємниці; розробити положення про КТ, яке є основним правовим захистом інформації; розробити договори-контракти для укладення їх із працівниками щодо нерозголошення КТ, розробити інструкції та порядок ознайомлення працівників із документами щодо захисту інформації; розробити правила внутрішнього розпорядку та посадові інструкції осіб, які мають доступ до таємної інформації; розробити інструкцію з дотримання режиму таємності та графік роботи з таємними документами. Рекомендується для покращення

контролю робочого часу працівників, встановити спеціалізоване програмне забезпечення, яке відслідковувало б робочий час співробітників. Зокрема, програмний продукт «Система обліку робочого часу «Бітрікс24».

Рекомендації щодо покращення обліку робочого часу на ДП «Ековудбуд» за рахунок впровадження програмного продукту «Бітрікс 24» надано на рис. 3.5.

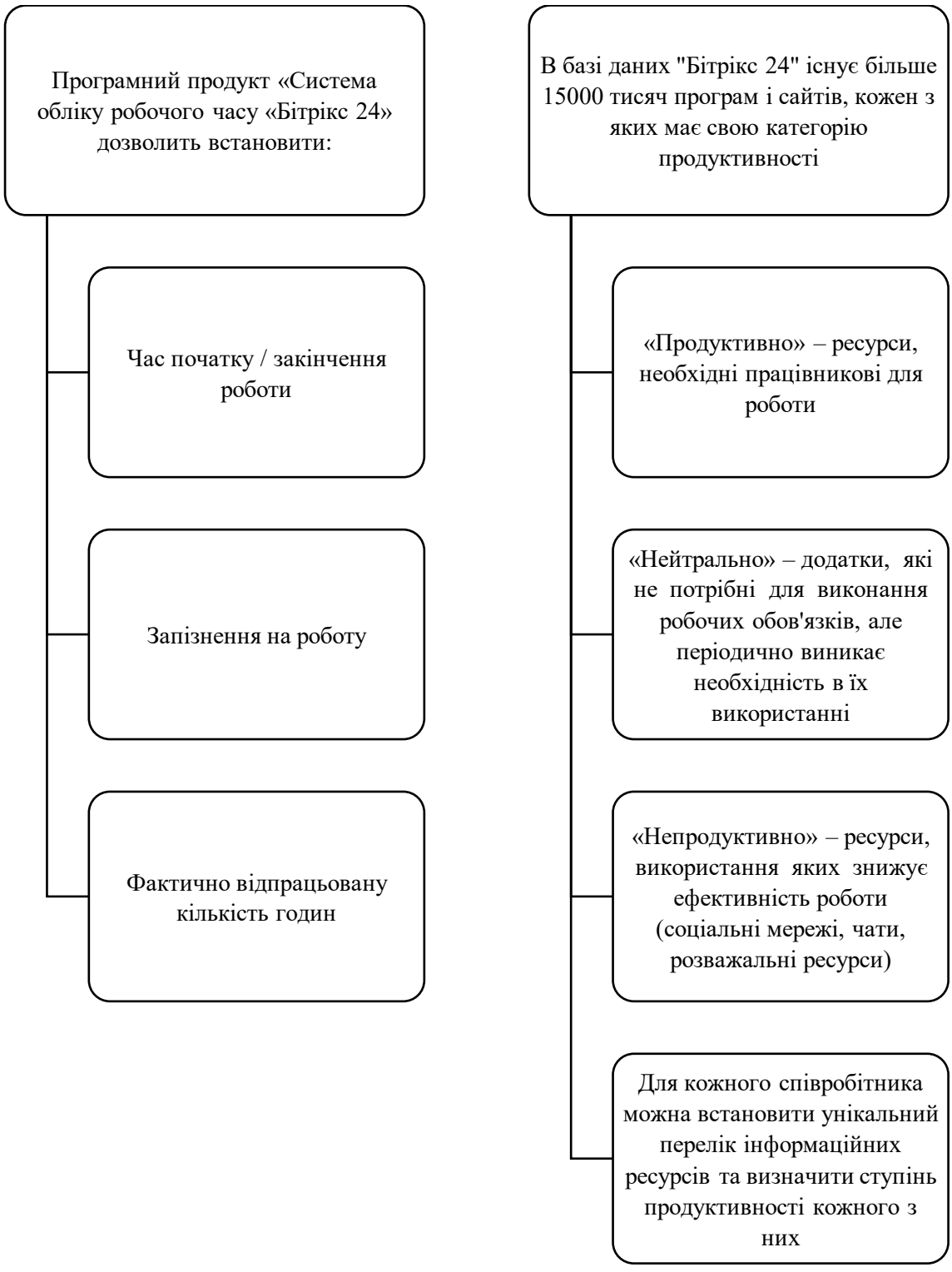

Рис. 3.5. Рекомендації щодо покращення обліку робочого часу на ДП «Ековудбуд» за рахунок впровадження програмного продукту «Бітрікс 24»

Автоматичний облік робочого часу співробітників допоможе дізнатися, як проходить робочий день співробітників і скільки насправді часу працівники приділяють роботі.

Програмне забезпечення фіксує, з якою програмою або сайтом працював співробітник і привласнює відповідну категорію продуктивності. При цьому одні й ті ж ресурси мають різну продуктивність для співробітників різних відділів. Наприклад, для менеджера з продажу Skype і чати – це продуктивний час роботи, а для бухгалтера і програміста – непродуктивний.

В кінці робочого дня, або тижня, або місяця формується звіт для керівника, який може оцінити ситуацію в своєму відділі. Дане програмне забезпечення також може допомогти дізнатися хто спізнюється. «Звіт про запізнення» покаже, як часто співробітник починає свій робочий день пізніше визначеного і наскільки систематично виникають подібні порушення. Керівник побачить кількість запізнень і точний час недопрацювань.

«Звіт про фактичне закінчення робочого дня» покаже, хто з працівників добровільно скорочує свій робочий день і залишає робоче місце раніше встановленого терміну.

У тому, що багато співробітників частину робочого часу використовують не за призначенням можна переконатися з результатів досліджень, присвячених цьому питанню. Візьмемо, наприклад, дослідження компанії Appleton Mayer: «Інтернет-користувачі: використання Інтернету в особистих цілях співробітниками українських компаній». Як показали результати дослідження, 69 % співробітників українських компаній щодня використовують корпоративний доступ до Інтернету в особистих цілях. І тільки 7% - виключно для роботи. Тому не дивно, що більшість керівників повинні вдаватися до використання сервісів для обліку робочого часу співробітників за комп'ютером і отримання об'єктивної оцінкиефективності їх робот

Слід дбати про створення і підтримку оптимально позитивного соціально-психологічного клімату в колективі в цілому, створення корпоративної культури, соціальну політику.

Также в полі контролю необхідно тримати людей схильних до залученню з боку конкуруючих організацій (в силу моральних якостей і займаної посади), зокрема, системні адміністратори, секретарі, помічники керівників, люди, які мають доступ до комерційних таємниць, до конфіденційної інформації або при виникненні потреби можуть дізнатися необхідні дані [26]. Перш за все, схильні до залученню посадові особи, які мають доступ (особливо необмежений) до активів компанії, до фінансової та бухгалтерської документації, до закритої інформації, внутрішніх ресурсів.

Перелік таких посад великий, тому повинен бути складений на ДП «Ековудбуд», яке таким чином повинне піклуватися про удосконалення управління знаннями компанії. Питання управління стратегічними знаннями компанії полягає в безпосередній оцінці працівників, наскільки вони за своїми морально-етичними нормами стійкі або схильні до залучення та, можливо, до передачі важливих знань компанії іншим компаніям.

Тому низька стійкість і моральна готовність до негативної поведінки на діяльність компанії в цілому і на локальному рівні. Співробітникам кадрової служби не варто цього забувати, оскільки саме вони і бути первинним ініціатором перевірки співробітників.

Тому необхідно створити анкету, обов'язкову при працевлаштуванні в компанію. Також варто створити мережу агентів серед співробітників, які співпрацюють на безоплатній основі для захисту стратегічних знань компанії:

створення мережі інформаторів або добровільних помічників серед персоналу;

визначення мотивації вчинення протиправних дій з боку співробітників;

проведення аналізу життя працівників (витрати, матеріальні цінності, кредитні зобов'язання та інше) – все те, що може підштовхнути на отримання власної незаконної матеріальної вигоди;

попередження ситуацій, при яких співробітник або близькі йому люди опиняються в критичному становищі;

запровадження соціальної політики з виплатою грошових компенсацій;

застосування психологічних прийомів при спілкуванні з працівниками;

контролювання адекватності співробітників, їх стійкість до стресів, вимір рівня стресостійкості (за допомогою опитування);

контролювання персоналу з боку служби безпеки;

контроль поведінки і дій під час робочого дня;

контроль звітності за матеріальними та економічними статтями;

контролювання службових і неслужбових контактів (вибірково).

# ВИСНОВКИ

Стратегічне управління знаннями підприємства в умовах цифрової економіки включає декілька ключових аспектів.

По-перше, необхідно визначити стратегічні цілі компанії та виділити основні галузі знань, які є критичними для досягнення цих цілей. Це може бути знання про ринок, клієнтів, конкурентів, технологічні інновації.

По-друге, компанія має розробити ефективні методи збирання, зберігання та передачі знань. В умовах цифрової економіки це може включати використання спеціальних інформаційних систем, баз даних, хмарних технологій та інших засобів управління знаннями.

Проведено аналіз глобального ринку систем безпеки в умовах цифрової економіки.

Визначено основні тенденції на ринку систем безпеки.

Визначено ключові тренди на ринку систем відеоспостереження.

Визначено основні переваги використання штучного інтелекту в системах безпеки.

Визначено переваги застосування хмарних рішень в системах безпеки.

Основними рекомендаціями для удосконалення інформаційної підтримки управління стратегічними знаннями на ДП «ЕКОВУДБУД» є такі:

удосконалення сайту, зокрема, за рахунок додавання 3D-відео обладнання, яке пропонує компанія;

більш яскрава демонстрація можливостей обладнання для систем безпеки;

розширення функцій сайту;

додавання на сайт інформації щодо найбільших бізнес-партнерів;

розроблення реклами для потенційних клієнтів;

удосконалення сторінок в соціальних мережах;

розробка блогу для сайту.

Таким чином, для розробки заходів удосконалення управління стратегічними знаннями на ДП «ЕКОВУДБУД» рекомендується

використовувати поєднання різних підходів до удосконалення інформаційного забезпечення управління стратегічними знаннями, та здійснювати заходи щодо удосконалення роботи персоналу відділів збуту та закупівель.

Рекомендується для покращення контролю робочого часу працівників відділу збуту, встановити спеціалізоване програмне забезпечення, яке відслідковувало б робочий час співробітників. Зокрема, програмний продукт «Система обліку робочого часу «Бітрікс24».

Програмне забезпечення фіксує, з якою програмою або сайтом працював співробітник і привласнює відповідну категорію продуктивності

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрєєв О.В. Перспективи розвитку державного регулювання у сфері автомобілебудування: теоретичні та практичні аспекти / О.В. Андрєєв // 2010. – № 4. – С. 5 – 1 0.

2. Антонюк О.І. Автотранспорт: суть та структура // Ділова Швейцарія. – 2009. – № 3. – С. 57-58.

3. Безверхий А. Маркетинговий огляд ринку в Україні / А. Безверхий // Експерт. – 2008. – № 5. – С. 12-17.

4. Бровкова О. Г. Роль стратегічного менеджменту у розвитку організації / О. Г. Бровкова, М. Л. Ілінчук, К. В. Мельникова // Науковий вісник [Одеського національного економічного університету]. – 2015. – № 12. – С. 34-43.

5. Виклюк М.І. Місце та роль транспортного машинобудування в інноваційному розвитку ЄС. – Науковий вісник. – 2010. – 17.8. – С. 32.

6. Власюк Т. О. Оптимізація імпортної політики як чинник зовнішньоторговельної безпеки // Проблеми економіки. 2015р. №3. С. 39 – 51

7. Вовк Ю. Я. Процес управління знаннями підприємства та його особливості / Ю .Я. Вовк // Науковий вісник НЛТУ України. – 2013. – Вип. 23.17. – С. 343-352.

8. Галушка З. І. Стратегічний менеджмент як нова управлінська філософія: суть та етапи розвитку // Маркетинг і менеджмент інновацій. – 2011. – № 3. Т. 1. – С. 20-24.

9. Герасимчук В. Г. Стратегічне управління підприємством. Графічне моделювання: Навч. посібник. – К. : КНЕУ, 2009. – 360 с.

10. Гіл Ч. Міжнародний бізнес: Конкуренція на глобальному ринку / пер. з англ. А. Олійник, Р. Ткачук. Київ : Видавництво Соломії Павличко "Основи", 2001. 856 с.

11. Горин М.Ф. З історії кон’юктурних економічних досліджень в Україні / Історія народного господарства та народної думки України. – 2014. – № 15 – С. 181-187.

12. Гриліцька А. Управління зовнішньоекономічною діяльністю підприємства / А. Гриліцька, І. Синиця // Збірник наукових праць ЧДТУ. – Випуск 36. - Ч. ІІІ. - 2014. - ISSN 2306-4420. - С. 63 – 67

13. Гриньов А. В. Стратегічне управління в системі маркетинг менеджменту підприємств машинобудівного комплексу / А. В. Гриньов // Вісник Національного технічного університету "ХПІ". Технічний прогрес та ефективність виробництва. – 2013. – № 46. – С. 92-96.

14. Гриньов А.В. Інноваційний розвиток ринку легкових автомобілів та їх промислових підприємств: стратегічне управління. – 2013. – № 308. – С. 218- 221.

16. Демків І. О. Гнучкість підприємства як засіб досягнення його конкурентоспроможності / І. О. Демків // Науковий вісник Полтавського університету економіки і торгівлі. Серія «Економічні науки». – 2011. – № 6 (51), ч. 2. – С. 164 – 168.

15. Дем’янченко А. Г. Оцінка ефективності організаційної структури експортної діяльності підприємства// Механізм регулювання економіки. – 2009. № 1, с. 130-137.

16. Дунська А. Р. Управління міжнародною конкурентоспроможністю вітчизняних підприємств на інноваційній основі / А. Р. Дунська. // Актуальні проблеми економіки. – 2012. – №7. – С. 104 – 109.

17. Економіко-статистична діагностика підприємства. Конспект лекцій / Т. О. Коваль, О. О. Пономаренко. – Харків: Вид. ХНЕУ, 2008. – 80 с.

18. Єлець О.П. Сутність конкуренції та конкурентоспроможності підприємства / Єлець О.П., Богдан Є.В.. // Шляхи та фактори зниження собівартості продукції промислового підприємства. – 2014. – С. 82–91.

19. Єрьоменко Н. Ю. Конкурентні переваги підприємства / Н. Ю. Єрьоменко. // Управління розвитком. – 2014. – №13. – С. 31–34.

20. Єфремов В. С. Стратегічне управління в контексті організаційного розвитку. // Менеджмент практичний. – 2009. – №1. – С. 3 – 13.

21. Завадський Й. С. Економічний словник / Й. С. Завадський, Т. В. Осовська, О. О. Юшкевич. – Київ: Кондор, 2006. – 356 с.

22. Заяць Р. Нетарифні бар'єри як форма державного регулювання виходу підприємств України на зовнішні ринки [Текст] / Роман Заяць // Інноваційні процеси економічного та соціально-культурного розвитку : вітчизняний та зарубіжний досвід : зб. тез доп. IX Міжнар. наук.-практ. конф. молодих учених і студентів / редкол. : Л. І. Вергун, Ю. В. Мельник, О. Легкий. - Тернопіль : ТНЕУ, 2016. – С. 34-35.

23. Зовнішньоекономічна діяльність підприємства [текст] / За ред. Ю. Г. Козака, Н. С. Логвінової, І. Ю. Сіваченка – Київ: Центр навчальної літератури, 2016. – 792 с.

24. Карпенко М.О. Удосконалення організації зовнішньоекономічної діяльності на підприємстві / М.О. Карпенко, О.В. Захарченко // Проблеми підвищення ефективності інфраструктури – 2010 - №26 – [Електронний ресурс]. – Режим доступу: http://jrnl.nau.edu.ua/index.php/PPEI/article/view/486

25. Конєв С. Критерії та основні способи виходу вітчизняних підприємств на міжнародний ринок за сучасних умов функціонування / С. Конєв // Економічний аналіз. - 2012. - Т. 10(3). - С. 297-300.

26. Кузьмін О.Є. Основи зовнішньоекономічної діяльності: теоретичні і прикладні аспекти: навчальний посібник. / О.Є. Кузьмін, О.Г. Мельник, Л.С. Ноджак – Львів: Видавництво Національного університету “Львівська політехніка”, 2016. – 502 с.

27. Кузьмін О. Є. Організація експортної діяльності підприємства/ О. Є. Кузьмін, А.В. Демчук // Сучасні проблеми економіки і менеджменту : тези доповідей міжнародної науково-практичної конференції/ Національний університет "Львівська політехніка". – Львів : Видавництво Львівської політехніки, 2011. – С. 173 – 174.

28. Міжнародна торгівля: навч.посібник / Ю. Г., Sporek T., Gribincea A., Molendowski E., Shengelia T. [та ін]. - 5-те вид., перероб. та доп. / За ред.. Ю. Г. Козака, Т. Спорека, Е. Молендовського – Київ-Катовіце-Краков: Центр учбової літератури, 2015. – 272 с

29. Облік і техніка зовнішньоекономічної діяльності: [навч. посібник] / В.Є. Єрмаченко, С.В. Лабунська, О.Г. Маляревська та інші. – Х. : ВД „ІНЖЕК”, 2010. – 480 с.

30. Про зовнішньоекономічну діяльність – Закон України № 4496-VI (4496-17) від 13.03.2012 // Відомості Верховної Ради України. – 2013. – № 2.

31. Ріпка Д.О. Формування системи управління знаннями підприємства / Д.О. Ріпка // Управління розвитком : зб. наук. робіт. – Харків : Вид. ХНЕУ, 2011. – № 22 (119). – С. 37 – 39.

32. Руденко М. В. Управління знаннями як конкурентна перевага підприємства / М.В. Руденко, В.О. Криворучко // Економіка та держава. – 2016. – №4. – С. 74-78.

33. Томах В.В. Сутність процесу управління знаннями підприємств промисловості / В.В. Томах // Проблеми економіки. – 2014. – №2. – С. 161-166.

34. Торгівля, маркетинг, реклама: термінол. словник / А. Г. Загородній, Г. Л. Вознюк, І. М. Комарницький ; М-во освіти і науки, молоді та спорту України, Нац. ун-т «Львів. політехніка». – Л. : Вид-во Львів. політехніки, 2011. – 312 с.

35. Управління зовнішньоекономічною діяльністю підприємства: навч. посіб. для вищ. навч. закладів / [Ю.В. Орловська, Г.В. Дугінець, П.А. Фісуненко та ін.; за ред. Ю.В. Орловської]. – Дніпропетровськ: ПДАБА, 2015. – 302 с.

36. Управління зовнішньоекономічною діяльністю: Навч. посібник: 2-ге вид. випр. і доп. / За заг. ред. А.І. Кредісова. - К.: ВІРА-Р, 2012. – 552 с.

37. Череп А. В. Організаційно-економічний механізм експортної діяльності підприємства / А. В. Череп, О. Л. Ортинська // Національне господарство України: теорія та практика управління. – 2015. – С. 232 – 236.

38. Шевчук О.А. Знання – як основний стратегічний ресурс підприємства / О.А. Шевчук // Технологічнй аудит. – 2013. – №2/2(10). – С. 46-49.

39. Андрющенко О. М. Підвищення ефективності діяльності підприємств / О. М. Андрющенко, О. П. Яковенко [Електронний ресурс]. – Режим доступу : http://1_NIO_2014/Economics/ 10_153634.doc.htm.