лише покращує ефективність роботи співробітників, але й допомагає адаптувати їх до нових реалій роботи на відстані.

Війна чітко показала важливість стратегічної готовності до кризових ситуацій. Віддалена робота змусила український бізнес переосмислити свої ланцюги постачання, операційні процеси та управлінські стратегії. Створення резервних фондів, впровадження гнучких логістичних рішень та розробка планів дій на випадок нових криз стали ключовими елементами довгострокових стратегій для кожного підприємства в Україні. Це дозволяє як малому, середньому так і великому бізнесу залишатися стійкими в умовах непередбачуваних обставин.

Віддалена робота, особливо в умовах війни, підсилює виклики, пов’язані з емоційним станом співробітників. Для запобігання вигоранню своїх працівників, керівництво впроваджує програми психологічної підтримки, надають доступ до консультацій фахівців та пропонують гнучкі робочі години на підприємстві. Підтримка ментального здоров’я та забезпечення балансу між роботою і особистим життям стають пріоритетними завданнями для українських підприємств, які прагнуть зберегти продуктивність і лояльність працівників в такому комфортному оточені.

В умовах пандемії та війни в Україні, віддалена робота стала ключовим інструментом для забезпечення стабільності українського бізнесу. Майже всі підприємства змогли адаптувати свої процеси, інвестували в нові технології, кібербезпеку, а також навчання персоналу, щоб зберегти гнучкість та стабільність. Віддалена робота не лише допомогла мінімізувати ризики під час кризи, але й відкрила можливості для виходу на нові ринки, розвитку міжнародних партнерств і збереження продуктивності праці. Стратегічне управління в умовах невизначеності передбачає не тільки операційні зміни, але й пріоритетну увагу до емоційного стану співробітників, що є важливим аспектом ефективності сучасного менеджменту при віддаленій роботі.

Список використаних джерел

1. Obłój Kr., Voronovska R. How business pivots during war: Lessons from Ukrainian companies’ responses to crisis. *Business Horizons.* 2024. Том 67. №1. С. 93-105.

2. Opatska S., Johansen W., Gordon A. Business crisis management in wartime: Insights from Ukraine. *Journal of Contingencies and Crisis Management*. 2023. Том 32. №1.

3. Кібератака на український Київстар обійдеться материнській компанії Veon майже в 100 мільйонів доларів від продажів. URL: https://www.reuters.com/business/media-telecom/cyberattack-on-ukraines-kyivstar-will-cost-parent-veon-almost-100-mln-sales-2024-01-18/ (дата звернення: 07.10.2024).

4. Релокація IT-бізнесу в Україні: як найбільші аутсорсери рятували працівників від війни. URL: https://thepage.ua/ua/business/relokaciya-biznesu-2022-dosvid-najbilshih-it-kompanij (дата звернення: 07.10.2024).

Загородня Альона Сергіївна,
доктор філософії (PhD),
доцент кафедри міжнародних відносин та політичного консалтингу;
Відкритий міжнародний університет розвитку людини «Україна»

ОРГАНІЗАЦІЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

В сучасному світі інформаційна безпека є критичним аспектом для будь-якого підприємства. В умовах цифровізації бізнес-процесів, зростання кіберзагроз та вимог до захисту персональних даних організація ефективної системи менеджменту інформаційної безпеки (СМІБ) стає необхідною для підтримання сталого розвитку, репутації та правової відповідності підприємств.

Кількість і складність кіберзагроз з кожним роком збільшуються. Хакерські атаки, зловмисне програмне забезпечення (malware), фішинг, атаки на сервіси та мережі можуть завдати значних збитків підприємству. *Втрати можуть включати:*

– фінансові збитки;
– порушення операційної діяльності;
– крадіжка конфіденційних даних (як клієнтів, так і працівників);
– шкода репутації [2].

Наявність СМІБ дозволяє підприємствам ідентифікувати та запобігати таким загрозам на ранніх етапах, впроваджуючи заходи з управління ризиками та забезпечення безпеки інформаційних систем.

Організація системи інформаційної безпеки – це бездоганне формування процесів на підприємстві з метою запобігання всілякої шкоди, що здійснюється за допомогою несприятливого впливу на інформацію.

Інформаційні технології використовують у всіх сферах нашого життя. Нехтуючи організацією системи інформаційної безпеки, багато хто наражає на небезпеку свою підприємницьку діяльність, а відповідно і статус підприємства [1].

Оцінка ризиків, економічні прогнози, політика підприємства, планування, регулювання кадрів та інші аспекти містить у собі Системи менеджменту інформаційної безпеки (СМІБ). Основною її метою є лімітований доступ до матеріалів конкретного оточення осіб.

Сучасні законодавчі норми, такі як Загальний регламент захисту даних (GDPR) в Європейському Союзі або Закон України «Про захист персональних даних», зобов'язують підприємства гарантувати безпеку особистих даних своїх клієнтів та працівників. Порушення цих норм може призвести до значних штрафів та судових процесів, а також завдати репутаційних втрат.

Організація СМІБ відповідно до стандарту ISO/IEC 27001 дозволяє впровадити процеси та політики, які відповідають вимогам законодавства і міжнародним нормам, забезпечуючи належний рівень захисту персональних даних.

Значною мірою Система забезпечення інформаційної безпеки є однією зі складових стандарту ISO 27001, про що вже зазначалось вище. Також, вона

передбачає захист від негативного впливу, розкрадання інформації шляхом новітніх технологій. Вона спрямована на розкриття, усунення сторонніх і потенційних загроз та гарантують дотримання координування інформаційних процесів.

Система менеджменту інформаційної безпеки виступає як регулювання різних сфер діяльності, відповідно до Міжнародного стандарту ISO/IEC 27001 «Системи менеджменту інформаційної безпеки. Вимоги» [3].

Міжнародний стандарт ISO/IEC 27001 «Системи менеджменту інформаційної безпеки. Вимоги» є основоположним стандартом у сфері управління інформаційною безпекою. Він визначає вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки (СМІБ). Метою стандарту є захист конфіденційності, цілісності та доступності інформації за допомогою процесів управління ризиками.

Організація може пройти сертифікацію на відповідність стандарту ISO/IEC 27001, що підтверджує її здатність забезпечувати інформаційну безпеку відповідно до міжнародних вимог. Така сертифікація додає довіри з боку клієнтів і партнерів та покращує конкурентоспроможність.

ISO/IEC 27001 охоплює широкий спектр питань інформаційної безпеки, від технічних аспектів (захист даних, шифрування) до організаційних (управління доступом, політики безпеки), що робить його універсальним і придатним для застосування в організаціях різних галузей.

В сучасному бізнес-середовищі наявність сертифікованої системи інформаційної безпеки може бути важливою конкурентною перевагою. Клієнти та партнери більш схильні довіряти підприємствам, які демонструють свою прихильність до захисту інформації. Це особливо актуально для компаній, що працюють у галузях з високими вимогами до безпеки, таких як фінанси, охорона здоров’я, IT та e-commerce.

Сертифікація за стандартом ISO/IEC 27001 може стати важливим фактором при укладенні договорів із новими партнерами, особливо на міжнародному ринку.

Список використаних джерел

1. Загоруйко Л.В., Мартьянова Т.А., Скирда А.В. Моделі аналізу ризику безпеки інформаційних технологій: збірник наукових праць «Методи та системи оптико-електронної і цифровфої обробки зображень та сигналів». 2021. С. 16-19.

2. Тупкало В. М., Ярмолатій А. В. Методологічні засади процесно-орієнтованого підходу до впровадження системи менеджменту інформаційної безпека підприємства. URL: https://confmanagement-proc.kpi.ua/article/view/303686.

3. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022. IDT. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=104398