Впровадження ISO27001:2022 в малих та середніх IT компаніях

Ігор Баранівський
здобувач групи МЕН/ЯСС-23м,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: baranivskyiim@krok.edu.ua
Леонід Віткін
доктор технічних наук,
професор кафедри управлінських технологій,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: Vitkin@krok.edu.ua,
ORCID: 0000-0002-0731-1333

Актуальність дослідження. У сучасному цифровому світі захист інформації є критично важливим завданням. ISO27001:2022 надає рамки для розробки, впровадження та підтримки ефективної системи управління інформаційною безпекою (ISMS), що дозволяє компаніям захищати конфіденційні дані та іншу важливу інформацію від кіберзагроз.

Багато клієнтів вимагають, щоб їхні постачальники мали сертифікат ISO27001:2022, який свідчить про їхню здатність забезпечувати безпеку інформації на високому рівні. Процедури оцінки відповідності повинні бути пропорційні рівню ризиків, які виникають у результаті невідповідності продукції встановленим вимогам.

Об'єктом дослідження є діяльність малих та середніх (small and medium enterprises (SME)) IT компаній, які впроваджують ISO27001:2022 на підприємстві

Предметом дослідження є процеси які здійснюють SME IT компаній під час впровадження ISO27001:2022.

Метою дослідження є аналіз діяльності та кроки, які здійснюють SME IT компаній під час впровадження ISO27001:2022 на підприємстві, а також способи покращення імплементації.

Для досягнення мети дослідження в роботі ставилися такі **завдання**:

• провести аналіз сучасного стану на SME підприємствах IT галузі;

• порівняти ступень впровадження ISO27001:2022 в великих компаніях та SME IT компаніях;

• вивчити заходи та напрями вдосконалення впровадження ISO27001:2022 в SME IT компаніях, знайти способи спрощення імплементації

Актуальні проблеми впровадження та підтримки ефективної системи управління інформаційною безпекою розглядалися в працях: Johannes Mattes, Luca Graf, Giovanna Culot, Guido Nassimbeni, Christian Lepping, Michael Becker, Ben Johnson, та ін.

В процесі дослідження використовували такі наукові методи як SWOT-аналіз, процесний підхід.

На першому етапі досліджували мету сертифікації ISO27001:2022. Було виявлено, що мета полягає в ефективному створенні та управлінні Системою управління інформаційною безпекою (СУІБ), яка базується на моделі Плануй-

Виконуй-Перевіряй-Дій (PDCA) і має на меті постійне поліпшення інформаційної безпеки [1].

Також було досліджено які нормативні вимоги потрібно виконати підприємству для отримання сертифіката, які викладені в розділах з 4-го по 10-й в ISO27001:2022 [1].

На другому етапі було проведено SWOT аналіз при впровадженні ISO27001:2022 в SME IT компаніях

В ході аналізу уло виявлено наступне:

• **Сильні сторони (Strengths):**

• Підвищення довіри клієнтів: Сертифікація за ISO 27001 може підвищити рівень довіри клієнтів до компанії, оскільки вона свідчить про серйозність компанії щодо захисту інформації

• Зменшення ризику безпеки інформації: Реалізація стандарту допоможе ідентифікувати та зменшити ризики безпеки інформації, що може заощадити компанії від фінансових втрат.

• **Слабкі сторони (Weaknesses)**:

• Високі витрати і часові затрати: Впровадження та сертифікація за ISO 27001 може бути дорогим та часовим заходом, особливо для малих підприємств.

• Відсутність необхідних ресурсів: SME можуть мати обмежені людські та фінансові ресурси для впровадження та підтримки системи управління інформаційною безпекою.

• **Можливості (Opportunities):**

• Ринкова конкурентоспроможність: Сертифікація за ISO 27001 може стати конкурентною перевагою на ринку, зокрема при залученні нових клієнтів, які вимагають високого рівня захисту інформації.

• Розширення ринків: Впровадження стандарту може відкрити нові ринки для компанії, оскільки деякі регіональні чи міжнародні ринки можуть вимагати сертифікації за ISO 27001.

• **Загрози (Threats):**

• Кіберзагрози: Інформаційна безпека залишається постійною загрозою, і навіть після впровадження ISO 27001 компанія може стати мішенню для кіберзлочинців.

• Складність забезпечення відповідності: Вимоги стандарту можуть бути складними для впровадження та підтримки, особливо для компаній з обмеженими ресурсами.

Завершальний етап дослідження був присвячений основним вдосконалення впровадження та використання ISO27001:2022 в SME IT компаніях.

Було виявлено кілька ключових напрямків вдосконалення, які можуть включати:

1. Своєчасне оновлення системи управління інформаційною безпекою (СУІБ): Зважаючи на те, що ISO 27001:2022 є оновленою версією стандарту, компаніям слід переглянути та оновити свої СУІБ, щоб вони відповідали новим вимогам та настановам стандарту.

2. Удосконалення управління ризиками: Покращення процесів інвентаризації, оцінки та управління ризиками допоможе компаніям ефективніше виявляти та управляти потенційними загрозами для інформаційної безпеки.

3. Оновлення політик та процедур безпеки: Компанії повинні переглянути та оновити свої політики, процедури та практики безпеки відповідно до нових вимог стандарту, а також врахувати актуальні тренди та загрози в області кібербезпеки [2].

4. Навчання та підвищення обізнаності персоналу: Забезпечення адекватного навчання та підвищення обізнаності персоналу щодо вимог ISO 27001:2022 та практик інформаційної безпеки є важливим елементом вдосконалення системи управління безпекою.

5. Автоматизація процесів: Використання автоматизованих інструментів та технологій для впровадження, управління та моніторингу системи управління інформаційною безпекою може сприяти підвищенню ефективності та зменшенню трудомісткості процесів [5].

Отже, впровадження стандарту ISO 27001:2022 зможе допомогти SME IT компаніям забезпечити високий рівень безпеки інформації, дотримуватися вимог клієнтів і регуляторів, зменшити ризики та підвищити довіру своїх зацікавлених сторін.

Ключові слова: ISO/IEC27001, інформаційні активи, конфіденційність, цілісність, аутентифікація, системи управління інформаційною безпекою (СУІБ).

Список використаних джерел

1. ISO/IEC 27001:2022 - Інформаційна безпека, кібербезпека та захист приватності. URL: https://www.iso.org/ru/standard/27001

2. Johannes Mattes, Luca Graf. Впровадження СУІБ відповідно до ISO 27001 у малих та середніх підприємствах. Біла книга | Червень 2020. URL: Whitepaper_ISO-27001-Implementation_SMEs.pdf (byght.de)

3. URL: https://ostec.blog/en/general/first-steps-iso-27000

4. ISO/IEC 27000. Серія стандартів. Веб-сайт. URL: https://intercert.com.ua/articles/regulatory-documents/210-iso-27000

5. Giovanna Culot, Guido Nassimbeni. Стандарт управління інформаційною безпекою ISO/IEC 27001: огляд літератури та дослідження на основі теорії. Журнал TQM 33(7):76-105. URL: https://www.emerald.com/insight/content/doi/10.1108/TQM-09-2020-0202/full/htm