УДК 004.056

Пірог О.В. , к.т.н., доцент
Шелуха О.О. , к.т.н., доцент
Державний університет «Житомирська політехніка»

ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ МАЛОГО ІТ-ПІДПРИЄМСТВА В УМОВАХ ПІДГОТОВКИ ДО СЕРТИФІКАЦІЇ ISO/IEC 27001

У сучасних умовах цифровізації, зростання кількості та складності кібератак, витоків даних і інших інцидентів інформаційної безпеки (ІБ) підвищує необхідність впровадження системного підходу до захисту інформаційних активів організацій. Додатковим фактором є підвищення вимог з боку клієнтів та партнерів щодо забезпечення належного рівня ІБ. Одним із найбільш поширених міжнародних стандартів у цій сфері є ISO/IEC 27001, який визначає вимоги до створення та функціонування системи управління ІБ (СУІБ). Водночас для малих ІТ-підприємств впровадження вимог ISO/IEC 27001 є складним завданням через обмежені ресурси та недостатню формалізацію процесів. Це обумовлює необхідність розроблення адаптованих моделей формування СУІБ, орієнтованих на специфіку малого ІТ-бізнесу та підготовку до сертифікаційного аудиту.

З метою спрощення процесу впровадження СУІБ для малих ІТ-підприємств пропонується поетапне формування СУІБ відповідно до вимог стандарту ISO/IEC 27001.

На першому етапі здійснюється аналіз контексту діяльності підприємства, визначаються основні інформаційні активи, зацікавлені сторони та вимоги до забезпечення ІБ. На цьому етапі формується базове розуміння процесів обробки інформації та визначаються потенційні загрози для інформаційних ресурсів.

Другий етап передбачає проведення оцінювання ризиків ІБ. Визначаються можливі загрози, вразливості інформаційних систем та оцінюється рівень ризиків для основних інформаційних активів підприємства.

На третьому етапі формується набір організаційних і технічних заходів захисту інформації, спрямованих на мінімізацію виявлених ризиків. Зокрема базові елементи СУІБ.

Четвертий етап передбачає формалізацію процесів та підготовку необхідної документації, що підтверджує відповідність СУІБ вимогам стандарту. Завершальним етапом є проведення внутрішнього аудиту та підготовка підприємства до проходження сертифікаційного аудиту відповідно до вимог ISO/IEC 27001.

Доцільно використовувати базовий перелік видів контролю на основі стандарту ISO/IEC 27001 з урахуванням ресурсних обмежень

малого бізнесу. До основних видів контролю, які доцільно впроваджувати на початковому етапі формування СУІБ, належать:

- політика ІБ;
- контроль доступу до інформаційних систем і ресурсів;
- управління обліковими записами користувачів;
- політика використання паролів та багатофакторної автентифікації;
- резервне копіювання даних;
- процедури управління інцидентами ІБ;
- контроль доступу до систем керування програмним кодом і репозиторіїв;
- захист робочих станцій та серверів;
- управління оновленнями ПЗ;
- навчання персоналу;
- контроль використання хмарних сервісів та зовнішніх інформаційних ресурсів;
- проведення внутрішнього аудиту СУІБ.

Застосування запропонованої моделі призведе до зменшення витрат на впровадження СУІБ, дозволить оптимізувати використання ресурсів, сприятиме скороченню термінів підготовки до проходження аудиту ISO/IEC 27001, підвищенню загального рівня ІБ підприємства, зменшенню ризиків виникнення інцидентів ІБ та забезпеченню більш надійного захисту інформаційних активів.

Список використаних джерел

1. ISO/IEC 27001:2022 - Information security management systems ISO URL: https://www.iso.org/standard/27001.

2. The Ultimate Guide to ISO 27001 for Small Business URL: https://hightable.io/iso-27001-for-small-business/.

3. ISO 27001 Certification Process for SMEs URL: https://sunbytes.io/blog/cybersecurity/complete-iso-27001-certification-process/.

4. Overcome SME Risk Challenges with ISO 27001:2022 URL: https://www.isms.online/iso-27001/risk-management/sme-challenges/.

5. Implementing ISO/IEC 27001:2022 in a SME: a case URL: https://www.theseus.fi/handle/10024/876470.

6. ISO 27001 – A Step-by-Step Approach Toward Certification URL: https://www.barradvisory.com/wp-content/uploads/2023/06/ISO-27001%E2%80%94A-Step-by-Step-Approach-Toward-Certification.pdf.