УДК 004.056
І. Містерман
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВНОЇ УСТАНОВИ НА ОСНОВІ РЕЗУЛЬТАТІВ ІНСТРУМЕНТАЛЬНОГО ОЦІНЮВАННЯ CSET

UDC 004.056
I. Misterman

INFORMATION SECURITY MANAGEMENT SYSTEM OF A GOVERNMENT INSTITUTION BASED ON THE RESULTS OF THE CSET INSTRUMENTAL ASSESSMENT

У роботі розглянуто науково-практичний підхід до формування та впровадження системи управління інформаційною безпекою (ISMS) у державній установі з використанням результатів інструментальної оцінки Cybersecurity Evaluation Tool (CSET). У сучасних умовах цифровізації, коли державні установи активно взаємодіють з інформаційними ресурсами та обробляють значні обсяги даних, питання забезпечення конфіденційності, цілісності та доступності інформації набуває стратегічного значення. Відповідно, застосування CSET дає змогу отримати структуровану й методично обґрунтовану оцінку кіберзахищеності, визначити ключові вразливості, а також співвіднести їх із вимогами міжнародних стандартів ISO/IEC 27001, NIST CSF та чинного законодавства України.

На основі аналізу звітів CSET ідентифіковано критичні розриви в управлінні ризиками, організації інцидент-менеджменту, контролі доступу, веденні журналів подій, захисті мережевої інфраструктури та у відсутності формальних політик інформаційної безпеки. Встановлено, що рівень конфіденційності, цілісності та доступності інформаційних активів установи відповідає низькому показнику SAL Low, що вимагає комплексної модернізації системи безпеки.

У межах роботи розроблено модуль ISMS, який включає організаційні, процедурні та технічні компоненти. Організаційна складова охоплює створення політик ІБ, визначення відповідальних осіб, формування Комітету інформаційної безпеки та розробку системи управління ризиками згідно з ISO/IEC 27005. Процедурний блок містить механізми управління інцидентами, регламенти резервного копіювання та відновлення, правила контролю доступу та моніторингу. Технічна складова модулю представлена заходами з модернізації мережевої інфраструктури, впровадженням захищених протоколів, централізованим антивірусним захистом, сегментацією мережі й побудовою системи збору та аналізу журналів безпеки.

Отримані результати мають практичну цінність для впровадження комплексної системи управління інформаційною безпекою в державних організаціях. Запропонований підхід може бути адаптований до інших установ подібного профілю та забезпечує підвищення рівня кіберстійкості, зменшення впливу ризиків кіберзагроз і формування відповідності вимогам національних та міжнародних нормативів інформаційної безпеки.

Література

1. CSET – Cybersecurity Evaluation Tool. U.S. Department of Homeland Security, 2023.
2. ISO/IEC 27001:2022 Information Security Management Systems – Requirements.
3. Закон України «Про основні засади забезпечення кібербезпеки України», 2017.