DOI 10.15276/imms.v12.no1-2.23
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 23-28

ІНФОРМАЦІЙНА СИСТЕМА НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ

В. П. Галицький, О. А. Стопакевич

Національний університет «Одеська політехніка»
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: val.gal1969@ukr.net, stopakevich@gmail.com

Зараз склалася ситуація, коли розроблено значна кількість міжнародних стандартів, які забезпечують потреби майже всіх галузей інформаційної та кібербезпеки. Але, в той же час, дуже значна частина підприємств і організацій майже всіх напрямків і галузей не відповідає вимогам цих стандартів, як мінімум в Україні. Більш того, дуже значна більшість керівників підприємств не володіють змістом цих стандартів. Приведено короткий опис системи менеджменту інформаційної системи на базі міжнародних стандартів ISO/IEC 27000, вимоги до її функціонування. Розроблена нова інформаційна система нормативного забезпечення кібербезпеки підприємств, яка забезпечує доступ до бази даних, що містить таблиці термінів з кібербезпеки та міжнародних стандартів з менеджменту інформаційної безпеки. Програмне забезпечення інформаційної системи складається з виконавчого файлу, написаного мовою програмування Python з графічним інтерфейсом. Для того, щоб систему використати її потрібно запустити під операційною системою Windows, але її можна легко адаптувати під любу операційну систему, де встановлено Python. Бажано, щоб комп'ютер був під'єднаний до Інтернету. При кожному виклику програми проходить перевірка на оновлення бази даних на web-сторінці програми та, при необхідності, інформаційна система завантажує оновлену базу даних клієнту. Зміну інформації в базі даних здійснює адміністратор програми. Якщо web-сторінка програми не знаходиться, програма працює без оновлення. Використання розробленої «Інформаційної системи нормативного забезпечення кібербезпеки підприємств» має дати змогу підвищити правову грамотність в сфері кібербезпеки та інформаційної безпеки у керівництва підприємств та працівників, яких це стосується. А також сприятиме впровадженню ефективного менеджменту, який буде якісно впливати на кінцевий результат підприємства. Система може бути корисна для викладачів та студентів учбових закладів, які пов'язані з кібербезпекою.

Ключові слова: Інформаційна безпека, кібербезпека, кіберпростір, програмне забезпечення, стандарт, ISO/IEC 27000.

Вступ

Зараз склалася ситуація, коли розроблена значна кількість міжнародних стандартів, які забезпечують потреби майже всіх галузей інформаційної та кібербезпеки. Але, в той же час, дуже значна частина підприємств і організацій майже всіх напрямків і галузей не відповідає вимогам цих стандартів, як мінімум в Україні. Більш того, дуже значна більшість керівників підприємств не знають про зміст цих стандартів.

За створення, впровадження, перевірку (аудит) та експлуатацію єдиної системи інформаційної та кібербезпеки відповідає менеджмент інформаційної безпеки (ІБ) та відповідна група міжнародних стандартів. Тут потрібно пояснити, що стандарти регламентують поведінку менеджменту не в економіці, а саме в створенні єдиної системи інформаційної і кібербезпеки.

Зародження перших принципів менеджменту інформаційної безпеки відбулося наприкінці 1980-х років у Великобританії, коли Міністерство торгівлі та промисловості ініціювало створення робочої групи, яка мала на меті розробити найкращі практики щодо забезпечення інформаційної безпеки. Як результат роботи у 1989 році було опубліковано перший стандарт PD 0003 *Практичні правила управління ІБ*. У 1995 році Британським інститутом стандартів (British Standards Institution) було прийнято

національний стандарт BS 7799-1 з тою ж назвою, який описував 10 областей та 127 механізмів, які були необхідними для побудови системи менеджменту інформаційної безпеки (СМІБ). Друга частина цього стандарту – BS 7799-2 *СМІБ. Вимоги та настанови щодо застосування* – з'явилася у 1998 році та містила вимоги до загальної моделі побудови СМІБ, а також набір інших обов'язкових вимог, на відповідність яким повинна була проводиться обов'язкова сертифікація. Це період початку активного розвитку системи сертифікації в галузі менеджменті безпеки. В кінці 1999 року експерти Міжнародної електротехнічної комісії IEC (International Electrotechnical Commission) та представники Міжнародної організації зі стандартизації (International Organization for Standardization) заявили, що в рамках існуючих стандартів відсутній спеціалізований стандарт менеджменту ІБ. У результаті взявши за основу BS 7799-1 було прийнято відповідний міжнародний стандарт ISO / IEC. Згодом обидві частини стандарту BS 7799 були переглянуті та адаптовані до міжнародних стандартів систем управління якістю ISO / IEC 9001 та екологією ISO / IEC 14001, а через рік стандарт BS 7799-1 був прийнятий як міжнародний стандарт ISO / IEC 17799-2000 *Інформаційні технології. Практичні правила управління ІБ* [1]. У 2008 року Національний Банк України почав застосовувати вимоги міжнародного стандарту на практиці та зобов'язав всі місцеві банки виконувати його вимоги, створюючи систему менеджменту інформаційної безпеки на основі стандартів безпеки ISO. Оскільки у складі ISO / IEC відповідальність за розробку сімейства міжнародних стандартів з менеджменту ІБ несе підкомітет №27, нумерація даного сімейства стандартів починається з 27000.

Короткий опис системи менеджменту ІБ

Відповідно до стандартів ISO 27000, цілі захисту інформаційної безпеки включають три основні аспекти.

1. Конфіденційність: конфіденційну інформацію можуть переглядати та розголошувати лише уповноважені особи. Тому доступ до цієї інформації має бути належним чином захищений. Конфіденційність порушується, наприклад, якщо зловмисник може підслуховувати комунікації.

2. Цілісність: інформація повинна бути захищена від невиявлених маніпуляцій, щоб зберегти її точність і повноту. Цілісність порушується, якщо, наприклад, зловмисник може змінити дані дослідження без виявлення.

3. Доступність: інформація, послуги або ресурси мають бути доступними для використання для законних користувачів у будь-який час. Доступність може бути порушена, наприклад, через DDoS-атаку, яка навмисно перевантажує системи.

4. Інші аспекти – це автентичність, підзвітність, відданість і надійність.

Ступінь досягнення інформаційної безпеки можна визначити на основі того, наскільки цілі захисту виконуються.

Позначення міжнародних стандартів менеджменту інформаційної безпеки має формат

ISO/IEC nnnnn :yyyy заголовок,

де nnnnn – номер стандарту, yyyy – рік опублікування, заголовок – предмет стандартизації.

ISO зараз налічує 157 національних членів із 195 країн світу.

Серія ISO/IEC 27000, на основі якої розроблятимемо інформаційну систему, містить рекомендації щодо менеджменту інформаційної безпеки, менеджменту ризиків та впровадження засобів контролю в контексті загальної системи менеджменту інформаційної безпеки (СМІБ). Серія застосовується до організацій будь-яких форм і розмірів, також охоплюють не тільки питання конфіденційності, а й технічної безпеки.

В поняття підприємство вкладатимемо більш широкий сенс, в нього входитимуть не тільки юридичні особи, а і фізичні (приватні підприємці, тощо), приватні особи. Великі підприємства можуть дозволити собі мати в штаті фахівця з кібербезпеки, а в деяких випадках і цілі відділи. А що робити приватному підприємцю?

Деяку допомогу йому може дати «Інформаційна система нормативного забезпечення в кібербезпеці». В цій системі він знайде всі стандарти, а також тлумачення визначень, які використовуються в стандартах СМІБ. Так, наприклад, слово «атака» в тлумачному словнику має два визначення, які геть не схожі на визначення згідно стандарту ISO/IEC 27000 і це потрібно розуміти.

СМІБ – це документована система менеджменту, яка складається з набору засобів контролю безпеки, які захищають конфіденційність, доступність і цілісність активів від загроз і вразливостей; це системний підхід до розробки, впровадження, функціонування, моніторингу, аналізу, забезпечення та покращення інформаційної безпеки організації для досягнення бізнес-цілей. Розробляючи, впроваджуючи, керуючи та підтримуючи СМІБ, організації можуть захистити свої особисті та конфіденційні дані від компрометації, розкрадання чи нищення [2].

СМІБ ґрунтується на оцінці ризиків та рівнях прийнятності рішень організації, встановлених таким чином, щоб результативно обробляти ризики та управляти ними. Успішна реалізація СМІБ можлива за умови аналізу вимог щодо захисту інформаційних активів та застосування засобів управління для забезпечення захисту цих інформаційних активів відповідно до ситуації. Також чинниками, які сприяють успішній реалізації системи управління інформаційної безпеки є [3]: усвідомлення необхідності забезпечення інформаційної безпеки; призначення відповідальності за інформаційну безпеку; поєднання зобов'язань керівництва з інтересами заінтересованих сторін; підвищення значення соціальних цінностей; оцінка ризику, що визначає відповідні засоби управління для забезпечення прийнятних рівнів ризику; безпека як невід'ємний елемент інформаційних мереж та систем; активне попередження та виявлення інцидентів інформаційної безпеки; забезпечення комплексного підходу до управління інформаційною безпекою; постійна переоцінка рівня інформаційної безпеки та внесення змін за потреби.

Ефективне впровадження СМІБ є дуже складним процесом, при імплементації якого потрібно враховувати наступні кроки [4]:

1. Визначення обсягу послуг. Керівництво компанії має чітко визначити сфери застосування, цілі та межі СМІБ.

2. Визначення активів, які повинні бути захищені СМІБ. Це можуть бути інформація, програмне забезпечення, послуги та фізичні активи, такі як комп’ютери, кваліфікація, навички та досвід співробітників, а також інші нематеріальні активи, такі як репутація та репутація. Головна мета на даному етапі визначити критично важливі для бізнесу активи, від яких залежить виживання компанії.

3. Визначення та оцінка ризиків. Для кожного активу, який варто захищати, мають бути ідентифіковані та класифіковані потенційні ризики на основі юридичних вимог або вказівок щодо відповідності. Організації повинні визначити, який вплив мав би кожен ризик, якщо було б порушено конфіденційність, цілісність і доступність, або яка ймовірність виникнення ризиків, для того, щоб оцінити, які ризики є прийнятними, наприклад, з огляду на очікувану суму заподіяної шкоди, і які необхідно усунути за будь-яку ціну.

4. Визначення заходів. На основі попередньої оцінки ризику повинні бути обрані та впроваджені відповідні технічні та організаційні заходи для пом’якшення чи уникнення ризику. Це включає визначення чітких компетенцій та відповідальності.

5. Перевірка ефективності: застосовані та впроваджені заходи необхідно постійно контролювати та регулярно перевіряти на ефективність, наприклад, шляхом аудитів.

6. Внесення покращення. Якщо перевірка запроваджених заходів виявляє недоліки або були виявлені нові ризики, процес СМІБ необхідно запустити знову з самого початку. Таким чином, СМІБ можна постійно адаптувати до мінливих умов або вимог, постійно покращуючи інформаційну безпеку в компанії.

За допомогою СУІБ інформаційну безпеку можна систематично впроваджувати в усій компанії та забезпечувати дотримання всіх необхідних стандартів безпеки. Цей комплексний профілактичний підхід має ряд переваг [2]:

1. СМІБ гарантує, що власні інформаційні активи (наприклад, інтелектуальна власність, дані персоналу або фінансові дані), а також дані, довірені клієнтами або третіми сторонами, будуть належним чином захищені від будь-яких загроз.

2. Використовуючи СМІБ для того, щоб зробити інформаційну безпеку невід'ємною частиною своїх бізнес-процесів, компанії можуть постійно підвищувати рівень безпеки та зменшувати ризики інформаційної безпеки. Таким чином вони протидіють ризику інцидентів безпеки, які порушують безперервність бізнесу.

3. Застосовуються суворі вимоги до відповідності, особливо в дуже регульованих секторах, таких як фінанси або критична інфраструктура. Порушення законодавчих норм і договірних угод можуть призвести до великих штрафів. Завдяки СМІБ компанії гарантують, що вони відповідають всім нормативним та договірним вимогам, що також надає їм більшу операційну та юридичну визначеність.

4. Сертифікуючи свої СУІБ, компанії можуть перевіряти третім сторонам, що конфіденційна інформація обробляється безпечно. Це сприяє кращому зовнішньому іміджу та формуванню довіри, що, у свою чергу, означає конкурентну перевагу.

5. Структурована координація та орієнтоване на ризики планування заходів у СУІБ допомагає розставляти пріоритети, ефективно використовувати ресурси та інвестувати в потрібних місцях. Таким чином, після початкових додаткових витрат накладні витрати можна скоротити в довгостроковій перспективі.

Інформаційна система

Інформаційна система нормативного забезпечення складається з бази даних, яка вміщує таблиці термінів з кібербезпеки та міжнародних стандартів з менеджменту інформаційної безпеки. Програмне забезпечення інформаційної системи складається з виконавчого файлу, написаного мовою програмування Python з графічним інтерфейсом. Вікно для роботи з термінами показано на рис.1. Для переходу на форму слід натиснути вкладку **Термін**.

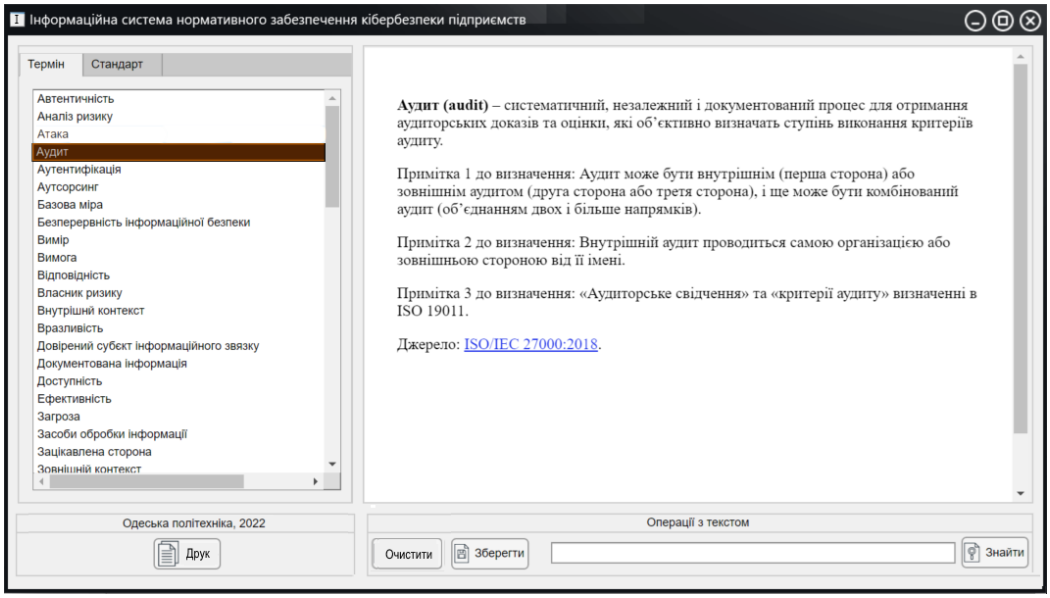

Рис.1. Вікно для роботи з термінами

Зліва в вікні можна вибрати термін, який інтересує користувача. При натисканні на термін у вікні справа з'явиться пояснення терміну, взяте із стандартів по менеджменту інформаційної безпеки серії 27000. Якщо користувач бажає знайти будь-який набір символів в тексті пояснення терміну треба ввести цей набір символів у поле знизу вікна

на натиснути кнопку **Знайти.** Якщо є бажання скопіювати чи роздрукувати виведений текст з допомогою стандартного діалогу Windows, треба натиснути кнопки **Зберегти** або **Друк**. Для того, щоби очистити поле пояснення терміну треба натиснути кнопку **Очистити**

Вікно для роботи з стандартами показано на рис.2. Для переходу на форму слід натиснути вкладку **Стандарт**. Зліва в вікні можна вибрати стандарт по менеджменту інформаційної безпеки серії 27000, який інтересує користувача. При наведені на термін у вікні справа з'явиться повний текст стандарту, взятий із стандартів по менеджменту інформаційної безпеки серії 27000 та двох законів України, які торкаються інформаційної безпеки. Подальша робота з вікном повністю аналогічна роботі з попереднім вікном.

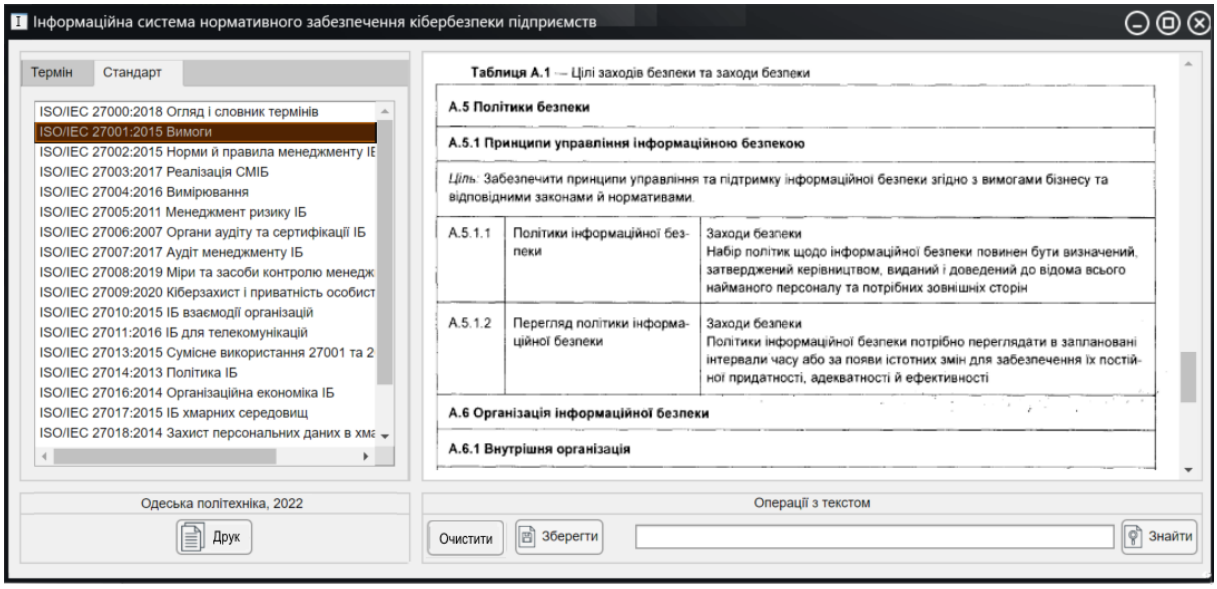

Рис.2. Вікно для роботи з стандартами

Для того, щоб дану систему використати її потрібно запустити на комп'ютер з операційною системою Windows, але її можна легко адаптувати під любу операційну систему, де встановлено Python. Бажано, щоб комп'ютер був під'єднаний до Інтернету. При кожному виклику програми проходить перевірка на оновлення бази даних на web-сторінці програми та, при необхідності, Інформаційна система загружає оновлену базу даних клієнту. Зміну інформації в базі даних здійснює адміністратор програми. Якщо web-сторінка програми не знаходиться, програма працює без оновлення.

Висновок

Використання розробленої «Інформаційної системи нормативного забезпечення кібербезпеки підприємства» має дати змогу підвищити правову грамотність в сфері кібербезпеки та інформаційної безпеки у керівництва підприємств та працівників, яких це стосується. А також впровадженню ефективного менеджменту, який буде якісно впливати на кінцевий результат підприємства. Система може бути корисна для викладачів та студентів учбових закладів, які пов'язані з кібербезпекою.

Список літератури

1. Kissel. Computer Security Division, Information Technology Laboratory. Revision 2. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2013.
2. Золотар О.О. Інформаційна безпека людини: теорія і практика. Київ: АртЕк, 2018. 446 с.
3. Поздняков А.И. Основы теории национальной безопасности. Альманах Пространство и Время. 2013. Т. 2. Вып. 1. 17 с.
4. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства: автореф. дис. канд. екон. наук: 08.00.04. Сімферополь, 2012.

INFORMATION SYSTEM FOR ENTERPRISES CYBER SECURITY NORMATIVE SUPPORT

V.P. Halytsky, O.A. Stopakevych

National Odessa Polytechnic University,
Shevchenko Ave., 1, Odessa, 65044, Ukraine; e-mail: val.gal1969@ukr.net

Now the situation has arisen, when a significant number of international standards have been developed and provided almost all areas of information and cyber security. But, at the same time, a very significant part of enterprises and organizations of almost all directions and industries do not meet the requirements of these standards, at least in Ukraine. Moreover, a very significant majority of managers of these enterprises do not know the content of these standards. A brief description of the management system of the information system based on international standards ISO/IEC 27000, requirements for its operation, is provided. The developed information system for regulatory support of cyber security of enterprises consists of a database that contains tables of cyber security terms and international standards for information security management. Information system software consists of an executable file written in the Python programming language with a graphical interface. In order to use the system, it needs to be run under a Windows operating system, but it can be easily adapted to any operating system where Python is installed. It is preferable that the computer is connected to the Internet. Each time the program is called, the database update is checked on the program web page and, if necessary, the Information System downloads the updated database to the client. The program administrator changes the information in the database. If the web page of the program is not achievable, the program works without updating. The use of the developed "Information system for regulatory support of cyber security of enterprises" should make it possible to increase legal literacy in the field of cyber security and information security among the management of enterprises and employees affected by it. And also, the implementation of effective management, which will have a qualitative impact on the final result of the enterprise. The system can be useful for teachers and students of educational institutions that are related to cyber security.

Keywords: Information security, cyber security, cyberspace, software, standard, ISO/IEC 27000

.