Усі заповіді, що я сьогодні наказав тобі,
Будете пильнувати виконувати…
Книга Повторення Закону, 8, в. 1

ВСТУП

Запропонований вашій увазі посібник відображає сучасні погляди на основи менеджменту інформаційної безпеки (ІБ) організації та орієнтований на підготовку фахівців у галузі знань F «Інформаційні технології», спеціальність F5 «Кібербезпека та захист інформації», освітня програма 6.F5.00.01 Кібербезпека. Посібник розрахований на освічених людей, які цікавляться аспектами управління ІБ, взагалі, інформаційними ризиками і політикою інформаційної безпеки (ПІБ), зокрема, у стрімко плинному навколишньому світі бізнес-процесів та інформаційний технологій, в якому не діють звичні стереотипи, переглядаються основи ведення бізнесу, економічні закони та людські цінності, а ***інформація стала*** *найголовнішим та водночас* ***найуразливішим активом***. Адже характерною рисою *інформаційно-індустріального суспільства* є визначальна роль систем розповсюдження, зберігання та оброблення інформації. І дійсно, запровадження інформаційних технологій на основі новітніх засобів обчислювальної техніки та систем зв'язку зробило інформаційну сферу незамінним атрибутом сучасного суспільства, забезпечуючи його життєдіяльність і прискорений розвиток. Стрімко зростає кількість цінної інформації в інформаційних системах, від якості, достовірності та оперативності одержання якої залежить прийняття важливих рішень на різних рівнях – від президента держави чи організації до рядового громадянина.

Як наслідок, *суспільство*, взагалі, і *громадянин*, зокрема, стають все більш залежними від *якості* функціонування *інформаційних систем та мереж*.

Водночас зворотною стороною цих вкрай позитивних процесів є поява все нових та зростаючих **загроз** *порушення режиму* **безпеки інформації** у результаті виникнення та розвитку в інформаційних системах та мережах **інцидентів інформаційної безпеки** (ІІБ) [1–11]. Аналіз показує, що з часом *інциденти ІБ* будуть набувати все більшого розмаху, а тому також *зростатиме залежність організації від інформаційних, комунікаційних систем та послуг,* які стають вразливішими до порушень режиму ІБ, що може зумовити ***втрату інформаційних активів*** організації та нанесення їй збитків аж до згортання бізнесу. Нагадаємо, що об'єктом міжнародного стандарту ISO/IEC 27001:2005 є саме ***інформаційний актив*** [2]:

- матеріальний та нематеріальний об'єкт;
- який є інформацією або містить інформацію;
- слугує для оброблення, зберігання або передавання інформації;
- має цінність для організації.

До інформаційних активів зазвичай відносять такі [8]:

а) ***<u>інформація</u>***: бази даних та файли даних, контракти та угоди, системна документація, дослідницька інформація, настанови для користувачів, навчальний матеріал, процедури функціонування або підтримки, плани безперервності бізнесу, заходи його відновлення, журнали аудиту та архіви;

б*) *<u>програмні активи</u>: прикладне програмне забезпечення, системне програмне забезпечення, засоби розробки та утиліти;

в*) *<u>фізичні активи</u>: комп'ютерне обладнання, телекомунікаційне обладнання, замінювані носії та інше обладнання;

г*) *<u>послуги</u>: обчислювальні та телекомунікаційні послуги, комунальні послуги, наприклад, опалення, енергопостачання та кондиціювання повітря;

ґ*) *<u>працівники та їхня кваліфікація, навички та досвід</u>;

д*) *<u>нематеріальні активи</u>, такі як репутація та імідж організації.

Графічна інтерпретація поняття *інциденту ІБ* наведено на рис. 1 [8]. Основним елементом даної моделі є інформаційні активи організації, оскільки саме проти них спрямовується негативна дія або низка небажаних і непередбачених подій ІБ, в результаті їхнього впливу відбувається порушення ПІБ.

Рис. 1. Модель інциденту ІБ [8]

Наявність **вразливостей** (рис. 1) свідчить про нездатність системи протистояти реалізації **загроз**. Використовують ці вразливості та створюють інциденти ІБ **порушники**. **Порушник** – це фізична або юридична особа, яка навмисно чи ненавмисно здійснює неправомірні дії щодо інформаційних активів. Вони можуть мати такі мотиви: корисні, дослідницькі, хуліганські, помста, соціальні, політичні та ігрові.

Описана вище модель (див. рис. 1) показує основні складові *інциденту ІБ*. Згідно з даними GFI (Security survey in the United States) [8] найбільший ризик з точки зору ІБ несуть інциденти, пов'язані з поштовими вірусами, завантаженнями з мережі «Інтернет», нападами хакерів (табл. 1).

Таблиця 1

Найбільш небезпечні джерела інцидентів інформаційної безпеки

Інцидент інформаційної безпеки	Ймовірність виникнення, %
Атака інсайдерів	7
Напади хакерів	10
Віруси в електронній пошті	39
Шкідливе програмне забезпечення	9
Інтернет-завантаження	22
Помилки в конфігураціях системи	5
Неконтрольоване використання портативних засобів	7
Інше	2

Реагування на загрози ІБ є важливим компонентом успішної роботи інформаційних технологій (ІТ). Загрози, пов'язані з безпекою, стали не лише більш численними та різноманітними, але й більш шкідливими і руйнівними. За останні роки виникли суттєві зміни у природі загроз ІБ. Профілактичні заходи, засновані на результатах *оцінювання ризиків* ІБ, можуть знизити кількість інцидентів, але не всіх інцидентів можна запобігти. Тому для швидкого виявлення загроз ІБ необхідно створити умови та можливості для реагування на інциденти, мінімізувати втрати та руйнування, видалити уразливості, які були використані, а також відновити роботу інформаційних систем. У посібнику наведені детальні рекомендації з *оброблення ризиків ІБ*

Встановлення чітких процедур для визначення пріоритетів в обробленні ризиків та інцидентів має вирішальне значення. Однак не менш важливим є впровадження ефективних методів збирання, аналізу та підготовка відповідних звітів та набуття досвіду.

А тому ***головною метою*** є ознайомити із *логікою кращих світових практик* та показати *сучасні підходи запровадження системи менеджменту ІБ організації*, зокрема, *системні ризик-орієнтовані підходи*, *методики оцінювання ризиків* та *повернення інвестицій* в ІБ, розроблення та впровадження *ПІБ*, ефективні *моделі ІБ* та *доступу* відповідно до міжнародних та вітчизняних стандартів, зокрема, стандартів Національного банку України.

Основну увагу зосереджено на понятті **менеджменту інформаційної безпеки** у контексті взаємодії співробітників, бізнес-процесів, організацій, а не лише управління, коли передбачається взаємодія програмно-технічних засобів. У проблемі менеджменту інформаційною безпекою є два ключові аспекти: *управління інформаційними ризиками* та *управління доступом*. Якщо проблема управління доступом широко висвітлена у літературі [1, 2], то проблема управління інформаційними ризиками є відносно новим напрямом наукових досліджень в Україні, а тому на ринку недостатньо навчально-наукової літератури вітчизняних авторів з цієї проблеми.

Менеджмент (управління) інформаційними ризиками – тема для багатьох неочевидна, однак значення якої у житті суспільства зростає. Ця область діяльності асоціюється у масовій свідомості з хакерами та комп'ютерними вірусами, а також з витоком даних. Насправді *інформаційна безпека знаходиться на стику загального менеджменту організації, інформаційних технологій, фізичної безпеки та психології*. Для успішного вирішення проблем інформаційної безпеки необхідні нетрадиційні підходи, а також поєднання знань та навичок з різних технічних та гуманітарних областей, які важко поєднати в одній людині. А зводяться усі ці непрості питання у кінцевому результаті до ***управління ризиками***.

Водночас управління ризиками є лише одним із ключових аспектів інформаційної безпеки організації, який створює підґрунтя, аналітичну базу для формулювання *стратегії і тактики* планування та впровадження методів і засобів захисту. Отже, стратегія і тактика інформаційної безпеки організації і є ***політикою інформаційної безпеки організації***.

Розрізняють *загальну стратегічну політику інформаційної безпеки*, взаємопов'язану зі стратегією розвитку бізнесу та стратегією організації, а також *часткові тактичні політики безпеки*, які деталізують вимоги інформаційної безпеки у процесі роботи з відповідними її інформаційними активами, системами та службами.

Поданий у посібнику матеріал викладено на основі кращих світових практик та сучасних підходів *управління ІБ*, зокрема, запровадження в організації технології розслідування ризиків та інцидентів ІБ на основі «*Рекомендацій з усунення інцидентів комп'ютерної безпеки*» Національного інституту стандартів і технології США (NIST)) [1]. У цьому контексті необхідно зазначити таке. Міжнародно-правові норми, зокрема, стандарти, які урегульовують питання ІБ, не є чимось застиглим та незмінним. З розвитком інформаційних технологій вдосконалюються технічні засоби захисту і водночас нападу, а також удосконалюються методи моделювання процесів захисту і водночас нападу. Як наслідок, виникають нові сутності у питаннях ІБ, які були не те що недостатньо враховані у чинних правових нормах, вони не були відомі їхнім розробникам.

Необхідно розуміти одну просту та водночас важливу істину: *власники створюють організації не як об'єкти для запровадження інформаційних технологій, а як структури для досягнення мети, зокрема, у випадку комерційних проєктів – для отримання прибутку*. Запровадження організацією інформаційних технологій може, за певних обставин, значно примножити прибуток, а за інших – поставити організацію на межу банкрутства. За такого підходу *інформаційна безпека повинна працювати на організацію* для забезпечення успішного її функціонування та досягнення мети. А тому результат роботи *служби інформаційної безпеки є* лише вхідною інформацією для керівництва організації при прийнятті управлінських рішень для отримання максимального результату при реалізації мети.

Наш досвід свідчить, що фахівець, який набув теоретичних знань з питань інформаційної безпеки, лише тоді *буде цінуватися на ринку інформаційних технологій*, якщо він, з одного боку, *усвідомить свої роль і місце* в організації, а з іншого, – набуде практичних навиків роботи на *прикладах кращих світових практик менеджменту інформаційною безпекою*. Можемо стверджувати, що *оволодіння практичними навиками побудови системи менеджменту ІБ організації на основі системних ризик-орієнтованих підходів є перепусткою та гарантією успішного працевлаштування* у провідних вітчизняних та зарубіжних бізнес-організаціях, органах влади та контролю тощо.

Посібник створено як на основі навчального курсу, які автори читають студентам Львівської політехніки, так і окремих результатів наукових досліджень у галузі інформаційної безпеки.

Володимир Ромака,
Львів