Якби ви вчились так, як треба,
То й мудрость би була своя.
Т. Г. Шевченко

ПЕРЕДМОВА

Нинішній етап розвитку суспільства має ту особливість, що на зміну *індустріальному* суспільству прийшло *інформаційно-індустріальне*, характерною рисою якого є визначальна роль систем розповсюдження, зберігання та оброблення інформації. 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 пересічного громадянина. Можемо стверджувати, що за своєю значущістю та актуальністю *проблема інформатизації* є *найважливішою* для сучасного суспільства. 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 та прискорений розвиток.

Як наслідок, *суспільство загалом* 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) [1–9].

Аналіз показує, що з часом *інциденти інформаційної безпеки* будуть набувати все більшого розмаху, а тому також буде *зростати залежність організації від інформаційних, комунікаційних систем та послуг,* які стають вразливішими до порушень режиму інформаційної безпеки (ІБ), що може зумовити втрату ***інформаційних активів*** організації та завдання їй збитків аж до згортання бізнесу. Нагадаємо, що об'єктом міжнародного стандарту ISO/IEC 27001:2005 є саме ***інформаційний актив*** [10]:

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

Графічну інтерпретацію поняття *інциденту інформаційної безпеки* подано на рис. 1 [6]. 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 політики інформаційної безпеки (ПІБ).

Рис. 1. Модель інциденту інформаційної безпеки [6]

До інформаційних активів зазвичай належать [6]:

a) *інформація*: 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 щодо його відновлення, журнали аудиту та архівна інформація;

b) *програмні активи*: прикладне програмне забезпечення, системне програмне забезпечення, засоби розробки та утиліти;

c) *фізичні активи*: комп'ютерне обладнання, телекомунікаційне обладнання, замінювані носії та інше обладнання;

d) *послуги*: обчислювальні та телекомунікаційні послуги, комунальні послуги, наприклад, опалення, енергопостачання та кондиціювання повітря;

e) *люди та їхня кваліфікація, навички та досвід*;

f) *нематеріальні активи*, такі як репутація та імідж організації.

Наявність вразливостей (рис. 1) свідчить про нездатність системи протистояти реалізації загроз. Використовують ці вразливості та створюють інциденти інформаційної безпеки 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 (рис. 1) показує основні складові *інциденту інформаційної безпеки*. Згідно з даними GFI (Security survey in the United States) [6], найбільший ризик з точки зору ІБ несуть інциденти, пов'язані з поштовими вірусами, завантаженнями з 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 *інциденти інформаційної безпеки* 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 та *інцидентів інформаційної безпеки*. Якщо ще кілька років тому загрози та інциденти були короткочасними та помітними, то тепер загрози є більш прихованими. Для збирання інформації протягом тривалого часу спеціально розробляються загрози для прихованого поширення в інформаційних мережах та системах. А це призводить до вилучення конфіденційної інформації та інших негативних впливів на інформаційну систему. Виявлення ознак цих загроз на ранніх стадіях є ключовим для запобігання можливої компрометації закритої інформації.

Профілактичні заходи, засновані на результатах *оцінювання ризиків* ІБ, можуть знизити кількість інцидентів, але не всіх інцидентів можна запобігти. Тому для швидкого виявлення інцидентів 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. Саме для цього в підручнику подано рекомендації щодо *оброблення інцидентів*, зокрема для аналізу даних, пов'язаних з інцидентом, і визначення відповідної реакції на кожен інцидент.

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

Представлений у підручнику матеріал викладено на основі найкращих світових практик та сучасних підходів запровадження в організації технології розслідування *інцидентів інформаційної безпеки*, зокрема, «**Рекомендацій з усунення інцидентів комп'ютерної безпеки**» Національного інституту стан-

дартів і технології США (NIST)) [11]. Такий опис проблеми допоможе організаціям успішно реагувати на інциденти інформаційної безпеки та ефективно їх вирішувати.

Запровадження ефективного реагування на інциденти інформаційної безпеки передбачає виконання низки основних рішень та дій. Однак найперше необхідно дати визначення терміна *інцидент інформаційної безпеки*, щоб він був для всіх зрозумілим. У цьому контексті важливо зазначити таке. Поряд із колосальними ресурсами, які витрачаються на виявлення та усунення інцидентів інформаційної безпеки, на сьогодні у міжнародних нормативно-правових документах ***немає єдиного трактування*** поняття *інциденту інформаційної безпеки*.

Нижче як приклад подано визначення поняття ІІБ у низці міжнародно-правових документів. Так, міжнародний стандарт ISO/IEC 20000:2005 постулює, що будь-яка подія, яка не є частиною стандартного функціонування послуги та яка призводить або може призвести до зупинки в наданні цієї послуги, або до зниження її якості, може називатися *інцидентом інформаційної безпеки* [12]. Своєю чергою міжнародний стандарт ISO/IEC 27000:2009 констатує, що *інцидентом інформаційної безпеки* є одна або декілька небажаних або несподіваних подій ІБ, які мають значну ймовірність завдання шкоди бізнес-операціям і загрожують ІБ [13]. З другого боку, у міжнародному стандарті ISO/IEC 13335-1:2004 мовиться, що будь-яка непередбачена або небажана подія, яка може порушити діяльність або ІБ, а саме ІІБ є: втрата послуг, обладнання або пристроїв, системні збої або перевантаження, помилки користувачів, недотримання політик чи рекомендацій, порушення фізичних заходів захисту, неконтрольовані зміни систем, збої програмного забезпечення і відмови технічних засобів, порушення правил доступу [14].

Автори міжнародного стандарту ISO/IEC TR 18044:2004 констатують, що *інцидентом ІБ* є подія, яка є наслідком однієї або декількох небажаних або несподіваних подій ІБ, що мають значну ймовірність компрометації бізнес-операції і створення загрози ІБ [15]. У тексті міжнародного стандарту ISO/IEC 27002 записано, що інцидентом інформаційної безпеки є подія, яка спричинила або може спричинити ушкодження інформаційних активів організації, репутації організації та інформації [16].

У вітчизняному просторі нормативно-правових документів використовується поняття *інцидент інформаційної безпеки* та *інцидент кібербезпеки*. У стандарті Національного банку України ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 [17] вживається термін *інцидент інформаційної безпеки* з формулюванням, ідентичним формулюванню міжнародного стандарту [13]. Натомість у Законі України «Про основні засади забезпечення кібербезпеки України» [5] поняття інциденту трактується так: *інцидент кібербезпеки* (далі – кіберінцидент) – подія

або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

У Британському стандарті з управління безперервністю бізнесу [18] *інцидентом* вважається *ситуація*, яка призводить чи може призвести до руйнування бізнесу, втрат, аварії, кризи. Рекомендації Національного інституту стандартів і технології США [11] трактують поняття *інцидент* як порушення комп'ютерної безпеки, політики, прийнятої політики використання або стандартної практики комп'ютерної безпеки.

Аналіз поняття *інцидент* показав, що інцидент – це [19]:

1) випадок, непорозуміння, подія (зазвичай неприємна), зіткнення;

2) подія, яка була створена людиною. Зазначена відмінність є вкрай важливою, коли подія є результатом злого умислу заподіяти шкоду. У цьому контексті необхідно зазначити, що ***всі інциденти є подіями, однак низка подій не є інцидентами***. Так, у випадку відмови в роботі системи або застосунку через будь-який дефект виникає надзвичайна подія. Однак випадкова помилка або невдача не є інцидентом;

3) несподівана подія зазвичай щось неприємне, пов'язане з конфліктом.

У Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [19] подано більш розлоге визначення терміна *інформаційна безпека*. Згідно з цим Законом, *інформаційна безпека* – стан захищеності важливих інтересів людини, суспільства і держави, при якому запобігається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

У згаданому вище Законі України «Про основні засади забезпечення кібербезпеки України» [5] також більш повним та всеохопним є визначення терміна *кібербезпека* – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Можемо констатувати, що у перелічених визначеннях поняття *інциденту* присутня його характеристика з різних сторін. Однак всі вони не беруть до

уваги повну множину характеристик, а деякі з них включають тотожні (частково або повністю) параметри. Зокрема, у роботі [20] мова іде про «*діяльність*», але не зрозуміло, чи це діяльність організації, чи окремо взятої ІС.

У роботі [8] на основі низки критеріїв оцінювання проведено аналіз дефініцій поняття *інцидент ІБ* у міжнародних та галузевих стандартах, наукових публікаціях, словниках, довідниках та інтернет-ресурсах. У результаті аналізу було виділено спільну множину базових характеристик, притаманних поняттю *інцидент*, а саме: **1) подія; 2) порушення комп'ютерної безпеки; 3) порушення політики безпеки; 4) порушення діяльності; 5) загроза ІБ; 6) підклас кризових і надзвичайних ситуацій; 7) випадок; 8) пригода; 9) відмова; 10) зниження якості послуги**.

Важливо зауважити, що,. крім базових характеристик захищеності інформації, подані вище визначення враховують властивості інформації. А тому у роботі [8] пропонується узагальнене визначення поняття *інцидент інформаційної безпеки*: подія, яка може порушити діяльність, пов'язану із використанням ІС, повноту, своєчасність та вірогідність оброблюваної інформації, а також її конфіденційність, цілісність та доступність.

Однак, на нашу думку, таке визначення не є коректним, адже термін ***подія*** не має визначення у міжнародних стандартах безпеки і не є зрозумілим, про що йдеться. Ми вважаємо, що лише **реалізація загрози інформаційної безпеки здатна порушити діяльність, пов'язану із використанням ІС, повноту, своєчасність та вірогідність оброблюваної інформації, а також її конфіденційність, цілісність та доступність**. Зазначимо, що термін *загроза інформаційної безпеки* використовується в усіх міжнародних стандартах, а самі загрози класифікуються та оновлюються. А тому можемо запропонувати визначення поняття *інцидент інформаційної безпеки*, **яке спирається на стандарти безпеки: інцидент інформаційної безпеки – реалізована загроза**. Саме під таким кутом зору побудовано виклад матеріалу у представленому підручнику.

У цьому контексті необхідно зазначити таке. Міжнародно-правові норми, зокрема, стандарти, які урегульовують питання інформаційної безпеки, не є чимось застиглим та незмінним. З розвитком інформаційних технологій вдосконалюються технічні засоби захисту й одночасно нападу, а також удосконалюються методи моделювання процесів захисту й одночасно нападу. Як наслідок, виникають нові сутності у питаннях інформаційної безпеки, які були не те що недостатньо враховані у чинних правових нормах, вони не були відомі їхнім розробникам.

Особливістю цього підручника є те, що для поглибленого пізнання проблем реагування на інциденти інформаційної безпеки критичні для інформаційної безпеки поняття висвітлюються на двох рівнях – *традиційно описовому* та із застосуванням *системних ризик-орієнтованих підходів*. Саме

такі підходи нині вважаються найкращими практиками при розслідуванні інцидентів інформаційної безпеки шляхом *моделювання* можливих ризикових ситуацій властивостей інформаційного активу і розроблення на цій основі контролів ІБ (методів та засобів захисту).

Автори підручника, окрім озвученої вище мети, поставили перед собою і надзавдання. Ми прагнули, як кажуть «між рядків», донести до читача-студента одну, на перший погляд, банальну 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 інформаційних технологій може, за певних обставин, значно примножити прибуток, а за інших – поставити організацію на межу банкрутства. При такому підході *інформаційна безпека* повинна працювати на організацію, а успішне *розслідування інцидентів інформаційної безпеки є* умовою отримання максимального прибутку.

Наш *досвід показує*, 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 другого – набуде практичних навиків роботи на *прикладах найкращих світових практик менеджменту інформаційної безпеки*. Можемо стверджувати, що **оволодіння практичними навиками та технологією розслідування інцидентів інформаційної безпеки 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.

Доречною до сказаного є цитата із преамбули «Практичні правила управління інформаційною безпекою» (PD 0003) британського стандарту «Управління інформаційною безпекою» BSFD/12, яка застерігає легковірних, що **«Сама по собі відповідність британському стандарту не звільняє від правових зобов'язань»**. Це твердження, враховуючи, що британський стандарт покладено в основу сімейства міжнародних стандартів ISO/IEC 27000, доречно розповсюдити на всі аспекти діяльності, пов'язані з інформаційною безпекою взагалі і з інцидентами інформаційної безпеки зокрема. Ми прагнули зробити так, щоб це твердження було рефреном запропонованого підручника з розслідування *інцидентів інформаційної безпеки*.

Львівська політехніка створила умови для набуття студентом практичних навиків забезпечення режиму інформаційної безпеки організації, передбачивши у навчальних планах та програмах за спеціальністю 125 «Кібербезпека» виконання цільових лабораторних, практичних та курсових робіт, а також переддипломної та дипломної практик як в університетських лабораторіях, так і в провідних організаціях України.

Автори не ставили собі за мету у межах одного підручника дати відповіді на всі проблеми, які пов'язані з *інцидентами інформаційної безпеки*. Дані теми є занадто персоналізованими, складними та багатогранними, щоб їх можна було викласти в одному підручнику. Однак можемо зазначити без зайвої сором'язливості, що читач, ґрунтовно ознайомившись з матеріалом підручника, ***a priori*** перейде у число небагатьох в Україні, хто розуміє цю проблематику та вміє реагувати на *інциденти інформаційної безпеки*.

Автори вдячні професорам *Михайлу Марчуку* та *Івану Опірському*, а також ст. наук. співробітнику *Вірі Пакош* за цінні поради, плідну дискусію та висловлені зауваження до рукопису підручника.

Підручник створено як на основі навчальних курсів, які автори читають студентам Львівської політехніки, так і окремих результатів наукових досліджень з інформаційної безпеки [1–4, 21–26].

За дорученням авторів,
Володимир РОМАКА, Львів, травень 2023 р.