ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ КИЇВСЬКОГО
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
КАФЕДРА КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ
ІНФОРМАЦІЇ

С. С. БУЧИК, С. В. ТОЛЮПА, І. І. ПАРХОМЕНКО

КОРПОРАТИВНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Навчальний посібник

Львів
Видавництво ПП «Магнолія 2006»
2026

УДК 004.056:005.934(075.8)
Б 90

Рекомендовано Вченою радою факультету інформаційних технологій Київського національного університету імені Тараса Шевченка в якості навчального посібника за спеціальністю F5 Кібербезпека та захист інформації освітнього ступеня «магістр» освітньої програми «Кібербезпека та захист інформації», протокол № 11 від 16 квітня 2026 р.

Рецензенти:

Дружинін В.А. доктор технічних наук, професор, завідувач кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Корнієнко Б.Я., доктор технічних наук, професор, професор кафедри інформаційних систем та технологій факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Субач І.Ю. доктор технічних наук, професор, Заслужений працівник освіти України, завідувач спеціальною кафедрою Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Бучик Сергій Степанович

Б 90 **Корпоративне управління інформаційною безпекою**. Навчальний посібник. / Бучик С.С., Толюпа С.В., Пархоменко І.І.– Львів: Видавництво ПП «Магнолія 2006», 2026. – 216 с.

ISBN 978-617-574-346-1

Дане видання є навчальним посібником, підготовленим відповідно до програми навчальної дисципліни «Корпоративне управління інформаційною безпекою».

Мета курсу – формування у студентів системи теоретичних знань та практичних навичок з управління корпоративною безпекою, невід'ємною складовою якої є інформаційна безпека (кібербезпека).

У посібнику розглянуто наступні ключові аспекти: загальні питання управління корпоративною безпекою; основні вимоги, правила та рекомендації щодо забезпечення кібербезпеки корпорації в кіберпросторі, засоби управління кібербезпекою (програмний рівень захисту, безпека корпоративних серверів, оцінка готовності до кіберзагроз); архітектура обміну інформацією та протоколи координації дій, тощо.

Навчальний посібник призначений для здобувачів вищої освіти галузі знань F «Інформаційні технології» за спеціальністю F5 «Кібербезпека та захист інформації».

Публікується в авторській редакції.

ISBN 978-617-574-346-1

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ДСТУ	–	Державний стандарт України
ДЦКЗ	–	Державний центр кіберзахисту та протидії кіберзагрозам
ІБ	–	інформаційна безпека
НД ТЗІ	–	нормативний документ технічного захисту інформації
КС	–	комп'ютерна система
ПЗ	–	програмне забезпечення
ACLs	–	Access Control Lists
APT	–	Advanced Persistent Threats
AS	–	autonomous system (автономна система)
CBT	–	Computer Based Training
CERT	–	Computer Emergency Response Team
CIS	–	Center for Internet Security
CRM	–	Customer Relationship Management (система управління відносинами з клієнтами)
IPSec	–	IP Security
IPO	–	Information Providing Organization
IRO	–	Information Receiving Organization
HSM	–	Hardware security module
HTTP	–	Hyper Text Transfer Protocol
URL	–	Uniform Resource Locator
IAP	–	Independent Application Provider
ISO	–	International Organization for Standardization
ISMS (СУІБ)	–	Information Security Management System (система управління інформаційною безпекою)
IEC	–	International Electrotechnical Commission
MFA	–	multi-factor authentication
NIST	–	National Institute of Standards and Technology
NDA	–	Non-Disclosure Agreement
NTP	–	Network Time Protocol
OSINT	–	Open-Source Intelligence
SDLC	–	Software Development Life-cycle
SSL	–	Secure Sockets Layer
TPM	–	Trusted Platform Module
RBAC	–	role-based access control

ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ

1) *кібербезпека, кіберзахищеність (cybersafety)* – стан захищеності від фізичного, соціального, духовного, фінансового, політичного, емоційного, професійного, психологічного, освітнього чи іншого типу наслідків несправностей, пошкоджень, помилок, нещасних випадків, збитків чи будь-яких інших подій у кіберпросторі, які можна вважати небажаними;

2) *кібербезпека, безпека кіберпростору (cybersecurity; cyberspace security)* – збереження конфіденційності, цілісності та доступності інформації в кіберпросторі;

3) *кібербезпека (cybersecurity)* – властивість захищеності активів від загроз конфіденційності, цілісності, доступності в кіберпросторі;

4) *кіберпростір (cyberspace)* – складне середовище, що є результатом взаємодії людей, програмного забезпечення та послуг у мережі Інтернет за допомогою технологічних пристроїв і підключених до них мереж; не можна сказати, що це середовище є в конкретній фізичній формі;

5) *кіберпростір (cyberspace)* – комплексне віртуальне середовище (що не має фізичного втілення), сформований в результаті дій людей, програм і сервісів в мережі Інтернет за допомогою відповідних мережевих і комунікаційних технологій;

6) *рекламні програми (adware)* – програми, які нав’язують користувачам рекламу чи збирають інформацію про онлайн-поведінку користувачів;

7) *програма (application)* – IT-продукт, зокрема програмне забезпечення, відповідні відомості та процедури, метою яких є допомога користувачу у виконанні певних завдань чи в розв’язанні IT-задач за допомогою автоматизації бізнес-процесів чи функцій;

8) *постачальник послуг з підтримки програм (application service provider)* – оператор, який за допомогою програм, розміщених на хості, надає послуги з підтримки як вебпрограм, так і програм у схемі клієнт-сервер;

9) *послуги програм (application services)* – програмне забезпечення з відповідною функціональністю, що надається онлайн за вимогою абонентів і містить як веб-програми, так і програми в схемі клієнт-сервер;

10) *прикладне програмне забезпечення (application software)* – програмне забезпечення, створене, щоб допомагати користувачам виконувати певні завдання чи розв’язувати деякі типи задач на відміну від програмного забезпечення, яке контролює роботу комп’ютера;

11) *актив (asset)* – усе, що має значення для людини, організації чи уряду;

12) *аватар (avatar)* – представлення особи в кіберпросторі;

13) *атака (attack)* – спроба знищити, викрити, змінити, відключити, вкрасти чи отримати несанкціонований доступ до активу або несанкціоновано використати актив;

14) *потенціал атаки (attack potential)* – шанси атаки на успіх у разі її запуску; залежить від досвіду нападника, його технічних засобів та мотивації;

15) *вектор атаки (attack vector)* – спосіб чи засоби, якими зловмисник може отримати доступ до комп'ютера чи мережевого сервера з метою заподіяти певну шкоду;

16) *гібридна атака (blended attack)* – атака, яка застосовує різні методи для максимізації рівня заподіяної шкоди та збільшення швидкості ланцюгових реакцій;

17) *бот, робот (bot, robot)* – автоматизований програмний засіб для виконання певних завдань;

18) *ботнет (botnet)* – програмне забезпечення з дистанційним керуванням, зокрема, це може бути набір шкідливих ботів, які працюють в автономному/автоматичному режимі на зламаних/уражених комп'ютерах;

19) *кукі (cookie)* [контроль доступу] – можливість (capability) або запис/тикет (ticket) у системі контролю доступу;

20) *кукі (cookie)* [IPSec] – відомості, якими обмінюються протоколи ISAKMP (Internet Security Association and Key Management Protocol) для запобігання DoS-атакам під час установлення SA-параметрів (security association);

21) *кукі (cookie)* [HTTP] – обмін відомостями між HTTP-сервером і браузером для зберігання поточної інформації на стороні клієнта з подальшим використанням цих відомостей сервером;

22) *контроль, контрзаходи (control, countermeasure)* – засоби керування ризиками, зокрема політики, процедури, керівні принципи, практики чи організаційні структури, які можуть бути адміністративними, технічними, управлінськими або можуть мати юридичний характер;

23) *кіберзлочин (cybercrime)* – кримінальна діяльність, коли послуги чи програми кіберпростору застосовують зі злочинною метою або коли кіберпростір стає джерелом, засобом, метою чи місцем злочину;

24) *послуги програм кіберпростору (cyberspace application Services)* – послуги програм, які надають у кіберпросторі;

25) *кібер-скватер, кібер-загарбник (cyber-squatter)* – окремі особи чи організації, які реєструють й утримують адреси (URL), що нагадують посилання або назви інших організацій у реальному світі або в кіберпросторі;

26) *шахрайське програмне забезпечення (deceptive software)* – програмне забезпечення, яке працює на комп'ютері користувача без його відома, без інформування користувача про свою мету та без дозволу користувача;

27) *хакінг, злам (hacking)* – зловмисне одержання доступу до комп'ютерної системи без дозволу користувача чи власника;

28) *хактивізм (hactivism)* – хакінг із політичною чи соціальною метою;

29) *інформаційний ресурс/актив (information asset)* – знання чи відомості, що мають цінність для людини чи організації;

30) *інтернет (an internet, internetwork)* – сукупність взаємопов'язаних мереж;

31) *Інтернет (the internet)* – глобальна система взаємопов'язаних мереж відкритого доступу.

32) *Інтернет-злочин (Internet crime)* – злочинна діяльність, за якої послуги або програми в Інтернеті застосовують для скоєння злочину або є об'єктом злочину, або коли Інтернет є джерелом, інструментом, метою або місцем злочину;

33) *Інтернет-безпека, Інтернет-захищеність (Internet safety)* – стан захищеності від фізичного, соціального, духовного, фінансового, політичного, емоційного, професійного, психологічного, освітнього чи іншого типу наслідків несправностей, пошкоджень, помилок, нещасних випадків, збитків чи будь-яких інших подій в Інтернеті, які можна вважати небажаними;

34) *Інтернет-безпека, Інтернет-захист (Internet security)* – збереження конфіденційності, цілісності та доступності інформації в Інтернеті;

35) *послуги Інтернет, служби Інтернет (Internet services)* – послуги, що надають користувачеві, щоб забезпечити доступ до Інтернету через призначення IP-адреси; зазвичай містять автентифікацію, авторизацію та доменні служби імен;

36) *постачальник послуг Інтернет, постачальник Інтернет-послуг (Internet service provider)* – організація, яка надає Інтернет-послуги користувачам, а також надає своїм клієнтам доступ до Інтернету;

37) *шкідливі програми, шкідливе програмне забезпечення (malware, malicious software)* – програмне забезпечення, розроблене зловмисниками зі злочинними намірами та має функції, які потенційно можуть завдати прямої чи непрямої шкоди користувачу та/або його комп'ютерній системі;

38) *шкідливий контент (malicious contents)* – програми, документи, файли, відомості або інші ресурси, що мають шкідливі функції, які можуть бути приховані в них чи замасковані;

39) *організація (organization)* – група людей та об'єктів з розподілом відповідальностей, повноважень і взаємовідносин;

40) *фішинг (phishing)* – шахрайська спроба отримати особисту або конфіденційну інформацію маскуванням під надійного об'єкта в електронних комунікаціях;

41) *фізичний актив (physical asset)* – актив фізичної або матеріальної, природи;

42) *потенційно небажане програмне забезпечення (potentially unwanted software)* – шахрайське програмне забезпечення, охоплюючи як шкідливе, так і нешкідливе програмне забезпечення, якщо воно має риси шахрайського програмного забезпечення;

43) *шахрайство (scam)* – обманні або шахрайські дії;

44) *спам (spam)* – зловживання в системах електронних повідомлень для відправлення великої, кількості повідомлень;

45) *шпигунські програми (spyware)* – шахрайське програмне забезпечення, яке збирає особисту або конфіденційну інформацію з комп'ютерів користувачів;

46) *стейкхолдер, зацікавлена сторона (stakeholder)* [керування ризиками] – фізична особа чи організація, яка може впливати, підлягати впливу відповідних рішень та дій (чи сприймати себе таким);

47) *стейкхолдер, зацікавлена сторона (stakeholder)* [система] – фізична особа чи організація, яка має право, частку, вимоги або інтереси щодо системи або її властивостей, які відповідають їхнім потребам й очікуванням;

48) *загроза (threat)* – потенційна причина небажаного інциденту, який може завдати шкоди системі, фізичній особі чи організації;

49) *троян, троянський кінь (trojan, trojan horse)* – шкідлива програма, яка маскується під звичайну програму;

50) *небажана пошта (unsolicited email)* – небажані або непрошені повідомлення електронної пошти;

51) *віртуальний актив (virtual asset)* – представлення активу в кіберпросторі;

52) *віртуальна валюта (virtual currency)* – грошові віртуальні активи;

53) *віртуальний світ (virtual world)* – змодельоване середовище з доступом до нього багатьох користувачів через онлайн-інтерфейс;

54) *вразливість (vulnerability)* – слабка сторона активу або системи контролю, яка може бути використана в разі створення загрози;

55) *зомбі, зомбований комп'ютер, дрон (zombie, zombie computer, dron)* – комп'ютер, який містить приховане програмне забезпечення, яке дає змогу керувати машиною віддалено, а метою такого керування найчастіше є атака на інші комп'ютери.

ВСТУП

Однією із складових управління корпоративною безпекою є інформаційна безпека та, відповідно, її складова – кібербезпека.

Вивчаючи зміст управління корпоративною безпекою, необхідно знати основи побудови комплексу засобів захисту інформації та систем управління інформаційною безпекою, а також технології забезпечення кібербезпеки. Вміти будувати елементи комплексу засобів захисту інформації та обирати комплекс засобів захисту, будувати систему управління інформаційною безпекою та застосовувати основні технології забезпечення кіберезобезпеки. Звичайно, елементарними навичками, якими має володіти фахівець з кібербезпеки, який вивчає інформаційну безпеку (кібербезпеку) як складову управління корпоративною безпекою, є математичне моделювання, прогнозування, а також методи аналізу та синтезу.

У навчальному посібнику розглядаються питання управління корпоративною безпекою в цілому, а також основні вимоги, правила та рекомендації щодо кібербезпеки корпорації в кіберпросторі. Розглядаються основні засоби управління кібербезпекою корпорації: засоби управління програмного рівня, захист серверів корпорації, готовність кбербезпеки корпорації, архітектура обміну інформацією та координування.

Таким чином, автори ставили за мету висвітлення в навчальному посібнику наступних основних здатностей: вміння виявляти, ставити та вирішувати проблеми за напрямком кібербезпека; проводити дослідження на відповідному рівні; до пошуку, оброблення та аналізу інформації з різних джерел; до абстрактного мислення, аналізу та синтезу; оцінювати та забезпечувати якість виконуваних робіт.

Основний матеріал навчального посібника був розроблений при підготовці до читання навчальної дисципліни «Корпоративне управління інформаційною безпекою» в Київському національному університеті імені Тараса Шевченка на кафедрі кібербезпеки та захисту інформації факультету інформаційних технологій. Вона була розрахована на десять лекцій та складалась з двох взаємопов’язаних розділів:

Розділ 1. Основні вимоги, правила та рекомендації щодо кібербезпеки корпорації в кіберпросторі.

Розділ 2. Засоби управління кібербезпекою корпорації.

В основу навчального посібника покладено декілька джерел, основними з яких на думку авторів є чудова книга Марка Карбиса «Управління корпоративною безпекою. Проблеми, ризики та стратегії», видання 2015 року та імплементований в Україні лише в 2016 році міжнародний стандарт «ДСТУ ISO/IEC 27032 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки», інша література та інформаційні ресурси в галузі інформаційної безпеки (кібербезпеки). Це підтверджує

адекватність викладеного матеріалу, але не виключає власного погляду авторів на зміст цього навчального посібника.

Матеріал, викладений в навчальному посібнику, розрахований на широке коло фахівців, які цікавляться питаннями кібербезпеки та корпоративним управлінням інформаційною безпекою (кібербезпекою).

Цей навчальний посібник розроблявся з 2021 року. Матеріал проходив багаторазові етапи уточнення та актуалізації відповідно до змін у ландшафті кіберзагроз. При підготовці, редагуванні та узагальненні окремих частин тексту, а також при створенні контрольних тестів, питань для самоконтролю, авторами використовувалися можливості моделі штучного інтелекту Gemini Pro.

Окремо, хотів подякувати студентам-магістрам 2021 року випуску, які витримали труднощі наведеного матеріалу та певними зусиллями внесли свій внесок, що надихнуло до написання даного навчального посібника.

Наступним етапом розвитку навчального посібника стало розширення авторського колективу. До роботи доєдналися:

Сергій Толюпа – доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації;

Іван Пархоменко – завідувач кафедри кібербезпеки та захисту інформації, кандидат технічних наук, доцент.

Їхній багаторічний практичний досвід і наукові напрацювання дозволили суттєво доповнити зміст посібника, поглибити аналіз актуальних проблем галузі та забезпечити відповідність матеріалу сучасним вимогам підготовки фахівців зі спеціальності F5 «Кібербезпека та захист інформації».

Окрема подяка адресована рецензентам даного навчального посібника, які зробили багато корисних зауважень у попередньому його варіанті.

Сергій Бучик
Київ
2026

Навчальне видання

С. С. БУЧИК, С. В. ТОЛЮПА, І. І. ПАРХОМЕНКО

КОРПОРАТИВНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Навчальний посібник

Формат 70x100/16. Папір офсетний. Друк цифровий.
Гарнітура Times New Roman.
Умовн. друк. арк. 17,55.
Видавництво ПП «Магнолія 2006»
м. Львів, 79053, Україна, Перфецького 11 А, тел.+380503701957
e-mail: magnol06@ukr.net
https://magnolia.lviv.ua
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції: серія ДК № 2534 від 21.06.2006 року,
видане Державним комітетом інформаційної політики,
телебачення та радіомовлення України.

Надруковано у друкарні видавця ФОП Марченко Т. В