

**Державний торговельно-економічний  
університет**

**В. І. Пашорін, Ю. В. Костюк**

**БЕЗПЕКА ІНФОРМАЦІЙНИХ  
СИСТЕМ**

*Навчальний посібник*

2-ге видання, виправлене і доповнене

Видавець ФОП Марченко Т.В.  
Львів

УДК 004.056

П 22

Автори: В. І. Пашорін, канд. техн. наук, проф.,  
Ю. В. Костюк, старш. викл.

Рецензенти: Н. В. Лукова-Чуйко, канд. фіз.-мат. наук, д-р техн. наук,  
доцент Київського національного університета ім. Тараса  
Шевченка, завідувач кафедри кібербезпеки та захисту  
інформації;  
В. А. Лахно, д-р техн. наук, професор Національного  
університету біоресурсів і природокористування України,  
завідувач кафедри комп'ютерних систем і мереж;  
В. П. Зверев, канд. техн. наук, ст. наук. співроб., професор  
кафедри інженерії програмного забезпечення та кібербезпеки,  
заступник керівника служби з питань інформаційної безпеки  
та кібербезпеки, керівник управління інформаційної безпеки  
Апарату РНБО України;  
М. В. Сашньова, канд. техн. наук, доцент кафедри інженерії  
програмного забезпечення та кібербезпеки Державного  
торговельно-економічного університету

*Рекомендовано до друку вченою радою  
Державного торговельно-економічного університету  
(протокол № 3 від 30 вересня 2021 р.)*

**Пашорін В. І.**

П 22 **Безпека інформаційних систем** : навч. посіб. / В. І. Пашорін,  
Ю. В. Костюк. – 2-ге видання, виправлене і доповнене – Львів:  
Видавець ФОП Марченко Т.В. – 376 с.

ISBN 978-617-8194-08-6

У навчальному посібнику розглянуто сучасні напрями забезпечення безпеки інформаційно-телекомунікаційних систем. Викладено технічні, криптографічні, програмні методи і засоби захисту інформації. Формулюються проблеми вразливості сучасних інформаційно-телекомунікаційних систем, розглядаються питання захисту інформації в розподілених інформаційних системах, організаційно-правове забезпечення захисту інформації. Розглянуті загальні питання технологій збереження даних в єдиному інформаційному просторі та впровадженню функцій протидії кіберзлочинності, здатності організувати та підтримувати комплекс заходів щодо забезпечення безпеки інформаційної та кібербезпеки, з урахуванням їхньої юридичної та економічної обґрунтованості, технічної реалізації, запобігання можливих зовнішніх впливів, імовірних загроз, а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, застосування технологій захисту інформаційно-телекомунікаційних систем.

Призначено для студентів галузі знань 12 «Інформаційні технології», аспірантів, що вивчають методи захисту інформації та безпеки інформаційних систем.

**УДК 004.056**

ISBN 978-617-8194-08-6

Пашорін В. І., Костюк Ю. В.  
Видавець ФОП Марченко Т.В.

# **ЗМІСТ**

<b>ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ</b> .....	8
<b>ВСТУП</b> .....	9
<b>Розділ 1. КІБЕРПРОСТІР ТА КІБЕРБЕЗПЕКА: КЛЮЧОВІ ПИТАННЯ ТА ВИЗНАЧЕННЯ</b> .....	11
ГЛАВА 1. Безпека інформаційних систем в умовах функціонування глобальних мереж .....	11
1.1. Актуальність безпеки інформаційно- телекомунікаційних систем (ІТС) .....	12
1.2. Класифікація та властивості інформації .....	19
1.3. Основні терміни і визначення безпеки ІТС .....	24
ГЛАВА 2. Кібербезпека – складова частина безпеки ІТС.....	27
2.1. Кіберпростір і кібербезпека .....	27
2.2. Ключові питання кібербезпеки.....	34
2.3. Кіберзброя, кібертероризм і кібервійни .....	38
Контрольні запитання .....	42
<b>Розділ 2. ВРАЗЛИВОСТІ ТА ЗАГРОЗИ ФУНКЦІОНУВАННЯ ІТС</b> .....	43
ГЛАВА 3. Загрози інформації в ІТС.....	43
3.1. Загрози безпеки функціонування ІТС .....	43
3.2. Вразливості та вади захисту системи .....	48
3.3. Класифікація загроз безпеки .....	52
3.4. Основні навмисні загрози .....	60
ГЛАВА 4. Мережеві загрози .....	64
4.1. Сучасні мережеві загрози: інтернет- шахрайство .....	64
4.2. Сучасні мережеві загрози: крадіжка особистості .....	75
4.3. Загрози приватності при роботі в відкритих мережах.....	79
4.4. Соціальна інженерія .....	83
Контрольні запитання .....	91

<b>Розділ 3. АТАКИ НА ІТС. ПОРУШНИКИ КІБЕРБЕЗПЕКИ</b> .....	92
ГЛАВА 5. Атаки на інформаційні системи .....	92
5.1. Визначення атаки на ІТС .....	92
5.2. Фази атаки. Ланцюг кібервбивства.....	94
5.3. АРТ-атака .....	102
ГЛАВА 6. Класифікація та приклади атак на ІТС .....	106
6.1. Таксономія та приклади кібератак.....	106
6.2. Мережеві атаки. Застосування бот-мереж .....	114
6.3. Сучасні типові атаки на ІТС.....	123
ГЛАВА 7. Порухники безпеки.....	130
7.1. Порухники безпеки ІТС .....	130
7.2. Хакінг та етичний хакінг .....	138
Контрольні запитання .....	146
<b>Розділ 4. ТЕОРІЯ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ІТС</b> .....	147
ГЛАВА 8. Технології та методи захисту ІТС .....	147
8.1. Сучасні технології захисту інформаційних ресурсів.....	147
8.2. Основні методи забезпечення безпеки ІТС .....	150
8.3. Комплексне обстеження ІТС (аудит безпеки ІТС) .....	154
ГЛАВА 9. Теоретичні аспекти захисту ІТС.....	157
9.1. Моделі безпеки ІТС .....	157
9.2. Особливості сучасних ІТС, з точки зору безпеки.....	161
9.3. Принципи побудови систем безпеки.....	163
9.4. Архітектурна безпека.....	166
Контрольні запитання .....	169
<b>Розділ 5. ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ЗАХИСТ ВІД РУЙНУЮЧИХ ПРОГРАМНИХ ДІЙ</b> .....	170
ГЛАВА 10. Комп'ютерні віруси: класифікація та характеристика .....	170
10.1. Поняття та класифікація шкідливого програмного забезпечення.....	170

## **ЗМІСТ**

---

---

10.2. Поняття та класифікація комп'ютерних вірусів .....	176
10.3. Коротка характеристика вірусів .....	181
<b>ГЛАВА 11. Шкідливе програмне забезпечення .....</b>	<b>185</b>
11.1. Мережеві хробаки .....	185
11.2. Троянські програми .....	191
11.3. Спеціальні шкідливі програми .....	197
<b>ГЛАВА 12. Захист від шкідливого програмного забезпечення.....</b>	<b>208</b>
12.1. Методи виявлення шкідливих програм .....	208
12.2. Типи і характеристики антивірусних програм.....	211
12.3. Технологія Whitelisting і антивірусні хмари .....	218
Контрольні запитання .....	221
<b>Розділ 6. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІТС .....</b>	<b>222</b>
<b>ГЛАВА 13. Закони, нормативні документи і стандарти.....</b>	<b>222</b>
13.1. Законодавство України по забезпеченню кібербезпеки.....	222
13.2. Нормативні документи системи технічного захисту інформації .....	225
13.3. Стандарти інформаційної безпеки. Стандарт TCSEC.....	228
13.4. Поняття кіберзлочинності. Класифікація кіберзлочинів .....	232
<b>ГЛАВА 14. Міжнародні стандарти.....</b>	<b>237</b>
14.1. Класи безпеки комп'ютерних систем.....	237
14.2. Міжнародні стандарти серії ISO 27000.....	240
Контрольні запитання .....	247

<b>Розділ 7. АДМІНІСТРАТИВНЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІТС</b>	<b>.....248</b>
ГЛАВА 15. Політика безпеки.....	248
15.1. Організаційний захист.....	248
15.2. Склад і структура політики безпеки .....	253
15.3. Зразок спеціалізованої політики безпеки допустимого використання.....	258
ГЛАВА 16. Процедури політики безпеки .....	261
16.1. Процедури реалізації політики безпеки .....	261
16.2. Оновлення ПЗ та зниження привілеїв.....	269
ГЛАВА 17. Управління ризиками .....	275
17.1. Ризики безпеки ІТС .....	275
17.2. Типові витрати на забезпечення безпеки ІТС.....	281
Контрольні запитання .....	287
<b>Розділ 8. ІНЖЕНЕРНО-ТЕХНІЧНИЙ ЗАХИСТ ІТС</b>	<b>.....288</b>
ГЛАВА 18. Технічні канали витоку інформації.....	288
18.1. Загальна характеристика інженерно-технічних засобів безпеки.....	288
18.2. Фізичний захист .....	290
18.3. Технічні канали витоку інформації.....	293
ГЛАВА 19. Економічна розвідка і принципи захисту від неї .....	305
19.1. Технічні засоби економічної розвідки.....	305
19.2. Принципи захисту від економічної розвідки .....	312
Контрольні запитання .....	317
<b>Розділ 9. ПРОГРАМНО-АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІТС</b>	<b>.....318</b>
ГЛАВА 20. Ідентифікація і автентифікація .....	318
20.1. Загальна характеристика програмних засобів безпеки ІТС .....	318
20.2. Ідентифікація, автентифікація та авторизація в ІТС .....	321

## **ЗМІСТ**

---

---

20.3. Види автентифікації суб'єктів в ІТС .....	325
20.4. Парольна автентифікація .....	327
20.5. Автентифікація на основі PIN-коду .....	330
<b>ГЛАВА 21. Види автентифікації.....</b>	<b>332</b>
21.1. Апаратна автентифікація .....	332
21.2. Автентифікація за допомогою біометричних даних .....	340
21.3. Автентифікація на основі цифрових сертифікатів .....	346
21.4. Централізовані системи автентифікації. Концепція єдиного логічного входу.....	348
Контрольні запитання .....	353
<b>Розділ 10. УПРАВЛІННЯ ДОСТУПОМ І АУДИТ ІТС ....</b>	<b>355</b>
<b>ГЛАВА 22. Управління доступом .....</b>	<b>355</b>
22.1. Поняття і технології управління доступом ....	355
22.2. Дискреційна модель розмежування доступу.....	358
22.3. Мандатна модель розмежування доступу .....	361
<b>ГЛАВА 23. Управління доступом і реєстрація подій в системі .....</b>	<b>364</b>
23.1. Рольова модель розмежування доступу .....	364
23.2. Реєстрація подій і аудит .....	367
Контрольні запитання .....	371
<b>СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ.....</b>	<b>372</b>

## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ**

<b>ІС</b>	– Інформаційна система
<b>ІТ</b>	– Інформаційні технології
<b>ІТС</b>	– Інформаційно-телекомунікаційна система
<b>ЦОД</b>	– Центр обробки даних
<b>ПЗ</b>	– Програмне забезпечення
<b>ІоТ</b>	– Інтернет речей
<b>ІоЕ</b>	– Інтернет всього
<b>НСД</b>	– Несанкціонований доступ
<b>КЦД</b>	– Конфіденційність, цілісність, доступність
<b>КСЗІ</b>	– Комплексна система захисту інформації
<b>ПБ</b>	– Політика безпеки
<b>ІБ</b>	– Інформаційна безпека
<b>ЕМВ</b>	– Електромагнітне випромінювання
<b>ПЕМВ</b>	– Побічне електромагнітне випромінювання
<b>ТЗР</b>	– Технічні засоби розвідки побічних
<b>ПЕМВН</b>	електромагнітних випромінювань і наведень
<b>ОС</b>	– Операційна система
<b>ЕОМ</b>	– Електронна обчислювальна машина
<b>ПК</b>	– Персональний комп'ютер
<b>LAN</b>	– Локальна комп'ютерна мережа
<b>WAN</b>	– Глобальна мережа
<b>UNIX</b>	– Сімейство операційних систем
<b>HTTP</b>	– Протокол передачі гіпертексту та інших типів даних
<b>MAC</b>	– Унікальний ідентифікатор обладнання для комп'ютерних мереж

# ВСТУП

Навчальний посібник містить основи теорії з дисципліни «Безпека інформаційних систем» для студентів галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека» спеціалізація «Безпека інформаційних та комунікаційних систем в економіці» та програмі дисципліни «Безпека інформаційних систем» денного, заочного та дистанційного навчання. Представлений матеріал відповідає вимогам робочої програми навчальної дисципліни «Безпека інформаційних систем» та навчальним планам і дозволяє охопити основні розділи даної дисципліни. Для кожної з частин визначені короткі теоретичні положення та контрольні запитання, що дозволяють оцінити знання студентів по кожному розділу дисципліни, що вивчається.

Посібник передбачає вивчення: законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделей та принципів управління доступом до інформаційних ресурсів; теорії систем управління інформаційною та/або кібербезпекою; методів і засобів виявлення, управління та ідентифікації ризиків; методів і засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів і засобів технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проектування.

Корисний для студентів інших спеціальностей: «Комп'ютерна інженерія», «Інженерія програмного забезпечення», «Системний аналіз», а також аспірантів і здобувачів наукового ступеня кандидата технічних наук, які вивчають методи захисту інформації, заснованих на науково обґрунтованому аналізі ситуації та доступі до систем збору, зберігання й обробки інформації.

Метою посібника є надання необхідних теоретичних основ для засвоєння курсу майбутніми фахівцями з управління інформаційною безпекою та кібербезпеки й закріплення необхідних у подальшій роботі знань з основ інформаційної безпеки та отримати фахову компетентність щодо здатності відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів і походження, а також здатність впроваджувати та забезпечувати функціонування комплексних систем захисту (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів). Матеріал дисципліни пов'язаний зі спеціальними дисциплінами, що викладаються у закладах вищої освіти технічного профілю.

Забезпечення і підтримка інформаційної та кібербезпеки включають комплекс різнопланових заходів, що запобігають, відстежують і усувають несанкціонований доступ третіх осіб. Заходи інформаційної безпеки спрямовані також на захист від пошкоджень, спотворень, блокування або копіювання інформації. Принципово, щоб усі завдання вирішувалися одночасно – тільки тоді забезпечується повноцінний, надійний захист.

Для того, щоб національна безпека України могла відповідати рівню провідних економічних держав, необхідні як послідовні дії з боку держави, спрямовані на підвищення ефективності й розвиток системи взаємодії учасників ІКТ-галузі та забезпечення безпеки критично важливих об'єктів інформаційної та кіберінфраструктур, так і приділення підприємствами та організаціями нашої держави більшої уваги до питань власної інформаційної та кібербезпеки. Зважаючи на цей безперервний розвиток та постійну інформаційну боротьбу, що складає один з важливих елементів сучасної світової політики, для забезпечення своєї незалежності Україні необхідно і далі удосконалювати та розвивати як правові засади (в тому числі й міжнародні), так і структурну й технічну складову кібербезпеки.

*Навчальне видання*

ПАШОРІН Валерій Іванович,  
КОСТЮК Юлія Володимирівна

## **БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ**

*Навчальний посібник*

2-ге видання, виправлене і доповнене

Формат 60x84/16. Папір офсетний. Друк цифровий.  
Гарнітура Times New Roman. Умовн. друк. арк. 19,42.

Видавець Марченко Т. В.  
м. Львів-53, 79053, Україна, тел.: +38 (050) 370-19-57  
e-mail: [magnol06@ukr.net](mailto:magnol06@ukr.net)  
<https://magnolia.lviv.ua>

Свідоцтво про внесення суб'єкта видавничої справи  
до Державного реєстру видавців, виготівників і  
розповсюджувачів видавничої продукції:  
серія ДК № 6784 від 30.05.2019 року,  
видане Державним комітетом інформаційної політики,  
телебачення та радіомовлення України.

Надруковано у друкарні видавця Марченко Т. В.