

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
“ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМ. ЮРІЯ КОНДРАТЮКА”

КАФЕДРА КОМП’ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ

Є.О. ЖИВИЛО

КОРПОРАТИВНА БЕЗПЕКА



НАВЧАЛЬНИЙ ПОСІБНИК

ПОЛТАВА – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
“ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМ. ЮРІЯ КОНДРАТЮКА”

КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ

Є.О. ЖИВИЛО

КОРПОРАТИВНА БЕЗПЕКА

НАВЧАЛЬНИЙ ПОСІБНИК

2025

УДК 004.056.53

ББК 32.988-5

Рецензенти:

О.В. Шефер, доктор технічних наук, професор, начальник кафедри Навчально-наукового інституту інформаційних технологій та робототехніки Національного університету “Полтавська політехніка ім. Юрія Кондратюка”;

В.В. Васюга, кандидат технічних наук, доцент, доцент кафедри комп’ютерних та інформаційних технологій і систем Навчально-наукового інституту інформаційних технологій та робототехніки Національного університету “Полтавська політехніка ім. Юрія Кондратюка”.

Корпоративна безпека: навч. посіб. / [Є.О. Живило]. – П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2025. – 156 с.

Навчальний посібник охоплює програмний матеріал підготовки студентів 12 Галузі знань «Інформаційні технології» за спеціальностями 122 - Комп’ютерні науки, 123 - Комп’ютерна інженерія та 125 - Кібербезпека та захист інформації. Навчальне видання укладено за матеріалами лекцій, групових та практичних занять з дисципліни “Корпоративна безпека”, а також з дисциплін “Кібер-безпека”, “Захист інформації”, “Захист інформації в інфокомунікаційних системах”, “Основи інформаційної та кібернетичної безпеки”, “Теорія інформаційної боротьби”. Посібник призначений для студентів, що навчаються за спеціальностями 12 Галузі знань «Інформаційні технології», а також для самостійної оцінки та тестування безпеки організаційних систем з метою виявлення вразливостей.

Розроблений мануал присвячений вивченню основ кібербезпеки та практичних навичок, які допоможуть краще зрозуміти, як захищати інформаційні системи та, водночас, виявляти вразливості в мережах і системах. Кожен розділ охоплює важливі аспекти цієї теми, починаючи з

основ і завершуючи складнішими питаннями, такими як тестування на проникнення і хакінг.

Зазначені розділи покривають ключові аспекти кібербезпеки та дають можливість навчитися працювати з інструментами, які використовуються фахівцями з безпеки для виявлення та усунення загроз.

Рекомендовано до друку науково-методичною радою Національного університету “Полтавська політехніка імені Юрія Кондратюка”

Протокол № 3 від 20 лютого 2025 р.

© Автори вказані на звороті титульного аркуша, 2025
© НУ “Полтавська політехніка ім. Юрія Кондратюка”,
2025

ЗМІСТ

	ПЕРЕЛІК СКОРОЧЕНЬ	8
	ВСТУП	9
РОЗДІЛ 1	ВСТУП ДО КОРПОРАТИВНОЇ БЕЗПЕКИ	10
	1.1. Визначення корпоративної безпеки.	10
	1.2. Основні загрози та ризики в корпоративному середовищі.	11
	1.3. Роль корпоративної безпеки в бізнес-процесах.	14
	1.4. Важливість конфіденційності та захисту даних.	16
РОЗДІЛ 2	ОГЛЯД ПОЛІТИК ТА СТАНДАРТІВ КОРПОРАТИВНОЇ БЕЗПЕКИ	19
	2.1. Огляд стандартів та політик безпеки (ISO/IEC 27001, NIST)	19
	2.2. Визначення політик безпеки в організації	21
	2.3. Нормативні акти та закони щодо захисту інформації.	24
РОЗДІЛ 3	АРХІТЕКТУРА БЕЗПЕКИ В КОРПОРАТИВНИХ СИСТЕМАХ	27
	3.1. Види архітектур безпеки: периметральна, багатоетапна, гнучка	27
	3.2. Роль мережевої безпеки	30
	3.3. Безпека хмарних технологій у корпоративному середовищі.	32
РОЗДІЛ 4	ОСНОВИ УПРАВЛІННЯ РИЗИКАМИ В КОРПОРАТИВНІЙ БЕЗПЕЦІ	35
	4.1. Визначення, оцінка та управління ризиками	35
	4.2. Методи зменшення та адаптації до ризиків.	37
	4.3. Впровадження контрзаходів для мінімізації ризиків	40
РОЗДІЛ 5	ЗАХИСТ ДАНИХ ТА УПРАВЛІННЯ ДОСТУПОМ	44
	5.1. Методи захисту даних	44
	5.2. Стратегії управління доступом	46
	5.3. Важливість аутентифікації та авторизації	49
РОЗДІЛ 6	ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРЗАХИСТ	52
	6.1. Захист від кіберзагроз (атаки, віруси, шкідливе ПЗ).	52
	6.2. Використання міжмережевих екранів, антивірусних систем та систем виявлення загроз.	54
	6.3. Роль моніторингу та реагування на інциденти безпеки.	57
РОЗДІЛ 7	ПРИВАТНІСТЬ ТА КОНФІДЕНЦІЙНІСТЬ ДАНИХ	61
	7.1. Визначення конфіденційності та приватності даних.	61
	7.2. Політики та регуляції (GDPR, CCPA, NIST Privacy Framework).	63
	7.3. Методи анонімізації та псевдонімізації даних.	66

РОЗДІЛ 8	ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ В КОРПОРАТИВНИХ СИСТЕМАХ	69
	8.1. Методи ідентифікації користувачів.	69
	8.2. Технології аутентифікації: паролі, двофакторна аутентифікація, біометрія	70
	8.3. Безпека аутентифікації в корпоративних мережах.	73
РОЗДІЛ 9	БЕЗПЕКА КОМУНІКАЦІЙ ТА ПЕРЕДАЧІ ДАНИХ	78
	9.1. Захист каналів зв'язку (VPN, SSL/TLS, шифрування).	78
	9.2. Проблеми безпеки при обміні даними	80
	9.3. Виявлення та запобігання витокам даних	82
РОЗДІЛ 10	СИСТЕМИ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ	87
	10.1 Створення систем моніторингу.	87
	10.2 Процес виявлення, аналізу та реагування на інциденти.	88
	10.3 Поглиблений аналіз інцидентів та зворотній зв'язок.	90
РОЗДІЛ 11	БЕЗПЕКА КОРПОРАТИВНОЇ МЕРЕЖІ ТА ІНФРАСТРУКТУРИ	97
	11.1 Захист мережевої інфраструктури та важливих сервісів.	97
	11.2 Безпека протоколів і мережевих додатків	99
	11.3 Захист хмарних і віртуалізованих середовищ.	101
РОЗДІЛ 12	СТРАТЕГІЇ ВПРОВАДЖЕННЯ КОРПОРАТИВНОЇ БЕЗПЕКИ	106
	12.1 Визначення стратегій корпоративної безпеки.	106
	12.2 Важливість розвитку культури безпеки в організації.	108
	12.3 Впровадження безпекових політик в компанії.	110
РОЗДІЛ 13	ПЛАНУВАННЯ ТА ВІДНОВЛЕННЯ ПІСЛЯ ІНЦИДЕНТІВ БЕЗПЕКИ	113
	13.1 Розробка планів реагування на інциденти	113
	13.2 Відновлення після атак та інцидентів	130
	13.3 Технічні і організаційні заходи для зниження впливу інцидентів.	132
РОЗДІЛ 14	АУДИТ ТА ОЦІНКА СИСТЕМ КОРПОРАТИВНОЇ БЕЗПЕКИ	136
	14.1 Порядок аудиту корпоративної безпеки	136
	14.2 Оцінка ефективності систем безпеки.	141
	14.3 Техніки оцінки вразливостей та тестування безпеки	143
РОЗДІЛ 15	ЗАХИСТ ВІД ВНУТРІШНІХ ЗАГРОЗ ТА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ	146
	15.1 Ризики, пов'язані з внутрішніми загрозами	146
	15.2 Протидія соціальної інженерії.	148
	15.3 Важливість навчання персоналу та розробка політик безпеки	151
	Перелік використаних джерел	154