Міністерство освіти і науки України
Запорізький національний університет

Р. В. Бараннік

КІБЕРБЕЗПЕКА
І УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ

Навчальний посібник
для здобувачів ступеня вищої освіти бакалавра
спеціальностей «Право» і «Правоохоронна діяльність»
освітньо-професійних програм «Право» і «Правоохоронна діяльність»

ЮРІНКОМ ІНТЕР
Київ–2025

УДК 004.056.5(075.8)
Б24

Рецензент

Р. Корольков, кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки та наноелектроніки НУ «Запорізька політехніка»

Бараннік Р. В.

Б24 Кібербезпека і управління інформаційними ресурсами : навч. посіб. Київ : Юрінком Інтер, 2025. 236 с.

ISBN 978-966-667-894-5

Навчальний посібник «Кібербезпека і управління інформаційними ресурсами» охоплює ключові аспекти забезпечення інформаційної безпеки в умовах цифрової трансформації. Розглядаються основи кібербезпеки, нормативно-правове регулювання цієї сфери, сучасні кіберзагрози та методи їх нейтралізації. Особлива увага приділяється управлінню інформаційними ресурсами, зокрема аналізу ризиків, впровадженню політик безпеки, захисту персональних даних та організації кіберзахисту в установах, на підприємствах та в організаціях.

Для закріплення здобутих знань запропоновано тестові завдання та питання для самостійної перевірки різного рівня складності, а для формування необхідних практичних навичок посібник містить практичні завдання до кожної теми. Тлумачення основних термінів, понять і абревіатур міститься у глосарії.

Посібник орієнтований на студентів та викладачів, а також може бути корисний тим, хто прагне підвищити свою обізнаність у сфері кібербезпеки та ефективного управління інформаційними ресурсами.

УДК 004.056.5(075.8)

Видавництво «Юрінком Інтер» прагне сталого майбутнього для нашого бізнесу, наших читачів і нашої планети. Ця книга виготовлена з паперу, сертифікованого FSC® та PEFC™

ISBN 978-966-667-894-5

ЗМІСТ

Тема 4. Захист даних

Тема 5. Відновлення після інцидентів кібербезпеки

Тема 6. Сучасні тенденції в кібербезпеці

ВСТУП

Сучасний інформаційний простір характеризується динамічним розвитком цифрових технологій та зростанням ролі інформації як стратегічного ресурсу суспільства. У цих умовах питання забезпечення кібербезпеки та ефективного управління інформаційними ресурсами набувають особливого значення, зокрема для майбутніх фахівців, здатних впроваджувати, розвивати та захищати сучасні інформаційні ресурси.

Навчальна дисципліна «Кібербезпека і управління інформаційними ресурсами» посідає важливе місце у структурно-логічній схемі підготовки здобувачів освіти, забезпечуючи інтеграцію знань із технічних, правових, управлінських та інформаційних напрямків. Цей курс сприяє формуванню фундаментальних компетентностей у галузі кіберзахисту, аналізу інформаційних ризиків, управління інформаційними потоками та ресурсами, а також забезпеченню стійкого функціонування інформаційних систем у сучасних умовах.

Розвиток цифрового суспільства супроводжується не лише безпрецедентними можливостями, але й суттєвими загрозами, такими як кібератаки, інформаційні витоки, порушення конфіденційності даних. У цьому контексті дана дисципліна є ключовою для формування у здобувачів освіти не лише базових знань про інформаційні ресурси та їх захист, але й здатності приймати ефективні управлінські рішення у сфері кібербезпеки, враховуючи нормативно-правові, етичні та технічні аспекти.

Мета дисципліни — сформувати у здобувачів освіти знання, вміння та компетентності, необхідні для забезпечення захисту інформаційних ресурсів, аналізу кіберзагроз, управління інформаційною безпекою організацій та побудови ефективних систем захисту.

Основні завдання, які досягаються вивченням даної дисципліни, це сформувати у здобувачів необхідні компетенції для роботи в сучасному цифровому світі:

– *Навчити захищати особисті дані та інформацію.* В умовах цифровізації велика кількість персональної інформації зберігається та обробляється у мережі. Знання принципів кібербезпеки допомагає студентам захищати власні дані від:

хакерських атак; фішингу; витоків конфіденційної інформації. Розуміння правових аспектів захисту інформації (наприклад, законодавства про захист персональних даних) дозволяє уникати порушень та зловживань.

– *Засвоїти основи безпеки професійної діяльності.* Більшість сучасних професій вимагає роботи з інформаційними ресурсами. Знання основ кібербезпеки дозволяє: ефективно працювати з корпоративними системами; розпізнавати потенційні загрози, пов'язані з цифровими атаками; зменшувати ризики втрати даних через дії третіх осіб чи внутрішні помилки.

– *Навчитися вправно управляти інформаційними ресурсами.* Знання принципів управління інформаційними ресурсами допомагає здобувачам: оптимізувати зберігання та використання даних; організовувати безпечний доступ до інформації; розробляти стратегії ефективного використання ресурсів у бізнесі чи інших організаціях.

– *Ознайомити з різноманіттям сучасних технологій.* Дисципліна знайомить студентів із основами сучасних технологій: мережевої безпеки; шифрування даних; роботи з хмарними сервісами; використання антивірусного та іншого програмного забезпечення для захисту систем. Розуміння цих технологій є ключовим для адаптації до швидких змін у сфері інформаційних технологій.

– *Провести тренування з попередження кіберзагроз.* Здобувачі дізнаються про види кіберзагроз: віруси, троянські програми, програми-вимагачі; атаки «відмова у наданні послуги» (DoS/DDoS); соціальна інженерія. Це допомагає їм попереджати такі ризики не лише у професійному середовищі, а й у повсякденному житті.

– *Вивчити етичний та правовий аспекти.* Вивчення правових норм та етичних принципів роботи з інформацією — дотримання авторського права; боротьба з цифровим піратством; відповідальність за розповсюдження шкідливих програм чи конфіденційної інформації — все це допомагає студентам

уникати конфліктів із законом та розвивати відповідальність у роботі з цифровими ресурсами.

– *Підготуватися до цифрових викликів майбутнього.* Глобалізація та стрімкий розвиток технологій роблять кібербезпеку однією з ключових компетенцій у багатьох сферах: від права й бізнесу до медицини й освіти. Розуміння основ кібербезпеки дає конкурентну перевагу на ринку праці, адже фахівці, які знають, як управляти інформаційними ресурсами та захищати їх, високо цінуються.

Отже, навчальний посібник «Кібербезпека і управління інформаційними ресурсами» спрямований на формування у студентів системних знань, практичних навичок та компетенцій у сфері кібербезпеки, захисту інформаційних систем і ефективного управління даними. У даному навчальному посібнику розкриті основні теми та питання, що стосуються сучасних технологій, таких як штучний інтелект, блокчейн, інтернет речей і квантові обчислення, що спрямовані на протидію кіберзагрозам. Навчальний посібник надає структурований виклад теоретичних основ, сучасних методів захисту інформації та підходів до управління інформаційними активами, а також допомагає:

- ✓ Опанувати основні поняття та принципи кібербезпеки.
- ✓ Засвоїти правові та організаційні аспекти забезпечення інформаційної безпеки.
- ✓ Ознайомитися з методами захисту інформації від загроз.
- ✓ Вивчити сучасні підходи до управління інформаційними ресурсами.
- ✓ Отримати практичні навички аналізу та оцінювання кіберзагроз.

Кожна тема супроводжується тестовими завданнями, питаннями для самоконтролю, а також практичними завданнями, що сприяє поглибленню знань та формуванню аналітичного мислення.

Тема 1

ОСНОВИ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Метою вивчення даної теми є формування у студентів фундаментальних знань про основні поняття, принципи та концепції кібербезпеки та інформаційної безпеки. Студенти повинні засвоїти ключові загрози інформаційним системам, методи їх захисту, а також роль нормативно-правового регулювання у сфері кіберзахисту. У результаті вивчення теми студенти зможуть: розуміти основні поняття кібербезпеки та інформаційної безпеки; визначати загрози та вразливості інформаційних систем; оцінювати ризики, пов'язані з інформаційною безпекою; ознайомитися з основними методами та засобами захисту інформації; усвідомити важливість правового регулювання у сфері кібербезпеки. Ця тема є базовою для подальшого вивчення більш складних аспектів кібербезпеки та управління інформаційними ресурсами.

План

1.1. Поняття кібербезпеки та інформаційної безпеки.
1.2. Історія розвитку кібербезпеки.
1.3. Класифікація загроз та актуальні загрози кібербезпеки.
1.4. Методи протидії загрозам кібербезпеки.
1.5. Законодавство в галузі кібербезпеки.

1.1. Поняття кібербезпеки та інформаційної безпеки

У сучасному світі інформаційні технології займають центральне місце в усіх сферах життя. Водночас зростає кількість загроз для інформаційних систем, що пов'язані з кібератаками, витоками даних та іншими порушеннями безпеки. Кібербезпека та інформаційна безпека — це ключові поняття для забезпечення захисту даних і систем. Ці два поняття тісно пов'язані між собою і часто використовуються як синоніми. Однак, між ними є певні відмінності, що важливо враховувати при розробці політик та заходів захисту.

Інформаційна безпека охоплює захист всієї інформації, що обробляється або зберігається на різноманітних носіях — як у цифровому, так і в фізичному вигляді.

Основними принципами інформаційної безпеки є:

- ✓ *Конфіденційність* — забезпечення того, щоб інформація була доступна лише тим, хто має право на її отримання.
- ✓ *Доступність* — забезпечення того, щоб інформація була доступна користувачам у разі потреби.
- ✓ *Цілісність* — захист інформації від несанкціонованих змін.

Основні характеристики інформаційної безпеки:

- ➢ *Широке поняття.* Охоплює всі аспекти захисту інформації, включаючи як цифрову, так і фізичну.
- ➢ *Цілі:* Збереження конфіденційності, цілісності та доступності інформації.
- ➢ *Засоби захисту:* Можуть включати як технічні засоби (шифрування, системи контролю доступу), так і організаційні заходи (політики безпеки, навчання персоналу).
- ➢ *Сфера застосування:* Всі сфери діяльності, де використовується інформація.