Міністерство освіти і науки України
Запорізький національний університет

Р. В. Бараннік

КІБЕРБЕЗПЕКА І УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ

Затверджено вченою радою ЗНУ
Протокол № 10 від “29” квітень 2025р.

Запоріжжя
2025

УДК 004.056.5(075.8)
Б241

Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ: Юрінком Інтер, 2025. 236 с.

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.

Рецензент *Р. Корольков,* кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки та наноелектроніки НУ “Запорізька політехніка”

Відповідальний за випуск
Р.В. Бараннік, кандидат юридичних наук, доцент, завідувач кафедри кримінального права та правоохоронної діяльності

ЗМІСТ

ВСТУП.....5

Тема 1. Основи кібербезпеки та інформаційної безпеки
1.1. Поняття кібербезпеки та інформаційної безпеки.....8
1.2. Історія розвитку кібербезпеки.....10
1.3. Класифікація загроз та актуальні загрози кібербезпеки.....14
1.4. Методи протидії загрозам кібербезпеки.....17
1.5. Законодавство в галузі кібербезпеки.....22
Тести та питання для самоконтролю.....23
Практичні завдання.....25

Тема 2. Захист інформаційних систем
2.1. Архітектура захисту інформаційних систем.....27
2.2. Засоби технічного захисту інформації (ЗТЗІ).....29
2.3. Методи шифрування та управління ключами.....35
2.4. Засоби захисту від витоків інформації.....37
2.5. Системи виявлення вторгнень (СВВ).....38
2.6. Захист мереж як складова архітектури захисту інформаційних систем.....40
Тести та питання для самоконтролю.....44
Практичні завдання.....47

Тема 3. Управління доступом до інформації
3.1. Поняття доступу до інформаційних ресурсів та його рівні.....49
3.2. Системи управління доступом (СУД).....53
3.3. Аутентифікація, авторизація та облік в СУД.....58
3.4. Моніторинг, аудит та адміністрування в СУД.....62
3.5. Роль людського фактору в забезпеченні інформаційної безпеки.....67
Тести та питання для самоконтролю.....69
Практичні завдання.....71

Тема 4. Захист даних
4.1. Класифікація даних за рівнем конфіденційності.....74
4.2. Методи шифрування даних.....78
4.3. Захист даних у хмарних сховищах.....82
4.4. Захист персональних даних.....89
Тести та питання для самоконтролю.....93
Практичні завдання.....97

Тема 5. Відновлення після інцидентів кібербезпеки
5.1. Планування відновлення після інцидентів.....100
5.2. Процес реагування на інциденти кібербезпеки.....104
5.3. Тестування планів відновлення.....108
5.4. Страхування кіберризиків.....111
Тести та питання для самоконтролю.....115
Практичні завдання.....118

Тема 6. Сучасні тенденції в кібербезпеці
6.1. Штучний інтелект в кібербезпеці: нові горизонти та виклики.....121
6.2. Блокчейн і кібербезпека: нові межі цифрової безпеки.....124
6.3. Інтернет речей і кібербезпека.....128
6.4. Квантові обчислення і кібербезпека.....130
Тести та питання для самоконтролю.....133
Практичні завдання.....137

ГЛОСАРІЙ.....139

РЕКОМЕНДОВАНА ЛІТЕРАТУРА ТА ІНФОРМАЦІЙНІ ДЖЕРЕЛА.....146

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:

ТЕМА 2
ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ

Метою вивчення даної теми є формування у здобувачів освіти теоретичних знань і практичних навичок щодо забезпечення безпеки інформаційних систем, виявлення, аналізу та нейтралізації загроз інформаційній безпеці, а також розроблення й впровадження ефективних методів, засобів і стратегій захисту інформації.

У процесі вивчення теми передбачається:

- ✓ Ознайомлення з основними принципами, нормативно-правовими актами та стандартами у сфері захисту інформаційних систем.
- ✓ Вивчення основних видів загроз інформаційній безпеці та методів їх ідентифікації.
- ✓ Оволодіння сучасними технологіями захисту інформації, включаючи криптографічні, антивірусні, брандмауерні та інші технічні засоби.
- ✓ Аналіз вразливостей інформаційних систем та розробка заходів щодо їх усунення.
- ✓ Застосування набутих знань для розроблення політик інформаційної безпеки та впровадження систем захисту інформації в реальних умовах.

Вивчення теми дозволить майбутнім фахівцям ефективно забезпечувати безпеку інформаційних систем, запобігати та реагувати на кіберзагрози, що є критично важливим у сучасному цифровому середовищі.

План

2.1. Архітектура захисту інформаційних систем
2.2. Засоби технічного захисту інформації (ЗТЗІ)
2.3. Методи шифрування та управління ключами
2.4. Засоби захисту від витоків інформації
2.5. Системи виявлення вторгнень (СВВ)
2.6. Захист мереж як складова архітектури захисту інформаційних систем

2.1. Архітектура захисту інформаційних систем.

Архітектура захисту інформаційних систем (ІС) є однією з найбільш важливих сфер у сучасному світі інформаційних технологій. З розвитком цифрових технологій та зростанням обсягів даних, які обробляються, зростає і кількість загроз, пов’язаних з безпекою інформації. Захист інформаційних систем є ключовим компонентом стратегії будь-якої організації, що прагне забезпечити безпеку своїх даних та уникнути репутаційних та фінансових втрат. У сучасному цифровому світі, де інформація є одним з найцінніших ресурсів, захист

інформаційних систем давно вже набув критичного значення. Кіберзагрози стають все більш витонченими та складними, що вимагає від організацій застосування комплексних та ефективних методів захисту.

У рамках цієї теми ми з Вами проаналізуємо ключові принципи, методи та інструменти захисту інформаційних систем, а також розглянемо сучасні виклики і перспективи розвитку в цій галузі.

Архітектура захисту інформаційних систем – це сукупність …

ТЕМА 3
УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЇ

Метою вивчення даної теми є набуття теоретичних знань і практичних навичок щодо методів, моделей та механізмів контролю доступу до інформаційних ресурсів, забезпечення конфіденційності, цілісності та доступності даних, а також захисту від несанкціонованого доступу.

У процесі вивчення теми передбачається:

- ✓ Ознайомлення з основними принципами, стандартами та нормативно-правовими актами щодо управління доступом до інформації.
- ✓ Вивчення моделей контролю доступу (дискреційної, мандаторної, рольової, атрибутивної тощо) та їх практичного застосування.
- ✓ Оволодіння методами аутентифікації, авторизації та обліку дій користувачів.
- ✓ Аналіз загроз і вразливостей, пов’язаних з управлінням доступом, та розробка заходів їх усунення.
- ✓ Застосування сучасних технологій і механізмів контролю доступу в інформаційних системах та комп’ютерних мережах.

Вивчення теми дозволить майбутнім фахівцям ефективно організовувати політику доступу до інформації, забезпечувати її захист відповідно до вимог безпеки та законодавства, а також розробляти та впроваджувати ефективні системи контролю доступу.

План

3.1. Поняття доступу до інформаційних ресурсів та його рівні
3.2. Системи управління доступом (СУД)
3.3. Аутентифікація, авторизація та облік в СУД
3.4. Моніторинг, аудит та адміністрування в СУД
3.5. Роль людського фактору в забезпеченні інформаційної безпеки

3.1. Поняття доступу до інформаційних ресурсів та його рівні

Сучасний розвиток інформаційних технологій і комунікацій призвів до формування нового глобального середовища, в якому інформація стала одним із найцінніших ресурсів. Питання доступу до інформаційних ресурсів стало центральним у правовій, соціальній та економічній сферах життя. Це особливо актуально для країн, що знаходяться на різних етапах розвитку демократії та інформаційного суспільства. Доступ до інформації розглядається не лише як засіб для отримання знань, але й як фундаментальне право, що підтримує інші права людини, включаючи свободу вираження думок та доступ до правосуддя. У рамках цієї лекції буде розглянуто поняття доступу до інформаційних ресурсів та його

рівні, а також аналіз нормативно-правових аспектів та приклади міжнародного досвіду.

Поняття доступу до інформаційних ресурсів

Доступ до інформаційних ресурсів можна визначити як …

ТЕМА 4
ЗАХИСТ ДАНИХ

Метою вивчення даної теми є формування у студентів знань і навичок для забезпечення належного захисту даних у сучасних інформаційних системах, розуміння важливості класифікації та шифрування даних, а також механізмів захисту даних у хмарних сховищах і забезпечення безпеки персональних даних.

Зокрема, вивчаючи дану тему студенти опановують знання про:

1. класифікацію даних за рівнем конфіденційності, розглядаючи методи визначення та управління різними категоріями даних в залежності від їх важливості та чутливості для організації та користувачів;
2. основні методи шифрування даних, включаючи симетричне та асиметричне шифрування, а також техніки для захисту даних під час їх передачі та зберігання, з акцентом на сучасні криптографічні алгоритми;
3. механізми захисту даних у хмарних сховищах, у тому числі питання безпеки хмарних платформ, а також методи шифрування і захисту доступу до даних в умовах використання хмарних технологій;
4. правові та технічні аспекти захисту персональних даних, зокрема, вчаться розуміти вимоги сучасних законодавчих актів, таких як GDPR, а також вивчають інструменти для безпечного збору, зберігання та обробки персональної інформації.

Вивчення цієї теми дозволить студентам здобути практичні навички щодо захисту даних на різних етапах їх обробки, зберігання та передачі, а також забезпечити відповідність організацій вимогам безпеки та законодавства у сфері захисту даних.

План

4.1. Класифікація даних за рівнем конфіденційності
4.2. Методи шифрування даних
4.3. Захист даних у хмарних сховищах
4.4. Захист персональних даних

4.1. Класифікація даних за рівнем конфіденційності

Сучасне суспільство характеризується стрімким розвитком інформаційних технологій та значною залежністю від обробки й зберігання даних. У цьому контексті питання забезпечення конфіденційності інформації набуває критичної важливості. Дані є основою для ухвалення рішень, ведення бізнесу, управління державними процесами та підтримки безпеки громадян. Водночас ризики несанкціонованого доступу, втрати або витоку інформації створюють серйозні загрози для окремих осіб, організацій та держав. Наприклад, …

ТЕМА 5
ВІДНОВЛЕННЯ ПІСЛЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ

Метою вивчення даної теми є надання студентам глибоких знань і практичних навичок щодо ефективного управління процесами відновлення після інцидентів кібербезпеки, що дозволяє забезпечити мінімізацію наслідків кіберзагроз і відновлення нормальної роботи організацій.

Зокрема, студенти повинні:

1. Ознайомитись з принципами планування відновлення після інцидентів, зокрема вивчити методи оцінки критичних функцій та ресурсів, а також розробки комплексних стратегій відновлення для різних типів кіберінцидентів.
2. Вивчити процес реагування на інциденти кібербезпеки, вивчаючи ключові етапи виявлення загроз, локалізації інциденту, мінімізації його впливу та прийняття швидких заходів для відновлення стабільності систем.
3. Розглянути методи тестування планів відновлення, зосереджуючи увагу на перевірці готовності організацій до можливих інцидентів через моделювання реальних ситуацій та оцінку ефективності планів у екстремальних умовах.
4. Проаналізувати роль страхування кіберризиків, визначаючи його значення для фінансового захисту організацій у разі інцидентів кібербезпеки, а також вивчаючи аспекти вибору страхових полісів та управління ними.

Вивчення цієї теми дозволить студентам здобути знання для розробки ефективних планів відновлення, належного реагування на кіберінциденти та вибору оптимальних механізмів для захисту від кіберризиків, що є критично важливим для забезпечення безпеки та стійкості інформаційних систем організацій.

План

5.1. Планування відновлення після інцидентів
5.2. Процес реагування на інциденти кібербезпеки
5.3. Тестування планів відновлення
5.4. Страхування кіберризиків

5.1. Планування відновлення після інцидентів

У сучасну епоху інформаційних технологій забезпечення кібербезпеки є пріоритетом для організацій будь-якого масштабу. Однак, навіть найкращі захисні заходи не гарантують повної безпеки, що зумовлює важливість планування відновлення після інцидентів кібербезпеки. Інциденти, пов’язані з витоками даних, атаками на IT-інфраструктуру чи компрометацією систем, можуть завдати значної шкоди репутації, фінансовим показникам і операційній діяльності організації. Тому

планування відновлення – це ключовий елемент забезпечення стійкості бізнесу.

Ми з вами проаналізуємо основні аспекти планування відновлення після кіберінцидентів, включаючи основні етапи, принципи, стратегії та найкращі практики. Ми також розглянемо приклади реальних інцидентів, нормативно-правові вимоги й роль людського фактору у відновленні.

Кіберінцидентами називають події, які порушують або загрожують безпеці інформаційних систем. Кіберінциденти охоплюють широкий спектр подій: …

ТЕМА 6
СУЧАСНІ ТЕНДЕНЦІЇ В КІБЕРБЕЗПЕЦІ

Метою вивчення даної теми є формування у студентів комплексного розуміння актуальних тенденцій у сфері кібербезпеки, їх впливу на інформаційну безпеку та правове регулювання. Зокрема, студенти повинні:

- ✓ Ознайомитися з ключовими напрямами розвитку кібербезпеки та їх значенням для цифрової безпеки.
- ✓ Проаналізувати роль штучного інтелекту у виявленні, запобіганні та протидії кіберзагрозам, а також виклики, які постають у зв'язку з його застосуванням.
- ✓ З'ясувати можливості використання блокчейн-технологій для підвищення рівня захисту даних та забезпечення цифрової довіри.
- ✓ Дослідити загрози, що виникають у зв'язку з розвитком Інтернету речей (IoT), а також стратегії їхньої нейтралізації.
- ✓ Оцінити потенційний вплив квантових обчислень на сучасні криптографічні методи захисту інформації.
- ✓ Розвинути навички критичного мислення щодо технологічних і правових аспектів кібербезпеки.

Вивчення теми дозволить студентам не лише отримати актуальні знання про новітні загрози та способи їх подолання, а й підготуватися до практичного застосування отриманих знань у сфері інформаційної безпеки та правового забезпечення цифрових технологій.

План

1. Штучний інтелект в кібербезпеці: нові горизонти та виклики
2. Блокчейн і кібербезпека: нові межі цифрової безпеки
3. Інтернет речей і кібербезпека
4. Квантові обчислення і кібербезпека

6.1. Штучний інтелект у кібербезпеці: нові горизонти та виклики

У світі, де цифрові технології проникли в усі сфери людського життя, кібербезпека стала одним із ключових чинників забезпечення стабільності, захисту даних та приватності. Але як боротися зі зростаючим числом кібератак, що стають дедалі складнішими й агресивнішими? Відповідь частково криється у використанні штучного інтелекту (ШІ), який уже зараз демонструє неабиякий потенціал у боротьбі з цифровими загрозами.

Давайте розглянемо, як ШІ змінює парадигму кібербезпеки, які нові можливості відкриваються завдяки його впровадженню та з якими викликами стикається це поле. Ми звернемо увагу на реальні приклади, а також поміркуємо

над етичними й правовими аспектами використання ШІ в цій галузі.

Для розуміння ролі ШІ у кібербезпеці необхідно спочатку усвідомити складність сучасного кіберсередовища. Уявімо собі …

ГЛОСАРІЙ

Авторизація **–** це процес надання або обмеження доступу користувача до певних ресурсів або функцій після його успішної аутентифікації.

Адміністрування в системі управління доступом до інформаційних ресурсів **–** це процес налаштування, управління та моніторингу доступу користувачів до інформаційних систем і ресурсів; управління ролями, правами доступу та обліковими записами.

Антивірус **–** програмне забезпечення для виявлення та блокування шкідливих програм.

Архітектура захисту інформаційних систем **–** це сукупність принципів, методів та засобів, що використовуються для забезпечення безпеки інформаційних систем.

Аудит **–** це процес ретельного аналізу та перевірки активностей, що вже відбулися, з метою оцінки дотримання встановлених політик і норм безпеки.

Аутентифікація **–** це процес перевірки особи користувача, що надає можливість системі переконатися в його правомірності.

База даних користувачів та прав доступу **–** містить інформацію про облікові записи, ролі та їхні права.

Верифікація **–** процедура підтвердження, що користувач є тим, за кого себе видає, встановлення достовірності даних, які особа надає про себе.

Внутрішні дані **–** це інформація, що призначена для внутрішнього використання в організації та не підлягає розповсюдженню серед сторонніх осіб, наприклад: робочі документи; організаційні політики.

Доступність інформації **–** забезпечення того, щоб інформація була доступна користувачам у разі потреби.

Журналювання **–** це процес запису всіх дій, що відбуваються в системі.

Захист інформації **–** захист даних від знищення, зміни чи викрадення.

Захист мереж **–** забезпечення безпеки даних, що передаються через мережі.

Інтерфейс користувача **–** забезпечує зручний доступ до системи для адміністраторів та користувачів.

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

Кібербезпека **–** це комплекс заходів, спрямованих на захист комп'ютерних систем, мереж і даних від несанкціонованого доступу, атак, зловмисного програмного забезпечення та інших кіберзагроз.

Кібервійни **–** використання кіберзасобів для здійснення атак на інфраструктуру іншої країни чи організації з метою завдати шкоди або знищити важливі ресурси.

Кіберзлочинність **–** злочинна діяльність, пов'язана з використанням інформаційних технологій для незаконного доступу до даних, систем, мереж і ресурсів.

Кіберрозслідування **–** процес виявлення, аналізу й документування обставин

кіберінцидентів з метою встановлення винних осіб та оцінки збитків.
Кібертероризм – застосування інформаційних технологій з метою здійснення терористичних актів або поширення паніки серед населення.
Кібершпигунство – отримання конфіденційної інформації з державних, військових, комерційних чи приватних структур для використання в інтересах ворогуючих держав або корпорацій.
Конфіденційні дані – це категорія, що охоплює інформацію, доступ до якої обмежено. Розголошення таких даних може спричинити репутаційні або фінансові втрати, наприклад: особисті дані співробітників; деталі бізнес-стратегій.
Конфіденційність інформації – забезпечення того, щоб інформація була доступна лише тим, хто має право на її отримання.
Критично конфіденційні дані – це дані, розголошення яких може призвести до серйозних наслідків, таких як порушення прав, суттєві збитки чи загроза національній безпеці, наприклад: військова інформація; дані, що становлять державну таємницю.
Культура безпеки – це сукупність цінностей, норм та практик, що спрямовані на забезпечення інформаційної безпеки.
Моніторинг – це процес безперервного спостереження за діями, які виконуються користувачами в інформаційних системах; відстеження активності користувачів для виявлення підозрілих дій та недопущення порушень.
Організаційні заходи протидії кіберзагрозам – це сукупність заходів і політик, які визначають, як організація повинна керувати кібербезпекою, зокрема, з точки зору процесів, процедур, стандартів, ролей і відповідальностей.
Політика кібербезпеки – це основний документ, який визначає принципи та правила захисту інформаційних систем організації від кіберзагроз.
Програмні засоби захисту інформаційних систем – це спеціалізовані програми або набори програм, що забезпечують захист даних від різних загроз, таких як віруси, несанкціонований доступ, витоки інформації та інші види кібератак.
Публічні дані – це інформація, доступна широкому загалу, розголошення якої не призводить до негативних наслідків, наприклад: державна статистика; публічні звіти компаній; контактні дані для загального доступу.
Службова інформація – це та, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень; або зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.
Смартконтракти – це програми, які автоматично виконують умови угоди, записані в коді. Їх використання може мінімізувати людський фактор і підвищити прозорість.

Соціальна інженерія – це метод психологічного впливу на працівників з метою отримання доступу до конфіденційної інформації або систем.
Таємна інформація – інформація, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.
Фішинг – це метод обману, коли зловмисники намагаються отримати конфіденційну інформацію, видаючи себе за надійні джерела, наприклад, через фальшиві листи від банків, корпорацій або урядових установ.
Цілісність інформації – захист інформації від несанкціонованих змін.
Шифрування – це процес перетворення відкритих даних у зашифрований вигляд за допомогою алгоритмів та криптографічних ключів. Декодування можливе лише з використанням відповідного ключа.
ABAC *(англ. Attribute-based access control systems)* – Атрибутивні системи управління доступом, модель контролю доступу до об'єктів, що базується на аналізі правил для атрибутів об'єктів або суб'єктів, можливих операцій з ними та оточення, що відповідає запиту.
AES *(англ. Advanced Encryption Standard)* – Розширений стандарт шифрування, симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт).
APT *(англ. Advanced Persistent Threats)* – Розвинена стала загроза або постійна загроза підвищеної складності – різновид складних кібератак з метою отримання несанкційованого доступу до інформаційних систем жертви та встановлення прихованого доступу до неї з метою використання або контролю в майбутньому
CASB *(англ. Cloud Access Security Broker)* – Посередник, який забезпечує захищений доступ до хмари, це точка примусового застосування політики безпеки, розташована між корпоративними користувачами й постачальниками хмарних служб.
CDN *(англ. Content Delivery Networks або Content Distribution Network)* – Мережі доставки контенту, географічно розподілена мережева інфраструктура, що дозволяє оптимізувати доправлення та розповсюдження контенту кінцевим користувачам в мережі Інтернет, сприяє збільшенню швидкості завантаження інтернет-користувачами аудіо-, відео-, програмного, ігрового та інших видів цифрового контенту.
CSPM *(англ. Cloud Security Posture Management)* – Управління станом безпеки хмари, рішення, що сканує хмарні системи та інфраструктури на наявність ризиків і неправильних конфігурацій.
DAC *(англ. Discretionary access control systems)* – Дискреційні системи управління доступом, керування доступом суб'єктів до об'єктів на основі списків керування доступом або матриці доступу. Також використовуються назви "дискреціонне керування доступом", "контрольоване керування доступом" або "розмежоване

керування доступом”.

DDoS-атака *(англ. Distributed Denial of Service)* – розподілена атака типу “відмова в обслуговуванні”, різновид DoS-атаки, при якій цільовий сервер, сервіс або мережа перевантажують трафіком, що виходить з декількох джерел (наприклад, з групи пристроїв).

DLP *(англ. Data Loss/Leak Prevention)* – технології запобігання витоку конфіденційної інформації з інформаційної системи назовні, а також технічні пристрої (програмні або програмно-апаратні) для такого запобігання витокам.

DoS-атака *(англ. Denial of Service)* – напад на комп’ютерну систему з наміром зробити комп’ютерні ресурси недоступними користувачам, для яких комп’ютерна система була призначена.

ECC *(англ. Elliptic Curve Cryptography)* – це метод криптографії з відкритим ключем, в основі якого лежить використання еліптичних кривих над скінченними полями. Найважливіша відмінність ECC від RSA – це співвідношення розміру ключа та криптографічної стійкості. ECC забезпечує той самий рівень криптографічної стійкості, що й система на базі RSA, але з використанням значно менших ключів. Наприклад, 256-бітний ключ ECC не поступається ефективністю 3072-бітному ключу RSA.

EDR *(англ. Endpoint Detection and Response)* – це програмне рішення для відстеження, аналізу та реагування на загрози на кінцевих пристроях (комп’ютери, сервери, мобільні пристрої).

ELK Stack *(Elasticsearch, Logstash, Kibana)* – Система для моніторингу та аналізу логів у реальному часі. Стек ELK, що часто називається Elasticsearch, надає можливість збирати журнали всіх ваших систем і програм, аналізувати їх і створювати візуалізації, щоб моніторити програми та інфраструктури, швидше усувати проблеми, аналізувати систему безпеки та багато іншого. Це розподілений пошуковий та аналітичний двигун на базі Apache Lucene.

Firewall Міжмережевий екран або брандмауер – програма чи пристрій, що здійснює захист комп’ютерних мереж.

GDPR *(англ. General Data Protection Regulation)* – Загальний регламент захисту даних, нормативно-правовий акт Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони.

HSM *(Hardware Security Module)* – це надійні, стійкі до зламування апаратні пристрої, які захищають криптографічні процеси шляхом генерації та захисту ключів, а також управління ключами, що використовуються для шифрування та розшифрування даних та створення цифрових підписів та сертифікатів.

IDS *(англ. Intrusion Detection System)* – Система виявлення атак (вторгнень), програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп’ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет.

IoT *(англ. Internet of things)* – Інтернет речей – мережа фізичних пристроїв, які

підключені до Інтернету

IPS *(англ. Intrusion Prevention System)* – Система запобігання вторгненням, програмна або апаратна система мережевої та комп'ютерної безпеки, яка виявляє вторгнення або порушення безпеки і автоматично захищає від них.

LDAP *(англ. Lightweight Directory Access Protocol)* – полегшений протокол доступу до директорій / каталогів).

MAC *(англ. Mandatory access control systems)* – Мандаторні системи управління доступом, розмежування доступу суб'єктів до об'єктів, що ґрунтується на призначенні мітки конфіденційності для інформації, що міститься в об'єктах, та видачі офіційних дозволів (допусків) суб'єктам на звернення до інформації такого рівня конфіденційності.

MFA *(англ. Multi-factor authentication)* – Багатофакторна аутентифікація, метод контролю доступу до ресурса, в якому користувачеві для отримання доступу необхідно пред'явити більше одного доказу своїх повноважень або своєї ідентичності.

OTP *(англ. One Time Password)* – це пароль, який є дійсним тільки для одного сеансу аутентифікації, його дія також може бути обмежена певним проміжком часу, його неможливо використовувати повторно.

Ransomware *(англ. Ransom – викуп і Software – програмне забезпечення)* – Програма-вимагач, тип шкідливої програми, який злочинці встановлюють на комп'ютерах користувачів з метою вимагання викупу. Така програма надає злочинцям можливість віддалено заблокувати комп'ютер, після цього програма відображає спливаюче вікно з повідомленням, що комп'ютер заблокований і що до нього немає доступу, доки не будуть сплачені кошти.

RBAC *(англ. Role Based Access Control)* – Контроль доступу на основі ролей, модель дозволів, при використанні якої зникає необхідність у підтриманні списків керування доступом.

RSA *(абревіатура від прізвищ Rivest, Shamir та Adleman)* – криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел. RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису.

SIEM *(англ. Security Information and Event Management)* – просунута технологія кібербезпеки, яка поєднує в собі компоненти моніторингу подій, аналізу безпеки та реагування на інциденти, забезпечує аналіз в реальному часі подій (тривог) безпеки, що виходять від мережевих пристроїв і додатків, використовується також для журналювання даних і генерації звітів з метою сумісності з іншими бізнес-даними.

SOC *(англ. Security Operations Center)* – Операційний центр безпеки, централізований підрозділ установи, який вирішує питання з інформаційної та кібербезпеки на організаційному та технічному рівні.

SSL *(англ. Secure Sockets Layer)* – рівень захищених сокетів, криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і

сервером.

TLS *(англ. Transport Layer Security)* – Безпека транспортного рівня, криптографічний протокол, що надає можливості безпечної передачі даних в інтернеті для навігації, отримання пошти, спілкування, обміну файлами, тощо.

UAM *(англ. User Activity Monitoring)* – Моніторинг і аналіз активності користувачів, контролюють активності співробітників та відстежують передачу конфіденційної інформації за допомогою різних каналів та додатків.

VPN *(англ. Virtual Private Network)* – віртуальні приватні мережі, узагальнена назва клієнт-серверних технологій, які дають змогу створювати віртуальні захищені мережі поверх інших мереж із нижчим рівнем довіри.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Антонюк Н. М. Використання штучного інтелекту у забезпеченні кібербезпеки. *Інформаційна безпека України*, 2023. № 2. С. 39–47.
2. Білецький О. О. Кібербезпека: основи, загрози та захист : навч. посіб. Київ : Видавничий дім “Кондор”, 2021. 320 с.
3. Бондаренко О. Г. Інформаційна безпека: концепції, стратегії, механізми : монографія. Харків : Право, 2020. 280 с.
4. Буров С. В. Кібербезпека: стратегії захисту та відновлення. Київ : Юрінком Інтер, 2021. 368 с.
5. Василенко А. В. Основи кібербезпеки : підруч. Львів : Львівська політехніка, 2019. 350 с.
6. Гончаренко В. В. Захист інформації в комп’ютерних системах : навч. посіб. Одеса : ОНПУ, 2020. 275 с.
7. Григоренко О. Ю. Проблеми забезпечення кібербезпеки та захисту персональних даних в умовах цифровізації. *Вісник Національної академії правових наук України*, 2023. Т. 31. № 1. С. 84–95.
8. Гриценко В. С. Кібербезпека: сучасні виклики та технології. Київ : Юрінком Інтер, 2022. 384 с.
9. Дьомін С. В. Реагування на кіберінциденти: методи, інструменти, технології. Київ : КНТ, 2020. 312 с.
10. Ковальчук В. Ф. Кіберзагрози та методи їх запобігання. Львів : Видавничий дім “Галицькі контракти”, 2022. 272 с.
11. Кривоніс О. І. Кібербезпека: правові та організаційні аспекти : навч. посіб. Київ : Центр навчальної літератури, 2022. 310 с.
12. Ліпкан В. А. Кібербезпека та національна безпека: сучасні виклики та загрози. Київ : Юрінком Інтер, 2023. 420 с.
13. Паламарчук В. Ф. Технології захисту інформації: сучасний стан та перспективи розвитку. Київ : Видавничий дім “КМ-Академія”, 2022. 348 с.
14. Пашорін В. І., Костюк Ю. В. Безпека інформаційних систем : навч. посіб. Київ : КНТЕУ, 2023. 376 с.
15. Полторак В. П. Інформаційна безпека та захист даних в комп’ютерних технологіях і мережах : навч. посіб. для студ. спец. 126 “Інформаційні системи та технології”. Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА ТА ІНФОРМАЦІЙНІ ДЖЕРЕЛА

Основна:

1. Біла О. О. Інформаційне право України : навчальний посібник. Київ : Юрінком Інтер, 2020. 312 с.
2. Білецький О. О. Кібербезпека: основи, загрози та захист : навч. посіб. Київ : Видавничий дім “Кондор”, 2021. 320 с.
3. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д., Бондарєв А. П. Захист інформації : навчальний посібник. Вінниця : ВНТУ, 2019. 580 с.
4. Василенко А. В. Основи кібербезпеки : підруч. Львів : Львівська політехніка, 2019. 350 с.
5. Василенко М. Д. Інтелектуальні системи захисту інформації в кіберпросторі : навч. посіб. Одеса : ОНУ, 2018. 220 с.
6. Гончаренко В. В. Захист інформації в комп’ютерних системах : навч. посіб. Одеса : ОНПУ, 2020. 275 с.
7. Городиський В. О. Захист інформації в інформаційних системах : навчальний посібник. Київ : КНТ, 2018. 280 с.
8. Кабанов О. М., Бондаренко О. В., Підгорний О. В. Доступ до публічної інформації для державних службовців та службовців органів місцевого самоврядування : навчально-методичний посібник для тренерів. Київ : Програма розвитку ООН в Україні, 2021. 120 с.
9. Копиленко О. Л. Правове регулювання доступу до інформації в Україні : монографія. Київ : Парламентське видавництво, 2019. 256 с.
10. Кривоніс О. І. Кібербезпека: правові та організаційні аспекти : навч. посіб. Київ : Центр навчальної літератури, 2022. 310 с.
11. Ліпкан В. А. Кібербезпека та інформаційний захист : підручник. Київ : Юрінком Інтер, 2022. 432 с.
12. Павленко Р. О. Інформаційна безпека: основи правового регулювання. Київ : Видавничий дім “КМ-Академія”, 2022. 304 с.
13. Пашорін В. І., Костюк Ю. В. Безпека інформаційних систем : навч. посіб. Київ : КНТЕУ, 2023. 376 с.
14. Полторак В. П. Інформаційна безпека та захист даних в комп’ютерних технологіях і мережах : навч. посіб. для студ. спец. 126 “Інформаційні системи та технології”. Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.

Додаткова:

1. Антонюк Н. М. Використання штучного інтелекту у забезпеченні кібербезпеки. *Інформаційна безпека України*, 2023. № 2. С. 39–47.
2. Антонюк Н. М. Правове регулювання захисту персональних даних в Україні та ЄС. *Науковий вісник Національного університету біоресурсів і природокористування України*, 2022. № 2. С. 37–45.

3. Антонюк Н. М. Правові засади регулювання доступу до інформації в Україні. *Науковий вісник Національного університету біоресурсів і природокористування України*, 2022. № 1. С. 45–52.
4. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: концептуальні та організаційно-правові засади : монографія. Київ : МК-Прес, 2006. 400 с.
5. Бондаренко О. Г. Інформаційна безпека: концепції, стратегії, механізми : монографія. Харків : Право, 2020. 280 с.
6. Брижко В., Цимбалюк В., Швець М. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти упорядкування інформаційних відносин у зв'язку з автоматизованою обробкою даних. Київ : ПанТот, 2006. 383 с.
7. Буров С. В. Кібербезпека: стратегії захисту та відновлення. Київ : Юрінком Інтер, 2021. 368 с.
8. Василенко П. О. Відновлення після кібератак: кращі практики та міжнародний досвід. *Інформаційна безпека України*, 2022. № 3. С. 48–56.
9. Герасимчук О. М. Управління інцидентами кібербезпеки: теоретико-прикладний аспект. Харків : Право, 2022. 280 с.
10. Григоренко О. Ю. Алгоритми реагування на кіберінциденти в контексті державної безпеки. *Вісник Національної академії правових наук України*, 2023. Т. 31. № 2. С. 97–108.
11. Григоренко О. Ю. Інформаційний суверенітет держави: проблеми захисту та забезпечення доступу. *Вісник Національної академії правових наук України*, 2023. Т. 30. № 2. С. 73–85.
12. Григоренко О. Ю. Нові підходи до протидії кібератакам у глобальному просторі. *Вісник Національної академії правових наук України*, 2023. Т. 32. № 1. С. 91–102.
13. Григоренко О. Ю. Проблеми забезпечення кібербезпеки та захисту персональних даних в умовах цифровізації. *Вісник Національної академії правових наук України*, 2023. Т. 31. № 1. С. 84–95.
14. Гриценко В. С. Захист інформації: правові основи та технічні аспекти. Київ : Юрінком Інтер, 2021. 384 с.
15. Гриценко В. С. Кібербезпека: сучасні виклики та технології. Київ : Юрінком Інтер, 2022. 384 с.
16. Гуцалюк М. А. Захист інформаційних ресурсів у кіберпросторі. *Інформаційна безпека та кіберзахист*, 2021. № 2(10). С. 45–58.
17. Дьомін С. В. Інформаційна безпека: концепції, технології, засоби. Київ : КНТ, 2020. 290 с.
18. Дьомін С. В. Новітні підходи до забезпечення інформаційної безпеки. Київ : КНТ, 2021. 328 с.
19. Дьомін С. В. Реагування на кіберінциденти: методи, інструменти, технології. Київ : КНТ, 2020. 312 с.

20. Іваненко Л. Ю. Кіберзагрози у сучасному світі: тенденції та виклики. *Вісник Національної академії внутрішніх справ*, 2022. № 3. С. 90–105.
21. Коваленко П. В. Криптографічний захист інформації: сучасні методи та перспективи розвитку. *Український журнал інформаційної безпеки*, 2021. Т. 27. № 4. С. 123–138.
22. Ковальчук В. Ф. Кіберзагрози та методи їх запобігання. Львів : Видавничий дім "Галицькі контракти", 2022. 272 с.
23. Ковальчук В. Ф. Кіберризики та управління інцидентами інформаційної безпеки. Львів : Видавничий дім "Галицькі контракти", 2021. 256 с.
24. Копиленко О. Л. Персональні дані: правові основи їх зберігання та обробки. Київ : Парламентське видавництво, 2019. 256 с.
25. Кузнецов Г. В., Фомичов В. В., Сушко С. О., Фомичова Л. Я. Математичні основи криптографії : навч. посіб. Дніпро : ДНУ, 2004. 312 с.
26. Кузнецов С. Доступ до інформації як конституційне право: теоретико-правові аспекти : монографія. Харків : Право, 2021. 320 с.
27. Ліпкан В. А. Кібербезпека та національна безпека: сучасні виклики та загрози. Київ : Юрінком Інтер, 2023. 420 с.
28. Ліпкан В. А. Штучний інтелект у кібербезпеці: перспективи та загрози. Київ : Юрінком Інтер, 2023. 410 с.
29. Марущак А. І. Інформаційне право: доступ до інформації. Київ : КНТ, 2007. 532 с.
30. Марущак А. І. Правові основи захисту інформації з обмеженим доступом. Київ : КНТ, 2007. 208 с.
31. Паламарчук В. Ф. Захист персональних даних: міжнародний та національний досвід. Київ : Видавничий дім "КМ-Академія", 2021. 328 с.
32. Паламарчук В. Ф. Роль штучного інтелекту у відновленні після кібератак. *Юридична Україна*, 2021. № 8. С. 23–30.
33. Паламарчук В. Ф. Технології захисту інформації: сучасний стан та перспективи розвитку. Київ : Видавничий дім "КМ-Академія", 2022. 348 с.
34. Ткаченко О. В. Виклики для кібербезпеки в умовах цифрової трансформації. *Юридична Україна*, 2022. № 5. С. 18–27.
35. Ткаченко О. В. Співвідношення права на доступ до інформації та права на захист персональних даних. *Юридична Україна*, 2021. № 7. С. 12–18.
36. Ткаченко О. В. Співвідношення права на конфіденційність та необхідності контролю за інформаційними потоками. *Юридична Україна*, 2021. № 6. С. 15–21.
37. Хорошко В. О., Капустян М. В. Аналіз захищеності інформаційних систем : монографія. Київ : НТУУ "КПІ", 2010. 350 с.
38. Черненко А. О. Квантові обчислення та їхній вплив на криптографічні методи захисту. *Науковий вісник КПІ*, 2022. № 4. С. 55–63.

Нормативно-правові акти:

1. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : Постанова Кабінету Міністрів України від 23.12.2020 р. № 1295. Дата оновлення: 07.09.2022. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text (дата звернення: 01.03.2025).
2. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI. Дата оновлення: 08.10.2023. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 01.03.2025).
3. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. Дата оновлення: 18.12.2024. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 01.03.2025).
4. Про затвердження Порядку забезпечення доступу до публічної інформації у Державному бюро розслідувань та його територіальних управліннях : Наказ Державного бюро розслідувань від 05.01.2023 р. № 8. Дата оновлення: 26.09.2024. URL: https://zakon.rada.gov.ua/rada/show/v0008911-23#Text (дата звернення: 01.03.2025).
5. Про затвердження Порядку забезпечення доступу до публічної інформації у Бюро економічної безпеки України та його територіальних управліннях : Наказ Бюро економічної безпеки України від 12.04.2022 р. № 67. Дата оновлення: 03.02.2025. URL: https://zakon.rada.gov.ua/laws/show/z0451-22#Text (дата звернення: 01.03.2025).
6. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 01.03.2025).
7. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 18.01.2025. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 01.03.2025).
8. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення: 15.11.2024. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 01.03.2025).
9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 28.02.2025).

Інтернет-ресурси:

1. Державна служба спеціального зв’язку та захисту інформації України (Національний центр кібербезпеки України) : рекомендації. URL: https://cip.gov.ua/ua/faqs (дата звернення: 01.03.2025).
2. Європейське агентство з мережевої та інформаційної безпеки (ENISA) : публікації. URL: https://www.enisa.europa.eu/publications (дата звернення:

01.03.2025).
3. Міністерство цифрової трансформації України : проєкти. URL: https://thedigital.gov.ua/projects (дата звернення: 01.03.2025).
4. Національна комісія з питань регулювання зв’язку та інформатизації : медіагалерея. URL: https://nkek.gov.ua/galleries (дата звернення: 01.03.2025).
5. Національний інститут стандартів і технологій США (NIST) : публікації з кібербезпеки. URL: https://csrc.nist.gov/publications (дата звернення: 28.02.2025).
6. Центр досліджень кібербезпеки НАТО (NATO CCDCOE) : бібліотека. URL: https://ccdcoe.org/library/publications/ (дата звернення: 28.02.2025).
7. Центр реагування на комп’ютерні інциденти України (CERT-UA) : зв’яжіться з нами. URL: https://cert.gov.ua/contact-us (дата звернення: 01.03.2025).

Навчальне видання
(українською мовою)

Бараннік Роман В’ячеславович

КІБЕРБЕЗПЕКА І УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ

Навчальний посібник

Рецензент *Р. Корольков*
Відповідальний за випуск *Р. В. Бараннік*
Коректор *Р. В. Бараннік*