ЗМІСТ

Правові основи кібербезпеки та захисту інформації

Анотація

Підручник, який ви зараз читаєте, задумано як своєрідний міст між теоретико-правовими засадами та практичними викликами у сфері кібербезпеки й захисту інформації. Видання комплексно розкриває особливості правового регулювання кібербезпеки та інформаційної безпеки, механізми захисту інформаційних систем і даних в умовах цифрової трансформації.

У підручнику проаналізовано ключові поняття, етапи розвитку, актуальні загрози й методи протидії, правові засади технічного та організаційного захисту інформації. Видання спрямоване на формування цілісного розуміння кібербезпеки як складової правового забезпечення держави, суспільства й економіки та підходів до захисту інформації як стратегічного ресурсу цифрової доби.

Підручник розрахований на студентів, аспірантів, викладачів, науковців і практичних працівників органів публічної влади, правоохоронних органів та фахівців з управління інформаційними ресурсами й кібербезпеки.

ЗМІСТ

ВСТУПНЕ СЛОВО

Сучасний етап державотворення в Україні позначений інтенсивною цифровою трансформацією, що охоплює публічне управління, економіку, соціальну сферу та систему суспільних відносин загалом. Інформаційно-комунікаційні технології стають невід'ємним складником здійснення владних повноважень, надання адміністративних послуг, функціонування судової та правоохоронної систем, управління критичною інфраструктурою, фінансовими потоками та соціальними сервісами. Водночас масштабна цифровізація об'єктивно породжує нові ризики й загрози, що безпосередньо впливають на стан національної безпеки, реалізацію прав і свобод людини та ефективність діяльності органів публічної влади.

У цьому контексті кібербезпека та захист інформації перестають бути виключно технічною проблемою чи вузькоспеціалізованою сферою діяльності фахівців з інформаційних технологій. Вони набувають виразного правового, безпекового, управлінського та інституційного виміру. Порушення цілісності, конфіденційності або доступності інформаційних ресурсів, зокрема внаслідок неправомірних втручань, здатне спричинити не лише технічні збої, а й істотні юридичні наслідки – від втрати доказової сили електронних документів і неправомірного обмеження прав громадян до збоїв у здійсненні публічних функцій та виникнення підстав для юридичної відповідальності посадових осіб і держави. Саме тому формування належного рівня правової культури у сфері кібербезпеки становить одне з ключових завдань сучасної юридичної освіти.

Підручник «Правові основи кібербезпеки та захисту інформації» підготовлено з урахуванням актуальних викликів цифрової епохи та потреб фахової підготовки майбутніх юристів, державних службовців, працівників органів виконавчої

влади й місцевого самоврядування, судової та правоохоронної систем, а також спеціалістів, професійна діяльність яких пов'язана з управлінням інформаційними ресурсами. Мета видання полягає у формуванні цілісного уявлення про кібербезпеку як комплексну сферу, що інтегрує правові, організаційні та технічні елементи, а також у виробленні навичок правового аналізу ризиків і загроз, пов'язаних із функціонуванням інформаційних систем.

Видання вирізняється органічним поєднанням теоретичного аналізу з практичними прикладами, актуальними кейсами та міждисциплінарним підходом. Воно ґрунтується на чинному законодавстві України, враховує європейські та міжнародні стандарти у сфері кібербезпеки й захисту інформації та відповідає сучасним вимогам до підготовки фахівців правничого профілю.

Переконана, що цей підручник стане вагомим навчальним і науково-методичним інструментом для студентів, аспірантів, викладачів, а також для практичних працівників органів публічної влади й інших фахівців, чия діяльність пов'язана з правовим регулюванням цифрового середовища. У ньому органічно поєднано ґрунтовні теоретичні положення з аналізом актуальних управлінських і правових викликів цифрової епохи, що надає виданню практичної спрямованості та високої пізнавальної цінності. Змістовне наповнення підручника формує надійне теоретико-методологічне підґрунтя для осмислення кібербезпеки як невід'ємного елементу сучасної правової держави та сприяє становленню професійної правової компетентності майбутніх юристів, здатних ефективно діяти в складному й динамічному цифровому середовищі.

Використання цього підручника в освітньому та науковому процесі сприятиме підвищенню рівня правової культури у сфері

кібербезпеки, що є необхідною передумовою зміцнення засад правової держави та забезпечення захисту національних інтересів України в умовах цифрової трансформації. Загалом підручник є своєчасним, актуальним і концептуально значущим внеском у розвиток юридичної науки та системи правничої освіти України.

Серьогіна Світлана Григорівна,
директор Науково-дослідного інституту
державного будівництва
та місцевого самоврядування НАПрН України,
доктор юридичних наук, професор,
член-кореспондент НАПрН України,
заслужений діяч науки і техніки України

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ТА АБРЕВІАТУР

AES (Advanced Encryption Standard – Розширений стандарт шифрування) – симетричний блоковий шифр, що може зашифровувати та розшифровувати дані.

AES-256 (Advanced Encryption Standard) – один із найбезпечніших у світі симетричних алгоритмів блочного шифрування, що використовує ключ довжиною 256 біт.

BIA (Business Impact Analysis) – аналіз впливу на бізнес, метод оцінки ризиків, що визначає наслідки збоїв у роботі компанії

BIOS (Basic Input/Output System – базова система введення-виведення) – набір мікропрограм, вшитих у мікросхему на материнській платі, що забезпечує запуск комп'ютера, тестування обладнання та ініціалізацію завантаження операційної системи.

BYOK (Bring your own encryption) – маркетингова модель безпеки хмарних обчислень, яка має на меті допомогти клієнтам хмарних послуг використовувати своє власне програмне забезпечення шифрування та керувати власними ключами шифрування.

CERT (Computer Emergency Response Team) – спеціалізовані команди експертів з кібербезпеки, що займаються виявленням, аналізом та нейтралізацією комп'ютерних загроз.

CERT/CC (Computer Emergency Response Team/Coordination Center) – провідний міжнародний центр координації комп'ютерної безпеки, створений у 1988 році на базі Інституту програмної інженерії (SEI) університету Карнегі-Меллона (США).

CERT-UA (Computer Emergency Response Team of Ukraine – Команда реагування на комп'ютерні надзвичайні ситуації України) – урядова команда реагування на комп'ютерні надзвичайні події, що діє при Держспецзв'язку, яка захищає український кіберпростір, аналізує загрози, допомагає державним органам та критичній

інфраструктурі протидіяти кібератакам, а також інформує про шкідливе ПЗ та вразливості.

ChatGPT (Generative Pre-trained Transformer – генеративний попередньо тренований трансформер) – чат-бот та віртуальний помічник з генеративним штучним інтелектом, розроблений компанією OpenAI.

DDoS (Distributed Denial of Service – розподілена відмова в обслуговуванні) – кібератака, під час якої велика кількість заражених пристроїв одночасно надсилає величезний обсяг сміттєвого трафіку на сайт або сервер.

DLP (Data Loss Prevention – запобігання втраті даних) – комплекс програмних інструментів та стратегій, призначених для захисту конфіденційної інформації від витоку, викрадення або несанкціонованого використання, як навмисного, так і випадкового.

DLP (Data Loss Prevention) – набір інструментів, процесів та стратегій, спрямованих на запобігання втраті, витоку або несанкціонованому використанню конфіденційних даних (персональних даних, комерційної таємниці, фінансів).

DLP-системи (Data Loss/Leak Prevention) – комплексні програмні або програмно-апаратні рішення, призначені для запобігання витоку конфіденційної інформації за межі корпоративної мережі.

ECC (Elliptic Curve Cryptography – криптографія на еліптичних кривих) – сучасний метод асиметричного шифрування, заснований на алгебраїчній структурі еліптичних кривих над скінченними полями, що забезпечує високий рівень безпеки (обмін ключами, цифрові підписи) з набагато меншим розміром ключів порівняно з RSA, підвищує швидкість роботи та зменшує навантаження на обчислювальні ресурси.

eIDAS (Electronic IDentification, Authentication and trust Services – Електронні послуги ідентифікації, аутентифікації та довіри) – регламент Європейського Союзу про електронну

ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку ЄС.

ENISA (European Union Agency for Network and Information Security – Агентство Європейського Союзу з питань кібербезпеки) – профільна агенція ЄС, створена у 2004 році (функціонує з 2005) для забезпечення високого рівня мережевої та інформаційної безпеки в Європі.

FIPS (Federal Information Processing Standards – Федеральні стандарти обробки інформації) – публічні стандарти та керівні принципи, розроблені Національним інститутом стандартів і технологій США для комп'ютерних систем у державних установах США, що забезпечують безпеку, сумісність та надійність шифрування, зокрема криптографічних модулів

GDPR (General Data Protection Regulation) – загальний регламент захисту даних ЄС, що встановлює суворі правила збору, зберігання та обробки персональних даних, дає користувачам більше контролю над їхньою інформацією, а компаніям обов'язки щодо безпеки.

Helsi – найбільша в Україні медична інформаційна система та однойменний мобільний додаток, що об'єднує пацієнтів, лікарів та медичні заклади, яка дозволяє онлайн записуватися до лікарів, зберігати електронну медичну картку, переглядати результати аналізів та призначень.

HSM (Hardware Security Module – апаратний модуль безпеки) – фізичний обчислювальний пристрій (спеціалізована плата або сервер), призначений для безпечного створення, зберігання та керування криптографічними ключами, а також виконання криптографічних операцій (шифрування, підпис), що забезпечує найвищий рівень захисту, ізолюючи ключі всередині захищеного від несанкціонованого доступу периметра.

HSM (Hardware Security Module – Апаратний модуль безпеки) – фізичний обчислювальний пристрій (спеціалізована плата або сервер), призначений для безпечного створення, зберігання та керування криптографічними ключами.

HSM (Hardware Security Module – Апаратний модуль безпеки) – спеціалізований фізичний пристрій (у вигляді плати PCI, USB-токена або мережевого пристрою), призначений для захищеної генерації, зберігання та використання криптографічних ключів, а також гарантує, що ключі шифрування ніколи не покидають захищений периметр, виконуючи криптографічні операції всередині стійкого до зламів корпусу.

HTTPS (HyperText Transfer Protocol Secure – Захищений протокол передавання гіпертексту) – безпечна версія протоколу HTTP, яка використовується веббраузерами для зашифрованого обміну даними з вебсайтами, а також забезпечує конфіденційність, цілісність даних та автентифікацію завдяки використанню сертифікатів SSL/TLS, захищаючи інформацію (паролі, картки) від перехоплення.

KMS-сервіс (Key Management Service) – технологія Microsoft для автоматичної активації корпоративних версій Windows та Office у локальній мережі.

KPI (Key Performance Indicators – ключові показники ефективності) – кількісні вимірювані метрики, які допомагають компаніям та працівникам оцінити ступінь досягнення стратегічних і поточних бізнес-цілей, а також показують, наскільки ефективно функціонують бізнес-процеси, відділи або окремі співробітники, і чи наближаються вони до запланованого результату.

MFA (Multi-Factor Authentication – Багатофакторна автентифікація) – метод захисту облікових записів, який вимагає від користувача підтвердження особи двома або більше різними способами (факторами), а не лише паролем.

NIS2 (Network and Information Security Directive 2) – оновлена директива ЄС (2022/2555) щодо кібербезпеки, що набула чинності у 2023 році та стала обов'язковою до виконання з 18 жовтня 2024 року, та яка суттєво посилює вимоги до захисту інформаційних систем, розширює перелік критичних секторів (енергетика, транспорт, охорона здоров'я, держуправління) та запроваджує суворі штрафи за порушення.