Європейські закони про кібербезпеку:



ТЕМА НОМЕРА

Без впровадження деяких основоположних актів нас не пустять до ЄС.

Є відомий вислів: «Америка винаходить, Китай копіює, Європа регулює». Євросоюз, найбільша бюрократія світу, дійсно став першопрохідцем у розробленні законів, що стосуються різних аспектів кібербезпеки. З 2018 року діє GDPR — Загальний регламент захисту персональних даних. Вісім років і мільйони євро штрафів потому цей регуляторний документ вже сприймається як даність. У 2024 році ЄС прийняв Акт про кіберстійкість, який змушує виробників підключеного обладнання та ПЗ забезпечувати кіберзахист своєї продукції. Директива NIS2 від 2022 року визначає, що повинні зробити держави-члени на національному рівні для покращення кібербезпеки. Україна є країною-кандидатом на вступ до Євросоюзу, і на цьому шляху потрібно адаптувати зокрема європейські вимоги щодо кібербезпеки. «МтБ» спробував розібратися в цих директивах та регламентах.

Директива NIS

Директива 2016/1148 «Стосовно безпеки мереж та інформаційних систем», ухвалена у липні 2016 року, стала першим загальноєвропейським законом про кібербезпеку. Метою директиви було забезпечення спільного рівня кібербезпеки в країнах ЄС, посилення транскордонної співпраці та обміну інформацією. Дія директиви поширювалась на т. зв. операторів основних послуг (essential services) — підприємств сфер енергетики, транспорту, банків і фінансів, охорони здоров'я, постачання питної води, — та постачальників цифрових послуг (хмарні сервіси, пошукові системи, онлайн-маркетплейси).

Директива NIS передбачала створення у всіх країнах-членах команд комп'ютерної безпеки з реагування на інциденти (CSIRT), національних компетентних органів (NCA) і єдиних точок контакту (SPoC) для відстеження, сповіщення, розслідування інцидентів та іншої транскордонної діяльності. На CSIRT-и країн-членів покладено такі завдання, як моніторинг подій кібербезпеки на національному рівні, розсилання попереджень і оголошень, здійснення аналізу ризиків і координація з аналогічними центрами інших держав-членів.

Директива вимагала від організацій вживати заходів у таких сферах, як безпека систем, тестування і відповідність міжнародним стандартам, але конкретних вимог не встановлювала. Документ вказував, що штрафи за невідповідність визначаються не Євросоюзом, а самими державами, але вони повинні бути ефективними, пропорційними і стримувальними, а організації-порушники надалі підлягають контролю з боку NCA. Також організації повинні за запитом надавати інформацію для оцінювання безпеки їхньої мережевої та інформаційної інфраструктури.

У 2022 році ЄС ухвалив оновлену директиву NIS2 (2022/2555). Вона усунула поділ на операторів основних

послуг і постачальників цифрових послуг, натомість розділивши їх на операторів основних (essential) і важливих (important) послуг. При цьому директива розширила сферу застосування з 7 до 18 секторів, додавши зокрема поштові сервіси, управління відходами, хімічну індустрію, космос тощо (**рис. 1**). Для обміну інформацією і скоординованого реагування на масштабні кіберінциденти було створено Європейську мережу організації контактів при кіберкризах (EU-CyCLONe). Також створено Координаційну групу, яка забезпечує стратегічні настанови для роботи CSIRT'ів.

Директива встановлює низку вимог до організацій у чотирьох напрямках.

- **Скорочення кіберризиків**: управління інцидентами, посилення захисту ланцюжків постачання, покращення захисту мереж і контролю доступу, шифрування.
- **Корпоративна відповідальність**: керівництво компаній повинне затверджувати і контролювати заходи з кібербезпеки, само проходити навчання, а злам може призводити до покарання, зокрема до тимчасового відсторонення від виконання обов'язків.
- **Звітність**: організації, які надають основні і важливі послуги, повинні впровадити процеси для швидкого сповіщення про інциденти, що можуть мати серйозний вплив на клієнтів і надання послуг. Директива встановлює конкретні терміни, зокрема 24 години на «раннє попередження».
- **Безперервність бізнесу**: організації повинні мати плани забезпечення безперервності бізнесу в разі серйозного інциденту, що включають зокрема аварійне відновлення систем, екстрені процедури і створення групи кризового реагування.

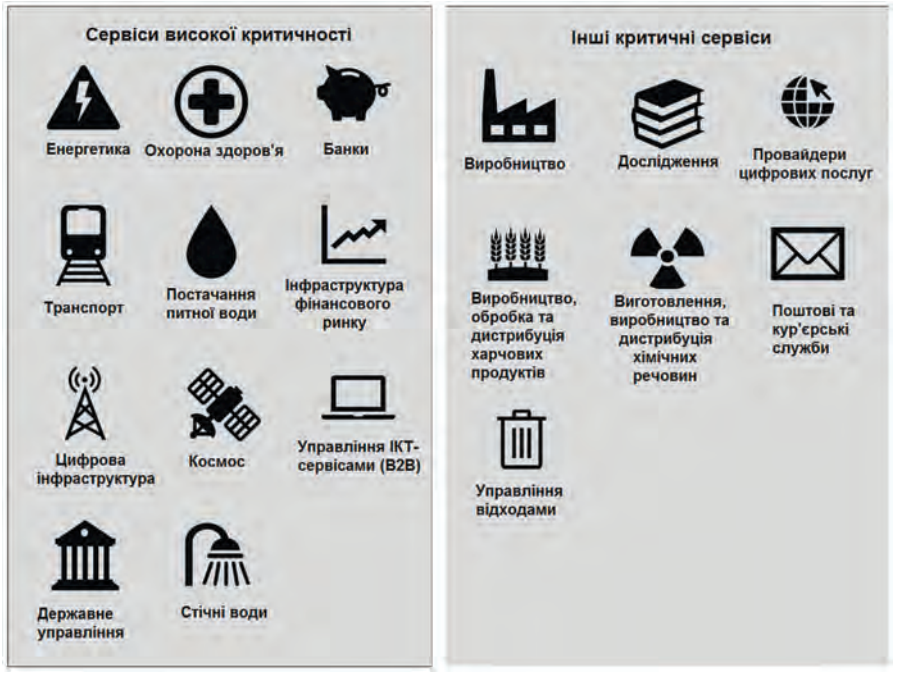


Рис. 1. Сектори, на які поширюється дія Директиви NIS2 (джерело: ірландський регулятор зв'язку ComReg)

Також передбачено 10 мінімальних заходів, яких повинні вжити оператори основних і важливих послуг для убезпечення проти можливих конкретних видів кібератак. Ці заходи включають, зокрема, процедури безпеки для користувачів з доступом до секретних або важливих даних; багатофакторну автентифікацію, рішення для безперервної автентифікації, шифрування голосових, відео– і текстових повідомлень; навчання кібербезпеці та базовій комп'ютерній гігієні; планування дій під час і після кіберінцидентів (зокрема підтримання актуальних бекапів і план дій для забезпечення доступу до IT-систем); захист ланцюжків постачання (відповідно до вразливостей кожного постачальника).

Acronis
Cyber Protect

Зберігайте свої дані в безпеці за будь-яких умов

- Найкраще резервне копіювання та відновлення
- Потужний захист від кіберзагроз
- Інтегроване управління безпекою



MEGATRADE
project distribution

Офіційний дистриб'ютор
Acronis в Україні
www.megatrade.ua
+380 44 538 00 06

На відміну від попередньої версії, NIS2 передбачає конкретні покарання за порушення. Для операторів основних послуг — €10 млн або 2% виручки попереднього фінансового року. Для операторів важливих послуг — відповідно €7 млн або 1,4% виручки. Також NCA можуть вчиняти додаткові адміністративні дії, такі як зобов'язання компаній у строгі терміни усунути порушення, виявлені аудитом, і оповіщення клієнтів організації про загрозу. Щоб знизити тиск на IT-відділи, які досі мусили самотужки піклуватися про кіберзахист компаній, і змінити уявлення про те, чия це відповідальність, передбачено кримінальні санкції проти менеджменту за недбальство у разі інциденту. Зокрема NCA може наказати організації публічно повідомити про факт порушення вимог директиви; також може публічно називати фізичних чи юридичних осіб, винних у порушеннях; і якщо йдеться про основні послуги, то у випадку повторних порушень, як уже йшлося, може усувати керівників з посад.

Директива NIS2 поширюється і на компанії не з країн Євросоюзу, які надають послуги на території ЄС, і ці компанії повинні призначити представника в ЄС, який діятиме від їхнього імені. Як зазначає Держспецзв'язку, Україна взяла на себе зобов'язання імплементувати NIS2 в рамках програми Ukraine Facility, а також цей крок сам по собі важливий для інтеграції в цифровий ринок Євросоюзу і загалом для вступу в ЄС.

Координацію імплементації NIS2 здійснює Держспецзв'язку у співпраці з експертними організаціями. Роль CSIRT виконує центр CERT-UA. У березні 2025 року Верховна Рада ухвалила закон №11290 («Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури»). Він передбачає зокрема створення національних систем реагування на кіберінциденти та обміну інформацією про них, введення штатних посад фахівців з кібербезпеки в держорганах, визначення процесу впровадження заходів з управління ризиками, функціонування системи оцінювання кіберзахисту виключно шляхом аудиту.

Ще один законопроєкт, 12207, викликав критику фахівців і профільних організацій і був відправлений на доопрацювання.

GDPR: суворий вартовий приватності

Загальний регламент про захист даних (EU Regulation 2016/679), що застосовується з травня 2018 року, фактично став світовим законом у цій царині, оскільки є таким першим, діє екстериторіально і передбачає суворі штрафи за невиконання.

GDPR визначає три ролі: суб'єкта, контролера і оператора даних. Перший є фізичною особою, якій належать дані. Контролер задає підстави для збору даних, оператор є стороннім виконавцем, який обробляє ці дані за дорученням контролера. Наприклад, контролером може бути роботодавець, медичний заклад, інтернет-магазин, а оператором — хмарний сервіс, аутсорсинговий бухгалтер тощо. У разі витоку даних оператор сповіщає контролера, а той — контролюючі органи.

Регламент встановлює чіткі правила та умови обробки даних (**рис. 2**).

- **Законність, прозорість і чесність**: персональні дані повинні оброблятись таким чином, щоб це було справедливо по відношенню до їхнього власника. Дані повинні збиратись лише на законних підставах, без маніпуляцій щодо цілей такого збору, і так, щоб суб'єкту даних було зрозуміло, хто і навіщо це робить.
- **Обмеження цілей**: повинна бути чітка мета обробки даних з поясненням, як вони будуть використовуватись і як довго зберігатись.
- **Мінімізація даних**: збираються лише ті дані, які необхідні для досягнення результату.
- **Точність**: компанія повинна стежити, щоб дані були актуальними і релевантними, а в разі потреби — виправляти їх.
- **Сумісність**: персональні дані не можна використовувати для цілей, які не сумісні з оригінальною метою збору.
- **Обмеження зберігання**: компанія мусить встановити ліміти часу, після яких дані знищуються або переглядаються.
- **Цілісність і конфіденційність**: повинні бути відповідні організаційні кроки і технічні засоби, які захищають від неавторизованої або незаконної обробки, втрати або псування і знищення даних.



Рис. 2. Правила обробки даних згідно з GDPR (джерело: IT Labs)

Також регламент встановлює ключові зобов'язання, яких повинні дотримуватись організації під час обробки даних.

Псевдонімізація за визначенням: для кожної особи повинен створюватись псевдонім, а її персональні дані — зберігатись відокремлено від інших.

Право на забуття: на вимогу користувача компанія повинна видаляти усі його персональні дані.

Право на перенесення даних: особа повинна мати можливість отримати від контролера передані нею дані у структурованому вигляді, або ж на її запит ці дані можуть бути передані іншому контролеру.

Приватність за задумом — захист повинен бути вбудований в систему на етапі розробки (наприклад, псевдонімізація і шифрування).

Приватність за замовчуванням — максимальний рівень конфіденційності без додаткових дій з боку користувача (зокрема пов'язано з принципом мінімізації даних).

Поінформована згода: необхідна згода користувача на збір і обробку даних (звідси відповідні дисклеймери і чекбокси на сайтах і в застосунках).

Обов'язкове повідомлення про витоки даних: компанія повинна повідомити користувачів і правоохоронні органи протягом 72 годин, тож мусить вміти сама у стислі терміни виявляти ці витоки.

Нарешті, GDPR передбачає два рівні штрафів за порушення: €10 млн або 2% виручки за менш суворі (!) і €20 млн або 4% виручки — за злісні порушення. При цьому беруться до уваги такі фактори, як серйозність інциденту (рівень збитків і кількість постраждалих), чи був лихий намір, чи вжила компанія заходів для зменшення збитків і чи були превентивні заходи, чи бували раніше такі інциденти, і т.д. Найбільший в історії штраф сплатила у 2023 році компанія Meta Platforms Ireland за перенесення даних користувачів Facebook з ЄС до США.

У жовтні 2026 році Єврокомісія запропонувала низку змін до GDPR. Ключові новації — по-перше, пропонується повідомляти контролюючим органам лише про витоки, які можуть становити великий ризик, і збільшити дедлайн з 72 до 96 годин. По-друге, контролери зможуть відхиляти запити фізичних осіб на доступ до персональних даних або брати за нього плату, якщо такі запити мають ознаки зловживання. По-третє, зазначається, що дані спеціальних категорій, випадково отримані ШІ-системами, повинні вилучатись або захищатись від подальшого використання.

GDPR один для всіх

Стаття 3 Регламенту визначає, що він застосовується у випадках, коли:

- контролер або оператор знаходиться на території ЄС незалежно від того, чи здійснюється обробка даних в ЄС;
- відбувається опрацювання даних суб'єктів даних, що знаходяться в ЄС, коли це опрацювання пов'язане з постачанням товарів чи наданням послуг цим суб'єктам даних, або моніторингом поведінки суб'єктів даних, якщо вона відбувається в межах ЄС;
- якщо контролер знаходиться за межами ЄС, але в місці, де застосовується законодавство країни-члена.

На практиці це означає, що під дію GDPR потрапляють зокрема іноземні компанії, які працюють в ЄС; компанії, що не присутні в ЄС, але здійснюють туди постачання (наприклад, інтернет-магазини); компанії, що надають послуги європейському бізнесу. Якщо магазин має версії своєї сторінки мовами країн ЄС, відправляє туди товари і бере плату в євро або їхніх валютах, на нього поширюється GDPR. Тому компанії всього світу, серед них і українські, одразу почали впроваджувати заходи щодо відповідності цьому регламенту.

Україна, знову ж таки, як країна-кандидат зобов'язана поступово узгодити своє законодавство з правом ЄС. У 2024 році ВР прийняла за основу законопроєкт № 8153 «Про захист персональних даних», який вводить положення GDPR. Законопроєкт детально прописує вимоги щодо надання згоди на обробку персональних даних: наприклад, нею вважається заповнення форм і проставлення позначок на вебсайті, але не вважається автозаповнення і взагалі бездіяльність користувача. Також не вважається згодою ситуація, коли нема можливості відмовити або відкликати раніше надану згоду.

Законопроєкт передбачає впровадження принципів приватності за задумом і за замовчуванням, створення інституту відповідального за захист персональних даних, а також прописує штрафи для фізичних та юридичних осіб.

Закон ЄС про кіберстійкість

Цей закон, або регламент 2024/2847 (CRA), ухвалений два роки тому, має повністю вступити в дію у грудні 2027 року. Він стосується виробників продуктів, що містять цифрові складові. Тобто тут предметом захисту є не дані, а самі пристрої, відповідальними ж — виробники. Знову-таки, щоб такі пристрої можна було продавати в ЄС, вони повинні відповідати CRA і мати відповідну позначку.

Як зазначено в поясненні на офіційному сайті регламенту, відповідальність за безпеку продуктів відтепер покладається не на користувачів, а на організації, які виводять ці продукти на ринок. При цьому головний тягар лежить на виробниках: проєктування з огляду на безпеку, підготовка технічної документації, оцінювання відповідності і усунення вразливостей. На імпортерів покладається обов'язок ввозити лише продукцію, яка відповідає CRA, а на дистриб'юторів — слідкувати, щоб були присутні знак CE і документація.

Під «продуктами з цифровими складовими» мається на увазі, що їхнє використання включає або передбачає інтернет-з'єднання. Сюди належать побутові пристрої, корпоративне обладнання, програми для мобільних пристроїв та ПК, операційні системи тощо. Не належать: продукти, які підпадають під секторальні документи — наприклад, медичні пристрої, автомобілі і літаки. А також некомерційне ПЗ з відкритим кодом. Сферу охоплення закону визначено



Рис. 3. Основні принципи закону ЄС про кіберстійкість

навмисне широкою. Продукти поділені на класи, які визначають процедуру оцінювання відповідності. Так, більшість належить до базового класу, для якого достатньо декларації відповідності, тоді як для критичного (розумні лічильники, карти, захищені елементи) необхідна сертифікація.

Вимоги закону розділені на дві групи: властивості продуктів і зобов'язання виробників (**рис. 3**).

- **Безпека за проєктом і за замовчуванням**: продукт повинен мати безпечну конфігурацію і мінімальну поверхню атаки.
- **Відсутність відомих вразливостей**: не повинен мати відомих вад, які зловмисники можуть експлуатувати.
- **Поводження з вразливостями**: повинен бути процес їх виявлення, документування, закриття і публікації.
- **Оновлення безпеки**: безкоштовні і вчасні оновлення протягом всього періоду підтримки; п'ять років за замовчуванням або залежно від життєвого циклу. У разі виявлення проблеми оновлення повинно доставлятись без затримки.
- **Програмний каталог матеріалів (SBOM)**: перелік компонентів продукту у форматі, зручному для машинного читання.
- **Сповіщення**: повідомлення про вразливості та інциденти відповідному CSIRT або Європейській агенції з мережевої та інформаційної безпеки (ENISA). Попередження про виявлену проблему протягом 24 годин; детальний звіт, що включає інформацію про коригувальні заходи — протягом 72 годин, і фінальний звіт після закриття вразливості — протягом 14 днів.

Порушення CRA тягне за собою штраф: до €15 млн або 2,5% річної виручки. В Україні CRA на законодавчому рівні не імплементується. Проте українські виробники можуть брати участь у європейській ініціативі Digital Europe Programme, в рамках якої можна отримати до €30 тис. на реалізацію проєктів, спрямованих на виконання вимог CRA.

Інші акти

Закон про кібербезпеку (регламент 2019/881) — це основоположний акт, який встановлює рамки сертифікації продуктів і сервісів у напрямку кібербезпеки (Cybersecurity Certification Framework). Закон посилив повноваження ENISA, яка на додачу до секретаріату CSIRT'ів стала центром, що розробляє схеми сертифікації та публікує сертифікати на своєму сайті.

У січні 2026 року Єврокомісія подала проєкт оновленого закону, який ще більше розширить роль ENISA, яка буде розсилати ранні сповіщення про кіберзагрози та інциденти, в координації з Європолом та CSIRT'ами допомагати компаніям боротися зі здирницькими атаками, а також має створити всеєвропейську службу управління вразливостями. Окрім того, оновлення має на меті зменшити ризики, пов'язані з ланцюжками постачання з третіх країн, де є проблеми з кібербезпекою, шляхом запровадження гармонізованого, пропорційного підходу на основі ризиків.

Закон про цифрову операційну стійкість DORA (регламент 2022/2554), що вступив у дію в січні 2025 року, покликаний забезпечити, щоб банки, страхові компанії, інвестиційні фірми тощо (загалом класифіковано 20 типів фінансових установ) могли



Рис. 4. Вимоги DORA (джерело: Datos Insights)

витримувати ІКТ-інциденти (кібератаки, системні збої), реагувати і відновлювати свою роботу. Визначено п'ять основних напрямків стійкості: управління ІКТ-ризиками, класифікація звітування (обов'язок повідомляти про кіберінциденти), тестування стійкості (включно з пентестами), управління ризиками сторонніх постачальників і обмін інформацією про кіберзагрози між фінансовими установами (**рис. 4**). Регламент доповнюють нормативні та імплементаційні технічні стандарти, а також настанови, які розробляються європейськими наглядовими органами.

Закон про кіберсолідарність 2025/38, що набув чинності в лютому 2025 року, розроблений для забезпечення спільного реагування ЄС на кіберзагрози, передбачає створення Європейської системи сповіщень про кіберзагрози, що складається з національних і транскордонних кіберцентрів (Cyber Hubs), які за допомогою ШІ та аналітики даних зможуть виявляти загрози і обмінюватись даними про них. Механізм аналізу інцидентів кібербезпеки передбачає, що за запитом Єврокомісії або EU-CyCLONe ENISA має досліджувати серйозні кіберінциденти і готувати звіти з результатами і рекомендаціями.

Також створюється екстрений механізм кібербезпеки, який має забезпечити покращення готовності і можливостей реагування. У червні 2026 року, після того як ВР ратифікувала відповідну угоду, Україна отримала доступ до однієї зі складових цього механізму — Резерву кібербезпеки ЄС. Він надає можливість під час масованих і критичних хакерських атак залучати допомогу перевірених європейських експертів та команд швидкого реагування.

Закон про ШІ (AI Act, регламент 2024/1689), що вступив у дію в серпні 2024 року, став першим у світі документом, що регулює розвиток і використання ШІ. Регламент встановлює засновані на ризиках правила для організацій, які розробляють і впроваджують ШІ, і є частиною ширшого пакета ініціатив, покликаних уможливити створення безпечного ШІ.

Регламент встановлює 4 рівні ризику для ШІ-систем. Найвищий (неприйнятний) рівень відведений для ШІ-систем, які становлять загрозу безпеці, засобам до існування і правам людей. Беззаперечно заборонені 9 практик, які включають маніпуляції та обман, експлуатацію вразливостей, ведення соціального рейтингу, скрапинг інтернету чи матеріалів відеоспостереження для створення баз розпізнавання облич, розпізнавання емоцій на робочих місцях чи в освітніх закладах, категоризацію біометричних даних для виявлення захищених характеристик, віддалену біометричну ідентифікацію в реальному часі в громадських місцях для правоохоронних цілей, і генерацію сексуально відвертого контенту (нудифікацію).

ШІ-системи, що становлять високий ризик — це, наприклад, компоненти критичної інфраструктури, відмова яких загрожує життю і здоров'ю громадян; ШІ-системи, які використовуються на екзаменах, у наймі на роботу, визначенні кредитного рейтингу, обробці візових заяв, підготовці судових рішень, біометричній ідентифікації тощо. Починаючи з 2 грудня 2027 року такі системи підлягатимуть суворим заходам безпеки, таким як підготовка для них високоякісних навчальних даних, журналювання всієї діяльності, складання всієї необхідної документації, за якою органи влади можуть оцінювати відповідність, і належний людський контроль.

На третьому рівні існує всього лише ризик непрозорості, відтак при спілкуванні з чат-ботом людина повинна бути попереджена, що вона взаємодіє з машиною, а ШІ-згенерований контент повинен бути чітко позначений.

* * *

У своєму звіті щодо прогресу України на шляху до членства, опублікованому на початку листопада, Єврокомісія серед іншого вказала, що законодавство, узгоджене з директивою NIS2, поки що розробляється, але необхідна повна імплементація. З іншого боку, комісія відзначила співробітництво з ENISA, відкриття доступу до «Резерву кіберстійкості» і постанову НБУ, що закладає основу для імплементації DORA. Також Україна повинна розробити необхідні структури, які відповідають AI Act (проєкт закону щодо регулювання ШІ вже підготовлений).

Василь ТКАЧЕНКО, **МтБ**