Савчук С.О.

ВИМОГИ ЄС ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Чинні нормативні акти ЄС сприяли розвитку екосистеми, у якій кібербезпека визнається спільною відповідальністю урядів держав, приватних підприємств та установ ЄС. В створеній системі встановлено офіційні процеси для звітування про інциденти, співпрацю та розробку спільних стандартів безпеки. Однак ефективність цих заходів залежить від ресурсів і можливостей, доступних окремим державам-членам, ступеня впровадження рекомендованих практик приватним сектором і глобального характеру кіберзагроз. Хоча законодавство ЄС, безсумнівно, підвищило базові заходи безпеки, залишаються значні прогалини в тому, наскільки ефективно ці заходи перетворюються на довгострокове зниження ризику, що підкреслює необхідність постійного вдосконалення як механізмів політики, так і оперативних можливостей.

Україна, прагнучи інтегруватися до європейського правового та політичного простору, стикається з низкою викликів у сфері кібербезпеки. Відповідно до вимог ЄС та практик його держав-членів, українське законодавство потребує наближення як у технічних аспектах (встановлення чітких стандартів безпеки, процедури інцидент-репортингу), так і в організаційній структурі (удосконалення координаційних органів, розподілу повноважень та відповідальності). Серед першочергових змін, які необхідні для гармонізації з європейською системою, можна виокремити кілька напрямів.

Перш за все, вкрай важливо ухвалити чи оновити законодавчу базу, яка встановлює вимоги до операторів критичної інфраструктури, а також до компаній, що надають цифрові послуги. Директива ЄС щодо безпеки мереж і інформаційних систем (NIS/NIS2) передбачає обов'язкове визначення «операторів основних послуг» і «важливих суб'єктів». Для України це означає потребу внести зміни до вже існуючих законодавчих актів або підготувати нові, що чітко формалізують критерії, за якими обираються критичні об'єкти, та встановити для них вимоги з управління ризиками й реагування на інциденти. Без формалізації цих вимог у національному праві важко досягти єдиного підходу в масштабах усієї держави.

Крім того, необхідно запровадити системи обов'язкового звітування про кіберінциденти. У країнах ЄС оператори essential services і digital service providers мають визначені строки та процедури інформування національних компетентних органів про інциденти, що можуть негативно впливати на безпеку надаваних послуг або на нормальну роботу критичної інфраструктури. Для України актуально розробити чіткий механізм, де буде вказано, хто й протягом якого часу зобов'язаний повідомляти про інциденти, як відбуватиметься їхня класифікація та які санкції застосовуватимуться в разі недотримання вимог. Такий підхід дасть змогу підвищити рівень прозорості та оперативності, з якими компанії і державні структури реагують на кібератаки.

Наступним важливим моментом є створення або посилення незалежного координаційного органу, відповідального за кібербезпеку на державному рівні. У контексті європейської інтеграції України потрібно забезпечити, аби цей орган мав чітко прописані функції щодо моніторингу, контролю, методичної підтримки й міжнародної взаємодії. У низці країн ЄС такими органами виступають національні CERT або спеціалізовані агентства, що підтримують зв'язок із ENISA (Агентство Європейського Союзу з кібербезпеки), а також беруть участь у спільних вправах і кризових координаційних ініціативах (наприклад, EU-CyCLONe). Участь України в подібних тренуваннях і обмін

досвідом з європейськими інституціями допомагають інтегрувати національну систему кіберзахисту в загальноєвропейський механізм реагування.

Окремо варто наголосити на важливості запровадження системи сертифікації та стандартів кібербезпеки, сумісних з EU Cybersecurity Act. На рівні ЄС поступово формується підхід до добровільної чи обов'язкової сертифікації ІТ-продуктів і цифрових послуг. Для України доречно передбачити механізм, який у перспективі дозволить вітчизняним виробникам та постачальникам послуг отримувати європейські сертифікати і виходити на європейський ринок без додаткових бар'єрів. Водночас це підвищить конкурентоспроможність українських компаній та стимулюватиме їх покращувати рівень безпеки власної продукції.

Не менш суттєвою є сфера захисту персональних даних. Загальний регламент ЄС із захисту даних (GDPR) хоч і не є виключно кібербезпековим, однак вимагає дотримання високих стандартів захисту інформації. Україна вже робить кроки до наближення свого законодавства про персональні дані до європейських стандартів, але задля повноцінної інтеграції потрібно вдосконалити підходи до контролю, інцидент-менеджменту та штрафних санкцій за порушення. Це дасть змогу уникнути суперечностей між різними аспектами регулювання (наприклад, інцидент-репортинг у рамках кібербезпеки та повідомлення про витік даних за нормами GDPR) і зробить систему більш цілісною.

У контексті реформування законодавства Україна також потребує підтримки в розвитку інституційної спроможності. Прийняття нових законів чи оновлених норм саме по собі не вирішить проблему, якщо на державному і приватному рівнях бракуватиме кваліфікованих кадрів або дієвих механізмів реалізації. Тому варто зосередитися на формуванні стратегії кібербезпеки, що передбачатиме підготовку спеціалістів, а також залучення необхідних фінансових та організаційних ресурсів. Окрему роль відіграє освіта для державного сектора і керівників приватних компаній, оскільки саме вони приймають стратегічні рішення щодо інформаційної безпеки та реагування на загрози.