МІНІСТЕРСТВО ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УКРАЇНИ

Мінцифри

вул. Ділова, 24, м. Київ, 03150, тел. (044) 207-17-30

E-mail: hello@thedigital.gov.ua, сайт: www.thedigital.gov.ua, код згідно з ЄДРПОУ 43220851

Комітет Верховної Ради України
з питань цифрової трансформації

Міністерство цифрової трансформації відповідно до листа Комітету Верховної Ради України з питань цифрової трансформації від 24.07.2025 № 04-33/03-2025/172801 опрацювало в межах компетенції проект Закону України «Про заборону використання та розповсюдження ворожих програмних продуктів та ворожих засобів інформатизації» (реєстр. № 13505 від 18.07.2025) (далі – проект Закону) та повідомляє.

У проекті Закону застосовано підхід, що ґрунтується на забороні використання продуктів за політично визначеною ознакою («ворожі програмні продукти» та «ворожі засоби інформатизації»).

Водночас, у проекті Закону визначення понять «ворожі програмні продукти» та «ворожі засоби інформатизації» не містять достатньої кількості критеріїв, що є необхідною вимогою для правової визначеності та унеможливлює неоднозначне тлумачення цих термінів. Відсутність таких критеріїв створює правові ризики та суперечить принципам законності і прозорості.

Пропонується змінити зазначений підхід на ризик-орієнтований та замінити терміни «ворожі програмні продукти» та «ворожі засоби інформатизації» на технічно нейтральне визначення «високоризикові програмні продукти» та «високоризикові засоби інформатизації». Такий підхід дозволить здійснювати оцінку загроз на основі сукупності об’єктивних критеріїв: технічних, корпоративних, операційних та пов’язаних із ланцюгом постачання, що забезпечить гнучкість та довгострокову стійкість механізму.

До того ж, критерії, визначені у статтях 3 та 4 проекту Закону, зосереджені переважно на походженні продукту та його зв’язку з державою-агресором. Проте зазначене формулювання не визначає механізм визначення таких фактів та застосування, що ускладнює практичну реалізацію норми та потребує доопрацювання.

Також відсутній детальний аналіз можливих економічних наслідків, що ускладнює формування обґрунтованих рішень і може вплинути на

конкурентоспроможність вітчизняного ринку, інвестиційний клімат та стабільність функціонування об’єктів критичної інфраструктури.

Статтею 5 проекту Закону передбачаються норми щодо заборони використання та розповсюдження ворожих програмних продуктів та ворожих засобів інформатизації.

Пунктом 2 частини другої статті 5 проекту Закону пропонується на період до 1 січня 2030 року заборонити використання при створенні (модернізації, модифікації, розвитку), перетворенні, припиненні, адміністрування та забезпечення функціонування засобів інформатизації, управління життєвим циклом таких засобів інформатизації, здійснення заходів із кібербезпеки, створенні *комплексних систем захисту інформації*, систем управління інформаційною безпекою з підтвердженою відповідністю, власником (розпорядником) яких є орган державної влади, у тому числі й тих заходів, що здійснюються за рахунок коштів міжнародної технічної допомоги, програмних продуктів, засобів інформатизації, записи про яких наявні у переліках програмних продуктів та засобів інформатизації, віднесених до ворожих програмних продуктів, ворожих засобів інформатизації затверджених Кабінетом Міністрів України або таких, що відповідно до статті 3 та 4 цього Закону, підпадають під критерії ворожих програмних продуктів та/або ворожих засобів інформатизації відповідно.

Звертаємо увагу, що Законом України від 27.03.2025№ 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури» внесено зміни до статті 8 Закону.

Так, новою редакцією цієї статті Закону передбачено, що умови обробки інформації в системі, об’єкті критичної інформаційної інфраструктури визначаються власником або розпорядником відповідної системи з урахуванням вимог щодо захисту інформації, визначених законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, у системах, об’єктах критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, мають оброблятися в авторизованих системах з безпеки або шляхом отримання сертифіката відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності.

Авторизація з безпеки систем, об’єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, а також підтвердження дотримання вимог з безпеки щодо таких систем, об’єктів критичної інформаційної інфраструктури протягом їх життєвого циклу здійснюються в порядку, встановленому Кабінетом Міністрів України.

Складовою такого порядку авторизації з безпеки має бути встановлення повідомного (декларативного) принципу щодо прийняття власником або розпорядником системи, об’єкта критичної інформаційної інфраструктури (крім тих, в

яких обробляється інформація, що становить державну таємницю) рішення про здійснення авторизації з безпеки з урахуванням відповідних профілів безпеки, а також строки та порядок підтвердження дотримання вимог відповідно до базового, цільового та галузевого (за наявності) профілів безпеки протягом життєвого циклу відповідної системи, об'єкта критичної інформаційної інфраструктури.

Підтвердження відповідності стандарту інформаційної безпеки за результатами процедури з оцінки відповідності національним стандартам України здійснюється органом з оцінки відповідності, який акредитовано національним органом України з акредитації чи національним органом з акредитації іноземної держави, якщо національний орган України з акредитації та національний орган з акредитації відповідної держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності.

Враховуючи зазначене, пропонуємо у пункті 2 частини другої статті 5 проекту Закону словосполучення «комплексних систем захисту інформації» виключити.

Абзацом першим частини другої статті 3 проекту Закону передбачено, що Кабінет Міністрів України *за поданням центрального органу виконавчої влади, що забезпечує формування та реалізує державну політику у сфері розвитку національних електронних інформаційних ресурсів та інтероперабельності* та Державної служби спеціального зв'язку та захисту інформації відповідно до критеріїв визначених у частині першій цієї статті, затверджує та оприлюднює *перелік програмних продуктів, віднесених до ворожих програмних продуктів*.

При цьому, відповідно до абзацу третього частини другої статті 3 проекту Закону перелік програмних продуктів, віднесених до ворожих програмних продуктів ведеться Державною службою спеціального зв'язку та захисту інформації у складі відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання.

Звертаємо увагу, що відповідно до абзаців другого та третього частини четвертої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» порядок формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання затверджується Кабінетом Міністрів України, а повноваження щодо забезпечення формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання покладаються на Державну службу спеціального зв'язку та захисту інформації України.

Таким чином, норми, запропоновані у абзаці першому частини другої статті 3 проекту Закону щодо відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання, фактично дублюють норми Закону України «Про основні засади забезпечення кібербезпеки України».

При цьому, зважаючи на повноваження Мінцифри та Держспецзв'язку, а також на те, що на законодавчому рівні вже закріплено обов'язок забезпечення формування та ведення відкритого переліку забороненого до використання програмного

забезпечення та комунікаційного (мережевого) обладнання за Держспецзв'язку, залучення центрального органу виконавчої влади, що забезпечує формування та реалізує державну політику у сфері розвитку національних електронних інформаційних ресурсів та інтероперабельності до подання Кабінету Міністрів України переліку програмних продуктів, віднесених до ворожих програмних продуктів є не доцільним.

Враховуючи вищезазначене, а також те, що норми про затвердження, оприлюднення та перегляд переліку програмних продуктів, віднесених до ворожих 5 програмних продуктів, доцільно визначати у порядку формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання, затвердженого Кабінетом Міністрів України відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», *рекомендуємо абзаци перший та другий частини другої статті 3 проекту Закону виключити*.

Перший заступник Міністра **Олексій ВИСКУБ**

Любов Потейчук poteichuk@thedigital.gov.ua