ЗАУВАЖЕННЯ І ПРОПОЗИЦІЇ

Служби безпеки України до проєкту Закону України “Про заборону використання та розповсюдження ворожих програмних продуктів та ворожих засобів інформатизації” (реєстр. № 13505 від 18.07.2025; далі – законопроєкт)

1. Частиною 2 статті 2 законопроєкту передбачено, що особливості організаційних засад використання програмних продуктів та засобів інформатизації, які відповідно до статей 3 та 4 цього Закону підпадають під критерії ворожих програмних продуктів та ворожих засобів інформатизації, суб’єктами господарювання, які надають банківські послуги, фінансові та/або супровідні послуги, платіжні послуги (крім операторів поштового зв’язку), державне регулювання та нагляд за діяльністю яких здійснює Національний банк, визначатимуться Національним банком України.

Вказана норма, на наш погляд, не має правової визначеності, оскільки не зрозуміло, що таке організаційні засади використання ворожих програмних продуктів та ворожих засобів інформатизації.

Також необхідно враховувати сферу дії майбутнього Закону (п. 2 ч. 1 ст. 2), який встановлює заборону розповсюдження та використання програмних продуктів, засобів інформатизації, що відповідно до критеріїв, визначених цим Законом, є ворожими програмними продуктами, ворожими засобами інформатизації.

Стаття 5 законопроєкту чітко встановлює заборону використання та розповсюдження ворожих програмних продуктів та ворожих засобів інформатизації та визначає період з 1 січня 2030 року заборони на продаж, використання та розповсюдження на території України програмних продуктів, засобів інформатизації, запис про які міститься у Переліку програмних продуктів, віднесених до ворожих програмних продуктів, або Переліку засобів інформатизації, віднесених до ворожих програмних продуктів відповідно.

Фактично до 1 січня 2030 року встановлюється перехідний період, необхідний для вжиття невідкладних заходів з переходу (виведення з використання) програмних продуктів, засобів інформатизації, запис про які міститься у Переліку програмних продуктів, віднесених до ворожих програмних продуктів, або Переліку засобів інформатизації, віднесених до ворожих програмних продуктів. На цей перехідний період також забороняється їх використання при створенні, перетворенні, припиненні, адмініструванні та забезпечення функціонування засобів інформатизації, здійснення заходів з кібербезпеки, створенні комплексних систем захисту інформації, систем управління інформаційною безпекою з підтвердженою відповідністю, а також забороняється запроваджувати заходи щодо застосування (модернізації) технічних засобів електронних комунікацій та кінцевого (термінального) обладнання при розгортанні високошвидкісних мереж широкосмугового доступу (у тому числі при розгортанні рухомого (мобільного) зв’язку п’ятого та наступних поколінь) з використанням таких ворожих програмних продуктів та ворожих засобів інформатизації.

Враховуючи викладене, частину 2 статті 2 законопроєкту пропонуємо викласти у такій редакції:

“Особливості використання програмних продуктів та засобів інформатизації, які відповідно до статей 3 та 4 цього Закону підпадають під критерії ворожих програмних продуктів та ворожих засобів інформатизації, суб’єктами господарювання, які надають банківські послуги, фінансові та/або супровідні послуги, платіжні послуги (крім операторів поштового зв’язку), державне регулювання та нагляд за діяльністю яких здійснює Національний банк, до 1 січня 2030 року визначаються Національним банком України.”.

2. Відповідно до статті 5 законопроєкту на користувачів/розповсюджувачів програмних продуктів та інших засобів інформатизації покладатиметься обов’язок щодо здійснення перевірок усіх наявних засобів на відповідність критеріям, викладеним у статтях 3, 4 законопроєкту, а також здійснювати надалі такі перевірки щодо кожного програмного продукту та іншого засобу інформатизації, які плануються до використання/розповсюдження.

У зв’язку з цим слід зазначити, що однією з базових засад юриспруденції, покладених в основу правового регулювання, є принцип “що не заборонено, те дозволено”, який означає, що прямо не заборонені законом дії є допустимими.

У випадках необхідності обмеження використання певних предметів на території країни, воно реалізується шляхом створення правовою державою переліків заборонених до обігу товарів, продуктів тощо (т.зв. “чорних списків”), на які в обов’язковому порядку повинні орієнтуватися усі місцеві та іноземні фізичні та юридичні особи. Відповідні засади закладені також у частині першій ст. 19 Конституції України.

Аналіз наповнення зазначених у статтях 3, 4 законопроєкту критеріїв (загалом по програмних продуктах та інших засобах інформатизації – 9 критеріїв, майже кожен з яких містить декілька умов) дозволяє дійти висновку щодо складності однозначного визначення відповідності програмних продуктів та інших засобів інформатизації вимогам майбутнього закону. Кожна перевірка фактично вимагає проведення окремого дослідження із залученням OSINT та IT-спеціалістів, юристів у сфері авторського та міжнародного права та інших фахівців.

У разі виникнення сумнівів щодо належності програмних продуктів та інших засобів інформатизації до ворожих, суб’єкт господарювання повинен ініціювати проведення державної експертизи, яка також потребуватиме певного часу та, ймовірно, фінансових витрат.

Таким чином, запропонований статтею 5 проєкту механізм, який на перехідний період (до 01.01.2030) встановлює обов’язок суб’єктів щодо здійснення перевірок усіх наявних засобів на відповідність критеріям, викладеним у статтях 3, 4 законопроєкту, а також здійснення надалі таких перевірок щодо кожного програмного продукту та іншого засобу інформатизації, які плануються до використання/розповсюдження, та створює в

майбутньому передумови до оскарження відповідних рішень про притягнення суб’єкта до відповідальності в судовому порядку.

З огляду на викладене пропонується в статті 5 законопроєкту обмежити обов’язок суб’єктів з проведення перевірок програмних продуктів та інших засобів інформатизації виключно зобов’язанням їх порівняння із публічними списками ворожих програмних продуктів та інших засобів інформатизації, розміщеними на ресурсах Державної служби спеціального зв’язку та захисту інформації.

3. Законопроєктом (пункт 1 частини другої статті 7) передбачено внесення змін до Закону України “Про Службу безпеки України” (доповнення статті 24 новим пунктом 25) у частині віднесення до обов’язків СБУ забезпечення моніторингу та надання пропозицій щодо внесення змін і доповнень до Переліку програмних продуктів, віднесених до ворожих програмних продуктів, та Переліку засобів інформатизації, віднесених до ворожих засобів інформатизації, відповідно до критеріїв, визначених у частині першій статті 3 та частині першій статті 4 Закону України “Про заборону використання та розповсюдження ворожих програмних продуктів та ворожих засобів інформатизації”, що заборонені до використання у сферах національної безпеки, громадської безпеки, оборони чи правоохоронної діяльності, включаючи розслідування, виявлення та розслідування кримінальних правопорушень.

У зв’язку з цим слід зазначити, що відповідно до пункту 3 частини 2 статті 8 Закону України “Про основні засади забезпечення кібербезпеки України” Служба безпеки України здійснює заходи із запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти основ національної безпеки України, миру і безпеки людства, а також кримінальних правопорушень терористичної спрямованості, що вчиняються у кіберпросторі або з його використанням; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом, кібердиверсіями та кібершпигунством; координує діяльність суб’єктів забезпечення кібербезпеки щодо протидії кібершпигунству, кібертероризму, кібердиверсіям; негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки.

Враховуючи зазначене, у межах визначеної законодавством компетенції Служба безпеки України має здійснювати заходи з виявлення ворожих програмних продуктів, ворожих засобів інформатизації та вносити обов’язкові для розгляду пропозиції щодо внесення змін і доповнень до Переліку програмних продуктів, віднесених до ворожих програмних продуктів, та

Переліку засобів інформатизації, віднесених до ворожих засобів інформатизації.

З урахуванням викладеного новий пункт 25 частини першої ст. 24 Закону України “Про Службу безпеки України” пропонуємо викласти у такій редакції:

“25) у межах визначеної законодавством компетенції здійснювати заходи з виявлення ворожих програмних продуктів, ворожих засобів інформатизації та вносити обов’язкові для розгляду пропозиції щодо внесення змін і доповнень до Переліку програмних продуктів, віднесених до ворожих програмних продуктів, та Переліку засобів інформатизації, віднесених до ворожих засобів інформатизації, відповідно до Закону України “Про заборону використання та розповсюдження ворожих програмних продуктів та ворожих засобів інформації”, що заборонені до використання у сферах національної безпеки, громадської безпеки, оборони чи правоохоронної діяльності.”.

4. Відповідно до пункту 3 частини другої статті 8 Закону України “Про основні засади забезпечення кібербезпеки України” Служба безпеки України здійснює заходи із запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти основ національної безпеки України, миру і безпеки людства, а також кримінальних правопорушень терористичної спрямованості, що вчиняються у кіберпросторі або з його використанням; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом, кібердиверсіями та кібершпигунством; координує діяльність суб’єктів забезпечення кібербезпеки щодо протидії кібершпигунству, кібертероризму, кібердиверсіям; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберзагрози у сфері державної безпеки.

Служба безпеки України є спеціально уповноваженим органом державної влади у сфері контррозвідувальної діяльності (частина перша ст. 5 Закону України “Про контррозвідувальну діяльність”).

З урахуванням викладеного та беручи до уваги, що відповідно до частини четвертої статті 2 законопроєкту дія майбутнього Закону не поширюватиметься на діяльність суб’єктів, визначених статтею 5 Закону України “Про розвідку”, пропонуємо частину третю статті 2 законопроєкту викласти у такій редакції:

“3. Особливості використання програмних продуктів та засобів інформатизації, які відповідно до статей 3 та 4 цього Закону підпадають під критерії ворожих програмних продуктів та ворожих засобів інформатизації, під час здійснення контррозвідувальної діяльності визначаються Службою безпеки України.”.

5. Стаття 6 законопроєкту визначає відповідальність за порушення цього Закону. Передбачено, що фінансові санкції будуть застосовуватися лише до суб’єктів господарювання, які здійснюють продаж, використання та/або

розповсюдження програмних продуктів та засобів інформатизації, віднесених до ворожих.

Слід звернути увагу на те, що законопроєкт не встановлює відповідальності посадових осіб органів влади Автономної Республіки Крим, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, державних підприємств, установ та організацій, суб'єктів владних повноважень та інших суб'єктів, яким делеговані такі повноваження, а також власників та операторів критичної інфраструктури за порушення майбутнього Закону.

Враховуючи зазначене, законопроєкт необхідно доповнити нормою про встановлення відповідальності за порушення майбутнього Закону для посадових осіб суб'єктів, зазначених у пункті 1 частини 2 статті 5 законопроєкту.