Щодо використання санаційного та ворожого програмного забезпечення 2026.

IT · https://nasu.com.ua/mdata/shhodo-vykorystannya-sanaczijnogo-ta-vorozhogo-programnogo-zabezpechennya-2026/

Про використання програмного забезпечення

(Роз’яснення без звернення)

Відповідно до Закону України “Про Національний банк України” Національний банк України (далі – Національний банк) у межах своїх повноважень здійснює державне регулювання та нагляд за діяльністю небанківських фінансових установ, реалізує державну політику у сфері захисту критичної інфраструктури у відповідній частині, а також визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки в небанківських фінансових установах.

Стратегією розвитку фінансового сектору, прийнятою Національним банком, передбачено запровадження принципу нульової толерантності до використання програмного забезпечення російського та білоруського походження на фінансовому ринку України.

Запровадження цього принципу зумовлене необхідністю комплексного управління системними ризиками на фінансовому ринку України. Такий підхід спрямований не лише на зниження операційних, безпекових та ІТ-ризиків, а й на мінімізацію правових, економічних, репутаційних і стратегічних наслідків, пов’язаних із залежністю від програмних продуктів, розроблених або контрольованих у юрисдикціях держави-агресора та держави, що її підтримує.

В умовах збройної агресії проти України використання такого програмного забезпечення створює додаткові фактори вразливості для стабільності фінансового ринку та не узгоджується з державними підходами до захисту інформаційної інфраструктури. У зв’язку з цим принцип нульової толерантності розглядається Національним банком як превентивний інструмент підвищення стійкості фінансового сектору та забезпечення його довгострокової операційної надійності.

Використання програмного забезпечення російського та/або білоруського походження може призводити до реалізації суттєвих ризиків, зокрема порушення безперервності надання фінансових послуг, втрати або модифікації інформації, несанкціонованого доступу до даних, а також формування технологічної залежності від обмеженого кола постачальників. Крім того, використання програмного забезпечення російського походження має фінансово-економічний вимір ризику, оскільки опосередковано сприяє формуванню доходів суб'єктів господарювання, пов'язаних з державою-агресором, зокрема через сплату ліцензійних платежів, вартості супроводу, оновлень та інших платежів. Зазначене, зі свого боку, може призводити до непрямого фінансування державиагресора та не узгоджується із загальнодержавною політикою із заборони економічної взаємодії з такими суб'єктами.

З метою мінімізації зазначених вище ризиків Національний банк раніше надавав учасникам ринку небанківських фінансових послуг відповідні рекомендації в листах від 22.01.2024 № 21-0006/5283 та від 30.04.2025 № 210007/33157, зокрема щодо аналізу використовуваного програмного забезпечення, оцінки наявності альтернативних рішень та планування заходів із заміни таких продуктів.

Крім того, Національний банк інформував про заходи, що вживаються на державному рівні, зокрема про застосування санкцій до окремих розробників програмного забезпечення та оновлення законодавства у відповідних сферах. Такі заходи є складовою реалізації послідовної державної політики у сферах, що підлягають державному регулюванню та пов'язані з функціонуванням критичної інформаційної інфраструктури.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" у зазначених сферах використання програмного забезпечення та комунікаційного (мережевого) обладнання допускається, якщо немає відповідних продуктів у відкритому переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання, який формується і ведеться Державною службою спеціального зв'язку та захисту інформації України (далі – Держспецзв'язок України)

Зокрема, до програмного забезпечення, використання якого заборонено відповідно до цього відкритого переліку, належать, серед іншого, програмні продукти сімейств "1С" та "BAS". Незважаючи на формальні зміни у структурі прав інтелектуальної власності, найменуванні правовласників або використання інших механізмів корпоративного та договірного відокремлення, вбачається, що програмні продукти сімейства "1С" та "BAS" зберігають зв'язок із юрисдикцією держави-агресора з огляду на походження програмного

коду, історію розроблення, модель розвитку та супроводження, а також наявні організаційні, технологічні або економічні залежності.

З огляду на практичне застосування зазначених вище підходів державних органів у регульованих секторах інформаційної інфраструктури та державних інформаційних ресурсів дотримання аналогічних принципів під час вибору програмного забезпечення є обґрунтованим також для діяльності суб’єктів на ринку небанківських фінансових послуг і розглядається як важлива складова забезпечення операційної стійкості, фінансової надійності, управління системними ризиками та інформаційної безпеки.

У зв’язку з цим очікується, що небанківські фінансові установи розглянуть як пріоритетне питання проведення інвентаризації програмного забезпечення, що використовується в їхній діяльності, оцінки наявності програмних продуктів, включених до опублікованого Держспецзв’язку України переліку забороненого до використання програмного забезпечення, аналізу можливості застосування альтернативних рішень, а також визначення заходів і орієнтовних строків переходу на програмне забезпечення інших виробників з урахуванням безперервності діяльності та пропорційності витрат.

Зі свого боку Національний банк у межах визначених законодавством повноважень враховуватиме рівень дотримання зазначених вище підходів під час здійснення регуляторної діяльності і наглядових процедур та під час формування подальших регуляторних ініціатив щодо використання програмного забезпечення на фінансовому ринку.

Лист НБУ № 21-0009/17019 від 26.02.2026