Аналіз
положень Указу Президента України від 13 лютого 2017 року №32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»

І. Пунктом 1 части 2 рішення РНБО поставлено завдання Кабінету Міністрів України:

1) **невідкладно** забезпечити підготовку законодавчих пропозицій стосовно:

визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та власників (розпорядників) об'єктів критичної інформаційної інфраструктури,

механізму взаємодії між ними під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків,

запровадження відповідальності за порушення вимог щодо кіберзахисту відповідних об'єктів та внести в установленому порядку на розгляд Верховної Ради України відповідний законопроект.

Звертаємо увагу, що на цей час у ВРУ готується до другого читання проект Закону про основні засади забезпечення кібербезпеки України (р.№2126а http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657), яким зокрема передбачається визначити вимоги, механізми та відповідальність, в опрацюванні якого беруть участь представники КМУ та відповідних ЦОВВ. Створення альтернативного проекту потребуватиме додаткових людських ресурсів та часу, що призведе до дублювання дій та розпорошення сил та ресурсів.

Крім того, 23 серпня 2016 року Кабінетом Міністрів України прийнято постанову № 563 (http://zakon2.rada.gov.ua/laws/show/563-2016-%D0%BF/print1443429249820555), якою затверджено Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави (далі - Порядок). Порядком затверджено термін «*об’єкти критичної інфраструктури - підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров’я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення*».

Порівняння завдання Президента та визначення стає незрозумілим, що є предметом кіберзахисту: чи це *підприємства та установи*, чи *інформаційно-телекомунікаційні систем*, і чи зможуть МСП бути віднесеними до об’єктів критичної інфраструктури.

При цьому завдання КМУ на приведення своїх НПА до визначених Президентом вимог не встановлено.

ІІ. Пунктом 2 частини 2 рішення РНБО поставлено завдання Кабінету Міністрів України:

2) забезпечити у місячний строк виконання завдання, передбаченого пунктом 2 Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, та вжити в установленому порядку заходів щодо притягнення до відповідальності осіб, які не забезпечили виконання такого завдання у визначений зазначеною постановою строк.

Звертаємо увагу, що пунктом 8 Порядку визначені негативні наслідки, з урахуванням яких органи формують пропозиції до переліку, проте до цього часу не сформовано критеріїв щодо визначення їх оцінки.

ІІІ. Підпунктом в) пункту 3 частини 2 рішення РНБО поставлено завдання Кабінету Міністрів України подати на розгляд Верховної Ради України законопроекти щодо імплементації положень Конвенції про кіберзлочинність (далі - Конвенція) передбачивши, зокрема:

- надання правоохоронним органам повноважень (**без рішення суду!**) щодо внесення обов'язкових до виконання приписів власникам комп'ютерних даних (операторам та провайдерам телекомунікацій, іншим юридичним і фізичним особам) про термінове фіксування та зберігання комп'ютерних даних, необхідних для розкриття злочину, на строк до 90 днів із можливістю продовження такого строку до 3 років, а також унормування порядку внесення зазначених приписів;

- установлення вимог щодо надання операторам та провайдерам телекомунікацій на вимогу правоохоронних органів (**без рішення суду!**) інформації, необхідної для ідентифікації постачальників послуг і маршруту, яким було передано інформацію;

- запровадження блокування (обмеження) за рішенням суду операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу).

Статтею 16 Конвенції дійсно передбачається можливість зберігання комп'ютерних даних, але лише з метою розкриття конкретних кримінальних розслідувань або переслідувань (пункт 1 статті 14 Конвенції).

При цьому, у статті 16 Конвенції мова йде про право видавати ордери на термінове збереження комп'ютерних даних протягом такого періоду, який буде необхідним для того, щоб компетентні органи мали можливість отримати дозвіл на їхнє розкриття, з максимальним терміном у 90 днів.

Мета ордеру - отримати дозвіл на розкриття комп'ютерних даних, тому пропозиція «продовження такого строку до 3 років» **не відповідає змісту Концепції**.

Також **не відповідає** змісту Концепції вимога **про термінове фіксування**.

При цьому згідно Конвенції, кожна Сторона забезпечує, щоб встановлення, імплементація і застосування повноважень і процедур, регулювалися умовами і запобіжними заходами, передбаченими її внутрішньодержавним правом, які б забезпечували адекватний захист прав і свобод людини, включаючи права, що випливають відповідних міжнародних угод з прав людини, і які б включали в себе принцип пропорційності (пункт 1 стаття 15 Конвенції).

Такі умови і запобіжні заходи включатимуть, судовий або інший незалежний нагляд, підстави, які виправдовують застосування, і обмеження сфери застосування і терміну таких повноважень або процедур» (пункт 2 ст. 15 Конвенції). При цьому, запровадження блокування **не передбачено** положеннями Конвенції.

Вищезазначені новації не базуються на принципі верховенства права, не відповідають Конституції України та положенням законодавства України та ЄС, несуть в собі потенційні загрози правової невизначеності та зловживань з боку правоохоронних органів (як це є сьогодні коли за надуманими підставами боротьби з нібито поширення дитячої порнографії або порушень прав

інтелектуальної власності тощо блокуються ресурси та вилучаються сервера), **а тому не можуть бути втілені в життя.**

Звертаємо увагу, що новацій стосовно блокування, а також без рішення суду безперешкодно отримувати доступ до будь-якої інформації, зокрема щодо споживача, телекомунікаційних послуг, повторюють аналогічні норми «диктаторського закону» 16-го січня 2014 року, прийнятих злочинною владою та скасованих завдяки Революції Гідності.

Звертаємо увагу, що ООН визнала право на доступ до Інтернету одним з невід'ємних прав людини. Поширення інформації в мережі Інтернет має бути максимально вільним, обмежуючись лише тими ситуаціями, коли воно може призвести до порушення чиїх-небудь прав, забезпечувати повсюдний доступ до мережі та співробітництво з ресурсами і організаціями, що сприяють вираженню громадської думки через Інтернет.

Новації стосовно обмеження доступу абонентів до ресурсів мережі Інтернет без рішення суду, є порушення норм Закону України «Про телекомунікації» щодо вільного доступу, загально прийнятої системи судочинства України, зокрема презумпції невинності, а також не узгоджуються зі статтею 12 Директиви 2000/31/ЄС Європейського парламенту та Ради «Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку» («Директива про електронну комерцію»).

Звертаємо увагу, що в Європейському Союзі зберігання комп'ютерних даних в правоохоронних цілях передбачалося Директивою 2006/24/ЕС щодо збереження персональних даних з метою розслідування злочинів.

Суд Європейського Союзу (Суд справедливості ЄС) у рішенні від 8 квітня 2014 року визнав Директиву 2006/24/ЕС недійсною, оскільки її положення:

- тягнуть за собою широкомасштабні та особливо серйозні порушення фундаментальних прав – права на захист персональних даних і права на повагу до приватного життя;

- не окреслюють, як з процесуальної так і матеріальної точок зору, поняття «серйозного злочину»;

- не встановлюють чіткі і точні правила щодо регулювання ступеню втручання у фундаментальні права;

- не створюють достатніх гарантій для забезпечення ефективного захисту збережених персональних даних від ризиків незаконного використання, доступу та використання цих даних;

- не забезпечують застосування достатньо високого рівня захисту і безпеки з боку провайдерів шляхом впровадження технічних та організаційних заходів;

- період збереження персональних даних (від 6 до 24 місяців) занадто загальний і має бути адаптований до конкретних цілей (злочинів, з якими необхідно боротися);

- не забезпечується незворотне видалення персональних даних наприкінці періоду збереження даних.

На підставі позиції Суду Європейського Союзу у більшості країн Європейського Союзу були визнанні неконституційними закони, прийняті на виконання вищезазначеної Директиви.

Таким чином, спроба надати правоохоронним органам повноважень **без рішення суду** контролювати інформацію до 3 років, зокрема для ідентифікації послуг і маршрутів тощо, **більш нагадує на створення системи тотального контролю за громадянами.**

Такий підхід не відповідає рішенням Верховної Рада України, яка ще 3 липня 2014 року визнала особливе місце у переліку пріоритетів стратегічного розвитку України захист прав, свобод і безпеки громадян в інформаційній сфері, відмова від ідей тотального контролю (постанова ВРУ №1565-VII).

Крім того, нововведення передбачають необхідність здійснення операторами непомірних витрат на придбання та встановлення дорогих спеціальних технічних засобів, що насамперед негативно вплине на господарську діяльність представників малого та середнього бізнесу. Оскільки більшість з них таки витрати просто не винесуть і повинні будуть припинити свою діяльність, а це десятки тисяч робочих місць.

До того ж, **запропоновані законодавчі зміни створять додаткові перешкоди для вільного доступу до ринку** телекомунікацій нових операторів, оскільки це збільшить розмір потрібних для цього початкових інвестицій та призведе до штучної монополізації телекомунікаційного ринку окремими великими компаніями.

Спроба встановити такі вимоги рішенням Президента **не відповідає Конституції України, згідно з якою у парламентсько-президентській республіки повноваження визначати засади внутрішньої і зовнішньої політики належать парламенту, а не Президенту.**

IV. Підпунктом в) пункту 4 частини 2 рішення РНБО поставлено завдання Кабінету Міністрів України забезпечити створення єдиних основного та резервного захищених дата-центрів збереження інформації і відомостей державних електронних інформаційних ресурсів, а **пунктом 7 частини 2 -** забезпечити протягом року створення та розгортання національної телекомунікаційної мережі, а також підключення до неї інформаційно-телекомунікаційних систем органів державної влади, інших державних органів, підприємств, установ та організацій державної форми власності.

Такій підхід не відповідає вимогам Указу Президента України від 24.09.2001 № 891/2001 та постанови Кабінету Міністрів України від 12.04.2002 р. № 522, якими визначено, що **забезпечення передачі** органам виконавчої влади, іншим державним органам і підприємствам, установам та організаціям, які одержують, обробляють, поширюють і зберігають державні інформаційні ресурси, даних глобальними мережами, **здійснюється визначеними на конкурсних засадах відповідно до закону підприємствами — операторами**, що здатні забезпечувати таку передачу з додержанням установлених законодавством вимог щодо захисту інформації та мають ліцензії на виконання робіт з технічного та криптографічного захисту інформації.

Пропозиції суперечать положенням Стратегії національної безпеки України, затвердженої Указом Президента України від 26.05.2015 року №287/2015 (далі — Стратегія), де одними із актуальних загроз національній безпеці України визначено слабкість, дисфункціональність, застарілу модель публічних інститутів, депрофесіоналізація та деградація державної служби, а також здійснення державними органами діяльності в корпоративних та особистих інтересах, що

призводить до порушення прав, свобод і законних інтересів громадян та суб'єктів господарської діяльності.

Такі підходи є не що інше, як позбавлення операторів телекомунікацій можливості надавати послуги державним органам та підприємствам та відповідно являється наміром повернення до кланово-олігархічної системи економічного управління та знищення конкуренції.

Слід токож зазначити, що в країнах ЄС доступ державних органів до Інтернету здійснюється виключно приватними операторами телекомунікацій.

Таким чином, пропозиція відсторонити суб'єктів ринку від надання послуг органам влади, **зумовлює реальну загрозу національній безпеці держави, оскільки вплив зовнішніх факторів на мережу одного оператора (внаслідок аварій, диверсій та ін.) одночасно зумовить припинення функціонування ресурсів усіх органів влади та паралізує їх діяльність**.

Зазначені завдання не узгоджуються з вимогами статті 19 Конституції України щодо визначення способу здійснення повноважень органами державної влади, та не враховують правової позиції Конституційного Суду України, оскільки не містять достатніх і завершених правових механізмів реалізації положень, як того вимагає принцип правової держави (Рішення від 30 травня 2001 року N 7-рп/2001).