ФОРМУЮЧИ НОВУ СТРАТЕГІЮ КІБЕРБЕЗПЕКИ УКРАЇНИ: ЧИ МОЖЕМО УНИКНУТИ ПОМИЛОК ПЕРШОЇ СПРОБИ СТРАТЕГУВАННЯ?

Д. В. Дубов, д. політ. н., с. н. с.,
завідувач відділу інформаційної безпеки та кібербезпеки
центру безпекових досліджень Національного інституту стратегічних досліджень

Із введенням 14 вересня 2020 року в дію нової Стратегії національної безпеки України було дано старт і підготовці проектів низки стратегічних документів, одним з яких є Стратегія кібербезпеки України (далі - Стратегія).

Чинна редакція прийнята в 2016 році (далі – Стратегія 2016) була першою спробою стратегування державної політики щодо сфери кібербезпеки. Документ формувався на фоні агресії РФ проти України, першого в Україні випадку кібератаки проти об'єкта критичної інфраструктури (ОКІ) енергетичного сектору (Прикарпаттяобленерго), а також загального зростання деструктивної кіберактивності.

Безпосередньо Стратегія 2016 реалізовувалась в межах щорічних Планів заходів, які приймались в 2016-2018 роках (на 2019-2020 відповідні плани не затверджувались). Плани мали конкретизувати широкі за формулюваннями пріоритети та напрями забезпечення кібербезпеки України, визначені в Стратегії 2016 року.

Досвід 5 років реалізації Стратегії 2016 дозволяє виокремити низку важливих проблем, які завадили її повноцінній реалізації і які мають бути враховані при підготовці нової редакції цього стратегічного документу.

Передусім – вже згадана надмірна широта формулювань пріоритетів та напрямів забезпечення кібербезпеки України. Більшість з них не мають зрозумілої кінцевої мети, або така мета не може бути конкретизована (тим більше – у вигляді зрозумілих показників ефективності). Багато з пріоритетів були сформульовані як «процеси», а не «цілі» яких треба досягти (наприклад, «формування конкурентного середовища у сфері електронних комунікацій, наданні послуг із захисту інформації та кіберзахисту»), або були надто неконкретними (наприклад, «досягненні сумісності з відповідними стандартами ЄС та НАТО»).

Друга важлива проблема – низька ефективність Планів заходів. Їх аналіз у порівнянні з відповідними пріоритетами Стратегії 2016 свідчить про низьку кореляцію цих документів між собою. Фактично склалась ситуація, за якої Плани заходів були мало пов'язані із самою Стратегією або стосувались досить обмеженого кола її пріоритетів. Часто Плани заходів, які мали б конкретизувати положення Стратегії були такими ж широкими та неконкретними, що ускладнювало їх реалізацію.

Третя проблема - надмірний акцент на участь у реалізації Стратегії 2016 суто суб'єктів сектору безпеки та оборони та мінімальне залучення цивільних міністерств і відомств (в т.ч. – наукових установ і НАН України). Таким чином ціла низка завдань пов'язаних із розвитку наукового потенціалу чи поширення кіберграмотності були покладені на відомства, що не мають відповідних повноважень та можливостей. Такі ЦОВВ як Міністерство закордонних справ України, Міністерство освіти і науки України, секторальні міністерства хоча і реалізовували окремі завдання, однак їх ролі та функції не були чітко артикульовані, ані у Стратегії, ані у Планах заходів з її реалізації.

Нова редакція Стратегії кібербезпеки України має врахувати цей досвід та створити запобіжні механізми зменшення їх впливу на реалізацію Стратегії на наступний п'ятирічний період.

Важливим є і врахування у новій Стратегії базових стратегічних засад, визначених (ст.4) у Стратегії національної безпеки України 2020 року - стримування, стійкості та взаємодії. Очевидно, що положення нової редакції Стратегії мають не просто вказувати на наявність цих засад, але і розкривати кожну з них у розрізі забезпечення кібербезпеки держави. Також важливим при формуванні нової Стратегії є врахування останніх стратегічних напрацювань Європейського Союзу, інтеграція до якого є одним ключових завдання зовнішньої та внутрішньої політики України. Таке врахування може відбуватись на декількох рівнях, що включає як оцінку безпекового середовища в якому формуються нові стратегічні пріоритети, так і самих пріоритетів. Європейський Союзу у грудні 2020 року оприлюднив свою нову Стратегію кібербезпеки, що дає розуміння викликів з якими стикається як сам Союз, так і його члени та до яких заходів він планує вдаватись щоб зробити європейський цифровий простір безпечнішим для громадян та бізнесу.

Зважаючи на вище вказане, структура нової редакції Стратегії може бути сформована наступним чином:

1. Загальні положення. Визначають загальні положення документу, зокрема його зв'язок з іншими документами стратегічного планування та законодавчими актами.

2. Глобальний рівень викликів та загроз. Оцінка глобального безпекового середовища, яке вказує на ключові довгострокові кібербезпекові тренди, які має враховувати Україна, формуючи свою національну стратегію кібербезпеки. До таких можна віднести: мілітаризацію кіберпростору, деструктивну кіберактивність Російської Федерації як довгостроковий виклик, загрози критичні інфраструктурі (а також цифровим сервісам і фінансовому сектору загалом), вдосконалення кіберзлочинцями своїх інструментів, спроби суверенізації інтернету, розвиток нових технологій та рішень (в т.ч. 5G-мережі, штучний інтелект, «Інтернет речей» тощо), а також наслідки пандемії COVID-19 для цифрових трансформацій.

3. Національний рівень викликів та загроз. Більшою мірою зосереджено на оцінці внутрішніх проблем, які заважають Україні ефективно досягати своїх цілей в сфері кібербезпеки. Їх аналіз та систематизація потребує більш тісної співпраці не лише безпосередніх учасників реалізації чинної редакції Стратегії, але й представників широкої експертної спільноти, забезпечивши багатосторонній підхід та залучення різних стейкхолдерів. Водночас вже зараз можна виокремити низку таких викликів та загроз, що можуть стати основою цього розділу, зокрема: продовження експлуатації (в т.ч. відсутність вчасних оновлень ПЗ) застарілих ІТ систем з відомими зловмисникам вразливостями, зростання інтенсивності кібератак проти критичної інфраструктури та можливість настання важких наслідків, деструктивні зусилля РФ, низький рівень кіберобізнаності та кібергігієни громадян України, поточний рівень державно-приватного партнерства, стрімкі процеси цифрової трансформації, що можуть створити ризики в сфері кіберзахисту, витоки масивів персональних даних громадян України, відсутність достовірних даних про стан кібербезпеки держави та інші.

4. Мета та напрями реалізації. Крім, власне, мети Стратегії цей розділ має визначити *візію*, сформувавши довгострокове бачення бажаного майбутнього для України в сфері кібербезпеки. Вже на цьому етапі важливо чітко зафіксувати, що Стратегія реалізується не заради зростання спроможностей суб'єктів кібербезпеки (що є лише інструментом досягнення візії та мети Стратегії), а процвітання (передусім - економічного) громадян України, забезпечення їх безпеки, життя, здоров'я, честі, гідності та недоторканності.

Із врахуванням вказаного та стратегічних засад, визначених у Стратегії національної безпеки України, візія може бути сформульована наступним чином: «Ми творимо Україну спроможною забезпечити своє процвітання в цифровому світі, що вимагає від нас набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, забезпечити кіберстійкість суспільства та національної економіки, а також сформувати ефективну модель взаємодії усіх суб'єктів забезпечення кібербезпеки на засадах партнерства та співпраці заради такої цілі». Відповідно до цього пропонується визначити і стратегічні цілі нової Стратегії, згрупувавши їх у три великі категорії: стримування, стійкість та взаємодія.

Стримування базується на розвитку спроможностей, що унеможливлять (або максимального ускладнять) агресію проти України в кіберпросторі чи його використання проти здоров'я, добробуту та безпеки українських громадян. З цією метою пропонуються наступні три стратегічні цілі:

Стратегічна ціль 1. Дієва кібероборона. Україна має не лише створити ефективні (кадрово та технологічно) підрозділи, що опікуються захистом держави від кібератак, але й сформувати належну правову, організаційну, технологічну модель їх функціонування та застосування, що неможливо без: належного навчання та фінансового забезпечення таких структур, систематичних (не рідше раз на півроку) проведення кібернавчань, оцінки спроможностей підрозділів шляхом проведення регулярних незалежних аудитів, розроблення та імплементація індикаторів оцінки діяльності таких підрозділів.

*Стратегічна ціль 2. Розвиток асиметричних інструментів стримування та міжнародне співробітництво***.** Тісна співпраця з міжнародними партнерами має бути спрямована як на розвиток взаємної довіри для спільної відповіді на

кібератаки, так і на суто практичну співпрацю: проведення спільних кібернавчань, обмін інформацією про кіберінциденти, обмін досвідом та найкращими практиками. Україна має активніше залучати інші інструменти стримування ворожої кіберактивності, в т.ч. через дипломатичні та економічні заходи (санкційна політика), посилення розвідувальних спроможностей в кіберпросторі.

Стратегічна ціль 3. Зниження спроможностей кіберзлочинності. Кіберзлочинність продовжує залишатись ключовою загрозою для добробуту кожного громадянина, що користується цифровими послугами чи можливостями цифрової економіки. Кіберзлочинці часто можуть використовуватись іноземними державами для проведення ворожих військово-політичних дій, а інструменти які застосовують кіберзлочинці можуть використовуватись і проти безпеки держави в цілому. Відтак важливою ціллю Стратегії є максимальне зменшення до 2025 року спроможностей кіберзлочинців реалізовувати свої задуми у кіберпросторі.

Кіберстійкість передбачає спроможність всіх суб'єктів кібербезпеки своєчасно ідентифікувати загрози кібербезпеці, розбудовувати захист, впроваджувати інструменти виявлення кібератак, забезпечувати належну реакцію на них та швидкого відновлювати стабільну роботу під час та після кібератак. З цією метою маємо протягом реалізації Стратегії досягнути таких стратегічних цілей:

Стратегічна ціль 4. Національна кіберготовність. Створити (та реалізовувати) чіткий та зрозумілий для всіх стейкхолдерів план поліпшення системи національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав та свобод кожного українського громадянина. Метою реалізації заходів з національної готовності має стати забезпечення спроможності всіх стейхколдерів (передусім сектору безпеки і оборони, а також ОКІ) своєчасно і ефективно реагувати на потенційні і реальні кібератаки, давати відсіч агресору в кіберпросторі, стримувати його, відновлюватись після кібератак тим самим забезпечивши практичну кіберстійкість та захищеність економічного потенціалу держави.

Стратегічна ціль 5. Навчання та професійне вдосконалення. Провести докорінну реформу системи пошуку, найму, підготовки та підвищення фахового рівня української ІТ-робочої сили, яка має не лише стати основою цифрових трансформацій економіки, але і захисту її від кібератак будь-якого рівня та складності.

Стратегічна ціль 6. Кіберобізнаність та кібергігієна. Кожен користувач Мережі є важливим учасником національної системи кібербезпеки (екосистеми кібербезпеки). До 2025 року кожен громадянин держави має бути охоплений заходами з розвитку кібергігієни та цифрової освіти, а також отримати такі мінімальні навички, які дозволять йому безпечно реалізувати свої цифрові права. Обізнаність щодо сучасних кіберзагроз та спроможність їм протидіяти має стати невід'ємним елементом освіти кожного українського громадянина.

Взаємодія передбачає поступове формування нової якості відносин між всіма суб'єктами кібербезпеки та формування нової архітектури кібербезпеки. Це включає в себе до кінця 2025 року:

*Стратегічна ціль 7. Формування екосистеми кібербезпеки***.** Продовжуючи розбудовувати національну систему кібербезпеки маємо перейти до більш адекватної реаліям сьогодення екосистеми кібербезпеки**,** в якій держава є лише

«першим серед рівних» суб'єктом кібербезпеки, активно взаємодіючи з іншими стейкхолдерами (операторами ОКІ, академічною спільнотою, громадянським суспільством та громадянами), що мають бути повноцінно долучені до формування та реалізації заходів з кібербезпеки.

*Стратегічна ціль 8. Сервісна модель державної участі в питаннях кібербезпеки***.** Впровадити ризик-орієнтовані підходи у всіх сферах, створити та розвивати сервісну модель державної участі у заходах з кібербезпеки, за якого державні органи будуть сприйматись не як джерело все нових вимог, а як партнер у розбудові більш ефективних систем кібербезпеки. Це неможливо без глибинної реформи, яка чітко позбавить державні структури надмірних функцій та завдань, прибере можливі інституційні конфлікти інтересів та розпочне процес дерегуляції.

*Стратегічна ціль 9. Прозорість та підзвітність***.** Маємо забезпечити прозорість державної політики та діяльності в кіберпросторі, а також створити механізми заохочення всіх зацікавлених сторін поліпшувати спроможності держави та приватного сектору в питаннях кібербезпеки.

5. Цілі та завдання. Цей розділ має конкретизувати ті завдання, що мають бути реалізовані в межах стратегічних цілей. Як вже вказувалось раніше, важливий досвід реалізації попередньої Стратегії 2016 вказує на те, що ці завдання мають бути виписані як цілком конкретні заходи, що можуть бути виміряні з точки зору виконання. Наприклад, в частині завдань «національної готовності» перевага має надаватись таким завданням, як «*розроблено та впроваджено механізм обміну інформацією про загрози (Threat Information sharing Mechanism) учасниками якого є основні суб'єкти національної системи кібербезпеки, оператори ОКІ, приватні компанії, міжнародні партнери*» або «*проводяться щорічні командно-штабні кібернавчання стратегічного рівня*» замість «*створенні умов для впровадження в Україні сучасних технологій кіберзахисту*». Те саме має стати принципом наповнення для всіх стратегічних цілей.

6. Очікувані результати та критерії їх оцінки. Визначає не лише загальні цілі реалізації Стратегії, механізми її уточнення, але й що не менше важливо – інструмент інформування громадськості щодо стану її реалізації. Не можна не відмітити, що чинна Стратегія 2016 року не заклала таких інструментів і суб'єкти, що були залучені до реалізації стратегічного документу не звітували про її реалізацію чи про здобутки в межах її виконання. Нова Стратегія має врахувати цю проблему, створивши чіткий та зрозумілий (як для громадськості, так і для державних органів) інструмент звітування. Наприклад щорічно координатор реалізації Стратегії може оприлюднювати публічний звіт про стан її реалізації та загальними оцінками стану кібербезпеки України. Додатково основні суб'єкти забезпечення кібербезпеки щороку мають оприлюднюють на своїх сайтах звіти про стан реалізації ними завдань Стратегії.

Ще одним питанням яке має визначати цей розділ – оприлюднення періодичних доповідей або оглядів (щорічних або раз на два роки) про стан національної системи кібербезпеки України. Такі огляди мають давати загальну оцінку стану кібербезпеки України та визначати прогрес виконання стратегічних цілей Стратегії. За результатами оглядів до Стратегії можуть вноситися зміни.

7. Організаційне та фінансове забезпечення реалізації стратегії та забезпечення відкритості. Законодавство загалом визначає основні координаційні механізми нагляду за виконання Стратегії і вони не потребують принципового

перегляду. Водночас коло суб'єктів залучених до реалізації Стратегії має бути істотно збільшено. Серед структур, що можуть і мають (відповідно до стратегічних цілей) бути більш активно залучені до її реалізації, вочевидь, входять Міністерство закордонних справ України, Міністерство освіти та науки України, Міністерство цифрової трансформації України, секторальні міністерства (в частині визначення завдань та політик для функціонування ОКІ), Національна академія наук України та інші установи. Принцип планування також має бути модифікований відповідно до виявлених проблем. Зокрема пропонується, щоб протягом 3 місяців з моменту прийняття Стратегії Національний координаційний центр кібербезпеки Ради національної безпеки і оборони України розробив та затвердив загальний план її реалізації (який визначає пріоритетність стратегічних завдань Стратегії та роки їх виконання) на весь період дії Стратегії. Цей план має бути основою формування Кабінетом Міністрів України щорічних планів реалізації Стратегії та здійснення відповідного контролю. При формуванні планів реалізації обов'язково враховується відповідність запланованих заходів конкретним стратегічним цілям визначених цією Стратегією.