Дзюндзюк Вячеслав Борисович,
д.держ.упр., проф., завідувач кафедри політології та філософії,
ХарРІ НАДУ, м. Харків
ORCID 0000-0003-0622-2600;

Котух Євген Володимирович,
к.т.н, доцент кафедри комп'ютерних наук,
Сумський державний університет, м. Суми
ORCID 0000-0003-4997-620X

УДК 351.865 **doi: 10.34213/db.20.02.01**

КІБЕРБЕЗПЕКА ЯК ОДИН З ПРІОРИТЕТІВ НАЦІОНАЛЬНОЇ ПОЛІТИКИ

У статті виокремлено базові складові політики у сфері кібербезпеки в Україні, сформульовано низку пропозицій для підвищення ефективності стратегій і політики кібербезпеки, запропоновано низку принципів, на яких має ґрунтуватися політика кібербезпеки в Україні.

Ключові слова: Інтернет; кібербезпека; кіберпростір; публічне управління; стратегія.

Постановка проблеми. В останнє десятиліття ми маємо змогу спостерігати еволюцію ролі Інтернету в суспільстві. Коли Інтернет був просто корисною платформою для окремих осіб та організацій, наслідки відмов можна було контролювати на рівні кожної окремої особи та організації, і політика органів влади полягала в тому, щоб допомогти їм запобігти таким інцидентам або ж управляти ними. Оскільки Інтернет став необхідним для економіки і суспільства, наслідки невдач можуть безпосередньо впливати на суспільство в цілому. Як наслідок, сфера застосування стратегій кібербезпеки повинна змінитися від захисту окремих осіб та організацій як окремих суб'єктів до захисту суспільства в цілому. Тому стратегії кібербезпеки мають бути спрямовані на досягнення двох взаємопов'язаних завдань: 1) зміцнення кібербезпеки для Інтернет-економіки, щоб сприяти економічному та соціальному процвітанню; 2) захист кіберзалежних суспільств від кіберзагроз. Управління складністю паралельного вирішення цих двох завдань при збереженні відкритості Інтернету і відповідних фундаментальних цінностей, ймовірно, є сьогодні головним завданням розробки політики у сфері кібербезпеки.

Аналіз останніх досліджень і публікацій. Питанням ролі Інтернету в діяльності та інфраструктурі як публічних, так і приватних організації присвятив свої дослідження Д. Варфілд. Дж. Сміт розглядав питання взаємозв'язку конфіденційності інформації, свободи слова, інтелектуальної власності та прав на комп'ютерну безпеку. С. Кемпбелл опікувався проблемами втручання органів влади в діяльність приватних організацій щодо забезпечення останніми кібербезпеки. Оцінці вразливостей та аналізу політик компаній у сфері кібербезпеки, а також загальному аналізу ризиків у кіберпросторі приділив увагу у своїх роботах П. Фетцер.

Мета статті полягає у виокремленні складових політики у сфері кібербезпеки в Україні та визначенні принципів, на яких має ґрунтуватися політика кібербезпеки в Україні.

Виклад основного матеріалу. Аналіз національних стратегій кібербезпеки, проведений автором раніше[1], показав фундаментальну еволюцію в розробці національної політики, відповідно до якої кібербезпека стає одним із пріоритетних завдань уряду й інших органів влади. До таких змін привело розуміння двох важливих факторів, які впливають на всі сучасні держави, в тому числі й на Україну. До цих факторів належать такі:

1. *Інтернет та ІКТ необхідні для економічного та соціального розвитку й утворюють життєво важливу інфраструктуру*. У загальному контексті економічного спаду, що став результатом останньої пандемії, викликаної COVID-19, відкритий Інтернет та ІКТ є новим джерелом зростання і рушійною силою інновацій, соціального благополуччя та індивідуального самовираження. У міру зростання Інтернет-економіки вся економіка і суспільство, включаючи публічний сектор, стають все більш залежними від цієї цифрової інфраструктури для виконання своїх основних функцій.

2. *Кіберзагрози розвиваються і зростають швидкими темпами*. Вони як і раніше ініціюються кримінальними діячами, але також надходять з нових

[1] Котух Є. В. Проблеми кібербезпеки в сучасному світі. *Актуальні проблеми державного управління* : зб. наук. праць. 2019. № 2 (56). doi: 10.34213/ap.19.02.03.

джерел, таких як іноземні держави та політичні групи, і можуть мати інші мотиви, крім заробляння грошей, такі як деякі види «хактивізму» (Anonymous), дестабілізація, кібершпіонаж, саботаж (наприклад, stuxnet) і навіть військові дії (наприклад, гібридна війна Росії проти України). Сучасні шкідливі актори стали краще організовані порівняно зі своїми попередниками, що, зокрема, дозволяє їм краще приховувати свої сліди, а ступінь складності кіберзагроз значно зросла, демонструючи явні ознаки професіоналізації тих, хто є їх джерелом.

Критичність Інтернету для сучасної економіки має кілька наслідків для розробки політики у сфері кібербезпеки, основним з яких є прийняття стратегій, які підходять до забезпечення кібербезпеки *комплексним і всеосяжним чином*. Нинішні органи влади мають визнавати необхідність розглядати всі аспекти кібербезпеки цілісно, а не фрагментарно, як у минулому. Тому нові стратегії кібербезпеки повинні поширюватися на весь публічний сектор та охоплювати економічні, соціальні, освітні, правові, правоохоронні, технічні, дипломатичні, військові та розвідувальні аспекти кібербезпеки. Для реалізації такого комплексного підходу необхідна наявність політичної волі на рівні голови держави або уряду, що має бути сигналом для всіх органів влади про значне підвищення кібербезпеки серед національних пріоритетів.

Проте, як показав аналіз, не в усіх стратегіях використовуються терміни «кіберпростір» і «кібербезпека», а деякі зі стратегій, які використовують ці терміни, також дають визначення, які варіюється в залежності від країни. Хоча більшість країн при цьому включають концепцію критично важливих інформаційних інфраструктур у сферу своєї стратегії, як це визначено в Рекомендації ОЕСР щодо захисту критично важливих інформаційних інфраструктур [5].

Однак можна виділити низку загальних аспектів, які, на наш погляд, мають бути присутніми в політиці та стратегії кібербезпеки в Україні (рис. 1).

Розглянемо зазначені складові політики у сфері кібербезпеки більш детально.

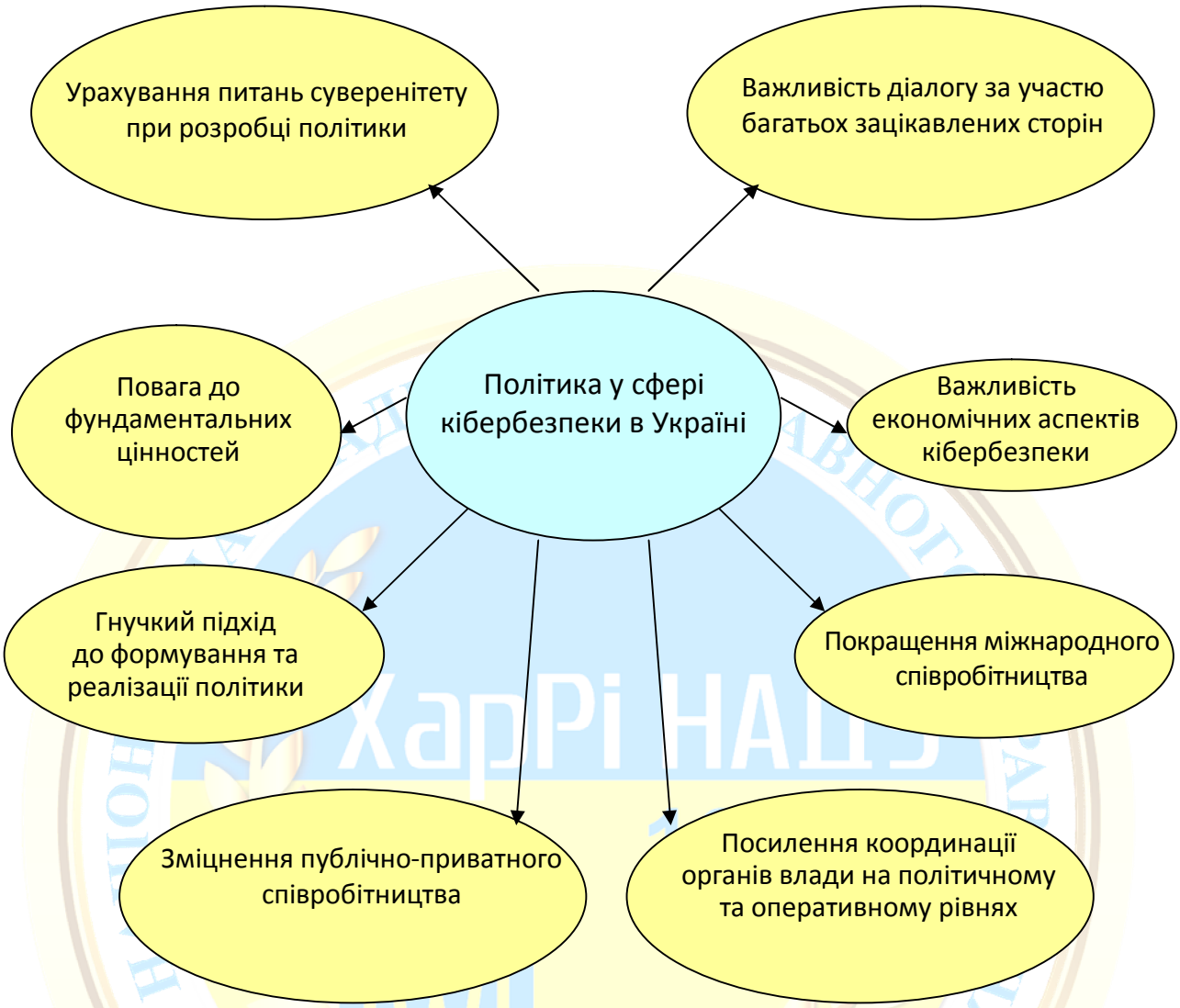

Рис. 1. Складові політики у сфері кібербезпеки в Україні [за 3; 8; 10]

Посилення координації органів влади на політичному та оперативному рівнях. Оскільки кібербезпека стає питанням національного пріоритету, відповідальність за розробку і реалізацію політики у сфері кібербезпеки чітко розподіляється всередині публічного сектора. Однак жоден з існуючих органів влади не може претендувати на всебічне розуміння і досить широкі повноваження для управління всіма аспектами кібербезпеки. Таким чином, координація між відповідними органами стає вкрай важливою. При цьому відповідальність за координацію має покладатися на конкретну існуючу або

нову установу, і відповідальність інших залучених публічних організацій також повинна бути чітко визначена, щоб сприяти співпраці, заохочувати взаємодію, уникати дублювання і об'єднувати ініціативи. Така модель являє собою еволюцію від багатовідомчого до міжвідомчого підходу і вимагає сильного лідерства, щоб забезпечити координацію і співробітництво в межах існуючих державних механізмів. Причому зрозуміло, що конкретні домовленості можуть розрізнятись в різних країнах і відображатимуть політичну культуру, яка має місце.

Зміцнення публічно-приватного співробітництва. Усі стратегії визнають, що кіберпростір значною мірою належить приватному сектору і керується ним, і що користувачі також відіграють ключову роль в його функціонуванні та безпеці. Тому політика кібербезпеки повинна ґрунтуватися на інклюзивних партнерських відносинах між публічним, приватним і третім секторами, які можуть включати бізнес, громадянське суспільство, Інтернет-спільноту й академічні кола.

Покращення міжнародного співробітництва. Як показав аналіз, міжнародне співробітництво та необхідність створення більш ефективних альянсів і партнерств з країнами-однодумцями або союзниками, у т.ч. сприяння створенню потенціалу в менш розвинених країнах, є основними завданнями значної частини стратегій. Більшість проаналізованих стратегій, однак, надають мало подробиць про те, як саме домогтися розширення міжнародного співробітництва. Виняток становлять Сполучені Штати, які розробили спеціальну міжнародну стратегію для кіберпростору, і Великобританія, яка ініціювала міжнародний діалог на Лондонській конференції 2011 р. з кіберпростору і просуває концепцію міжнародних норм поведінки в кіберпросторі. У зв'язку з цим слід при розробці національної стратегії звернути увагу на необхідність більш високого ступеня гармонізації законодавства проти кіберзлочинності, зокрема, Будапештської конвенції 2001 р. про кіберзлочинність, відповідних документів міжнародних і регіональних організацій, такі як Рада Європи, Європейський Союз, Форум з управління

Інтернетом, Організація з безпеки і співробітництва в Європі (ОБСЄ) і ООН, включаючи Міжнародний союз телекомунікацій.

Повага до фундаментальних цінностей. Усі стратегії роблять сильний акцент на необхідності політики кібербезпеки поважати фундаментальні цінності, які зазвичай включають в себе конфіденційність, свободу слова і вільний обмін інформацією. У декількох стратегіях прямо згадується про необхідність підтримувати відкритість Інтернету, і жодна стратегія не пропонує зменшити відкритість на користь посилення кібербезпеки. Навпаки, відкритість Інтернету зазвичай описується як вимога для подальшого розвитку Інтернет-економіки.

Урахування питань суверенітету при розробці політики у сфері кібербезпеки, тобто комплексне урахування аспектів національної та міжнародної безпеки, розвідки, оборони та військової справи. Цей принцип є прямим наслідком того, що кібербезпека спрямована на захист суспільства в цілому і вимагає комплексного підходу з боку органів влади. Питання суверенітету виникають на різних рівнях внутрішньої політики:

1) на стратегічному рівні, скажімо, з визнанням кіберзагроз, спрямованих на військових, або ризиків кібершпіонажу з боку іноземних держав;

2) на організаційному рівні, оскільки органи влади та їх підрозділи, чия діяльність пов’язана з дипломатією, розвідкою і збройними силами, як правило, включені до міжурядової координації для вироблення політики, а також до міжвідомчої структури, що відповідає за координацію діяльності щодо забезпечення національної безпеки , в тому числі, і кібербезпеки;

3) на оперативному рівні, коли, наприклад, розвідувальні органи відіграють ключову роль як джерело інформації для обізнаності про поточну ситуацію.

Міркування суверенітету також з’являються на рівні міжнародної політики: по-перше, в стратегіях згадується необхідність міжнародного діалогу щодо «правил участі» в кіберпросторі або «заходів зміцнення довіри»; по-друге, стратегії підкреслюють роль деяких організацій, таких як НАТО і ОБСЄ щодо вирішення різних політичних питань; по-третє, стратегії згадують

необхідність оперативного співробітництва щодо обміну розвідувальною інформацією між союзниками.

Гнучкий підхід до формування та реалізації політики. Інтернет – це динамічне середовище, в якому технології та інструменти постійно розвиваються непередбачуваним чином в інтересах зростання та інновацій, але загрози також знаходяться в постійному розвитку. У зв'язку з цим деякі стратегії просувають гнучку політику кібербезпеки, яка зберігає відкритість Інтернету і вільний потік інформації, а також інші фактори, які дозволяють Інтернету генерувати економічні й соціальні вигоди і пристосовуватися до фундаментально динамічного середовища. Ці стратегії підтримують політики, які забезпечують швидкі й обґрунтовані процеси прийняття рішень, впроваджують механізми швидкого зворотного зв'язку і включають в себе ефективні цикли навчання та покращення для швидкого і ефективного впровадження нових кібер-інструментів. Такі стратегії акцентують на саморегулюванні в кіберпросторі і вважають, що законодавче регулювання щодо кіберпростору слід використовувати тільки в тих випадках, коли саморегулювання не є можливим або неефективно.

Важливість економічних аспектів кібербезпеки. У той час як всі стратегії спрямовані на вирішення проблеми кібербезпеки з метою підтримки і подальшого розвитку економічного і соціального процвітання за допомогою безперервного розвитку динамічної Інтернет-економіки, економічні аспекти кібербезпеки стають все більш помітними особливо в декількох стратегіях. Ці стратегії підкреслюють, що більш високий рівень кібербезпеки забезпечить економіці їхньої держави конкурентну перевагу, а також вони визнають, що економічні фактори відіграють ключову роль у підвищенні кібербезпеки. Тому деякі стратегії вимагають більш глибокого розуміння структури стимулів учасників ринків щодо кібербезпеки і заохочення відповідних заходів, таких як використання міток безпеки, які застосовуються до продуктів і послуг, для кращого інформування ринку. Кілька стратегій поставили за одну з ключових цілей політики істотний розвиток сектора кібербезпеки, включаючи розвиток

людського потенціалу та розвиток сектора страхування кібербезпеки. У свою чергу, інші стратегії визначають як важливу мету політики більш високий ступінь технологічної незалежності щодо інформаційної безпеки.

Важливість діалогу за участі багатьох зацікавлених сторін. Багато стратегії поділяють думку, що діалог з неурядовими стейкхолдерами (громадськими організаціями та бізнес-структурами) є ключем до ефективного формування і реалізації політики кібербезпеки. Однак рівень деталізації щодо того, яким чином органам публічної влади налагоджувати діалог за участі багатьох зацікавлених сторін варіюється, при цьому багато стратегій містять мало або взагалі не містять подробиць з цього аспекту. У деяких стратегіях передбачається створення спеціального органу, що включає всі зацікавлені сторони для надання інформації та консультацій органам публічної влади різного рівня.

Стратегії кібербезпеки зазвичай включають або супроводжуються прийняттям планів дій, спрямованих на зміцнення ключових пріоритетних сфер, до яких, як правило, відносяться такі [3]:

1. Державна безпека: плани дій включають безліч ініціатив, починаючи від розвитку потенціалу ситуаційної обізнаності та закінчуючи раціоналізацією урядової мережевої інфраструктури і узагальненням аудитів у публічному секторі.

2. Захист критично важливої інформаційної інфраструктури: плани дій зазвичай включають заходи, пов’язані із захистом критично важливих інформаційних інфраструктур.

3. Боротьба з кіберзлочинністю: в плани дій входять різні ініціативи з розвитку потенціалу правоохоронних органів, вдосконалення нормативно-правової бази та розвитку міжнародного співробітництва на основі Будапештської конвенції про кіберзлочинність.

4. Підвищення обізнаності: плани дій включають в себе різні ініціативи, спрямовані на конкретні групи населення, такі як особи, які приймають рішення в органах влади і критично важливих інфраструктурах.

5. Освіта: в планах дій визнається, зокрема, необхідність розвитку кадрового потенціалу у сфері кібербезпеки. Більше того, деякими країнами розвиток навичок кібербезпеки визначено як ключовий пріоритет.

6. Реагування: в планах дій визнається важлива роль, яку відіграють групи реагування на інциденти у сфері кібербезпеки (CSIRT), тому вони передбачають створення національної CSIRT або її розвиток там, де вона вже існує.

7. Науково-дослідні та дослідно-конструкторські роботи (НДДКР): на їх важливості стали акцентувати не так давно, але в планах дій останніх років їм приділяється серйозна увага, особливо в контексті взаємодії з приватним сектором.

Разом з тим, на наш погляд, до переліченого вище слід додати ще кілька важливих ключових сфер, яким треба відвести спеціальне місце як в політиці кібербезпеки, так і у відповідних планах дій:

– розвиток можливостей для ситуаційної обізнаності та моніторингу в режимі реального часу, в основному для публічних інфраструктур;

– визначення і моніторинг об’єктів, які, не будучи критично важливими інформаційними інфраструктурами на даний момент, можуть за певних умов завдати значної шкоди кібербезпеці;

– партнерство з Інтернет-провайдерами для усунення загрози ботнетів за участю їх клієнтів;

– проведення навчань з кібербезпеки, в тому числі, і міжнародних;

– розробка та широке впровадження систем цифрової ідентифікації;

– реалізація спеціальної політики захисту дітей в Інтернет.

Також, з огляду на сучасну спрямованість на багатосуб’єктність у забезпеченні кібербезпеки, яка передбачає співпрацю публічного, приватного і третього секторів, можна сформулювати ще низку пропозицій для підвищення ефективності стратегій і політики кібербезпеки, а саме:

1. Спільна систематична оцінка відповідності заходів кібербезпеки, пропонованих органами влади, іншим ініціативам у сфері кібербезпеки.

Наприклад, законодавство, яке встановлює кримінальну відповідальність за хакерство, могло б взяти до уваги, що деякі дослідження сприяють підвищенню кібербезпеки, використовуючи такі ж методи, як і хакери.

2. Публічні організації як власники й оператори інформаційних систем і мереж можуть подавати приклад іншим акторам, застосовуючи передовий досвід, технології і навіть законодавчі вимоги. Технології, розроблені для одного із секторів, також можуть принести користь іншим секторам.

3. Політики можуть звернутися за порадою до технічного товариства Інтернету якомога раніше в процесі розробки політики, щоб уникнути прийняття технологічно помилкових рішень.

4. Політика у сфері кібербезпеки може стимулювати розробку відкритих стандартів, що дозволяють впроваджувати інновації для рішень у даній сфері, спираючись на фахівців зі стандартизації Інтернету (шанованих в експертному співтоваристві і таких, що добре зарекомендували себе), уникаючи при цьому односторонньої зміни стандартів Інтернету.

5. Варто заохочувати збір емпіричних даних, щоб краще оцінювати актуальність стратегій і політик, а також підтримувати підходи, засновані на оцінці ризиків. Для протидії існуючим перешкодам, з якими багато акторів стикаються при наданні додаткової інформації про кіберінциденти, слід виділяти додаткові ресурси і впроваджувати узгоджені механізми повідомлення про порушення безпеки, з якими стикаються представники всіх трьох секторів.

Крім багатосуб'єктності, слід враховувати і міжнародний вимір політики у сфері кібербезпеки, який дає не тільки позитивні результати (про які багато говориться), але і негативні. Так, вимоги, що пред'являються деякими країнами до галузі ІКТ, створюють для неї технічні бар'єри у взаємодії, наприклад, у формі вимог місцевих стандартів, надлишкових схем сертифікації безпеки або втручань в глобальний ланцюжок створення вартості (якщо мова йде про комерцію); знижують функціональність, обмежують інновації і спотворюють рівні умови гри. Щоб уникнути цього, необхідно розгортання глобальних рентабельних галузевих рішень, впровадження міжнародних стандартів, систем

взаємного визнання відповідності та підвищення обізнаності менш розвинених країн з цих питань.

Ще одним важливим питанням у контексті розробки політики кібербезпеки є втручання / невтручання держави в діяльність організацій приватного сектора щодо забезпечення їх кібербезпеки.

Дійсно, сьогоднішній масштабний вплив кіберзагроз змушує уряди і органи безпеки багатьох країн зосередити увагу на кібербезпеці не тільки в публічному, а й у приватному секторі. Однак навколо даного питання існує дискусія щодо того, чи можуть органи влади диктувати, яким чином приватний сектор повинен забезпечувати свою кібербезпеку, і якщо так, то наскільки це ефективно. До цієї дискусії додається суспільна заклопотаність з приводу інформаційної прозорості та її впливу на права і свободи громадян.

Інформаційно-комунікаційні системи пов'язані між собою на глобальному рівні. Безперервна робота цих систем для надання життєво важливих послуг залежить від їх невразливості для кібератак. Однак при цьому, по-перше, дуже часто як публічні, так і приватні організації не знають, яку дійсну роль Інтернет відіграє в їх інфраструктурі [11], по-друге, приватні підрядники все частіше надають органам влади послуги із забезпечення функціонування систем обміну критично важливою інформацією. Тому, на наш погляд, органи влади обов'язково повинні мати можливість впливати на організації приватного сектора щодо забезпечення їх кібербезпеки, що має здійснюватися на базі обміну інформацією, співпраці і спільних дій. Більш того, подібна співпраця має реалізовуватися не тільки на національному, а й на міжнародному рівні, зі створенням урядових коаліцій.

Подібні коаліції вже існують, зокрема, в рамках таких організацій як Організація економічного співробітництва і розвитку (ОЕСР), Європейське поліцейське управління (Європол) та Асоціація держав Південно-Східної Азії (АСЕАН). Запобігання міжнародних кіберзлочинів, таких як шпигунство і злам, вимагає спільних зусиль, і міжурядові органи мають виступати посередником при їх розслідуванні, оскільки відсутність розуміння в цьому питанні між

країнами становить загрозу міжнародній боротьбі з кіберзагрозами. Що стосується приватного сектора, то органи влади можуть співпрацювати (і в багатьох країнах співпрацюють) щодо розробки програм, технологій і керівництв щодо дотримання передових галузевих практик кібербезпеки.

Однак, як показує практика, забезпечення інформаційної прозорості в приватному секторі виявляється складним завданням, особливо у фінансовій галузі. У низці країн компанії зобов'язані розкривати всю інформацію про витік даних своїм клієнтам, проте не всі країни дотримуються одних й тих же законів і правил, що ще більше ускладнює інформаційну безпеку міждержавних даних споживачів. Конфіденційність інформації, свобода слова, інтелектуальна власність і права на комп'ютерну безпеку досі є невизначеними в глобальному масштабі, оскільки не існує єдиної точки зору на співвідношення цих понять. Наприклад, у США The National Journal Daily писав: «Оскільки Конгрес прагне прийняти більше законів про кібербезпеку, щоб стимулювати обмін інформацією між урядом і приватним сектором, це може відкрити скриньку Пандори щодо конфіденційності та громадянських прав і свобод» [7].

Органи влади мають співпрацювати, а не диктувати приватному сектору, тому вкрай важливо, щоб обидві сторони працювали разом, щоб допомогти захистити країну від кіберзагроз. Однак, часта проблема, з якою стикаються обидва сектора – це відсутність довіри між ними. Так, приватні компанії не вирішуються передавати інформацію та свою репутацію до рук органів влади, оскільки витік інформації може мати згубні наслідки для приватних компаній. Що стосується громадської думки, то вона досить показово описана Кемпбеллом: «Більшість опитаних людей не вважають, що уряд повинен диктувати, як саме приватні компанії повинні зберігати свої дані, в той же час 31,5% не впевнені, що уряд робить достатньо для регулювання того, як приватні компанії захищають наші дані» [2]. Тобто громадяни все ж хотіли б, щоб органи влади певною мірою втручалися в діяльність приватних організацій щодо забезпечення тими кібербезпеки, тобто здійснювали певні інтервенції.

Органи влади можуть здійснювати інтервенції за допомогою публічної

політики в певній сфері і через законодавство. Наприклад, це може бути прийняття закону про посилення кібербезпеки в публічному та приватному секторі або про обмін інформацією між органами влади та приватними організаціями. Також хорошим прикладом є прийнятий в США в 2002 р. Федеральний закон про управління інформаційною безпекою (FISMA), який об'єднав інформаційну, економічну і національну безпеку шляхом забезпечення виконання оцінок ризиків, керівних принципів конфігурації і політик безпеки.

Відповідна політика може бути спрямована на впровадження загальних стандартів і протоколів безпеки незалежно від сектора. Прикладом у цьому сенсі, гідним наслідування, є Базовий план конфігурації уряду США (USGCB), що містить правила комп'ютерної безпеки, регульовані державними системами США, яким повинна відповідати будь-яка організація, яка підключається до державної системи кібербезпеки, як публічна, так і приватна.

Слід згадати ще один приклад із США. У 2014 р. комітет Сенату з розвідки прийняв закон про кібербезпеку, що дозволяє обмінюватися інформацією між приватним сектором і урядом щодо загроз безпеці [8]. Однак цей закон був підданий критиці через потенційні негативні наслідки розголошення особистої інформації органами влади, внаслідок чого в закон були внесені поправки, що регулюють приватну інформацію громадян, яка отримується приватними підприємствами.

Асланов, Уайт і Етткін відзначають, що вплив вразливостей кібербезпеки, які не усунуті заздалегідь, має серйозні операційні наслідки [1]. При цьому, за оцінками авторів, тільки 25 % приватних організацій здійснюють необхідні заходи безпеки в рамках своїх стандартних операційних процесів [1]. У той же час, недостатній захист і фінансових систем, і критичної інфраструктури, якщо вони стануть жертвами кібератак та інших шкідливих дій, може мати руйнівні наслідки для організацій (як приватних, так і публічних) і громадян. І в цьому сенсі використання політик кібербезпеки, які адмініструються органами влади, може сприяти впровадженню передових методів і посиленню безпеки для розробників програмного забезпечення, постачальників і організацій, що

зберігають важливу інформацію і забезпечують функціонування критично важливих галузей і об'єктів, а також навчанню технічного персоналу методам протидії кіберзагрозам, заснованим на оцінці ризику.

Проте, питання конфіденційності, дотримання громадянських прав і свобод викликають заклопотаність у багатьох, коли органи влади вводять обов'язкові правила кібербезпеки, особливо щодо збору інформації та обміну нею між секторами, зокрема при проведенні розслідувань, не пов'язаних з кібербезпекою. Концепція обміну інформацією, про яку в даному випадку йде мова, полягає в тому, щоб дати можливість органам влади збирати інформацію про загрози у кіберсфері, і ділитися нею з організаціями приватного сектора. Ця концепція реалізована, зокрема, в США, де подібний обмін здійснюють Центри обміну і аналізу інформації (ISAC). При цьому існує певне законодавство, що регулює обмін інформацією про кібербезпеку.

У свою чергу, приватні компанії займаються виробництвом програмного забезпечення, обладнання, комп'ютерів і мережевих компонент, якими згодом користуються організації публічного сектора, в тому числі, і для забезпечення функціонування критично важливої інфраструктури, зокрема, оборонної. Відповідно, органи влади зацікавлені в дотриманні приватними організаціями максимальних заходів захисту від кіберзагроз. У США був неприємний випадок, коли хакери з КНР вкрали надсекретні плани винищувача F-35 Joint Strike Fighter, які, за деякими даними, включали в себе відомості про найбільш інноваційні термоядерні боєголовки. Сталося це через те, що приватні підрядники оборонної промисловості не дотримувалися належних нормативних заходів контролю кібербезпеки [10].

Як показує практика, компанії, що використовують підхід до кібербезпеки, заснований на оцінці ризиків, який передбачає конкретну кількісну оцінку ризиків кіберзагроз, досягають більшого успіху в захисті систем і даних. Хакери шукають уразливості в високочутливих критичних системах, тому оцінка вразливостей і аналіз політик компанії будуть сприяти загальному аналізу ризиків [4]. Поряд з цим компанії повинні проводити

постійний поведінковий аналіз, вимірювати потенційні загрози, вразливості і наслідки.

У 2010 р. Google разом з 20 іншими компаніями став жертвою штучно створеної кібератаки, що виходила з Китаю, під час якої зловмисники намагалися пошкодити вихідний код сайту [6; 1]. WikiLeaks повідомляє, що цей напад був санкціонований Постійним комітетом Політбюро компартії КНР [6]. Атака не мала того успіху, на який розраховували зловмисники, але після цього випадку Google став активно співпрацювати з Агентством національної безпеки (АНБ), вони разом тестували програмні, апаратні та уразливі місця, щоб визначити можливу поведінку зловмисників і пом'якшити негативні наслідки в майбутньому. Таке партнерство між Google і АНБ показало приклад успішної взаємодії між публічним і приватним сектором. Маючи велику технічну підтримку, яку він міг отримати від таких компаній, як Facebook або Microsoft, Google вирішив співпрацювати з питань кібербезпеки з АНБ замість Департаменту внутрішньої безпеки США. Дивно, але Google довірив АНБ об'єднати ресурси для пошуку недоліків в системі безпеки, використовуючи ефективні засоби контролю кібербезпеки, а також дотримуючись протоколів кібербезпеки, розроблених урядовими установами.

Звичайно, урядові протоколи можуть в деяких випадках стримувати інновації, а не сприяти посиленню контролю безпеки. Але, як видно з прикладу партнерства Google з АНБ, у великих гравців є певний рівень довіри з боку уряду, і вони визнають свій обов'язок захищати національну безпеку, застосовуючи заходи безпеки, визначені в у політиці, постановах і протоколах, прийнятих урядом.

Таким чином, приватні суб'єкти разом з органами влади несуть відповідальність за забезпечення національної кібербезпеки. Фундаментальна архітектура кібербезпеки на 90 % належить і управляється приватними суб'єктами. Ці основні компоненти критично важливої інфраструктури включають в себе, зокрема, транспорт, фінанси, енергозабезпечення та ін., і працездатність цих компонент залежить від стійкості мереж приватного

сектора. Тому потреба у створенні сильної та оперативної структури кібербезпеки очевидна, при цьому приватні компанії повинні застосовувати заходи безпеки відповідно до урядових протоколів. З іншого боку, органи влади повинні розробляти протоколи безпеки і нормативні акти, що стосуються кібербезпеки, через робочі партнерства з приватним сектором, щоб враховувати також і його інтереси, зокрема, щодо контролю інформації.

Висновки з даного дослідження та перспективи подальших розвідок у даному напрямку. Виходячи з усього викладеного вище, на наш погляд, політика кібербезпеки в Україні має ґрунтуватися на таких принципах:

– впровадження стратегічного підходу до забезпечення кібербезпеки;

– комплексне вирішення проблем кібербезпеки, включаючи використання ефективних механізмів координації, адаптованих до культури і стилю управління в країні;

– своєчасність, гнучкість і адаптивність у прийнятті рішень у сфері забезпечення кібербезпеки;

– розвиток національного потенціалу команд з протидії кіберінцидентам;

– впровадження передових методів забезпечення кібербезпеки;

– покращення захисту критично важливих інформаційних інфраструктур;

– повага до фундаментальних цінностей свободи інформації, але з використанням належних запобіжних заходів, стримувань і противаг;

– підвищення кіберграмотності суспільства;

– використання системи стимулів для розвитку сфери кібербезпеки і відповідного кадрового потенціалу;

– співпраця з приватними та неурядовими організаціями, розвиток публічно-приватного партнерства;

– посилення боротьби з кіберзлочинністю;

– заохочення досліджень і розробок у сфері кібербезпеки;

– розвиток міжнародного співробітництва, зокрема, шляхом участі в розробці загальних норм поведінки в кіберпросторі.

Що стосується останнього пункту, то визначення в рамках національних стратегій точок координації з міжнародними партнерами створює можливість для активізації міжнародного співробітництва на стратегічному та оперативному рівнях. При цьому кожна країна може розглянути питання про розширення зусиль з координації, визначивши в своєму уряді «міжнародний контактний пункт», який буде доступний, наприклад, для сприяння поширенню серед відповідних національних установ запитів іноземних держав, пов'язаних з кібербезпекою, будь то для надзвичайних, інформаційних або інших цілей.

У цілому, як можна бачити з досвіду багатьох країн, розробка політики у сфері кібербезпеки виходить на новий рівень зрілості в порівнянні з попередніми політиками, характерними для першого десятиліття XXI століття, з більш кваліфікованим керівництвом, кращою координацією і більш широкою участю зацікавлених сторін. У той же час проблеми, пов'язані з розробкою політики, збільшуються, що говорить про те, що уряди також стикаються з новим рівнем складності. Наприклад, необхідно задовольняти потребу в більшій координації між агентствами за допомогою більш високого ступеня централізації, одночасно забезпечуючи динамічні та швидкі, майже в реальному часі, процеси прийняття рішень на всіх рівнях. Ще однім складним завданням є необхідність запровадження цілісних підходів, що враховують суверенітет та економічні / соціальні проблеми, участь широкого кола органів публічної влади і розширення співпраці з приватним сектором. Також проблемою є необхідність збереження відкритості Інтернету і фундаментальних цінностей відповідно до Рекомендації 2011 р. Ради по принципам формування Інтернет-політики.

На вирішення цих та інших проблем потрібний час, між тим, на даний момент ключовим завданням для публічного сектора у сфері кібербезпеки є підготовка до можливих серйозних кіберінцидентів і протидія їм, але таким чином, щоб не підірвати відкритість Інтернету.

References

1. Asllani, A., White, C.S. & Ettkin, L. (2012). Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals. *Allied Academies International Conference: Proceedings Of The Academy Of Legal, Ethical & Regulatory Issues (ALERI), 16 (1), 1–2.*
2. Campbell, S. (2013). Who Should Drive Cybersecurity Policy: Government or Private Industry? URL: http://www.threattracksecurity.com/blogs/cso/best-cybersecurity-policy-driver-government-private-industry/.
3. ENISA (2012). National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace. URL: www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper.
4. Fetzer, P. (2014). A Compilation of Enforcement and Non-Enforcement Actions – 30 April 2014. *Mondaq Business Briefing*. May 2. URL: http://bi.galegroup.com.ezproxy.umuc.edu /essentials/article/GALE%7CA366740594/da1cb a907f837d6534b75f26925c2f8c?u=umd_umuc.
5. OECD (2002). Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Paris. URL: www.oecd.org/ document/42/0,3746,en_2649_34255_15582250_1_1_1_ 1,00.html.
6. Rosenzweig, P. (2011). Cybersecurity and Public Goods: the Public/Private Partnership. In P. Berkowitz (Series Ed.). *Emerging Threats in National Security and Law (pp. 2–35)*. URL: http://www.emergingthreatsessays.com.
7. Smith, J. (2012). Groups Warn of Privacy Concerns in Cybersecurity. *Bills. National Journal Daily*. February 9. URL: http://bi.galegroup.com.ezproxy.umuc.edu/essentials/article/ GALE%7CA296609515/1bdddd15100244706117f040a6f0096a?u=umd_umuc.
8. UK Home Office (2010). Cyber Crime Strategy. URL: www.official-documents.gov.uk/document/cm78/7842/7842.pdf.
9. United States: US Senate Intelligence Committee approves Cybersecurity Information Sharing Act. (2014). *TendersInfo News*. July 10. URL: http://bi.galegroup.com.ezproxy.umuc.edu/ essentials/article/GALE%7CA374562170/47ae2 c726538f15d98557c7726d5ccf0?u=umd_umuc.
10. US Department of Defense. (2011). Department of Defense Strategy for Operating in Cyberspace. URL: www.defense.gov/news/d20110714cyber.pdf.
11. Warfield, D. (2013). Critical infrastructures: IT Security and Threats from Private Sector Ownership. *Information Security Journal: A Global Perspective, 21(3), 2012, 127–136.* doi10.1080/19393555.2011.652289.

Dziundziuk V. B.,
Doctor of Public Administration,
Full Professor, Head of Political Science and Philosophy Department,
KRI NAPA, Kharkiv
ORCID 0000-0003-0622-2600;

Kotukh Ye. V.,
PhD in Technical Sciences, Associate Professor of Computer Science Department, Sumy State University, Sumy
ORCID 0000-0003-4997-620X

Cybersecurity as one of the priorities of national policy

The criticality of the Internet for today's economy has several implications for cybersecurity policy development, the main of which is the adoption of strategies that approach cybersecurity in a comprehensive and comprehensive manner. That is, cybersecurity policy should include:

- *The importance of multi-stakeholder dialogue;*
- *The importance of economic aspects of cybersecurity;*
- *Flexible approach to policy formation and implementation;*
- *Consideration of sovereignty issues in the development of cybersecurity policy;*

– *Respect for fundamental values;*
– *Improving international cooperation;*
– *Strengthening public-private cooperation;*
– *Strengthening government coordination at the political and operational levels.*

Cybersecurity policy in Ukraine should be based on the following principles:

– introduction of a strategic approach to cybersecurity;

– comprehensive solution to cybersecurity problems, including the use of effective coordination mechanisms adapted to the culture and style of governance in the country;

– timeliness, flexibility and adaptability in decision-making in the field of cybersecurity;

– development of national capacity of teams to counter cyber incidents;

– introduction of advanced methods of cybersecurity;

– improving the protection of critical information infrastructures;

– respect for the fundamental values of freedom of information, but with the use of appropriate precautions, checks and balances;

– increasing the cyber literacy of society;

– use of a system of incentives for the development of cybersecurity and the corresponding human resources;

– cooperation with private and non-governmental organizations, development of public-private partnership;

– strengthening the fight against cybercrime;

– encouragement of research and development in the field of cybersecurity;

– development of international cooperation, in particular, by participating in the development of common norms of behavior in cyberspace.

In general, as can be seen from the experience of many countries, cybersecurity policy development is reaching a new level of maturity compared to previous policies of the first decade of the 21st century, with better leadership, better coordination and greater stakeholder involvement. At the same time, the challenges of policy-making are increasing, suggesting that governments are also facing a new level of complexity. For example, the need for greater coordination between agencies needs to be met through a higher degree of centralization, while providing dynamic and fast, almost real-time, decision-making processes at all levels. Another challenge is the need to implement integrated approaches that take into account sovereignty and economic / social issues, the participation of a wide range of public authorities and the expansion of cooperation with the private sector. Another problem is the need to maintain the openness of the Internet and fundamental values in accordance with the 2011 Recommendation of the Council on the principles of Internet policy-making. These and other challenges take time, while the key task for the cybersecurity public sector at the moment is to prepare for and counter possible serious cyber incidents, but in a way that does not undermine the openness of the Internet.

Keywords: Internet; cybersecurity; cyberspace; public administration; strategy.

Надійшла до редколегії 20.11.2020 р.