Рада з кібербезпеки України (концепція)

Володимир Стиран, експерт з кібербезпеки, CISSP CISA OSCP
Співзасновник Berezha Security, співзасновник практичної конференції з кібербезпеки NoNameCon, лідер Київського відділення OWASP Kyiv.
Резюме: https://github.com/sapran/cv
sapran@protonmail.com +380631784683

Проблематика

В Україні на державному рівні кібербезпека відсутня інституційно. Це означає, що відповідальність за формування компетентних рішень та надання професійної експертизи щодо кібербезпеки покладено на установи та органи, які або не є компетентними в предметній області, або їхні фахові знання морально застаріли в дев'яності роки минулого століття.

Державне регулювання в галузі кібербезпеки здійснюється шляхом затягування галузі в минуле, де все ще діють застарілі методичні вказівки, та через обмеження поля діяльності бізнесу та держустанов ефемерними рамками бюрократичних протоколів.

Формування кібербезпеки як галузі вимагає створення осередку сучасних експертних знань, професійного авторитету, та політичної волі, в рамках якого учасники галузі зможуть ефективно обмінюватись аргументами та проводити консультації та дебати з метою формування консенсусу. Зважені компроміси між учасниками Ради кібербезпеки України зможуть вважатися надійними експертним висновками з стратегічних питань в цій галузі.

Рада кібербезпеки України зможе закласти основу подальшим процесам побудови в державі галузі кібербезпеки та налагодженню співпраці між її суб'єктами. Але навіть на початку роботи, Рада зможе виступати компетентним консультантом всіх учасників галузі з питань кібербезпеки – якого наразі держава не має та на чиєму місці юрбляться десятки некомпетентних шарлатанів.

Джерело натхнення

Основою для запропонованої концепції стала Рада кібербезпеки Королівства Нідерланди. Нідерланди є зразковим прикладом побудови національної системи кібербезпеки, яка є одночасно економічно ефективною, сумісна із відповідними системами союзників, та не потерпає від успадкованих вад бюрократичних апаратів НАТО та ЄС. Автор концепції може надати докладні матеріали щодо доцільності вибору Нідерландської моделі розвитку як найбільш успішної та оптимальної для України, але серед основних аргументів хочеться назвати такі:

1. Безпрецедентна ефективність Нідерландської моделі кібербезпеки в плані економічної доцільності. Дослідники економіки кібербезпеки наводять приклад голландського Національного ревю кібербезпеки як фреймворку для оцінки стану

безпеки, який перевищує найпоширеніші міжнародні та галузеві стандарти, такі як ISO27001 або PCI DSS.

2. Тісні культурні та професійні зв'язки Нідерландів та України на тлі збройної агресії РФ, які значно прогресують з часів трагічної катастрофи рейсу MH17. Професійні спільноти Нідерландів та України ефективно обмінюються досвідом, а голландські спецслужби відіграють важливу роль в протистоянні російській агресії в кіберпросторі.

Мета

Рада з кібербезпеки України (РКУ) – незалежний дорадчий орган, який формулює ***стратегічні поради та рекомендації*** українським державним та комерційним організаціям, самостійно та у відповідь на їхні запити. РКУ бере участь у формуванні ***стратегії кібербезпеки*** та здійснює ***моніторинг її виконання***. РКУ складається з представників ***державних та приватних організацій*** України.

Основні напрямки діяльності РКУ:

1. Дорадча: ***Допомога*** в прийнятті стратегічних рішень шляхом обміну ***професійними знаннями та досвідом*** в галузі кібербезпеки.
2. Освітня: Підвищення ***обізнаності з питань кібербезпеки*** в суспільстві та органах влади. Сприяння створенню та розвитку ***навчання з кібербезпеки***. Симулювання та популяризація ***досліджень з кібербезпеки***.
3. Економічна: Сприяння розвитку приватного сектору, зокрема, ***українських стартапів з кібербезпеки***.
4. Дипломатична: Координація ***міжнародних відносин*** України в галузі кібербезпеки. Сприяння соціальним процесам, які позитивно відбиваються на рівні кібербезпеки України.
5. Наглядова: ***Моніторинг*** політичних, економічних, наукових та суспільних тенденцій з метою своєчасного виявлення їхнього потенційного впливу на кібербезпеку України. Моніторинг виконання стратегії кібербезпеки України.

Склад

З метою покриття якнайширшого спектру питань з кібербезпеки, склад РКУ складається із представників приватних та державних організацій в таких пропорціях:

- ***6 представників державних установ*** – органів влади, державних та спеціальних служб, які здійснюють діяльність в галузі кібербезпеки. Державні службовці та функціонери, які дотримуються прогресивних поглядів щодо кібербезпеки та готові аргументовано доводити позицію держави в раді.
- ***6 представників приватних установ*** – відомих та успішних українських комерційних компаній, які засновані в Україні та мають український капітал; та недержавних некомерційних організацій, які здійснюють діяльність в Україні.

Іншими словами, офшори, дочірні іноземні компанії та осередки іноземних NGO в склад ради не допускаються.

- ***3 представники освітніх та наукових закладів*** – авторитетних та прогресивних академічних установ, які здійснюють навчання спеціалістів в галузі кібербезпеки та проводять відповідні дослідження. Науковці та викладачі, які мають авторитет серед студентства, колег та професійної спільноти.

Перший склад ради формується шляхом проведення ***відкритого конкурсу***. Члени ради визначають ***заступників***, які можуть представляти їх у засіданнях ради. Члени ради та заступники обираються в РКУ ***щороку на один рік*** та не можуть засідати в раді довше двох років поспіль. Наступний склад РКУ визначається голосуванням за кандидатів 1/3 складу наприкінці року роботи ради. В перший та другий рік РКУ покидають 1/3 її членів, визначені випадковим жеребкуванням. (Таким чином 1/3 ради першого покоління буде змушена «відбути» три терміни.)

Рівень членства в РКУ – не статусний та не політичний, а професійний та функціональний. ***Члени ради та заступники повинні бути*** дійсними (протягом п’яти останніх років) ***практиками кібербезпеки***, і це повинно підтверджуватися досвідом, рекомендаціями визнаних експертів, дослідженнями, виступами, публікаціями, престижними міжнародними сертифікатами тощо.

Секретар ради визначається РКУ щороку голосуванням на першому засіданні за поданням члена ради. Секретар не може суміщати роль члена ради або заступника.

Голова та ***заступник голови*** ради визначаються на рік шляхом голосування на першому засіданні ради, на якому головує найстарший за віком член ради. Голова та заступник голови представляють відповідно приватний та державний сектор ради або навпаки.

Порядок роботи

РКУ проводить ***чергові засідання щомісяця***. Участь в засіданнях – персональна або дистанційна за допомогою відео зв’язку із належними засобами захисту. ***Позачергові засідання*** ради проводяться за ініціативи не менш ніж трьох дійсних членів. Кворум засідання – 11 членів або заступників. У разі відсутності члена ради, заступники беруть участь та мають право голосу. Заступники також можуть брати участь в присутності відповідного члена ради, але право голосу зберігається за останнім. Рішення РКУ приймаються прямим чи таємним голосуванням простою більшістю.

Порядок денний засідань визначається секретарем та поширюється серед членів РКУ та заступників напередодні засідань. РКУ здійснює обговорення, аргументовані дебати та голосування із метою визначення спільної позиції щодо питань порядку денного. На базі прийнятих рішень, РКУ робить рекомендації та надає поради авторам звернень та надає відповіді адресно або публічно, згідно із бажанням автора та чутливістю звернення.

Секретар ради протоколює засідання зручним способом та забезпечує збереження матеріалів засідань. У разі неможливості розглянути на черговому засіданні усі накопичені питання порядку денного, призначається наступне позачергове засідання.

Автори звернень можуть бути присутні на відповідних засіданнях ради, якщо це не суперечить рівню чутливості інших питань, що розглядаються. Рішення про присутність авторів звернень приймає Голова ради.

Рішення ради

РКУ розглядає звернення ***українських суб'єктів*** галузі кібербезпеки, а також може самостійно виносити на розгляд питання на подання членів ради та заступників.

Поради та рекомендації РКУ повинні надаватися членами ради на основі власного професійного досвіду, з використанням сучасних результатів досліджень, методичних посібників та міжнародних стандартів в галузі кібербезпеки. Вони повинні мати ***системний характер*** та бути застосовними для класу або типу проблем та задач. Так, рекомендації видані в певному контексті, повинні бути застосовні не лише до спеціального випадку та відповідного звернення, але й до більшості випадків в цьому контексті.

Рішення ради публікуються офіційними та популярними способами із метою забезпечення якнайширшого поширення серед потенційно зацікавлених суб'єктів. Щонайменше, РКУ має представництва в профільних та популярних соціальних мережах та список розсилки електронної пошти, а також активно підтримує робочий простір для спілкування із громадськістю в вигляді онлайн-форумів, груп, чатів тощо.

Рішення ради можуть виноситися на засідання інших державних органів України, таких як РНБОУ, КМУ, ВРУ тощо, із метою формування безпекового та політичного порядку денного української держави.

Інша діяльність

Рада проводить різноманітну діяльність поза засіданнями та прийняттям рішень. Зокрема, члени ради та заступники проводять консультаційні зустрічі із організаціями, виступають з підтримкою на професійних заходах, беруть участь в дослідницьких проектах, представляють Україну на міжнародних професійних подіях, беруть участь складах комісій з розслідування інцидентів стратегічного значення, виступають із мотиваційними промовами перед студентством, виступають як ментори державних службовців в галузі кібербезпеки тощо.