1. Огляд ринку кібербезпеки України

Станом на початок 2021 рік в України сформувався стійкий ринок товарів та послуг індустрії кібербезпеки, ступінь конкуренції на якому оцінюється як висока.
Достовірної статистики стосовно ринку кібербезпеки України на теперішній день не існує через відсутність всеукраїнської професійної асоціації та/або єдиного державного регулятора (координатора), до яких би надходили релевантні дані для подальшого аналізу та оприлюднення.
За експертними оцінками, більшість учасників ринку (близько 60-70%) орієнтовано на внутрішнього споживача, близько 15-20% має пріоритет на зовнішній ринок, виключно на зовнішній ринок працює не більше 5-10% гравців ринку.

Розподіл ринку кібербезпеки в Україні в цілому збігаються з розподілом ринку країн з розвинутою кібер-індустрією, і його напрямки можна умовно поділити на три нерівні частини:

- виробники (вендори) кібербезпекового програмного забезпечення (software) та відповідного обладнання (hardware): на українському ринку прямо чи через посередників представлені практично усі провідні світові вендори: Cisco, Fortinet, Mikrotik, McAfee, PaloAlto, FireEye. Безпосередньою реалізацією обладнання, рішень, софта та технологій вендорів на території України займаються компанії-дистриб’ютори (ERC, МУК, Бакотек, Softprom);
- компанії-інтегратори, які вбудовують (адаптують) рішення від різних виробників в існуючі комп’ютерні мережі українських клієнтів: таких компаній найбільше і, як правило, вони обслуговують декілька (до 10) великих замовників; (OptiData, It-solutions, Integrity Vision, Світ-IT, IT IS, RMRF, NetWave);
- консалтингові компанії, які здебільшого надають послуги з кібербезпеки: аудит безпеки IT-інфраструктури, тестування на проникнення, аналіз коду, організація проведення Bug Bounty, відповідність нормативним вимогам (compliance), кібер-розвідка (Threat Intelligence), тощо; такі компанії спеціалізуються здебільшого на високо-рівневих технічних аспектах кібербезпеки і кількість таких компаній невелика відносно загальної кількості учасників українського кібер-ринку; (Berezha Security, 10Guards, Advantio, UnderDefense, Імпрувмент Сервіс.)

Організації державної форми власності (державні органи та державні компанії) також представлені на кібер-ринку України, але переважно у ролі споживача товарів та послуг. Їхня доля на ринку є малопомітною через низькі фінансові можливості та законодавчі обмеження стосовно процедур закупівлі послуг з кібербезпеки, орієнтованих на найнижчу ціну, що прямо впливає на симетрично найнижчу якість таких послуг.

Українська спільнота фахівців з кібербезпеки (кібер-ком’юніті) є доволі активною та також впливає на розвиток ринку та підвищення загально-національного рівня кібер-захищеності. Активність кібер-ком’юніті полягає у проведенні масштабних (до 600 учасників) кібер-конференцій, впливу на роботу державних інституцій через громадські об’єднання, а також популяризації ідей кібербезпеки у публічних медіа та соціальних мережах.

Основними споживачами товарів та послуг індустрії кібербезпеки України є переважно великий та середній бізнес: банки та кредитно-фінансові організації, транспортна галузь, енергетика, машинобудування, зв'язок, розробники програмного забезпечення, торгівельні та виробничі компанії та багато інших компаній, робота яких прямо чи опосередковано залежить від рівня кібер-захищеності їхніх комп’ютерних та інформаційних мереж.

Головними ризиками споживачі товарів та послуг індустрії кібербезпеки України вважають наступні:

- Можливі витоки та компрометація даних
- Потенційна можливість викрадання грошових коштів та ресурсів компанії
- Можливе блокування зловмисниками публічних інформаційних ресурсів як методу комунікації з клієнтами
- Промислове шпигунство як метод конкурентної боротьби
- Недружнє ставлення органів влади, корупція

Однією з ключових проблем функціонування внутрішнього кібер-ринку та його інтеграції з ринками ЄС є відсутність єдиного центру компетенції та довіри. Особливо це актуально для тих споживачів товарів та послуг, які не мають можливості самостійно оцінити компетентність та надійності окремих «продавців» на даному ринку. Через це на ринку існують некомпетентні та нечесні гравці, які наносять репутаційну шкоди іншим гравцям та знижують рівень довіри до індустрії загалом.
Для вирішення подібних проблем зазвичай створюється професійна асоціація учасників місцевого ринку, але справжньої достатньо авторитетної професійної асоціації наразі в Україні не існує. Натомість існує багато маловідомих об’єднань, які називають себе професійними асоціаціями учасників ринку кібербезпеки, але засновані вони одним або кількома учасниками ринку (часто з сумнівною компетенцією або діловою репутацією) і не викликають довіри в усіх інших учасників. Причин для такого стану справ існує кілька: нерівний рівень кваліфікації різних гравців, висока конкуренція, різні підходи до оцінки якості послуг, репутаційна неоднорідність ринку, його неструктурованість.
Але головною причиною є системна недовіра між учасниками ринку товарів та послуг кібербезпеки, хоча більшість з них готова до

створення професійної асоціації та багато учасників неодноразово наголошували на такій потребі для ринку в цілому.

----

2. Наявні проблеми в сфері кібербезпеки та захисту персональних даних в Україні, які заважають інтеграції до DSM

2.1
Існування та розвиток ринку кібербезпеки України відбувається завдяки самим учасникам ринку, відповідно до законів економічного розвитку та за умови практично повної відсутності державного регулювання.
Завдяки цьому ринок розвивається, і на ньому існує здорова конкуренція.

Разом з тим, відсутність загально-національної координації та єдиних “правил гри” теж має свої негативні сторони.

Серед найпомітніших з них є розсинхронізована державна політика щодо захисту національних інтересів держави Україна у кіберпросторі.
Згідно Закону України “Про основні засади забезпечення кібербезпеки України”[1], основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України.
Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.
Усі зазначені організації є державними органами, більшість з яких відносяться до силового блоку.
Приватний сектор та кібер-ком’юніті, кількість представників яких загалом у кібер-індустрії переважає 80%, серед основних суб’єктів національної системи кібербезпеки не представлені взагалі. Також не представлені підприємства критичної інфраструктури, на захист яких мають спрямовувати свої зусилля зазначені у Законі “основні суб’єкти”.
Через такий дисбаланс відсутнє поле для діалогу та взаємопорозуміння, можливості напрацювання спільних ефективних рішень є обмеженими, а ефективність шляхів побудови ефективної моделі національної кібербезпеки залишається низькою.

Крім того, навіть поміж основними суб’єктами національної системи кібербезпеки не існує чітких домовленостей та єдиного бачення

[1] https://zakon.rada.gov.ua/laws/show/2163-19#Text

шляхів розвитку національної кібербезпеки. Рівень міжвідомчої конкуренції за фінансування та повноваження залишається між ними високим, що, за умов ігнорування значного потенціалу приватного сектору, негативно впливає на стан національної кібербезпеки та державної політики у цій сфері.
У 2019 році було створено Міністерство цифрової трансформації України[2], яке також претендую на лідируючу роль у формуванні державної політики у сфері кібербезпеки, хоча не має для цього законодавчих підстав. Але завдяки фактичним преференціям з боку найвищих посадовців виконавчої влади України, Міністерство активно втручається у питання національної кібер-захищеності України, що додає ентропії у і без того розбалансовану державну кібер-політику.

2.2
Питання свободи доступу до глобальної мережі Інтернет та свободи поширення інформації у ньому досить гостро стоїть у сучасній Україні.

Під приводом посилення боротьби зі злочинністю (дитяче порно, тероризм, сепаратизм, шахрайство) владні структури та правоохоронні органи не полишають спроб налагодити масове стеження за користувачами Інтернет і таким чином обмежити права громадян на вільне поширення інформації та свободу слова.

Українськими судами формально заблоковано доступ до більш, ніж 100 інформаційних ресурсів в Інтернет. При цьому легітимність цих судових рішень є досить сумнівною, а рішення могли бути прийняті під значним тиском правоохоронної системи.

Указом Президента України № 133/2017 від 15 травня 2017 року[3] про введення в дію рішення РНБО України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».
Особливістю нових санкцій стала вимога блокування інтернет-провайдерами доступу до веб-ресурсів інтернет-компаній ВКонтакті, Одноклассники, «Mail.ru», «Яндекс», «Лабораторія Касперського», «Dr.Web», офіційного дистриб'ютора «1С» на території України та інших строком на 3 роки.
Зазначений Указ протирічив деяким нормам українського законодавства та багаторазово критикувався професійною юридичною спільнотою, а його його легітимність досить сумнівна. Також Указ не містив механізмів технічної імплементації блокувань, тому деякі провайдери рішення даного Указу не виконували або виконувли частково.

[2] https://thedigital.gov.ua
[3] https://www.president.gov.ua/documents/1332017-21850

Враховуючи те, що владні структури не мають ані технічних можливостей заблокувати певні ресурси, ані відповідних повноважень, продовжуються спроби закріпити у законах України право працівників правоохоронної системи мати безконтрольний доступ як до метаданих про українських користувачів Інтернет, так і до змісту інформації, що передається каналами Інтернет-комунікацій.

Подібні ініціативи з боку влади мали місце у 2017 та 2018 роках, коли у Верховну Раду України вносився законопроект № 6688, згідно якого оператори та провайдери Інтернет-комунікацій зобов'язувалися за власні кошти встановити на своїх вузлах спеціальне обладнання для перехоплення інформації їхніх користувачів. При цьому законопроектом передбачалася можливість прямого доступу без рішення суду невизначеної кількості правоохоронців, слідчих, прокурорів до трафіку користувачів без запровадження механізмів контролю за цією діяльністю.

У 2017 та 2018 роках законопроект №6688 викликав бурхливі та масові протести як з боку провайдерів/операторів зв'язку, так і з боку IT-середовища, громадських організацій, професійної спільноти. Внаслідок зазначених протестів законопроект обидва рази 6688 був переглянутий, а згодом відкликаний.

Але спроби владних структур та правоохоронців встановити контроль за комунікаціями в Інтернет не припиняються.
Так, у січні 2021 року набув чинності Закон України «Про електронні комунікації»[4], в ст. 121 якого заначено дав принципових для правоохоронних органів моменти:
"2. Зняття інформації з електронних комунікаційних мереж постачальників електронних комунікаційних послуг забезпечується єдиною системою технічних засобів, що використовується усіма уповноваженими законом органами, на умовах автономного доступу до інформації у порядку, визначеному законодавством"
Цим пунктом фактично узаконено можливість доступну поліцейських структур напряму в мережі провайдерів/операторів. Механізм контролю за можливими зловживаннями у Законі не визначено.
У наступному пункті закріплено зобов'язання провайдерів/операторів сприяти наданню такого безконтрольного прямого доступу до своїх мереж та інформації абонентів:
"3. Постачальник електронних комунікаційних послуг та/або мереж повинен забезпечити можливість підключення технічних засобів, зазначених у частині другій цієї статті, в точці для такого доступу в електронній комунікаційній мереж, визначеній постачальником електронних комунікаційних мереж та/або послуг».
Таким чином, фактично у Законі України «Про електронні комунікації» закріплено право правоохоронних структур України запровадити масове стеження за невизначеною кількістю користувачів Інтернет,

[4] https://zakon.rada.gov.ua/laws/show/1089-20#Text

при цьому не зазначено запобіжники до можливих зловживань та перебільшення повноважень з боку працівників органів правопорядку.

Натомість у жодному із законів України не закріплена заборона втручання у безперешкодне функціонування мережі Інтернет, а також не захищені права громадян на вільний доступ до інформації в Інтернет та свободу поширення не забороненої законом інформації. Наявність такого Закону позитивно вплинула б на стан захисту прав та свобод громадян України, а також сприяла б оздоровленню стосунків між державою та громадянином та позначила б дійсне прагнення до побудови правової держави.

2.3
Чинне українське національне кібер-законодавство є застарілим та слабо корелюється з ландшафтом сучасних кібер-загроз та викликів. Законодавчих, підзаконних, регуляторних та нормативно-правових актів існує велика кількість, але багато з них не узгоджені між собою (а інколи протирічать одне одному), не регулюють актуальні аспекти національної кібербезпеки та функціонування відповідного сектору економіки, часто не є актуальними для сучасних загроз, незручні у користуванні, деякі вимоги важко виконати без значних ресурсів, багато нормативних актів мають корупційну складову.
Також українське законодавство не адаптовано до термінології, вимог та сутності законодавства ЄС та міжнародних актів. Зокрема, Конвенції з кіберзлочинності[5], яка ратифікована українським парламентом у 2005 році, але досі не імплементована у чинне законодавство у повному обсязі.
Тобто наразі кібер-сфера України законодавчо регулюється лише частково, фактична діяльність у цій сфері централізовано координується лише для держструктур, і теж частково та з недостатньою ефективністю.
Як виконавча, так і законодавча гілки влади усвідомлюють складність завдання реформувати законодавче забезпечення кібер-сфери, але також розуміють нездатність зробити це силами лише державних чиновників та посадовців.
Численні заклики влади до професійної спільноти долучитися до процесу реформування законодавчої сфери галузі кібербезпеки не знаходять розуміння через непрозорість умов такої співпраці, невпевненість у практичній імплементації її результатів, високі корупційні ризики процесу розробки законодавства (лоббізм з боку великих компаній), а також через загальну недовіру до компетентності представників державного сектору.
Через ситуацію, що склалася, процес реформування кібер-законодавства України наразі знаходиться у патовій позиції, оскільки драйвером цього процесу мав би бути ринок, але ринок переважно не довіряє владі та не вірить у перспективи подібної співпраці. Влада,

[5] https://zakon.rada.gov.ua/laws/show/994_575#Text

зі свого боку, продемонструвала системну неспроможність реформувати кібер-законодавство без тісної співпраці з недержавним сектором.
Також для бізнесу та ком'юніті не зрозуміло з якою з дев'яти державних інституцій слід співпрацювати, яка з них здатна імплементувати нове законодавство, та яка з них нестиме відповідальність за розробку нових чесних правил гри та за результати реформи сектору в цілому.
Додатково викликає сумніви рівень підготовки фахівців державного сектору та ступінь їх мотивації для реалізації відповідних реформ.
Таким чином, на даний час жоден з 9 основних суб'єктів національної системи кібербезпеки не має повноважень, відповідальності та бажання системно підійти до реформування кібер-сфери за зразком NIS Directive та ENISA Regulation:
Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013[6] concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (ENISA Regulation)[7]; Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016[8] concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

Для започаткування проекту суттєвої актуалізації системи кібер-законодавства як невід'ємної частини докорінного реформування всього сектору кібербезпеки, в Україні станом на 2021 рік відсутні як політична воля правлячих еліт, так і належна компетенція виконавців, а також відчувається брак розуміння необхідності такого реформування. Також у державних установах мало вкрай недостатньо представлено прагнення до співпраці з приватним сектором на рівних умовах та здатність нести відповідальність за результати подібних масштабних змін.

2.4
Питання захисту персональних даних є однім з найпроблемніших в Україні 2021 року.
Фактично цей аспект усунуто з переліку актуальних завдань, а захист персональних даних громадян не здійснюється, а лише імітується.
До 201 року в Україні існувала Державна служба захисту персональних даних[9], яка системно займалися даною

[6] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

[7] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[8] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[9] https://uk.wikipedia.org/wiki/Державна_служба_України_з_питань_захисту_персональних_даних

проблематикою.
Але у 2014 році зазначена Державна служба була розформована, а функції захисту персональних даних покладено на Уповноваженого Верховної Ради України з прав людини (омбудсмена)[10].
З метою забезпечення виконання Уповноваженим функцій контролю за виконанням законодавства в сфері захисту персональних даних в Секретаріаті Уповноваженого Верхової Ради України з прав людини створено Департамент у сфері захисту персональних даних.
Але зазначений Депртамент не має дієвих повноважень, сил та засобів з ефективного захисту персональних даних громадян України, а працівники Департаменту не мають належної кваліфікації.
Внаслідок такої ситуації права громадян на захист персональних даних постійно та масово порушуються, і практично ніхто не несе за це відповідальності.
Тому утворення незалежного уповноваженого органу з питань захисту персональних даних, як того вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних[11] та GDPR[12] є нагальною потребою та першочерговою задачею для України на шляху до комплексного вирішення проблем інформаційної та кібербезпеки.

---

3. Прогноз щодо змін в Україні після ухвалення Digital Service Act, Cybersecurity Strategy, інших важливих європейських ініціатив

На жаль, держава Україна системно демонструє низький рівень уваги до питань власної кібербезпеки, незважаючи на тяжкі наслідки активної фази російсько-української кібервійни 2014-2018 років.
У той час, коли ЄС запроваджує поліпшені правила NIS Directive, GDPR, Open Internet Access Regulation[13] та ENISA Regulation, українська влада лише імітує зацікавленість у підвищенні кіберзахисту громадян, критичної інфраструктури, бізнесу та економіки.
Недосконалий та частково непрацюючий Закон України «Про основні засади забезпечення кібербезпеки», який неодноразово піддавався критиці експертним середовищем – системно не оновлювався з 2017 року.
Правова база із захисту критичної інфраструктури почала розроблятися лише у 2020 році.
Стан захисту персональних даних лише погіршується.

---

[10] https://ombudsman.gov.ua/ua/page/zpd/

[11] https://zakon.rada.gov.ua/laws/show/994_326#Text

[12] https://gdpr-info.eu

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.310.01.0001.01.ENG&toc=OJ:L:2015:310:TOC

Судова практика по блокуванню веб-ресурсів містить прямі порушення законодавства та порушує основні права громадян.
Державні органи, уповноважені займатися кібербезпекою та кібер-захистом недостатньо компетентні у цих питаннях, а державно-приватне партнерство у цій сфері дотепер не налагоджено і перспективи його налагодження доволі сумнівні.
Силові структури не полишають спроб налагодження масового стеження за громадянами у Інтернет.
Координація національної системи кібербезпеки країни по суті – не здійснюється.
Каналами міжнародної технічної допомоги у країну надходять технології, обладнання, проводяться тренінги та консультації, але ключові проблеми залишаються невирішеними, і на загальний рівень кібербезпеки країни міжнародні програми допомоги не впливають.

Аналіз фактичної діяльності та/або бездіяльності органів державної влади України у сфері кібербезпеки та кіберзахисту свідчить про фактичне небажання наслідувати прогресивні світові практики. При цьому офіційні особи формально, на словах, визнають важливість ролі кібербезпеки у сучасному Світі, але практичними ділами подібні заяви майже не підкріплені.
Існує велика вірогідність того, що розробка та прийняття нових важливих європейських ініціатив досить мало або ніяк не вплине на покращення ситуації з національною кібербезпекою та станом кіберзахисту критичної інфраструктури в Україні.

---

4. Пропозиції щодо бажаних подальших дій

Враховуючи неефективність заходів органів державної влади України з питань покращення національної кібербезпеки, а також низьку ефективність поточних міжнародних програм допомоги у цій сфері, вважається доцільним зосередити зусилля міжнародних донорів та друзів України на напрямку вдосконалення фундаментальних основ побудови системи національної кібербезпеки– довіри між стейкхолдерами - із широким залученням професійної спільноти та українського кібер-бізнесу.
Як відомо, успішні практики побудови ефективних систем колективного кібер-захисту будуються на взаємні довірі та повазі між усіма її учасниками, і цей ключовий елемент повністю відсутній у конструкції будівлі національної кібербезпеки України.
Ключові стейкхолдери – кібер-бізнес, кібер-спільнота, державні інституції та кібер-наука – критично мало довіряють один одному і не мають чітких спільних позицій навіть всередині своїх розрізнених та неструктурованих екосистем.

Напрацювання довіри між усіма ключовими стейкхолдерами українського кібербезпекового сектору у рамках нового окремого проекту за умов незалежного фінансування групою міжнародних

донорів повинен стати першим, але визначальним етапом для створення у подальшому працюючого прототипу моделі національної кібербезпеки України.
Підтримка проекту усіма ключовими стейкхолдерами та отриманий від них кредит довіри буде використаний для налагодження ефективної взаємодії всередині країни, зокрема для побудови працюючого прототипу національної системи обміну інформацією про інциденти.
У свою чергу, працюючий прототип системи обміну інформацією про інциденти міг би стати основою для продовження побудови ефективної системи національної кібербезпеки в усіх секторах економіки (у тому числі у критичній інфраструктурі), що суттєво підвищило б кібер-захищеність України.

Цілями подібного проекту повинні бути:
- Напрацювання довіри між ключовими стейкхолдерами: кібер-бізнесом, кібер-ком'юніті, органами державної влади (виконавча та законодавча гілки), кібер-наукою/академією, IT-громадськістю, операторами/провайдерами, міжнародною кібер-спільнотою.
- Побудова горизонтальних зв'язків між ключовими стейкхолдерами.
- Створення стійкого механізму співпраці та партнерства у сфері кібербезпеки між ключовими стейкхолдерами.

Принципи проекту:
- Домінування професіоналізму та ділової репутації
- Якісні публічні комунікації, засновані на відкритості та фаховості
- Максимальна прозорість щодо фінансування проекту
- Врахування інтересів різних стейкхолдерів на засадах рівноправ'я
- Заохочення професійного підходу та розвитку ринку кібербезпеки
- Незалежність від державного фінансування
- Нульова толерантність до корупції та будь-якої "нечесної гри"

Шляхи можливої реалізації:
1) В рамках вибудовування довіри між усіма суб'єктами кібербезпеки, створити незалежну Об'єднану Раду Кібер-Експертизи (робоча абревіатура ОРКЕ), до якої на громадських засадах увійдуть найавторитетніші експерти усіх основних стейкхолдерів. Кожен з них має бути відомим професіоналом з бездоганною діловою репутацією, що сприятиме підвищенню довіри до новоствореного осередку кібер-експертизи.

2) За сприяння ОРКЕ будувати горизонтальні зв'язки як між суб'єктами забезпечення кібербезпеки як по галузях, так і між суб'єктами різних стейкхолдерів: офіціні та неформальні зустрічі кібер-фахівців та їхніх керівників, семінари з обміну досвідом, міні-конференції, змагання, кібер-навчання, тощо.

3) Під егідою ОРКЕ розробити зрозумілі та прозорі правила та принципи для моделі державно-приватного партнерства у сфері національної кібербезпеки. Розроблені принципи та правила запропонувати на затвердження органами влади.

4) Під егідою ОРКЕ започаткувати проект з розробки нового кібер-законодавства, синхронізованого як всередині країни, так і з міжнародними стандартами, конвенцією з кіберзлочинності, NIS, GDPR та іншими нормативними документами ЄС. Підготовлені напрацювання запропонувати на затвердження органами влади.

5) Під егідою ОРКЕ розробити принципи створення незалежного національного регулятора з питань захисту персональних даних (у відповідності до GDPR), а також законодавства із захисту цифрових свобод громадян.
Підготовлені напрацювання запропонувати на затвердження органами влади.

6) З використанням ОРКЕ та за участі учасників ринку, розробити загальні правила взаємодії його учасників, Code of Conduct для кібер-ринку, набір мінімальних вимог до компаній на кібер-ринку, за потреби – розробити систему оцінювання кібер-фахівців, тощо. Сприяти у заснуванні незалежної асоціації учасників ринку кібербезпеки України (за ініціативою за безумовної підтримки учасників ринку)

7) Максимальна популяризація мінімальних правил кібербезпеки (кібер-гігієна) та тематики «кібербезпека» загалом: блог, подкаст, канал на YouTube, регулярні повідомлення у соціальних мережах, коментарі та інтерв'ю членів ОРКЕ для медіа (телеканали радіостанції, періодичні видання), відкриті онлайн-дискусії. Організація регулярних мітапів, конференцій, круглих столів на теми кібербезпеки під егідою ОРКЕ, виступи експертів перед студентами профільних факультетів, організація кібернавчань, CTF, тощо.

8) Підготовкою рішень ОРКЕ та операційними питаннями імплементації її рішень займатиметься постійно діюча робоча група (виконавчий комітет) з числа професіоналів у відповідних галузях за ринковох вартістю їхніх послуг.

Схожі за ідеями "Пропозиції з реформування національної системи кібербезпеки"[14] були підготвлені ініціативною групою у складі сімох найвідоміших українських експертів з кібербезпеки, але її ключові ідеї та принципи залишаються нереалізованими та незатребуваними. Окремі положення та ініціативи із зазначених "Пропозицій.." деякі органи влади намагаються реалізувати, але відбувається це без врахування системних ідеологічних засад: рівноправного

[14] https://www.slideshare.net/KostiantynKorsun/sean-brian-townsend

партнерства стейкхолдерів, відмови від “керівної ролі держави” під час реформування, реалізація інтересів держави через інтереси її громадян, прозорий механізм фінасування проекту з реформування сектору національної кібербезпеки, напрацювання кредиту довіри суспільства як головного драйвера подальшого розвитку.

У якості позитивного прикладу створення об’єднання кібер-стейкхолдерів можна навести CyberScotland Partnership (Партнерство КіберШотландії) [15], до якого увішли 10 організацій, у тому числі бізнес-асоціація Scottish Business Resilience Centre (Шотландський Центр Кібер-Відновлювальноздатності), але також і Уряд Шотландії та Поліція Шотландії.
Коаліція з 10 організацій, які увійшли до складу CyberScotland Partnership проголошує своєю метою “…реагувати на виклики задля ясності навколо кібербезпеки як від приватних осіб, так і від бізнесу” to respond to calls for clarity around cyber security both from private individuals and businesses.)
Також CyberScotland Partnership не є і не може мати якихось владно-примусових повноважень, оскільки це добровільне об’єднання ключових кібер-стейкхолдерів на основі взаємної довіри.
CyberScotland пропонує свої ресурси кожному (не тільки для державних органів), хто шукає інформацію та підтримку з питань кібербезпеки та проблем відновлювальноздатності бізнесу, а також у питаннях кібер-кар’єри, розвитку навичок, чи то настанов.» (…central online hub to offer resources for anyone seeking information and support across a number of cyber security and business resilience issues – as well as cyber careers and skills support and guidance.)
Задля підтримки бізнесу, CyberScotland Partnership обіцяє “сприяти розквіту шотландських кібербезпекових продуктів та послуг” (…the partnership will help to promote Scotland’s flourishing cyber security products and service industry.)
Нове кібер-об’єднання Шотландії також запобігатиме «дублюванню зусиль».
Кілька цифр про CyberScotland Partnership: національний кібербезпековий «кластер» налічує близько 230 компаній, з яких 48% засновані у Шотландії, і при цьому кожен рік з’являється близько 10 новий підприємств.
Приклад Шотландії не слід сприймати як зразок та прямий приклад до наслідування через невідповідність ряду ключових вхідних умов: культурологічних особливостей, характеру стосунків сусіпільства та влади, давнішу історію демократичного урядування у країні, наявність більш справедливої системи судочинства, вищий рівень довіри до владних інституцій, тощо.
Але разом з тим, використати дух та ідеї подібного кібер-об’єднання під час розбудови принципово нової системи національної кібербезпеки було б корисно для усіх українських кібер-стейкхолдерів задля покращення рівня кібербезпеки України.

[15] https://www.computerweekly.com/news/252496747/CyberScotland-offers-centralised-security-resource-hub