НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ICWR
INSTITUTE OF CYBER WARFARE RESEARCH

ОЧІКУВАННЯ ТА РЕАЛЬНІСТЬ КІБЕРВІЙНИ

З ЧИМ ЗІТКНУЛАСЬ ТА ЯК ВІДПОВІДАЛА УКРАЇНА НА КІБЕРАГРЕСІЮ

Дослідження «Очікування та реальність кібервійни. З чим зіткнулась та як відповідала Україна на кіберагресію» підготовлене Інститутом дослідження кібервійни завдяки підтримці, наданій Агентством США з міжнародного розвитку (USAID), через Проєкт USAID «Кібербезпека критично важливої інфраструктури України». Думки авторів, висловлені в цьому дослідженні, не обов'язково відображають погляди Агентства США з міжнародного розвитку або Уряду США

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ICWR
INSTITUTE OF CYBER WARFARE RESEARCH

ЗМІСТ

ВСТУП

Метою цього дослідження було визначено не зробити новий зріз вивчених уроків кібервійни, а зосередитись на безпосередньому досвіді та очікуваннях (а отже і якості планування) українських фахівців з кібербезпеки та тією кібербезпековою ситуацією, з якою вони реально стикнулись після 24 лютого 2022 року. Цей аспект має важливе значення, оскільки розуміння якості планування кібербезпекової політики як на рівні держави, так і окремих організацій, дозволяє краще зрозуміти актуальність викликів, до котрих готувалась держава в умовах активної кібервійни, та які конкретні кроки щодо недопущення ескалації були найбільш вдалими, а також яка теперішня ситуація з кібербезпекою в державі.

ПОПЕРЕДНІ ДОСЛІДЖЕННЯ УРОКІВ КІБЕРВІЙНИ

З перших місяців російського вторгнення експерти намагались оцінювати, з одного боку, вплив кіберскладової на військово-політичну ситуацію та особливості розгортання конфлікту (наприклад, роботи «Кіберфронт. Як рф атакує Україну та чи готові ми захищатися»[1], «Russia's War in Ukraine: The War in Cyberspace»[2], «Defending Ukraine: Early Lessons from the Cyber War»[3], «An overview of Russia's cyberattack activity in Ukraine»[4] або дискусії під час CYBERUK 2022 у травні 2022 року), а з іншого – визначити на загальному рівні, які саме стратегічні уроки можна винести з кібервійни між росією та Україною.

У перших оцінках динаміки кібервійни зазначалась низька варіативність російських кібератак (здебільшого – традиційний DDoS та фішинг як основи), відсутність помітного ефекту для діяльності українських об'єктів критичної інфраструктури (винятком є кейс кібератаки на VIASAT і, як стало відомо пізніше, декілька спроб використати viper'и для атаки на енергетику), проведення кіберактивності в тісній співпраці зі спеціальними службами Республіки Білорусь. Також перші місяці протистояння показали таке:

- ✓ не допущено виведення з ладу важливих для життєдіяльності держави IT-систем;
- ✓ українським та міжнародним кіберфахівцям вдалося контратакувати цілу низку об'єктів на території рф, викрасти дані численних російських компаній та організацій (серед них – дані про російських військовослужбовців, що беруть участь у війні проти України);
- ✓ здатність протистояти кібератакам більше, ніж коли-небудь, залежить від дієвої співпраці на міжнародному рівні;
- ✓ розвідка кіберзагроз та впровадження EDR суттєво допомогли протистояти руйнівним кібератакам;
- ✓ росія розуміє важливість порушення єдності партнерів, тому атакує не лише Україну, але і її союзників;
- ✓ кібершпигунство досі є вагомим елементом кіберактивності, хоча очікувались більш руйнівні наслідки кібератак під час конфлікту.

[1] Кіберфронт. Як РФ атакує Україну та чи готові ми захищатися // https://biz.nv.ua/ukr/experts/kiberataki-rosiji-na-ukrajinu-yak-prohodyat-ta-chim-zagrozhuyut-ostanni-novini-50236927.html2 Russia's War in Ukraine: The War in Cyberspace // https://icds.ee/en/russias-war-in-ukraine-the-war-in-cyberspace/3 Defending Ukraine: Early Lessons from the Cyber War // https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/?fbclid=IwZXh0bgNhZW0CMTEAAR3n7BOFahiVi_nGsrHVfexR4Gh7_MDMYBRvNxolQBl6f1RRq5u3GRAlXQk_aem_AaGO9RmBwcq2yg-ID_weJVJhiCZdO0gk4ljzztt76nG9Cw64AqJuceSA_1QvMua1coKU-7vB4dBwgtGdb9GrOgJ24 An overview of Russia's cyberattack activity in Ukraine // https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd5 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[2] Russia's War in Ukraine: The War in Cyberspace // https://icds.ee/en/russias-war-in-ukraine-the-war-in-cyberspace/

[3] Defending Ukraine: Early Lessons from the Cyber War // https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/?fbclid=IwZXh0bgNhZW0CMTEAAR3n7BOFahiVi_nGsrHVfexR4Gh7_MDMYBRvNxolQBl6f1RRq5u3GRAlXQk_aem_

[4] AaGO9RmBwcq2yg-ID_weJVJhiCZdO0gk4ljzztt76nG9Cw64AqJuceSA_1QvMua1coKU-7vB4dBwgtGdb9GrOgJ2

Прогнози квітня 2022 року вказували на те, що кібератаки проти України будуть лише посилюватись, а злочинні російські актори активно виходитимуть за межі України й ареалу конфлікту[5].

Перші ж узагальнення ситуації (переважно з боку західних аналітичних центрів або чиновників) та обережні формулювання уроків кібервійни почали з'являтись лише з осені 2022 року. До таких оцінювань слід віднести:

✓ **Жовтень 2022.** Висновки директора з кібербезпеки Агентства національної безпеки США (АНБ) Роба Джойса щодо російсько-української кібервійни[6] з акцентом на важливості державно-приватного партнерства, спільної роботи з міжнародними партнерами та необхідності розвивати навички стійкості.

✓ **Грудень 2022.** Аналіз від Carnegie Endowment For International Peace[7]. Аналітик центру пропонує комплексний погляд на вплив кібероперацій росії проти України з моменту вторгнення. Основний висновок – операції не мали стратегічного впливу, але також немає й уроків, які б могли використати інші країни.

✓ **Січень 2023.** Аналіз ситуації від спеціалізованого видання Breaking Defense. Загальний аналіз причин безуспішності російських кібератак в Україні і як це пов'язано із наданою міжнародною допомогою[8].

✓ **Лютий 2023.** Оцінки Mandiant першого року кібервійни[9]. Акцент на помітній політизації кіберзлочинних груп стосовно російсько-української війни, а також прогнози щодо посилення інформаційних операцій, що поєднували ІПСО та кіберскладові, не лише проти України, але і її союзників.

✓ **Лютий 2023.** Дослідження ESET щодо ролі wiper'ів у російсько-українській кібервійні[10]. Основний висновок – кібератаки wiper'ами не є чимось новим для України, хоча складно не відзначити істотне зростання динаміки їх використання, що розпочалася з лютого 2022 року.

✓ **Лютий 2023.** Європейська ініціатива з дослідження кіберконфліктів (ECCRI) підготувала доповідь «Кібервимір російсько-української війни», яка, окрім уже наданих оцінювань щодо характеру кіберконфлікту, концентрується на ролі кіберактивістів обох сторін та на розмитті їх статусу в сучасних конфліктах.

[5] An overview of Russia's cyberattack activity in Ukraine // https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[6] https://www.infosecurity-magazine.com/news/nsa-6-takeaways-war-ukraine/?fbclid=IwZXh0bgNhZW0CMTEAAR0uikj7syNknUvPyYNxrwtqCx-iDBzPYqX7M9P5awvJ_4K7Fye0cWzhtAqE_aem_AaFB_BtyRlvNLwDDx5IRecc_mITNUWEbtE95aWeCmFmmguW5hqFUrJBdRwaVTsFWEj002sxeO-JpEluUDNin_AZ5c

[7] https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en

[8] https://breakingdefense.com/2023/01/no-big-bang-cyber-successes-in-ukraine-are-no-cause-for-complacency-in-us/?fbclid=IwZXh0bgNhZW0CMTEAAR0HhLJuJ1rPeBHTRiK2iy-ndxmVU3BEtmPTqHgzYFi6afG9xzAw0TuvkfM_aem_AaF8zPdmVzRutnKz0XhJOaz_Vs-FARz-7N_e3tQnl8lf_7wsicuBPIJuQz00oE28XlsaERAJHuNF4d7C9qizgIHq

[9] https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/?fbclid=IwZXh0bgNhZW0CMTAAAR1k5om7iA33TJM5H2KjM1cYyXgYtRDYlXqX2ARcOXrDEOVwe-Ydm6Q3Inc_aem_AaGkwze-VkbbKrrb8Etm2kvp5S91w-l3bM0H67QIkbtuE0k0j_Fj422TAkwz3h-hJrp_tDmMg4ci8j8F3SXR9BcC

[10] https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/?fbclid=IwZXh0bgNhZW0CMTEAAR01PriLB7nKV-9W0UFrZlYJ7jgwZD8mdZoZNAfQcmnHwrGpzFKW3iG5ek4_aem_AaGu4ds0kaFbzmmRJAi2wrPzfDlquW99f7QVlPQey10KQMEtlJoaSYpIH8JuF-SKbTrNwuDAN4YEPYx8yoXJsIJ0K

✓ **Березень 2023.** Оцінка Microsoft[11], яка визначає фактор wiper'ів у перший рік війни (щонайменше 9 нових сімейств), водночас вказує на новий помітний трек російської кіберактивності – більше атак проти країн-союзників із шпигунською метою.

✓ **Березень 2023.** Аналітичне узагальнення International Institute for Strategic Studies (IISS)[12], яке зосереджене не лише на оцінюванні зусиль України та росії, а й на довгострокових викликах, що постають перед Україною у випадку затяжного конфлікту (наприклад, проблемі імпровізованості багатьох рішень кіберзахисту, активного перегрупування російських кіберфахівців тощо). Загальний висновок автора підтверджує аналогічний від Carnegie Endowment – досвід України може виявитись настільки унікальним, що не зможе бути адаптований як надійна стратегія іншими країнами.

✓ **Травень 2023.** Американський аналітичний центр Center for Strategic and International Studies (CSIS)[13] представив комплексне дослідження «Розвиток кібероперацій та можливостей». У серії есе описуються різні аспекти кіберпротистояння, зокрема важливість обміну інформацією між союзниками, необхідність ДПП, але водночас зауважують на обережностях у спробі скопіювати український досвід спротиву, адже агресор зі свого боку продемонстрував значну некомпетентність, якої будуть уникати всі інші агресори.

✓ **Липень 2023.** Американський аналітичний центр Center for Strategic and International Studies (CSIS)[14] представив ще одне дослідження першого року кібервійни і вказав на відсутність достовірних (такі, що можуть бути перевірені) даних про те, що російська кіберактивність з лютого 2022 року переорієнтувалась чи змінилась стосовно тих цілей, які були актуальні для неї в попередні роки. Разом з цим, хоча динаміка атак зросла, але серйозність і результативність – знизились.

✓ **Вересень 2023.** Оцінки Національних кіберсил (NCF) Великобританії[15], що ґрунтуються на оцінюваннях генерала Тома Копінгер-Саймса (Tom Copinger-Symes). Вони зосереджені на питаннях міграції українських даних у хмарні сервіси за кордоном, визначальній ролі обміну розвідданими з приватними компаніями як фактором ефективної протидії кібератресії.

✓ **Грудень 2023.** Комплексне дослідження Chatham House «Російська кібернетична та інформаційна війна на практиці»[16]. У частині вивчених уроків підкреслюється важливість українського гнучкого законодавства (зокрема, для швидкої закупівлі чи використання

[11] https://aka.ms/ThreatIntel-Russia

[12] https://www.iiss.org/research-paper//2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences?fbclid=IwZXh0bgNhZW0CMTEAAR2PyIrEkD6mzK3L7B3I9KOyYcaWmUtYMLtHe3IGQPf5b3-MibIRXQZRH_k_aem_AaHS-xvk2JzNQAH0zgTuaPrVPDA7EnkHRJH4kM-fKfnIoXWa0CPBPMHkJocJ2T3z972ogQQ2CORN4rtoJHRa15Jb0

[13] https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-05/230518_Lewis_Evolving_Cyber_2.pdf?VersionId=CG3NiGS8QK8RZt.1xZAd-JSBpVFxEAamB

[14] https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war?fbclid=IwZXh0bgNhZW0CMTEAAR1sdQ1_OeCPeBx2gxCv_3fRx-erjLR-q09bHNtYQcXlnywaV95blWEkF1QA_aem_AaGOUSg-tV1hyKQ30O5dQS7mNQ3mdBN6mIBa_vMkoLOjGLq33rKtQDw7ZgeQteSb4r3kSTvIqcRkf1HLgwhBeAs-

[15] https://therecord.media/uk-hunt-forward-operations-lt-gen-tom-copinger-symes?fbclid=IwZXh0bgNhZW0CMTEAAR0Ke10Vv93yMK_-sho4RjsGVU6mHE6MzJVgTpnxQfUACddZL6owaMkpU_M_aem_AaH0uuiyhUn4Wk0LqUroRztyt6iCZ_jeUVPLwTPXb_hJgg_mIKfIXeJx_WReLFJA71na6yHB2UtY-p867qE82q3Q

[16] https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/05-lessons-observed

дослідних технологій), швидкої релокації даних у хмари та створення кіберпроксі (IT-армія). Як і декілька інших досліджень, фахівці Chatham House відзначають, як фактор спротиву – краще розуміння Україною російської стратегічної культури, доктрин ведення війни та ментальності росіян. Також зауважується обмеженість впливу кібероперацій у випадку кінетичного конфлікту – за таких умов кібероперації здебільшого є розвідувальними, а не деструктивними.

✓ **Лютий 2024.** Ще один аналіз ситуації та уроків від Carnegie Endowment For International Peace[17]. Автор дослідження зауважує, що забезпеченню кіберстійкості України багато в чому сприяли постійні кібератаки з боку росії, розпочаті з 2014 року, вони, фактично, «загартували» українську систему кібербезпеки, яка була готова до активностей ворога.

З боку українських фахівців схожих рефлексій-уроків кібервійни все ще не дуже багато (принаймні – у частині публічних оцінювань, які разом з тим не є виступами на різноманітних заходах). З помітних слід відзначити:

✓ **Травень-Липень 2022.** Фахівці НІСД зробили декілька[18, 19, 20] оглядів перших уроків кібервійни. Водночас, це здебільшого узагальнення наявних на той момент даних, а не власні висновки та оцінки.

✓ **Січень 2023.** Дослідження[21] команди ГО «Рада економічної безпеки України» щодо зв'язку між кібератаками, кінетичними атаками та пропагандистськими акціями москви. Хоча дослідження прямо не було спрямоване на вивчення уроків кібервійни, але автори роблять деякі висновки: відсутність «нових» видів кібератак – ворог користується відомими інструментами, кібератаки часто узгоджуються з іншими доменами протистояння, немає підстав вважати, що інтенсивність кібератак буде зменшуватися.

✓ **Березень 2023.** Дослідження Держспецзв'язку України щодо вивчених уроків 2022 року[22]. Документ закцентований на тих змінах фокусу уваги російських зловмисників, які відбувалися в обох половинах 2022 року. Зокрема, у другій половині дослідження Держспецзв'язку України зафіксували зміщення фокусу російських хакерів із медіа та телекомунікаційних галузей, котрі були одними з головних цілей на початку війни, на енергетичну систему, яка також перетворилася на одну з основних цілей ракетних атак росії з жовтня 2023 року. Крім того, змінилися й цілі російських хакерів: від великої кількості деструктивних атак до шпигунства та крадіжки даних.

✓ **Лютий 2024.** До 2024 Kyiv International Cyber Resilience Forum група авторів підготувала огляд «Десятиліття в окопах кібервійни: історія української стійкості»[23], який містить аналіз еволюції кібербезпекового ландшафту України з початку 2013 року. Окремий розділ документа присвячений кіберпротистоянню 2022–2023 років і вказує на зміну тактики

[17] https://carnegieendowment.org/research/2024/02/russias-countervalue-cyber-approach-utility-or-futility?lang=en

[18] https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/svitove-vidlunnya-rosiysko-ukrayinskoho-kiberprotystoyannya

[19] https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/doslidzhennya-shchodo-bezpeky-danykh-vid-verizon-holovni-vysnovky

[20] https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/kiberskladnyk-rosiysko-ukrayinskoyi-viyny-uroky-ta-otsinky

[21] https://reb.org.ua/storage/164/zagalnii-analiz-vimiriv-rosiiskoi-viiskovoi-agresi....pdf

[22] https://cip.gov.ua/services/cm/api/attachment/download?id=53466

[23] https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf

російських зловмисників між періодами 2013–2021 років та з початку 2022 року. Перший період характеризувався варіативністю технік, тактик і процедур, проте під час активної фази ворог зосередився на найбільш апробованих та дієвих підходах.

Ці, а також деякі інші, що не стали частиною цього огляду, спроби узагальнення уроків кіберпротистояння між росією та Україною можна сформулювати таким чином:

✓ **росія не змогла досягнути бажаних стратегічних цілей кібератаками.** Фахівці здебільшого погоджуються з тим, що росії не вдалось досягнути бажаного в кіберпросторі. Це призвело до того, що агресор був змушений більш активно використовувати класичні кінетичні атаки проти об'єктів, які до того планував вразити кіберзасобами. Водночас, є дискусія між різними фахівцями щодо релевантності цілей і, можливо, реальні цілі були досягнуті в межах завдань, визначених ініціаторами кібератак (однак, ці завдання були істотно вужчими, ніж очікували сторонні оглядачі). Деякі експерти вважають надмірною раціоналізацію дій російських державних хакерів, водночас їх мотиви та дії більше зумовлені внутрішніми імперативами організацій, у яких вони діють[24];

✓ **критична інфраструктура все ще бажана ціль для агресора, але можливості вплинути на неї менші ніж очікувалось.** Відомо лише про декілька дійсно вдалих атак проти ОКІ за цей період: кібератака на провайдера супутникового зв'язку VIASAT (супутник KA-SAT)[25], спроба кібератаки у квітні 2022 року на енергооб'єкти України за допомогою Industroyer2 та CADDYWIPER[26], вдала кібератака проти оператора «Київстар» у грудні 2023 року. Такі здобутки є досить сумнівними з погляду «великої кіберстратегії», якщо така дійсно є у росії;

✓ **під час військової агресії кібершпигунство стає ще важливішим.** Можливості агресора здійснити вдалу кібердиверсію досить сильно обмежені у випадку, якщо побудовано ефективну систему кіберзахисту. Війна в Україні показала, що єдині кібероперації, які залишаються ефективними в цей період – кібершпигунство або підтримка інформаційних операцій;

✓ **фізична безпека дата-центрів так само важлива як і їх кібербезпека.** Хоча більшість загроз у контексті безпеки дата-центрів розглядаються з погляду їх кібербезпеки, однак фізичний захист також виявився важливим. Американські фахівці влучно вказують на те, що при проєктуванні дата-центрів зрідка враховується ймовірність нанесення по них ракетного удару, але ця ймовірність не нульова[27];

✓ **стрімке зростання кількості кібератак спостерігалося напередодні вторгнення.** Кібератаки січня та лютого 2022 року проти державних реєстрів та низки сайтів були більш піковими[28], ніж подальша кіберактивність. Експерти[29] кажуть, що після масованих

[24] https://www.svoboda.org/a/tseli-stanut-masshtabnee-kto-pobezhdaet-v-kibervoyne-rossii-i-ukrainy-/32741896.html?fbclid=IwZXh0bgN-hZW0CMTEAAR11aa_oHy4BzZcwoRd1paxHpASJZ5QjYIeh1Ww_p23vEmlJN3aDpGrttjM_aem_AZsNfh-ScN1DyFNlUDiph906bftP51voMUVS-naqeFtqTuUbCDi0iT0ulN_ZD3Sw-cE0RvvJsEqYf3xrXuHtQmiEC

[25] https://dev.ua/news/hakeri-zlamali-suputnik

[26] https://cert.gov.ua/article/39518

[27] https://www.youtube.com/watch?v=ZMlkA85a5PY

[28] https://cutt.ly/nGKYY4s

[29] No Name Podcast with the Grugq - https://www.youtube.com/watch?v=zb_W_hRkX4o , 26.0.2022

кібератак перших 3–7 днів агресії спостерігалась помітна пауза в кіберактивності. Малоймовірно, що такі пікові показники в інших кейсах можна надійно трактувати як підготовку до військового вторгнення, але це не виключено;

✓ **характер діяльність підрозділів кіберзахисту мало змінюється в частині функціональності – зростає лише інтенсивність роботи.** Хоча очікувалось, що військовий стан і масштабне кіберпротистояння змінить завдання та функції підрозділів кіберзахисту, однак найбільш помітною зміною стало лише зростання інтенсивності їх роботи;

✓ **співпраця держави з приватним сектором та окремими громадянами критично важлива, але потребує доопрацювання.** Швидка допомога Україні відомих кібербезпекових компаній була критично важлива в перші місяці війни. Вони надавали розвідувальну інформацію про кіберзагрози (маючи власну розгалужену мережу сенсорів, які збирають телеметрію), допомагали полювати на кіберзагрози, а експертна підтримка була необхідна для швидкого відновлення функціонування уражених систем[30]. Важливою виявилась і пряма допомога з боку окремих громадян державним структурам (без набуття цими громадянами статусу військових). Водночас, така співпраця була несистемною і слабко інституціалізованою;

✓ **агресором майже не використовувались нові тактики, техніки та процедури (TTP).** Дослідники не відзначають помітної зміни структури кібератак, хоча й вказують на появу низки нових зловмисних груп та шкідливого ПЗ (Ransomware [31] та Wiper[32]) у період до початку агресії та в перші місяці після неї. До небагатьох змін у тактиках хакерів можна віднести такі: замість довготривалих спроб атакувати безпосередні цілі вони почали концентруватись на периферійних – брандмауерах, маршрутизаторах та серверах електронної пошти;

✓ **під час військових дій агресор мало приховує свою включеність у деструктивну кіберактивність.** Якщо до початку війни російські хакери намагались приховувати інфраструктуру, з якої вони проводили кібератаки, то з початком агресії кібератаки йшли майже відкрито з території росії. Тож, в умовах повномасштабного військового конфлікту проблема атрибуції кібератак майже зникає з порядку денного;

✓ **забезпечення спеціального зв'язку (між керівництвом та Збройними силами держави).** росія намагалась порушити такий зв'язок, вочевидь, сподіваючись на посилення хаосу та зменшення керованості підрозділів ЗСУ. З цією метою було атаковано супутниковий зв'язок VIASAT (KA-SAT[33]), яким активно користувались ЗСУ. Дублювання каналів зв'язку та створення альтернатив є важливим для збереження керованості ситуації у найбільш важкі перші тижні агресії;

[30] https://www.infosecurity-magazine.com/news/nsa-6-takeaways-war-ukraine/?fbclid=IwAR0kYnGtvRe9Naypct_i7qpmH5LKHaY16IsHv2-8bVUwsBYjBy5u8OzVVVo

[31] Ransomware – одночасно й назва типу вірусів, і назва типу зловмисної діяльності. За допомогою шкідливого програмного забезпечення вся інформація атакованого об'єкту зашифровується і за його розшифрування вимагається викуп (ransom).

[32] Wiper - шкідливе програмне забезпечення, метою якого є стерти жорсткий диск машини-жертви, тобто знищити дані за допомогою різних способів. Часто імітують діяльність Ransomware.

[33] https://dev.ua/news/hakeri-zlamali-suputnik

✓ **при плануванні наступальних кібероперацій важливий правильний баланс між факторами «інтенсивність – швидкість – управління».** Кіберактивність агресора показала, що він так і не зміг знайти оптимального балансу між трьома факторами, які безпосередньо впливають на результати кіберактивності: *швидкість* (як швидко можуть здійснюватися атаки), *інтенсивність* (наскільки потужними та тривалими вони будуть) та *управління* (наскільки вони керовані та скоординовані). Фактично кожному, хто застосовує кібернаступальні засоби доводиться балансувати ці фактори, акцентуючи одночасно лише на двох з трьох[34];

✓ **масовий рух кіберволонтерів важливий, але потребує належної координації.** Хоча діяльність масових рухів кіберволонтерів є важливою, однак характер застосовуваних ними технік атак (переважно DDoS-атаки) порушує питання про важливість їх ефективної координації з тими, хто проводить більш складні кібероперації. Експерти вказують[35], що DDoS-атаки проти сайтів держави-агресора в умовах масштабної військової агресії мають здебільшого ефект психологічного розвантаження для великих груп осіб, ніж можуть дійсно змінити поведінку агресора. При цьому нескоординовані атаки могли заважати іншим операціям впливу проукраїнських кіберфахівців. Ще один висновок від масштабної діяльності кіберволонтерів – їх активна включеність у кіберпротистояння продовжує розмивати межі між цивільними та військовими учасниками, а відтак – і питання відповідальності (юридичної) за певні дії[36].

Крім зазначеного, у дискусіях експертів актуальним досі є питання – наскільки досвід російсько-української кібервійни взагалі може бути екстрапольований на інші схожі ситуації (наприклад, потенційне загострення навколо Тайваню) та чи ці уроки можуть бути вивчені іншими країнами, аби ліпше підготуватись до можливої агресії. Усе частіше висловлюється думка, що можливості такого застосування за межами України досить невисокі, а сам український кейс багато в чому є унікальним. Фізичні розміри України, специфіка українсько-російських відносин з 2013 року, недооцінка росією України напередодні вторгнення – усе це фактори, які складно повторити в іншому регіоні. Фахівці слушно вказують на малоймовірність такої ж недооцінки іншим агресором свого супротивника аби повторити російські помилки.

Єдине, з чим погоджуються майже всі дослідники – це спільні уроки, які можуть і мають бути застосовані всіма, це:

- ☞ поглиблення партнерства між державою та приватним сектором;
- ☞ обмін даними кіберрозвідки між країнами-партнерами;
- ☞ більша увага на фінансуванні та побудові захисних систем (які довели свою ефективність);
- ☞ постійна стратегія розвитку «стійкості» замість жорсткого «захисту»;
- ☞ розуміння взаємодії з потенційними кіберволнтерами.

[34] https://www.youtube.com/watch?v=olgf_gFhuBc

[35] https://youtu.be/olgf_gFhuBc?t=590

[36] https://warontherocks.com/2022/12/disentangling-the-digital-battlefield-how-the-internet-has-changed-war/

МЕТОДОЛОГІЯ ТА ДИЗАЙН ДОСЛІДЖЕННЯ

Основною базою дослідження виступило опитування експертів з державних органів, об'єктів критичної інфраструктури та приватного сектору методом анкетування. За сприяння Апарату РНБО України анкети були розіслані респондентам, що представляють основних суб'єктів національної системи кібербезпеки, ЦОВВ та регіональні органи влади, приватні компанії та об'єкти критичної інфраструктури.

Опитувальник поділено на три смислові блоки:

Метою першого блоку питань було ретроспективно зрозуміти, якими саме були очікування суб'єктів кібербезпеки, до яких викликів вони готувались та як сприймали рівень кіберготовності держави.

Другий блок мав дати ширше розуміння того, що сталось після 24 лютого 2022 року, наскільки події цього періоду відповідали очікуванням та заходам підготовки, наскільки добре були скоординовані дії різних суб'єктів.

Третій та четвертий блок – оцінка найбільш ефективних ужитих заходів, та які заходи спрацювали, а котрі – ні.

Усього за результатами було отримано 287 анкет, серед них:

☑ 108 – державні органи, які не є основними суб'єктами кібербезпеки;
☑ 119 – експерти одного з основних суб'єктів кібербезпеки;
☑ 44 – об'єкти КІ;
☑ 5 – приватні компанії та окремі незалежні експерти;
☑ 3 – органи місцевого самоврядування.

Загалом респонденти самовизначилися як:

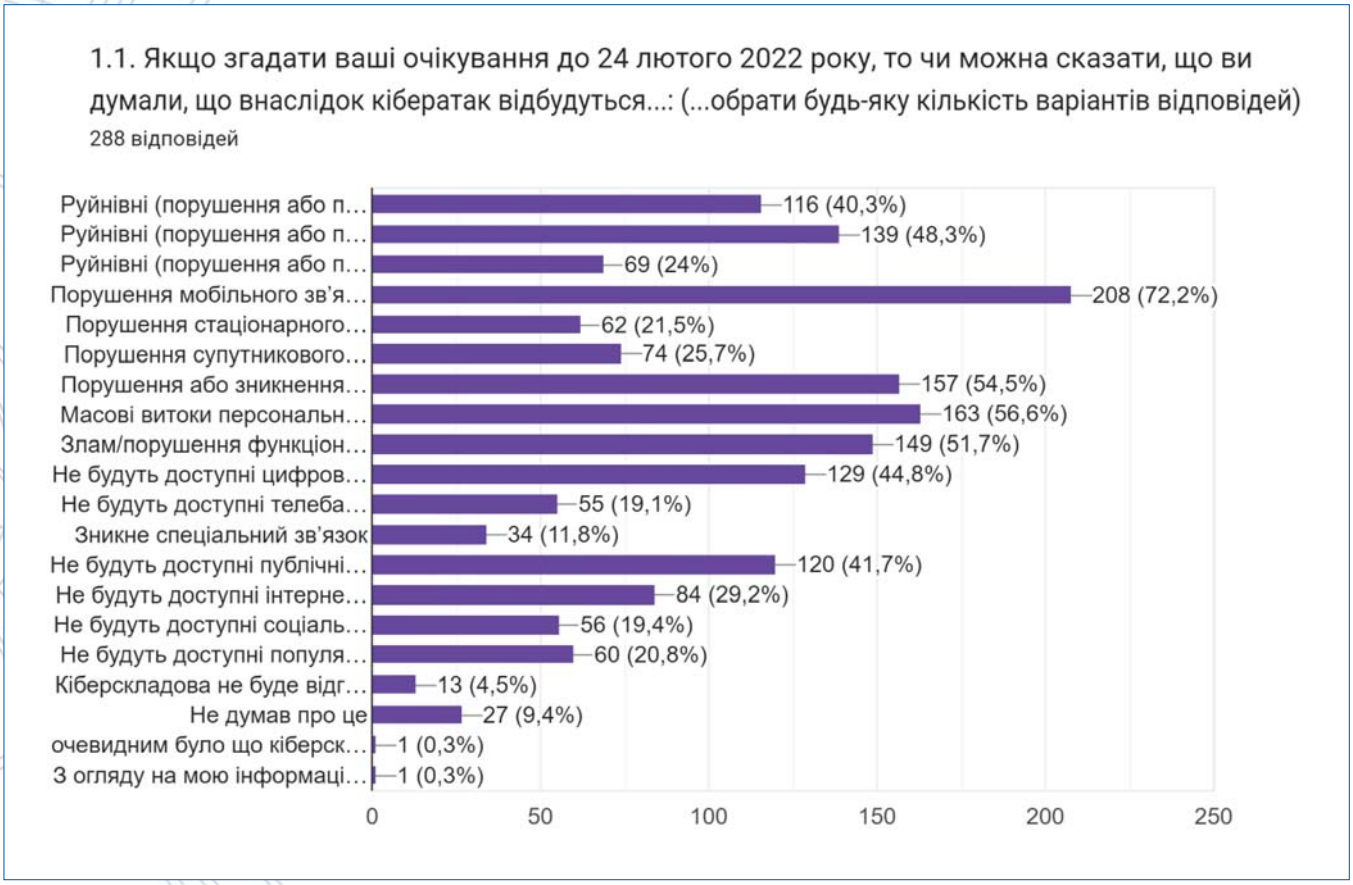
☑ 163 – фахівці;
☑ 43 – керівники самостійних підрозділів у межах департаментів (керівники відділів);
☑ 17 – керівники департаментів;
☑ 15 – заступники керівників самостійних підрозділів у межах департаментів;
☑ 12 – заступники керівників організації;
☑ 2 – керівники організації;
☑ 41 – інші варіанти (головні спеціалісти, фахівці, співробітники непрофільних підрозділів тощо).

67% опитаних розпочали свою роботу в організації до 24 лютого 2022 року, тому мають можливість порівнювати очікування організацій. Майже всі опитані є фахівцями з кібербезпеки або пов'язаною з нею діяльністю.

КЛЮЧОВІ ВИСНОВКИ

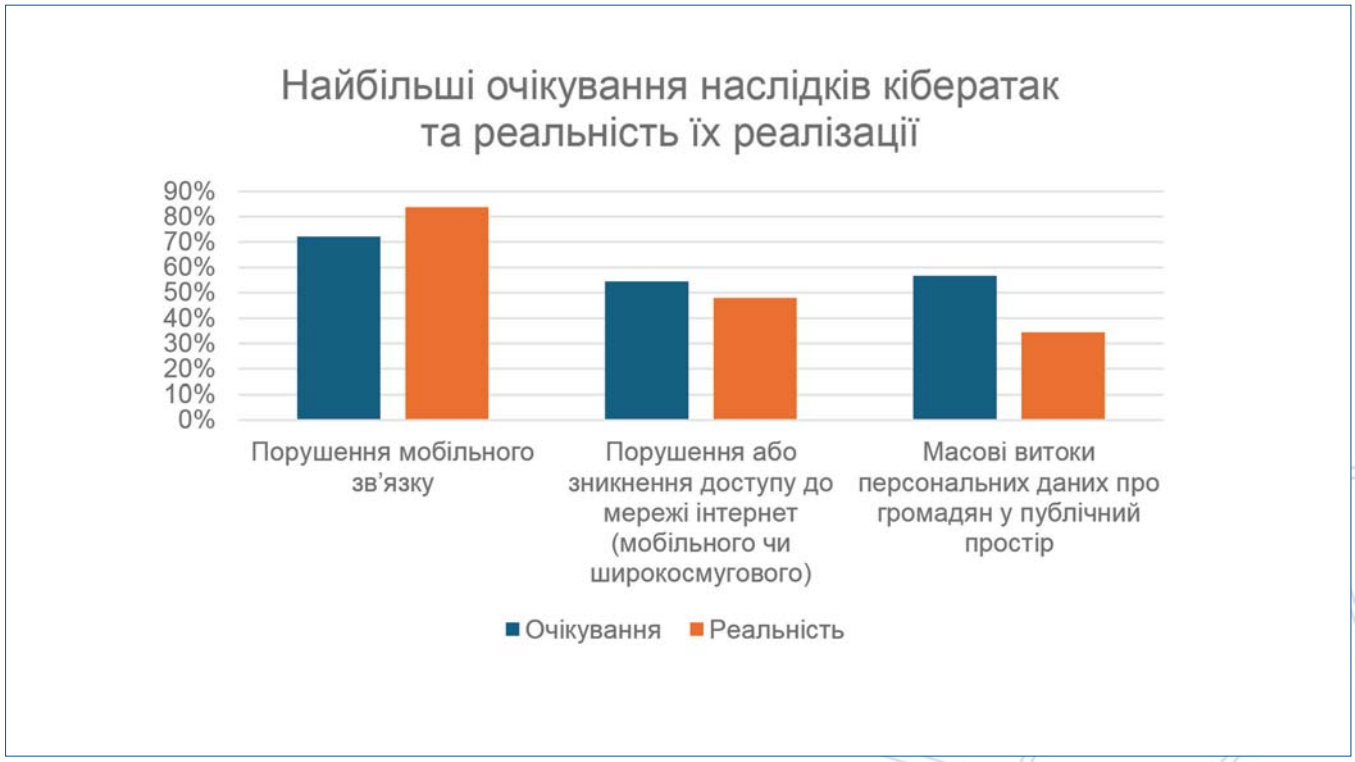
I. Очікування виявились гіршими, ніж реальність

Із заздалегідь підготовленого експертами списку відповідей, респондентам було запропоновано обрати низку типових очікувань того, що може статись унаслідок кібератак.

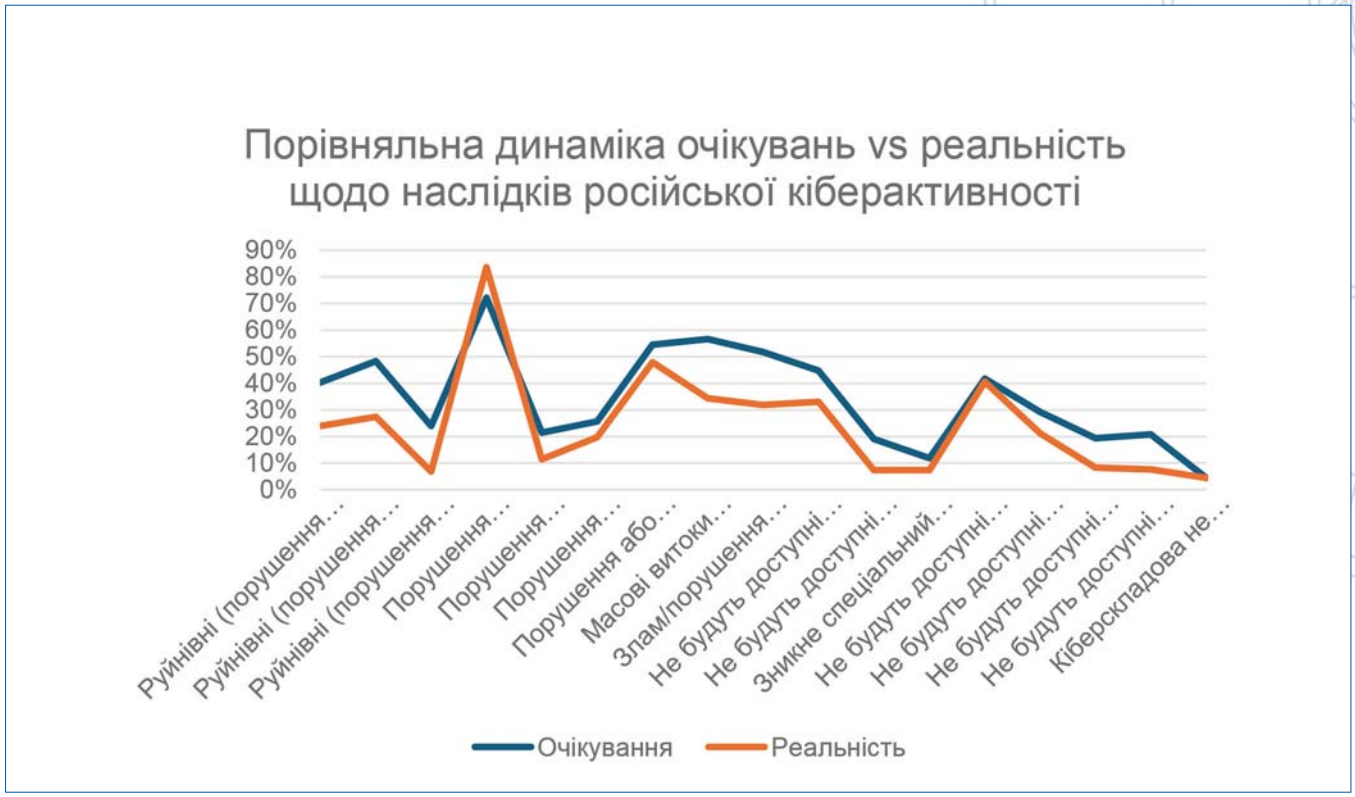


Абсолютним рекордсменом стало очікування, що відбудуться руйнівні атаки (тобто пряме порушення або припинення функціонування) мобільного зв'язку як такого (72%), стануться масові витоки персональних даних (56,6%), порушення або зникнення мобільного / широкосмугового доступу до мережі «Інтернет» (54,5%). Один із респондентів прямо зазначив, що «оскільки більшість організацій державного та приватного сектору не мають адекватного захисту (навіть на базовому та середньому рівні), то я очікував повного колапсу інфраструктури зв'язку, а також припинення / сповільнення роботи всіх підприємств та державних органів».

Насправді, ці загальні очікування частково виправдались. Відповідаючи на питання «Зважаючи на набутий досвід та знання, з позицій сьогоднішнього дня, що з нижче вказаного справдилось після 24 лютого 2022 року саме через кібератаки» респонденти підтвердили, що ці очікування справдились.



Водночас, цікавою є й більш загальна рамка очікувань реалізації кіберзагроз, передусім – у розрізі порівняння з фактичною ситуацією (або швидше тим, як вона сприймалася з позиції після 24 лютого 2022 року).

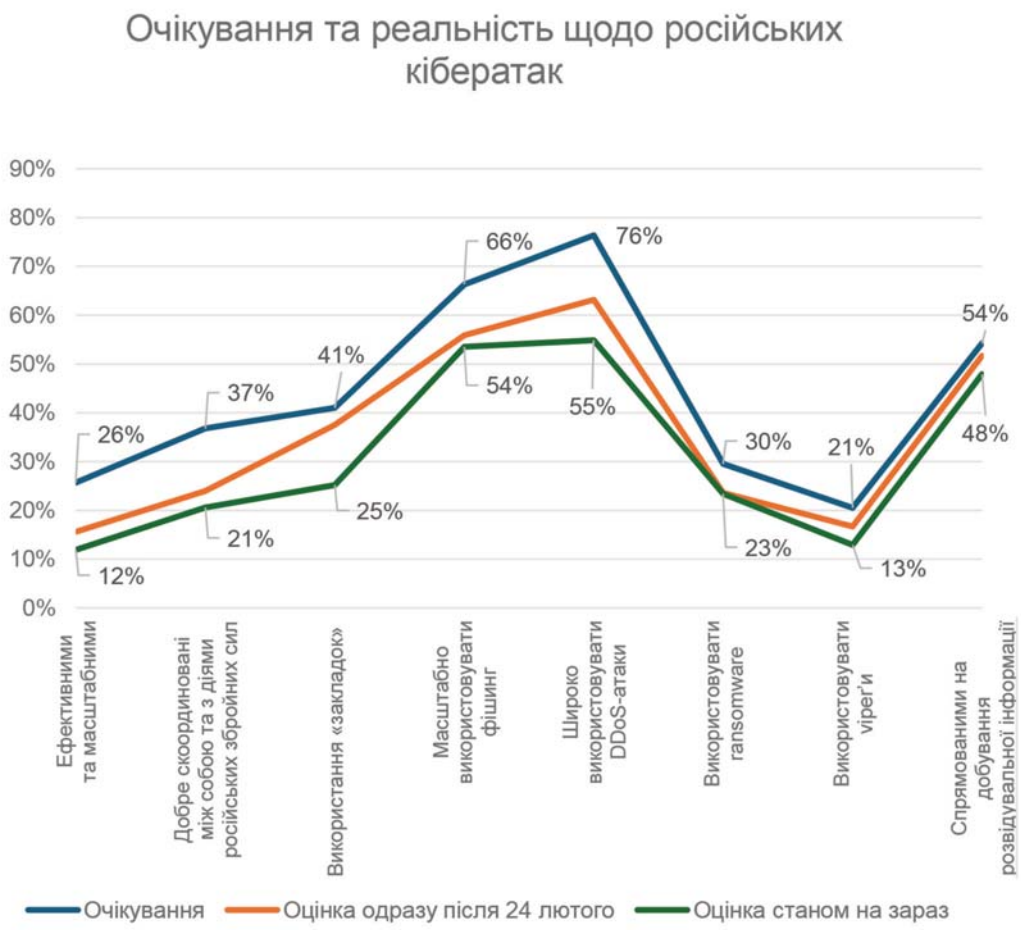


Складно не помітити, що загалом очікування були значно катастрофічніші, ніж фактичний результат. Окремі позиції (наприклад, загроза доступності телебачення, радіомовлення, соціальних мереж, месенджерів) виявились переоцінені майже в 3 рази.

Також цікавим є той факт, що майже 50% респондентів високо оцінили ймовірність руйнівних атаки на енергетичний, банківський та транспортний сектори, однак оцінка фактичного стану відображає істотно меншу загрозу цим секторам, ніж можна було очікувати (для транспортного сектору фактичний стан загроз виявився в 3 рази меншим, ніж очікувалось).

II. Російські кіберспроможності щодо методів та скоординованості атак були переоцінені

Аналогічно до попереднього спостереження можна відзначити дуже завищені очікування респондентів щодо методів, до яких будуть вдаватись росіяни, та ефективності їх застосування.



Особливо показовими є окремі цифри. Так, очікування щодо загальної ефективності та масштабності російської кіберактивності відрізняються майже у два рази між тим, що очікувалось і тим, як це відбувалося. 26% респондентів очікували, що російські кібератаки виявляться масштабними та добре скоординованими. Ця оцінка суттєво більша, ніж фактична після 24 лютого 2022 року та зараз – 12%. Також було велике занепокоєння щодо можливості

використання «закладок» – 41% респондентів були впевнені, що ця загроза реальна. Фактично, після 24 лютого 2022 року лише 25% респондентів зауважили, що ця загроза виявилась актуальною. Найменшою є розбіжність в питанні щодо добування розвідувальної інформації (54% очікувань проти 48% фактичного стану), використання ransomware (30% проти 23%) та фішингу (66% очікували такої активності, лише 54% вказують, що ця загроза справдилась).

Опитування не ставило за мету виявити причини: чому респонденти саме так оцінювали ці загрози. Водночас можна припустити, що така завищена оцінка базувалась на публікаціях ЗМІ, оцінках російського кіберпотенціалу з боку інших країн, а також загальних очікуваннях, що ґрунтувались на попередньому досвіді українських кіберфахівців (кібератак проти Прикарпаттяобленерго, NotPetya тощо).

III. Організації сумнівались у своїй готовності до кібератак, однак загалом виявились підготовленими

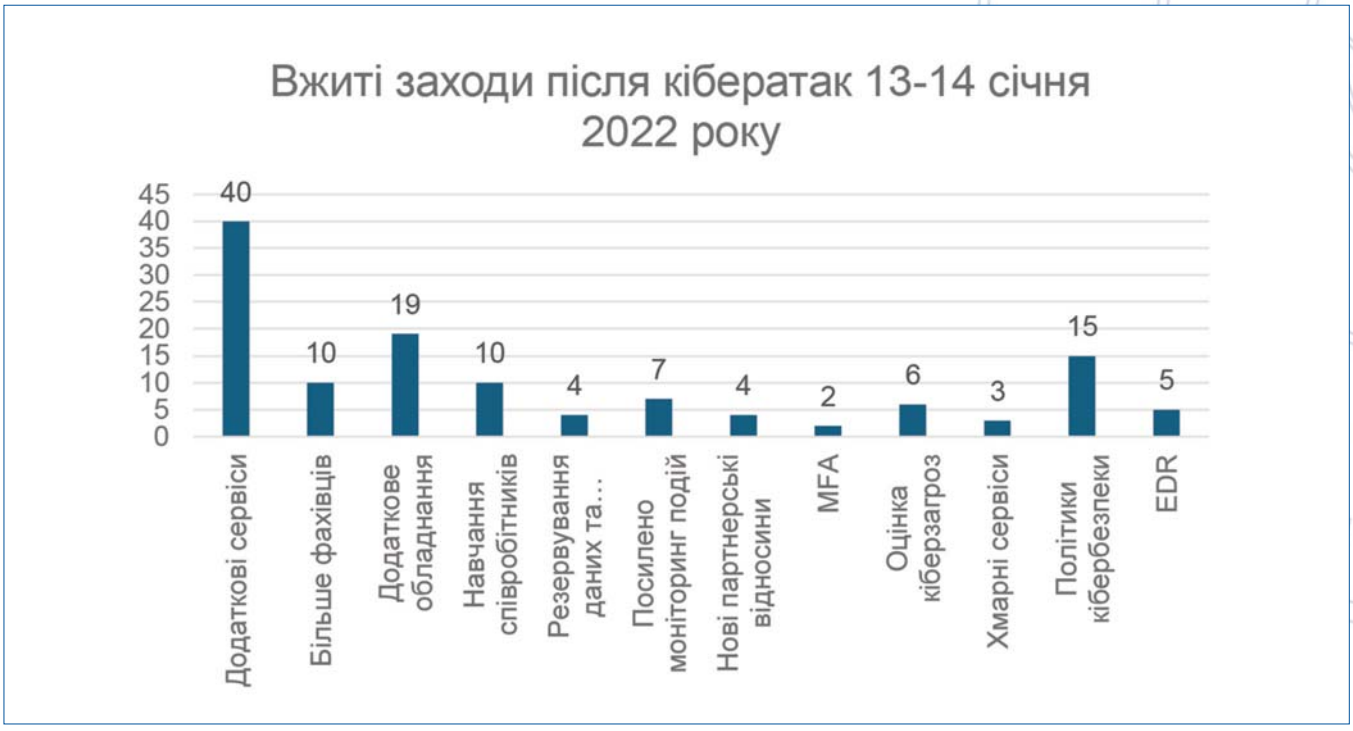
54% опитаних указали, що до 24 лютого 2022 року оцінювали готовність своїх організацій до кібератак як «часткову» (лише 26,7% чітко стверджували про таку готовність). Це кореспондується з іншими даними щодо впевненості в тому, що «Організації державного сектору добре захищені від кібератак». 59% респондентів вказують на часткову захищеність (лише 10% відповіли «Так» на це питання).

Ці дані доповнюються аналогічним питанням про фактичну ситуацію з кібербезпекою в організаціях після 24 лютого – 63% відповіли «Так» на питання «Оцінюючи кіберактивність після 24 лютого 2022 року, чи можна сказати, що Ваша організація виявилась готовою до кібератак проти неї?». Одним з факторів такої готовності, ймовірно, виявились кібератаки 13–14 січня 2022 року (перша фаза кіберагресії). 51,2% респондентів указали, що їхні організації врахували ці атаки та посилили заходи кібербезпеки, 27,2% – не вжили додаткових заходів. Уже, оцінюючи, чи допомогли ці заходи у відбитті кібератак після 24 лютого 2022 року, 37,6% опитаних відзначили ефективність ужитих заходів. Деякі організації прямо вказували, що для

підготовки до кібератак були проведені додаткові навчання з персоналом, повністю перебудована інфраструктура, розгорнуті додаткові ресурси. Зокрема, респонденти відзначали (з тих, які згодились конкретизувати свою відповідь – всього 77 організацій) додаткові заходи, а саме:

- ✓ підключили додаткові сервіси кібербезпеки та посилили заходи з моніторингу;
- ✓ залучили більше фахівців;
- ✓ підключили додаткове обладнання;
- ✓ підвищили рівень кібергігієни та провели посилене навчання працівників;
- ✓ запровадили технологію Active Directory;
- ✓ забезпечили резервування критично важливої інформації та систем;
- ✓ розгорнули систему Cisco Umbrella;
- ✓ розгорнули поштовий шлюз FortiMail тощо.

Загалом ці заходи можуть бути узагальнені у 12 принципових категоріях. Їх аналіз дозволяє зробити висновок, що типовою реакцією організацій на кібератаки стало підключення додаткових сервісів кібербезпеки, підключення додаткового обладнання та впровадження / зміна політики кібербезпеки в організації. Також часто проводилось додаткове навчання співробітників (як тих, що відповідають за кібербезпеку, так і загалом по організації), залучались додаткові фахівці та посилювався моніторинг загроз.



Слід зазначити, що 36,6% усіх респондентів підтвердили, що додаткові заходи вживались, але не мали істотного впливу на події після 24 лютого 2022 року.

IV. Знання власних можливостей і слабке уявлення про інші організації

Переважна більшість респондентів (81,9%) були абсолютно впевнені в тому, що знають до кого звертатись у випадку кібератаки проти їх організації (лише 8,3% відповіли «Ні» на це запитання). Цей показник підтверджено і в блоці оцінювання фактичного стану – 91,3% чітко знали, до кого могли звернутись у випадку кібератак на них.

Однак, їх знання про можливий порядок дій інших суб'єктів (відтак, і загальна обізнаність про діяльність інших суб'єктів кібербезпеки) були досить слабкими: лише 36,8% відповіли ствердно на питання «Чи знали ви як саме будуть реагувати та діяти інші організації в разі кібератак проти них?» – майже стільки ж (38,2%) відповіли «Ні». Цікаво, що майже 25% респондентів відповіли «Не знаю, не думав про це». Це може свідчити, що фахівці суб'єктів кібербезпеки не усвідомлюють взаємозалежний характер кіберзагроз і що дії інших суб'єктів (і загрози їм) можуть бути тісно пов'язані з безпекою їхніх власних організацій.

Ті самі 25% зазначили, що не слідкували і не думали про те, як інші суб'єкти кібербезпеки реагують на кібератаки. Водночас лише 10% відповіли «Так» на питання «З огляду на підвищену кіберактивність після 24 лютого 2022 року чи можна сказати, що інші організації реагували на кібератаки саме так, як ви і передбачали/очікували?» – 58% сказали, що це «Скоріше так, ніж ні».

V. Ефективність координації оцінюється позитивно і є тенденція до поліпшення

12,5% респондентів (36 осіб) указали на те, що особисто брали участь у різних командно-штабних навчаннях (наприклад – «Національна кіберготовність 2021», які проводились за підтримки НКЦК). Ще майже 18,1% респондентів відповіли, що брали участь представники їхніх організації. Однак, 37,3% опитаних відмітили, що навіть не знали про існування таких навчань. Це може вказувати на необхідність посилення інформаційної кампанії із залучення різних суб'єктів до такого роду активностей.

Складно оцінити ефективність таких навчань з погляду відпрацювання реальних заходів координації. Однак 11,8% опитаних (фактично співвідноситься з кількістю тих, хто брав участь) підкреслили, що цей досвід став їм у пригоді для реагування на ворожу кіберактивність після 24 лютого 2022 року. Ще 9,8% респондентів відзначили корисність вправ, але визнали, що не діяли відповідно до тих протоколів взаємодії, які були в центрі тих навчань.

Хоча один із респондентів зазначив, що «очікував на більш скоординовану діяльність основних суб'єктів», однак загалом респонденти позитивно оцінили координаційні зусилля держави в сфері кібербезпеки одразу після 24 лютого 2022 року. 24,7% респондентів прямо відзначили, що координація була на належному рівні, а 40,3% респондентів знають, що вона відбувалась, хоча і не дуже помітно.

Респонденти чітко вказують на позитивну динаміку в практиці координації – 50,7% кажуть, що вона значно поліпшилась за останні 2 роки, а 22% підкреслюють, що вона не стала гіршою («є, але на тому ж рівні»). Хоча опитувальник не містив відкритих питань, які вказували б на причини поліпшення ситуації, однак можна припустити, що це пов'язано з прийняттям низки

координаційних інструментів (наприклад, «Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти / кібератаки») або запровадження практики постійних навчань (тренінги, командно-штабні заняття та ін.).

VI. Фахівці приватного сектору були важливі в кіберспротиві, однак їх вплив на ситуацію не завжди помітний для суб'єктів кібербезпеки

Хоча більшість міжнародних досліджень указують на виключну роль приватного сектору в ефективному спротиві російській кіберагресії, респонденти дослідження (49,7%) указали, що не мають інформації з цього приводу, тому не стикалися з фахівцями приватного сектору в контексті кіберактивності після 24 лютого 2022 року. Це, частково, підтверджується відповідями 54,9% респондентів, які не мають точної інформації щодо динаміки та форм залученості українських кіберекспертів із недержавного сектору в перші місяці повномасштабного вторгнення та на момент опитування. Такі високі показники необізнаності свідчать не про брак зусиль приватного сектору, а, більше, про не публічність допомоги, та, ймовірно, специфічний її характер, коли допомога надавалась відносно невеликому колу ключових організацій (основних суб'єктів національної системи кібербезпеки) та мала мультиплікативний характер. Цікаво, що 39,2% усіх респондентів вважають, що масштабне долучення кіберекспертів з приватного сектору стало фактором, який допоміг Україні бути ефективною в протидії кіберагресії.

17,4% респондентів вважають, що фахівці приватного сектору швидко та ефективно долучились до кіберзахисту країни. Респонденти майже в рівних пропорціях розподілили форми залучення по 4 форматах.

14,7% респондентів вважають, що тепер динаміка залученості українських кіберекспертів із недержавного сектору не лише не зменшилась, але й зросла. У ці 14,7% входять відповіді «Залученість зросла у тих самих формах», а також «Залученість зросла, але змінились форми допомоги». Ще 8% опитаних вважають, що рівень і форми залученості не змінились, але 17,4% підкреслюють, що залученість знизилась.

Оцінюючи координацію дій приватних експертів з державними органами, майже 14% респондентів вважають, що приватні та державні кіберфахівці ефективно координувались один із одним, а 16% вважають, що кіберексперти з приватного сектору діяли здебільшого самостійно (хоча й ефективно).

VII. Міжнародні партнери і допомога

Ще одним фактором, який міжнародні експерти відзначають як важливий чинник українського кіберспротиву, є міжнародна допомога. Оцінки респондентів з цього питання більш позитивні, ніж у випадку приватного сектору. Загалом 75,7% опитаних або отримували таку допомогу після 24 лютого 2022 року, або чули, що така допомога надавалась.

Цікаво, що 35,1% респондентів відзначають вагому значимість міжнародної технічної допомоги щодо підготовки України до відбиття кіберагресії після 24 лютого 2022 року.

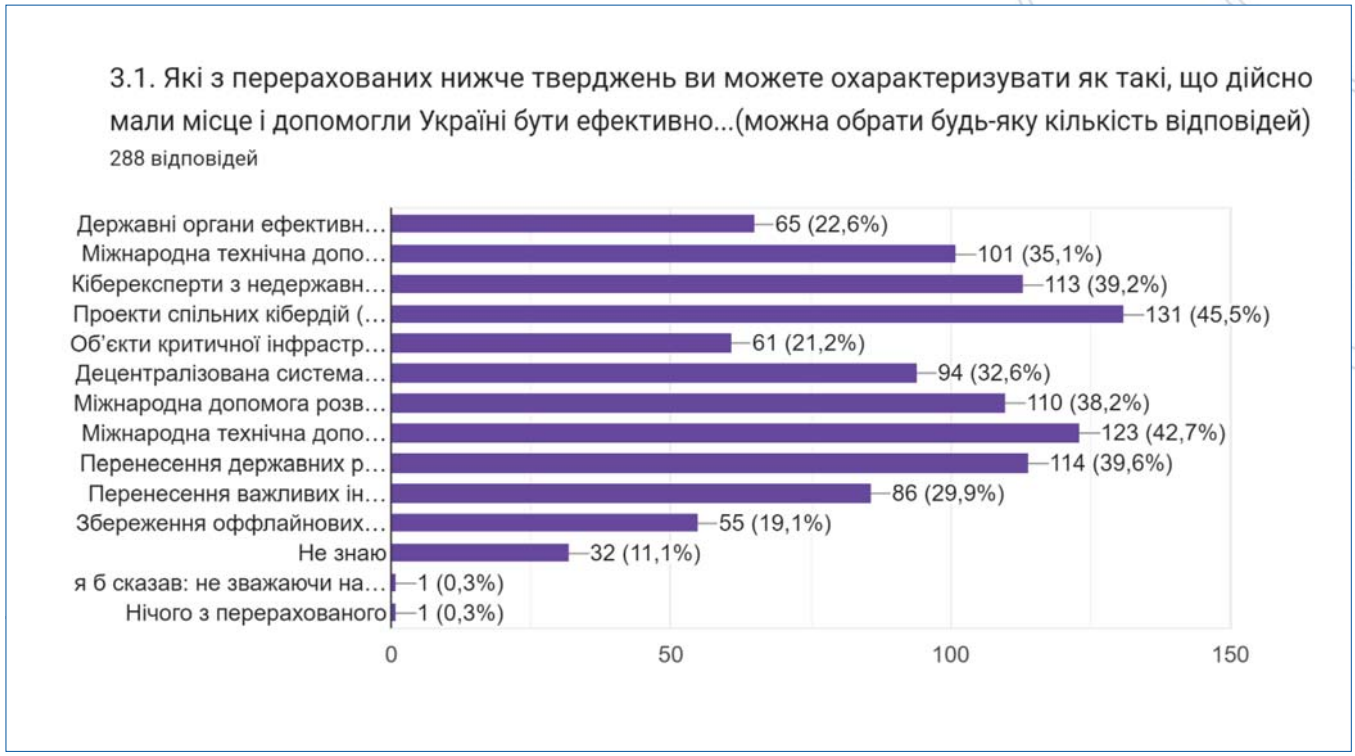
Ще 42,7% опитаних підкреслюють роль такої допомоги (нові технології чи закупівлі обладнання) після 24 лютого 2022 року. Водночас 23,6% опитаних указують на брак зрозумілих процедур для звернення по міжнародну допомогу у сфері кібербезпеки в екстрених умовах.

VIII. Проєкти спільних дій, міжнародна технічна допомога та експерти приватного сектору – основні елементи ефективної протидії кіберагресії

Автори дослідження підготували для респондентів перелік тверджень, метою яких було визначити ключові складові, які, на думку респондентів, дійсно мали місце й допомогли Україні бути ефективною в протидії кіберагресії. Більшість експертів поставили на перше місце проєкти спільних дій (зокрема, IT-армію) як приклад діяльності, що суттєво допомагала своїми діями відбиттю кіберагресії – з цим твердженням згодні 45,5% респондентів. На другому та третьому місцях – міжнародна технічна допомога із закупівлями (42,7%) та перенесення державних реєстрів у хмару (39,6%).

Цікаво, що лише 21,2% респондентів (однин із найнижчих показників в цьому блоці) погодились із думкою, що об'єкти критичної інфраструктури виявились готовими до кібератак, бо завчасно вкладали кошти у свій кіберзахист. Одночасно з цим 45,8% респондентів стверджують, що ОКІ добре справлялись із кібератаками після 24 лютого 2022 року, а 27,8% респондентів вважають, що вони робили це посередньо.

Так само низький показник схвальних оцінок стосувався твердження про те, що «Державні органи ефективно розбудовували кіберзахист до початку вторгнення 24 лютого 2022 року». З цією тезою погодились лише 22,6% опитаних. Це підтверджується відповідями респондентів на питання «На вашу думку державні органи робили достатньо до 24 лютого 2022 року задля забезпечення кібербезпеки України?» – 65,3% відповіли негативно, погодились із цим твердженням лише 17,4% опитаних. Фактично, загальною оцінкою респондентів є негативне



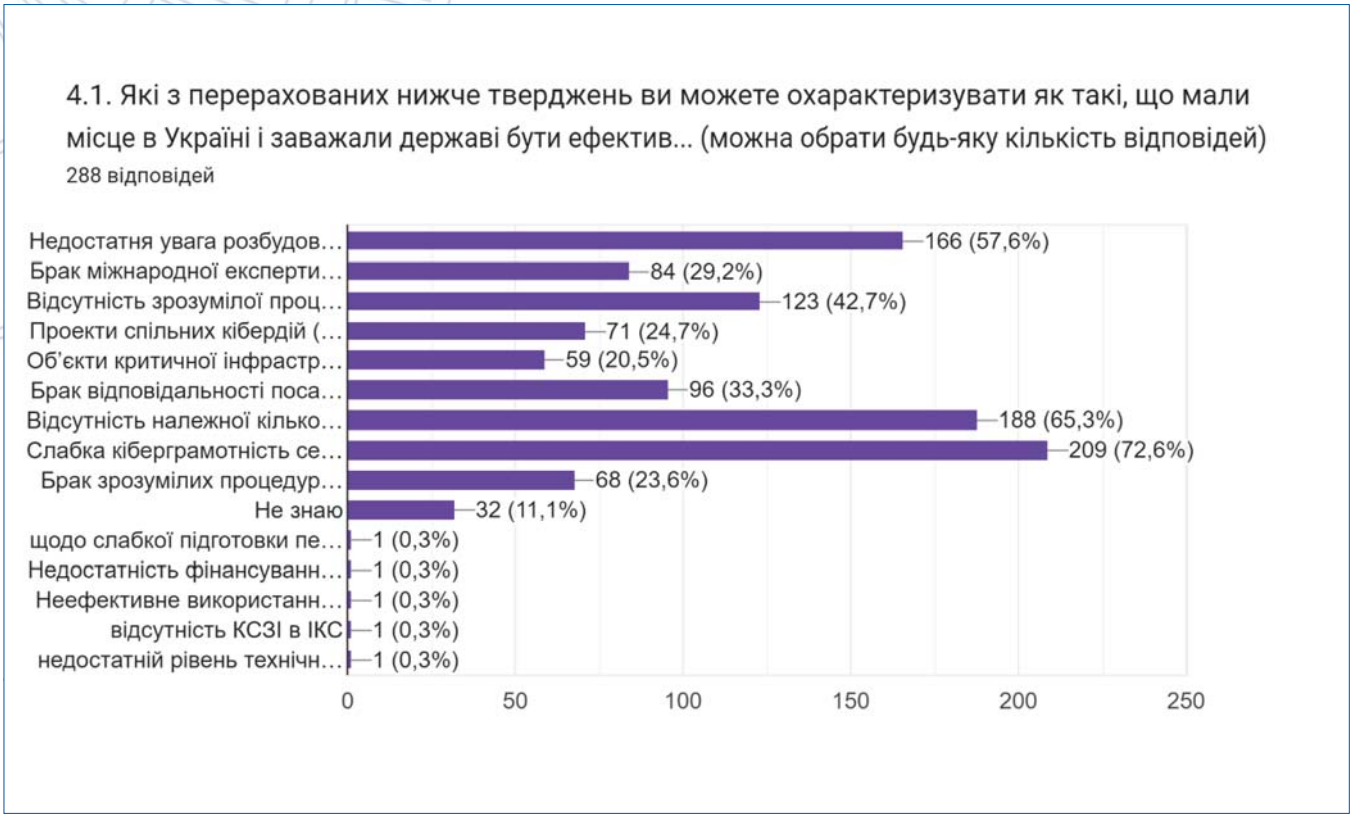
сприйняття (швидше як недостатнє) тих зусиль, яких доклала держава до 24 лютого 2022 року у сфері кібербезпеки. Цікаво, що цей результат слабко корелюється з позитивними оцінками ефективності протидії ворожій кіберактивності, якості координації дій та дисбалансом у частині очікувань та реальності кіберзагроз (з акцентом на помітне перебільшення очікувань від загроз), з якими стикнулась Україна. Можна припустити, що стійка негативна оцінка всіх докладених зусиль частково є результатом традиційного скептичного ставлення до ефективності дій держави в будь-якій сфері.

Серед інших важливих факторів, респонденти відмічали важливість перенесення державних інформаційних ресурсів у хмари (39,6%), міжнародну допомогу розвідданими щодо кіберзагроз (38,2%) та фактично децентралізовану систему надання доступу до мережі «Інтернет», що забезпечило її невразливість до кібератак (32,6%).

IX. Брак кіберграмотності, відсутність фахівців та недостатні зусилля з розбудови кіберзахисту – ключові завади на шляху до кіберспротиву

Респондентів просили обрати з визначеного списку проблем, що найбільше заважали державі бути ефективною в протидії кіберагресії.

Загалом, показники щодо цього питання були традиційними. Ключовою проблемою, з чим погодились 72,6% опитаних, стала слабка кіберграмотність усіх користувачів незалежно від секторів діяльності. Також, 65,3% опитаних відзначили відсутність достатньої кількості кіберфахівців. То ж на цих двох ключових проблемах сконцентрувала увагу більшість опитаних. На третьому місці – недостатня увага до розбудови ефективного кіберзахисту упродовж останніх 5 років (57,6% відповідей).



До головних проблем також можна віднести відсутність зрозумілої процедури залучення кіберекспертів із приватного сектору до кіберзахисту в умовах війни – з цим твердженням погодились 42,7% респондентів.

Трьома найменш критичними проблемами стали: не готовність об'єктів критичної інфраструктури до кібератак (20,5%), брак зрозумілих процедур для звернення за міжнародною технічною допомогою в екстрених умовах (23,6%) та неналежна координація проєктів спільних кібердій (держави та недержавного сектору або в межах самого недержавного сектору) – з цим погодились лише 24,7% респондентів.

РЕКОМЕНДАЦІЇ

1. Загалом оцінка потенційних кіберзагроз відповідала реальним результатам. Водночас, деякі з них були помітно переоцінені респондентами. Така надміру катастрофічна оцінка може свідчити про не зовсім коректне розуміння суб'єктами кібербезпеки реального ландшафту кіберзагроз у країні, що стратегічно може призвести до неефективного використання коштів на розбудову кібербезпеки, а також неправильної підготовки кіберфахівців до можливих сценаріїв загроз. Доцільно запровадити щонайменше один загальнонаціональний документ (можливо, як частину Огляду стану кібербезпеки), який би надавав узагальнені актуальні оцінки найбільш важливих загроз (карта ландшафту кіберзагроз), подавав їх градацію та потенційну небезпеку реалізації. Це сприяло б оптимізації зусиль кібербезпекових органів та їх фокусування на найбільш важливих напрямках протидії.

2. Більше 1/3 організацій відзначають проведення оцінювання ситуації та впровадження заходів після атак у січні 2022 року, і що це позитивно вплинуло на їхню готовність до нової хвилі кібератак. Відтак, організації, які проводять аналіз кіберінцидентів, здійснюють процес «вивчених уроків» та вживають заходи за їх результатами, дійсно більше готові до нових інцидентів. Водночас невідомо, чи всі структури володіють методологією проведення такого оцінювання і мають відповідну підготовку. Вбачається доцільним розробити типову процедуру «Після кіберінциденту: як оцінити свої дії та вивчити уроки за результатами», яка була б затверджена рішенням НКЦК та поширена між урядовими організаціями для застосування на практиці.

3. Продовження функціонування організацій в умовах кризової ситуації – критично важливо при реалізації концепції стійкості на рівні системи національної безпеки. Одним з важливих інструментів такого сталого функціонування є Плани продовження бізнес діяльності. Розроблення, затвердження та відпрацювання таких планів має стати невід'ємним елементом підготовки організацій до кіберінцидентів. Зважаючи на результати опитування, ці документи також мають включати зрозумілі кроки організацій із залучення додаткових кібербезпекових сервісів, обладнання, фахівців та процедур навчання персоналу.

4. Організації (крім, можливо, основних суб'єктів національної системи кібербезпеки) слабко обізнані з можливими діями інших організацій на кіберінциденти. Це не є проблемою для ізольованих систем, але для supply chain attacks може створити ситуацію, коли організації, які перебувають на одному управлінському рівні, будуть залежати від того, як реагують їхні партнери чи колеги. Поліпшення цієї ситуації можливе за рахунок збільшення кількості ТТХ різних форматів (включаючи технічні), а також запровадженню нових форм взаємодії між різними суб'єктами. Одним із варіантів останнього можуть бути секторальні / тематичні робочі групи при НКЦК РНБО або при підрозділах реагування основних суб'єктів національної системи кібербезпеки.

5. Міжнародні дослідження вказують на виключну важливість взаємодії державних організацій з фахівцями з кібербезпеки приватного сектору. Майже половина опитаних зазначили, що не знають про такі факти або не знають, як саме такі фахівці були залучені після 24 лютого 2022 року. Вочевидь, така допомога була зосереджена навколо невеликої кількості організацій, однак це ставить питання про необхідність ширших зусиль державних органів щодо більш чітких процедур такої співпраці (та координації, яку ефективною вважають лише 14% опитаних), зокрема на виконання пункту 8 Стратегічної цілі С.4 Стратегії кібербезпеки України «розроблення дієвих механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі». НКЦК було б доцільно активізувати дії відповідальних структур (Кабінет Міністрів України та СБУ) щодо виконання цього пункту.

6. Загальне сприйняття «недостатності дій держави в кіберпросторі» помітно контрастує з оцінками міжнародних експертів та оцінками самих респондентів щодо готовності державних органів до кібератак. Вочевидь, ця проблема є більше когнітивною, ніж реальною й потребує так само інформаційно-комунікаційного рішення. Наразі НКЦК готує та поширює інформаційні матеріали, які узагальнюють інформацію про дії держави у сфері розбудови кіберпростору (наприклад, Cyber Digest тощо), однак цих зусиль недостатньо. Ймовірно, проблемою є те, що «відчуття достатності дій» дуже залежить від особистої залученості учасників у процеси, які б вони могли вважати заходами з такого посилення. Можливо, держава потребує створення мережі різноцільових експертних груп (за принципом такої мережі державно-приватного партнерства в американської CISA), яка б об'єднувала таких фахівців, давала їм можливість частіше перетинатись поза межами їх прямих посадових обов'язків, а дтакож взаємодіяти з питань покращення кібербезпекової ситуації (з видимими результатами).

7. 72,6% опитаних вказують на проблему кіберграмотності / кіберобізнаності користувачів. Хоча ця проблема вже вирішується за рахунок національних кампаній кіберграмотності, місячника кібербезпеки, низки неурядових ініціатив щодо цього та численними курсами на порталі «Дія». Однак цих зусиль усе ще недостатньо. Україна, вочевидь, потребує дійсно системної Національної програми кіберграмотності, як це передбачено чинною Стратегією кібербезпеки України, яка б базувалась і на національному досвіді, і на кращих світових практиках (наприклад, шляхом імплементації проєкту ENISA AR-in-the-box). Наступною і вкрай важливою рекомендацією є запровадження обов'язкових тестів на кіберграмотність для всіх державних службовців та працівників ОКІ (спочатку державної, а в перспективі – усіх форм власності).