# ПРОБЛЕМНІ ПИТАННЯ КОМУНІКУВАННЯ КІБЕРАТАК В УКРАЇНІ: МОЖЛИВІ ШЛЯХИ ВИРІШЕННЯ

За останні 4 роки Україна зазнала принаймні декілька масштабних кібератак різного рівня складності та поширення. Можна обґрунтовано припустити, що більша їх частина була пов'язана із російською агресією проти України, яка розпочалась у 2014 р.. Незважаючи на цілу низку прийнятих протягом цих років нормативно-правових документів (Закону України «Про основні засади забезпечення кібербезпеки України», Стратегії кібербезпеки України, декількох рішень РНБО України), які мали позитивно вплинути на кібербезпеку держави, стан захищеності окремих державних інформаційних ресурсів та інформаційних систем об'єктів критичної інфраструктури все ще потребує вдосконалення. Крім того, слід враховувати, що навіть найбільш ефективна система убезпечення об'єкту захисту від кібератак не гарантує абсолютного захисту, а отже в багатьох випадках органам державної влади доведеться мати справу із наслідками кібератак, а відтак – комунікувати їх суспільству.

Остання проблема постає особливо гостро, зважаючи на те, що швидке та чітке пояснення кіберінцидентів важливе для розуміння суспільством реального стану справ, впевненості в адекватності дій державних органів у кризовій ситуації, створенні відчуття контрольованості ситуації з боку держави. Особливо важливо це у випадку атаки на об'єкти критичної інфраструктури та тоді, коли ураженими виявляються державні установи, які задіяні у повсякденному інформуванні населення або наданні йому послуг.

Кібератаки, вочевидь, загалом можуть бути кваліфіковані як кризові ситуації[1], а відтак вимагають реагування за правилами комунікації у кризі. Існує три таких основних правила[2]:

---

[1] «Кризовою ситуацією вважається крайнє загострення протиріч, гостра дестабілізація становища в будь-якій сфері діяльності, регіоні, країні» відповідно до Закону України «Про Раду національної безпеки і оборони України» // http://zakon2.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80

[2] Coombs T. Ongoing Crisis Communication: Planning, Management and Respoding : 3rd ed. / T. Coombs. – Thousand Oaks : Sage Public., 2012. – 248 p.

- швидкість (speed) – здатність надавати інформацію та відповідати на запити щонайшвидше після події/нового етапу розгортання кризи. **Відповідь та перша заява потрібні протягом першої години**, вони заповнять інформаційний вакуум та/або структурують потік надмірної інформації з різних джерел;
- координованість (coherence) – несуперечливість, послідовність повідомлень. Представники органів влади мають озвучувати однакові меседжі у своїх заявах;
- відкритість (openess) – готовність працювати з цільовими аудиторіями, зокрема медіа. Правило підтримання зв'язків із пресою під час кризових ситуацій становить фундаментальну умову управління кризою[3].

**Комунікування кібератак у 2015-2017 рр.: Прикарпаттяобленерго, Укренерго та NotPetya**

З 2015 по 2017 рік відбулось кілька масштабних кібератак, які демонстрували системні проблеми у комунікативній реакції органів влади або атакованих установ.

23 грудня 2015 р. кібератаці було піддано «Прикарпаттяобленерго»[4] – вважається, що початок атаки припадає на приблизно на 15:30. Механізмом атаки стали фішингові листи, які містили віруси BlackEnergy (підготовка до атаки розпочалась ще з середини 2015 р.)[5]. Внаслідок реалізації кібератаки перерва в електропостачанні склала від 1 до 3,5 годин, а без світла залишилось 225 тис. споживачів.

Крім безпосередньо атаки на об'єкт енергетичної інфраструктури, організатори атаки спробували вивести з ладу і систему колл-центру – телефонні системи центру були забиті тисячами фіктивних дзвінків, які, як

[3] Коваль І. О. Вплив медіа на президентський дискурс у кризових ситуаціях / І. О. Коваль // Стратегічні пріоритети. - 2015. - № 3. - С. 134-142.
[4] Разом з тим, атакованими були і ще декілька інших обленерго, але публічні наслідки від кібератаки проявились лише у випадку із «Прикарпаттяобленерго».
[5] Дані доповідачів міжвідомчого семінару на базі Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова (18 лютого 2016 року)

пізніше виявилося, йшли з Москви, для того, щоб ніхто інший не міг додзвонитися[6]. Тим самим хакери намагались зменшити можливості для вчасного реагування та надання вчасної інформації на звернення громадян.

Безпосереднє інформаційне реагування було амбівалентним та недостатньо ефективним. Найбільш відповідно до вимог кризового комунікування реагувала сама «Прикарпаттяобленерго»: перше повідомлення на сайті компанії з'явилось[7] через годину (16:54) після відключення. У повідомленні вказувалось, що проблема існує і що техніки зайняті її вирішенням. Цікаво, що у цьому ж повідомленні відмічається, що абонентів просять утриматись від дзвінків у колл-центр – вочевидь тоді атака на колл-центр вже була активно розгорнута.

Друге повідомлення з'явилось[8] в 17:37 де було подано загальну канву історії: вказано, що причиною аварії є втручання сторонніх осіб, вказано які райони постраждали та де вже розпочались відновлювальні роботи, а також окреслено стратегічний напрям вирішення проблем.

Фіналізуюче повідомлення щодо даної ситуації було подано на сайті компанії 12 січня 2016 р. (майже через 3 тижні після атаки) – з цього приводу було підготовлено прес-реліз[9], в якому ситуація була додатково деталізована і не суперечила першим заявам.

Слід визнати, що державні структури (у цьому матеріалі увага була зосереджена на ключових суб'єктах національної системи кібербезпеки[10] та окремих структурах, що подають інформацію про події в Україні зовнішнім аудиторіям, зокрема МЗС) комунікували цю подію значно менш ефективно. При цьому слід особливо підкреслити, що на сьогодні питання комунікування кіберінцидентів офіційно на рівні нормативно-правових документів не вирішено і жодне з відомств фактично не має такого

[6] http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109
[7] http://www.oe.if.ua/showarticle.php?id=3412
[8] http://www.oe.if.ua/showarticle.php?id=3413
[9] http://www.oe.if.ua/showarticle.php?id=3415
[10] Передусім Служба безпеки України, Держспецзв'язок (та CERT-UA), Національна поліція України (Департамент кіберполіції).

зобов'язання. Водночас є суспільні очікування щодо такого комунікування – саме від державних відомств населення очікувало б[11] отримання інформації про те, що сталось та які заходи вживаються.

Офіційні реакції державних установ були різноформатні та з'являлись зі значним запізненням[12].

Перша офіційна[13] реакція була з боку Служби безпеки України від 28 грудня 2015 р. На відміну від повідомлення Прикарпаттяобленерго воно було лаконічним, без конкретизації кого атакували (вказано, що це були «*мережі окремих обласних енергетичних підприємств*»), але при цьому чітко визначала організатора атаки – російські спецслужби.

18 січня (майже через місяць після інциденту) – з'явилось повідомлення[14] від Державного центру кібернетичного захисту та запобігання кібернетичним загрозам ДССЗЗІ, яке виступило із заявою про можливі повторення атак. Водночас базових повідомлень про саму атаку на сайті ДССЗЗІ немає, відтак не зовсім зрозуміло про які «повторні атаки» йдеться. Ще одне повідомлення відноситься до 25 січня з більш докладними рекомендаціями щодо протидії вірусу Black Energy[15]. На сайті CERT-UA інформаційних повідомлень із реагування на зазначений кіберінцидент немає, проте за місяць до атаки було повідомлення[16] про те, що українські ЗМІ атакують за допомогою Black Energy. Пізніше ці атаки почали вважати складовою багатоетапної підготовки атаки на Прикарпаттяобленерго[17].

Наступною була реакція МЗС України 19 січня 2016 р. Водночас це

---

[11] Слід підкреслити, що у суспільній свідомості вочевидь дуже слабо встановлено кореляції між кібератакою та тим, хто відповідно до чинного законодавства має відповідати за подолання її наслідків.

[12] При моніторингу реакцій враховувалась передусім публікації на офіційних сайтах державних установ, без урахування заяв для ЗМІ чи повідомлень у Facebook, які не були про дубльовані на офіційному сайті. Це було обумовлено гіпотезою, що повідомлення ЗМІ можуть бути не помічені споживачами, але якщо людина хоче спрямовано знайти інформацію про певний інцидент, то вона буде шукати на профільних сайтах органів державної влади.

[13] https://goo.gl/2p3odt

[14] https://goo.gl/WTgFWb

[15] http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=241099&cat_id=240232

[16] http://cert.gov.ua/?p=2370

[17] Дані доповідачів міжвідомчого семінару на базі Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова (18 лютого 2016 року)

було не авторське повідомлення підготовлене прес-службою МЗС, а передруком новини про вже загадану вище заяву ДССЗЗІ, але не з посиланням напряму на сайт ДССЗЗІ, а на повідомлення Euronews[18].

12 лютого 2016 р. з'явилось повідомлення Міненерговугілля про намір утворити групу за участю представників усіх енергетичних компаній для вивчення можливостей щодо запобігання несанкціонованому втручанню в роботу енергомереж[19]. Ця заява супроводжувалась найбільш детальним описом атаки та її наслідків для України з усіх тих, що були на той момент озвучені. Водночас чи була така група створена і якщо так, то чим закінчилась її робота з повідомлень сайту залишилось незрозумілим.

Фактично, коментування цієї події з боку державних установ було спорадичним і більше спрямованим на фахівців, ніж на широке коло громадян. Цей інформаційний вакуум заповнювали повідомлення іноземних агенцій, прес-релізи антивірусних компаній та заяви представників інших держав. Наприклад - заяви і коментарі урядових структур США: ще 7 січня 2016 року з'явилось повідомлення[20], що Центральне розвідувальне управління, Агентство національної безпеки США та Департамент внутрішньої безпеки США почали розслідування цього інциденту. Через місяць (25 лютого) з'явились[21] дані про те, що за результатами цього розслідування був підготовлений звіт згідно якого безпекові структури дійшли висновку, що за цими атаками стоїть РФ. До сьогодні подібних відкритих звітів щодо цього інциденту від українських безпекових структур так і не було оприлюднено.

Фактично, більшість українських громадян дізнались про цю подію з передруків західних видань та заяв іноземних структур. Не помітна була і будь-яка узгодженість заяв чи повідомлень як під час кризи, так і у посткризовий період. Більше того – посткризова комунікація виявилась

[18] https://goo.gl/V1Ss6v
[19] http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109
[20] http://www.pravda.com.ua/news/2016/01/7/7094696/
[21] http://www.pravda.com.ua/news/2016/02/28/7100535/

надзвичайно обмеженою та незавершеною.

18 грудня 2016 р. відбулась ще одна атака на роботу енергомереж України – в ніч з 17 на 18 число на підстанції «Північна» НАК «Укренерго» відбувся збій в автоматиці керування. Електропостачання вдалось швидко відновити (щоправда в окремих районах світло зникло на 6 годин). Найбільш оперативно подію коментував очільник Укренерго В.Ковальчук – він в 11:34 18-го грудня зробив відповідну заяву на своїй сторінці ФБ[22]. З його ж повідомлення можна дізнатись, що одразу розпочала роботу команда з аналізу кіберінциденту. 21-го грудня з посиланням на заяву пана Ковальчука, Reuters повідомив, що Україна розпочала розслідування. При цьому жодних даних про те, хто займається цим розслідуванням, якими є наслідки такого розслідування так і не були повідомлені. Варто зазначити, що даних на офіційному сайті компанії немає. Аналогічно за цей час жодної інформації на сайті безпекових структур з цього приводу так і не з'явилось. Лише 11 січня 20017 р. з публікації BBC, стали відомі окремі подробиці атаки із посиланням на залучених до аналізу експертів[23].

Загальними проблемами комунікування зазначеного кіберінциденту були наступні:

- залишилась незрозуміла позиція суб'єктів національної системи кібербезпеки України (як вони реагували на кіберінцидент, чи брали участь у розслідуванні, а якщо так, то з яким результатом, чого варто очікувати споживачам якщо такі атаки повторяться);
- координація комунікації;
- відсутня чітка та зрозуміла версія події для суспільства та фахівців (жодних експертних заяв з цього приводу так і не було озвучено);
- майже повна відсутність посткризової комунікації.

Ще одним кіберінцидентом який потребував ефективного

[22] https://www.facebook.com/permalink.php?story_fbid=1798082313797621&id=100007876094707
[23] https://espreso.tv/news/2017/01/11/u_grudni_khakery_vidklyuchyly_elektryku_v_chastyni_kyyeva

комунікування з боку органів державної влади – атака вірусу NotPetya.

27 червня 2017 р. було виявлено кіберінцидент, пов'язаний із функціонуванням вірусу NotPetya. Згідно з даними Департаменту кіберполіції Національної поліції України, під час масованої хакерської атаки в Україні були інфіковані понад 12,5 тисяч комп'ютерів[24]. Основним каналом розповсюдження вірусу стало програмне забезпечення M.E.Doc, сервери якої було зламана задовго до самої атаки. Незважаючи на те, що вірус маскувався під дію віруса-здирника його цілями були шпигунство та подальше знищення атакованих систем.

Більшість даних вказують на те, що активна фаза атаки розпочалась приблизно о 10:30-11:00 27 червня 2017 р. При цьому перші офіційні реакції розпочались лише о 16:40[25]. Відтак публічне комунікативне реагування відбулося із суттєвим запізненням, відносно вимоги реакції протягом першої години. На момент заяв вже декілька годин випуски новин на телебаченні, повідомлення в медіа, обговорення в соціальних мережах були зосереджені довкола кібератак. Висловлювалися різні версії події, влада втратила першість (надання першої інтерпретації), яка дозволяє взяти вирішення проблеми під інформаційний контроль[26].

Крім того, більшість з цих реакцій відбувались на сторінках у ФБ посадовців, у той час як офіційні ресурси залишились практично без уваги.

Експерти наголошували, що комунікація профільних органів влади на цьому етапі була недосконала. 5 годинне мовчання в такій ситуації – це потенційний шлях до паніки. Ситуацію ускладнювали і певні панічні заяви окремих міністрів, про те, що все «лягло» і нічого не працює[27]. Ці заяви

[24] https://glavcom.ua/interviews/glava-kiberpoliciji-sergiy-demedyuk-instrukciji-do-virusu-petyaa-pisali-rosiyskoyu-movoyu-ce-dovedeniy-fakt-429072.html

[25] Більш докладно про комунікативну складову реагування на цей кіберінцидент – аналітичний матеріал НІСД «Кібератака «NotPetya»: попередні оцінки та можливі наслідки» від липня 2017 року.

[26] Управление PR в кризисных ситуациях // Конспект лекций [Електронний ресурс]. – Режим доступу: http://gendocs.ru/v8629/public_relations

[27] https://goo.gl/Cks9Lc

швидко поширювались різноманітними ЗМІ[28] [29]. У ці перші 5 годин (до появи офіційних заяв) різноманітними експертами та квазіекспертами було продуковано значну кількість версій, що додатково хаотизувало інтерпретації події та дискредитувало державу.

Позитивним фактором цієї атаки було те, що заяв було багато і від найрізноманітніших відомств (передусім – РНБО, КМУ, СБУ та Департамент кіберполіції). Така активна інформаційна позиція структур актуалізувала проблему координації заяв та узгодження основних месиджів. Відсутність координації призводила до того, що часто змінювався ключові параметри повідомлень, зокрема найбільш вірогідний автор атаки (від РФ та тимчасово непідконтрольних територій до внутрішніх джерел), а рекомендації до державних структур з протидії кібератаці надходили з щонайменше 3 різних установ (деякі з таких рекомендацій розміщувались на сайтах установ, інші спрямовувалися напряму до міністерств і відомств). Усе це потенційно створювало хаотизацію комунікації та брак усвідомлення реального стану із поширенням вірусу.

Позитивною відмінністю комунікування цього кіберінциденту стала відкритість органів державної влади для ЗМІ. Майже на всіх ключових телеканалах та радіо були виступи урядовців та очільників безпекових структур, які намагалась надати максимум інформації журналістам, а відтак – показати контрольованість ситуації загалом. Водночас часто такі заяви були нечіткими та не могли дати відповіді на ключові питання, які традиційно виникають до повідомлень щодо кризової ситуації: що власне сталося, хто постраждав та що конкретно робиться для вирішення проблеми. Не можна не відмітити і низьку інтенсивність реакції професійних комунікаторів (у т.ч. – недержавних) на цю подію.

Ще одна проблема повідомлень від безпекових структур – надмірна «технічна» мова. Подекуди це призводило до того, що медіа навіть не

[28] https://goo.gl/38a6WG
[29] https://goo.gl/PWSPKp та https://goo.gl/fa8oNd

передруковували їх. Неможна не відзначити і надміру швидку появу заяв щодо вини за принципом «кому вигідно». При цьому перші обережні підтвердження участі Росії з'явились лише через декілька днів.

Традиційно слабким був посткризовий супровід ситуації. Хоча окремі розгорнуті інтерв'ю почали з'являтись вже за 2 місяці після кібератаки, але вони не дають громадянам цілісного уявлення про те, що відбулось, хто постраждав, як держава планує цього уникати в майбутньому, та що для цього робиться.

## Комунікування кіберінцидентів другої половини 2017 р.

Кінець 2017 р. відмітився декількома випадками кіберінцидентів.

Ключовий з них – атака вірусу BadRabbit. 24 жовтня 2017 р. за допомогою цього вірусу було атаковано київський метрополітен (призвело до збоїв у оплаті проїзду платіжними картками) та Одеський аеропорт (були уражені окремі інформаційні системи аеропорту). Крім того, з метою попередження атаки на інформаційні ресурси Міністерства транспорту було відключено їх офіційний сайт.

Першою реакцією (о 14:36) було повідомлення прес-служби Мінтрансу, що сайт відключено у зв'язку із можливими атаками[30]. Майже одночасно (о 16:30) на ситуацію відреагували твіттер-аккаунт Київського метро[31] (жодної інформації про суть події – лише повідомлення про те, що не працюють окремі функції) та Одеського аеропорту[32] (повідомлення містить інформацію про суть проблеми, про поточний стан, але не вказано жодних відомостей щодо того, що робиться для її вирішення). За півгодини потому (17:06) – повідомлення про факт атаки від CERT-UA[33] (при цьому їх повідомлення було адресовано системним адміністраторам і було не зрозуміло рядовому користувачу). Приблизно в той самий час – перший

[30] https://goo.gl/miDVou
[31] https://twitter.com/kyivmetroalerts/status/922818286546452480
[32] http://www.odessa.aero/uk/node/1269
[33] http://cert.gov.ua/?p=2945 та http://cert.gov.ua/?p=2950

коментар Національної поліції (фактично жодної додаткової інформації не було повідомлено, лише підтверджено факт атаки)[34]. О 19-й годині – повідомлення СБУ[35] в якому у стислому вигляді пояснено, що відбулось, які системи уражено, якими є наслідки та що потрібно робити для мінімізації наслідків (чи попередження ураження). О тій же 19-й годині – повідомлення[36] Нацбанку про відсутність повідомлень українських банків про ураження їх систем в результаті хакерських атак. Перше повідомлення на сайті Департаменту кіберполіції – лише 25-го жовтня з розгорнутими показниками ураження, механізму реалізації ураження та рекомендаціями для попередження ураження систем (для технічних спеціалістів)[37].

Загалом реакція як організацій що були уражені вірусом, так і суб'єктів протидії кібератакам була достатньо оперативною. Водночас не можна не відмітити хаотичність повідомлень, часто – низьку інформативність (або повне ігнорування причин виникнення кризової ситуації) та відсутність зрозумілих пояснень для громадськості щодо суті події (найбільш повним та адекватним ситуації в цьому сенсі було повідомлення СБУ).

Другий випадок, який вимагав активного інформаційного позиціонування державних структур, пов'язаний із діяльністю українського співтовариства хактивістів «Ukrainian Cyber Alliance», які у листопаді 2017 р. розпочали акцію[38] (флешмоб) під загальним хештегом #F*ckResponsibleDisclosure[39]. За словами організаторів його мета – «*громадська акція для підвищеня рівня IT-гігієни*» (за суттю акція є формою краудсорсингового пен-тесту[40] державних інформаційних систем). У межах «флешмобу» були протестовані уразливості наступних структур:

[34] http://www.pravda.com.ua/news/2017/10/24/7159520/
[35] https://goo.gl/Yhu6Kx
[36] https://goo.gl/NZ8vYK
[37] https://goo.gl/6VKa1Y
[38] https://petrimazepa.com/disclosure.html
[39] Більш докладно про сутність поняття «Responsible Disclosure» та небажання авторів флешмобу його дотримуватись у матеріалі за посиланням «https://www.facebook.com/vstyran/posts/10155958884177372»
[40] Пентест (penetration test, pentest) - оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї

Національное агентство з питань попередження корупції, Комунальна наукова-дослідна установа «Науково-дослідний інститут соціально-економічного розвитку міста», Міністерство внутрішніх справ, Департамент кіберполіції Національної поліції України, Херсонська обласна рада, Судова влада України, Державна служба фінансового моніторингу України, Енергоатом, Головне управління Національної поліції в Київській області, Київводоканал, ОАО «Запорожсталь», Державна служба з надзвичайних ситуацій, Комунальний концерн «Центр комунального сервісу», Укртелеком, Закарпатський військомат, низка регіональних Центрів зайнятості, Міністерство охорони здоров'я України, Міністерство юстиції України, Міністерство оборони України, Запорізька АЕС, Інститут електрозварювання НАН України, Міністерство освіти України та НАН України.

З 23 державних установ (міністерств, їх підрозділів чи об’єктів критичної інфраструктури), лише 3 (Національне агентство з питань попередження корупції[41], Херсонська обласна рада[42] та Енергоатом[43]) публічно відреагували на ситуацію. У більшості своїй це були спростування загального характеру, в яких йшлося про те, що, незважаючи на спроби кібератак, активістам не вдалось отримати доступ до внутрішніх мереж, інформації з обмеженим доступом чи порушити роботу підприємств.

Найбільш жорстким публічне протистояння виявилось між ініціаторами флешмобу та компанією «Енергоатом», які спочатку взагалі відмовлялись визнавати наявність уразливості, але в подальшому спробували залучити організаторів до їх усунення[44].

Зважаючи на те, що акція отримала розголос у ЗМІ, ігнорування проблеми (відсутність повідомлень та жорсткі спростування) видається малоефективним механізмом у реагуванні на подібні ситуації. Навіть у тих випадках, коли спростування наводились, вони часто запізнювались у часі й

[41] https://nazk.gov.ua/news/zvertayemo-uvagu
[42] https://goo.gl/bjF2PD
[43] https://goo.gl/5UUCGe
[44] https://goo.gl/WYtxBK

були надто загальними. Крім того, із них залишалось незрозумілим чи були вжиті якісь заходи (крім звернення до Департаменту кіберполіції, як це було у випадку із Херсонською обладміністрацією).

## ВИСНОВКИ

1. Протягом останніх 3-х років Україна зазнала принаймні п’яти масштабних кібератак, які можуть бути охарактеризовані як кризові ситуації та які потребували активного комунікування з боку державних структур.

2. Даючи загальну оцінку ефективності комунікування кожного з цих інцидентів можна зазначити наступне:

- ситуація із «Прикарпаттяобленерго»: ефективне комунікування з боку атакованого об’єкту, при цьому малоефективна комунікація з боку державних (у т.ч. – правоохоронних) установ;
- ситуація із «Укренерго»: комунікація фактично відсутня, а та, що відбувалась, не мала чіткої структури та змісту;
- ситуація із вірусом «NotPetya»: активне, але слабко скоординоване комунікування державних структур, що складало враження какофонічного комунікування та відсутності чіткого розподілу обов’язків;
- ситуація з вірусом «BadRabbit»: загалом ефективна та вчасна комунікативна реакція з боку державних установ (передусім, правоохоронних органів) і вкрай слабке комунікування інцидентів з боку уражених структур;
- флешмоб групи «Ukrainian Cyber Alliance»: майже відсутня комунікація з боку державних структур і слабка (часто – непродумана) реакція з боку атакованих групою установ.

3. Загальними проблемами комунікування кіберінцидентів з боку держструктур є:

- значні проміжки часу між подією та першою реакцією;
- відсутність єдиної, зрозумілої та достовірної історії, яка має

доноситись до аудиторій та надмірна орієнтованість повідомлень на технічних фахівців;

- проблема координації (внутрішня та міжвідомча) комунікації;
- майже відсутня посткризова комунікація кіберінцидентів.

## РЕКОМЕНДАЦІЇ

*суб'єктам національної системи кібербезпеки*

1. Опрацювати можливість створення внутрішньовідомчих процедур для профільних комунікативних департаментів на випадок кіберінцидентів, які мають включати формалізований порядок взаємодії з підрозділами, що безпосередньо задіяні у подоланні наслідків (недопущення реалізації) кіберінциденту та/чи кібератаки, а також завчасну підготовку форм повідомлень для найбільш типових випадків кіберінцидентів/кібератак, пов'язаних, зокрема, із:

- об'єктами критичної інфраструктури;
- інформаційними системами установи;
- масового ураження шкідливим програмним забезпеченням;
- інформацією у ЗМІ про витік відомчої інформації внаслідок кіберінциденту/кібератаки.

2. Відповідні процедури мають містити граничні показники для появи повідомлень відомств про суть інцидентів (обов'язково встановлюючи вимогу появи першої заява про інцидент протягом першої години);

3. У межах наявних міжвідомчих форматів співпраці суб'єктів національної системи кібербезпеки (передусім, у межах роботи Національного координаційного центру кібербезпеки) опрацювати конкретні процедури взаємодії для обміну інформацією, яка необхідна іншим суб'єктами національної системи кібербезпеки для власного комунікативного реагування.

4. На базі Національного координаційного центру кібербезпеки опрацювати формати посткризової комунікації як невід'ємної складової

загального комунікування кіберінцидентів. Видається необхідним запровадити формат публічного звітування суб'єктів національної системи кібербезпеки у формі «аналітичного звіту» (або його варіанту), який має бути сформований за результатами службового розслідування кіберінциденту та в якому мають бути подані для громадськості дані щодо:

- тривалості інциденту;
- його сутності;
- загальних показників щодо кількості уражених об'єктів та основних сфер, які були охоплені інцидентом;
- заходів, які вживались суб'єктами національної системи кібербезпеки для його вирішення чи мінімізації наслідків;
- заходів, які вживались атакованими структурами (якщо такі не відносяться до державного сектору) для його вирішення чи мінімізації наслідків інциденту;
- попередні оцінки щодо можливих ініціаторів та виконавців кібератаки;
- які заходи вживались суб'єктами національної системи кібербезпеки для недопущення таких інцидентів у майбутньому;
- рекомендації щодо попередження таких інцидентів у майбутньому (для широких верств громадян та технічних фахівців).

5. Обсяг такого звіту не має бути значним, він має бути написаний максимально доступно для неспеціалістів, а його мета – дати чітку та несуперечливу версію держави щодо того, що відбулось, як саме відреагувала держава та які висновки були зроблені.

*Д.В. Дубов*
Відділ інформаційної безпеки
та розвитку інформаційного суспільства
Національного інституту стратегічних досліджень