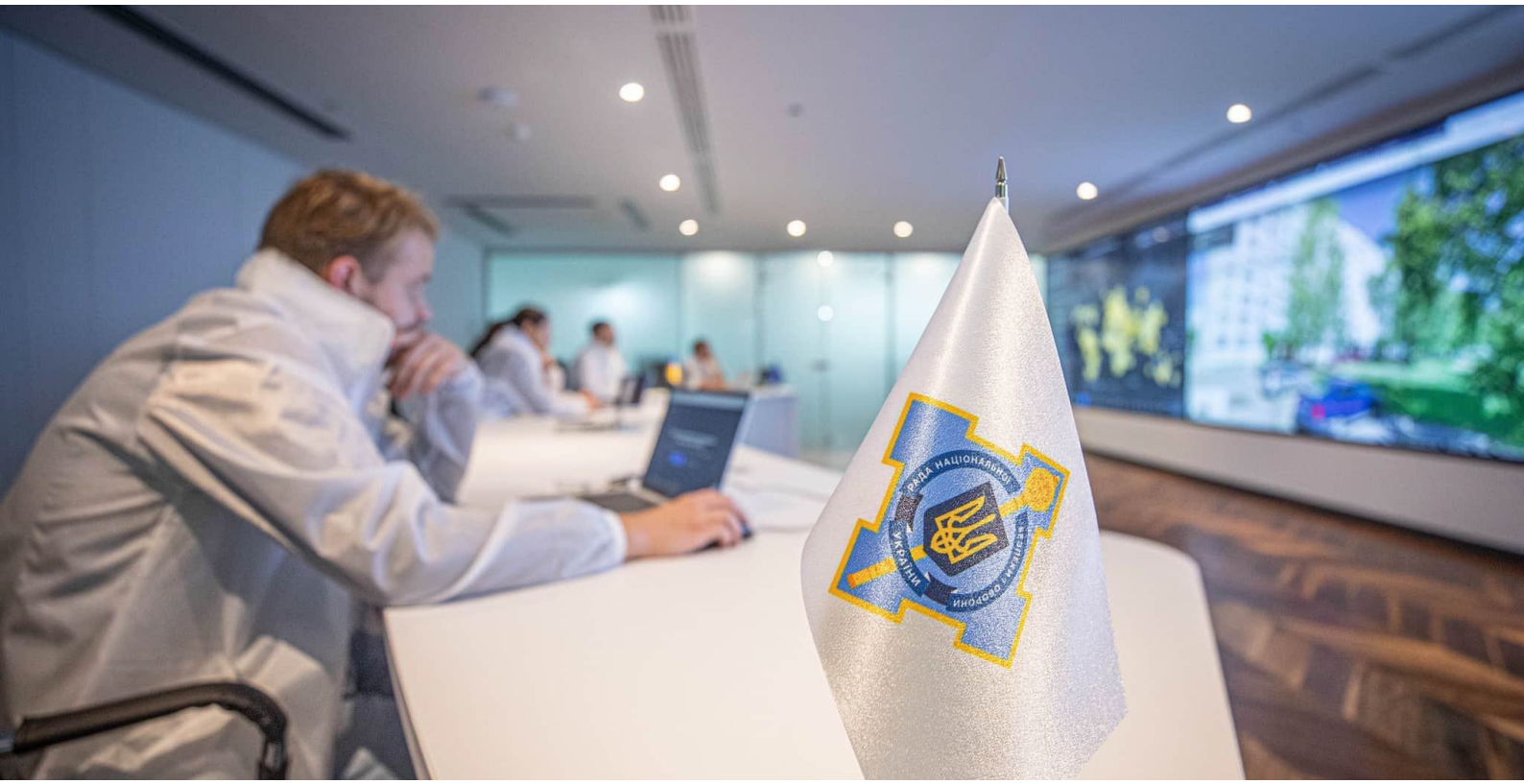
Апарат РНБО України

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ



ОЦІНКА СТАНУ КОМУНІКАЦІЇ, КООРДИНАЦІЇ ТА ВЗАЄМОДІЇ МІЖ СУБ'ЄКТАМИ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

АНАЛІЗ ЗА РЕЗУЛЬТАТАМИ ПІЛОТНОГО ДОСЛІДЖЕННЯ

2021

Публікація підготовлена проектом USAID «Кібербезпека критично важливої інфраструктури в Україні» на запит Агентства США з міжнародного розвитку (USAID). Погляди, відображені в цій публікації, є власними поглядами її авторів та не обов'язково відображають позицію Агентства США з міжнародного розвитку

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

Держспецзв’язку	Державна служба спеціального зв'язку та захисту інформації України
ЗМІ	засоби масової інформації
КБ	кібербезпека
КІ	критична інфраструктура
НКЦК	Національний координаційний центр кібербезпеки РНБО України
ОКІ	об’єкти критичної інфраструктури
РНБО	Рада національної безпеки та оборони України
СБУ	Служба безпеки України
CERT-UA	Урядова команда реагування на комп'ютерні надзвичайні події України
CSIRT	Команда реагування на інциденти комп'ютерної безпеки (Computer security incident response team)
SOC	Центр управління безпекою (Security Operations Center)
MISP-UA	Платформа для обміну інформацією про шкідливе програмне забезпечення (Malware Information Sharing Platform “Ukrainian Advantage”)
NIST	Національний інститут стандартів і технологій США
NIS	Директива Європейського парламенту і Ради ЄС 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу
USAID	Агентство США з міжнародного розвитку

ПРО ДОСЛІДЖЕННЯ

Це дослідження є результатом співпраці Національного координаційного центру кібербезпеки Ради національної безпеки і оборони України та проєкту USAID «Кібербезпека критично важливої інфраструктури України», що спрямований на підвищення рівня готовності України до кіберзагроз та її спроможності захищати критичну інфраструктуру шляхом створення сприятливих умов для розвитку кібербезпеки, підготовки спеціалістів та розбудови потужної індустрії кібербезпеки.

Одним із інструментів оцінювання прогресу в досягненні цих стратегічних цілей є дослідження поточного стану комунікації, координації та взаємодії між основними суб'єктами національної системи кібербезпеки, міністерствами та об'єктами критичної інфраструктури (ОКІ) для визначення пріоритетних напрямків удосконалення державної політики в сфері кібербезпеки. Респонденти були відібрані за критерієм їх залученості до співпраці між суб'єктами національної системи кібербезпеки.

Дослідження ґрунтується на результатах онлайн-опитування трьох основних груп респондентів: основні суб'єкти забезпечення кібербезпеки, міністерства та державні агенції, а також близько 60 ОКІ. Всього для опитування було відібрано 103 організації.

Анкета для опитування була розроблена фахівцями НКЦК РНБО України та проєкту USAID «Кібербезпека критично важливої інфраструктури України» з урахуванням Настанови із кібербезпеки Національного інституту стандартів і технологій США (NIST Cybersecurity Framework), що визначає 5 функцій кібербезпеки: ідентифікація, захист, виявлення, реагування та відновлення. Опитування мало на меті виявити готовність організацій виконувати кожну з цих функцій. Застосування цієї моделі зумовлене також необхідністю формування належної системи взаємодії та координації діяльності суб'єктів національної системи кібербезпеки на всіх етапах реагування на кіберзагрози відповідно до положень Закону України «Про основні засади забезпечення кібербезпеки України».

Опитування проводилося НКЦК РНБО України у жовтні 2020 року. Респондентам був надісланий лист із посиланням на онлайн-анкету. Зі 103 респондентів, відібраних для проведення опитування, було отримано відповіді від 46 організацій, серед яких основні суб'єкти національної системи кібербезпеки, урядові структури, державні підприємства, об'єкти критичної інфраструктури (ОКІ), серед іншого, з енергетичного, транспортного та банківського секторів.

Опрацювання отриманих даних тривало протягом листопада 2020 року, і за результатами такого опрацювання був проведений аналіз, результати якого представлені нижче, та розроблені рекомендації, які можуть бути застосовані учасниками опитування для вирішення проблемних питань та реалізації потенціалу для покращення ефективності національної системи кібербезпеки.

Це пілотне дослідження може бути основою для проведення щорічного оцінювання стану розвитку національної системи кібербезпеки.

РЕЗУЛЬТАТИ АНАЛІЗУ

1. Розуміння архітектури національної системи кібербезпеки

Більшість респондентів стверджують, що вони чітко розуміють, який нормативно-правовий акт визначає завдання та повноваження суб'єктів національної системи кібербезпеки (профільний закон), проте понад 30% респондентів зазначили, що архітектура та завдання суб'єктів системи визначають стратегічні документи (стратегія національної безпеки та стратегія кібербезпеки), що свідчить про недостатню обізнаність значної частини учасників із законодавчою базою.

Рисунок 1. Документи, що формують архітектуру кібербезпеки

Рисунок 2. Головна роль в координації КБ

2. Ефективність горизонтальної координації

Понад 80% респондентів зазначили, що у них створено підрозділ із питань кібербезпеки, який бере участь у взаємодії з основними суб'єктами забезпечення кібербезпеки (понад 33%), з об'єктами критичної інфраструктури (понад 15%) та міністерствами (13%).

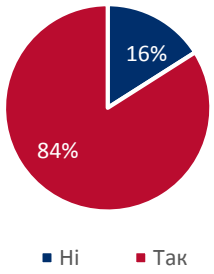


Рисунок 3. Існує підрозділ з кібербезпеки/ реагування на кіберзагрози

При цьому на секторальному рівні ефективність координації та взаємодії між суб'єктами є недостатньою. Майже 60% респондентів зазначили, що на рівні відомств, відповідальних за визначений сектор критичної інфраструктури (КІ), не створено підрозділу, який би відповідав за взаємодію із операторами КІ. Понад 70% респондентів відповіли, що на рівні їхнього сектору не визначений порядок обміну інформацією. Лише 20% респондентів відзначили, що їхні організації (установи) готували протягом останнього року будь-який звіт (аналіз) дій при виникненні кіберінцидентів. Звіт із питань кібербезпеки та кіберзахисту готували 40%. Відсутність секторальних (галузевих) CSIRT або його аналогів відзначили понад 70%. При цьому більшість респондентів відповіли, що взаємодія з іншими учасниками системи (недержавним сектором) є неформалізованою (відносини формалізували менше 30% респондентів) і фактично здійснюється на добровільних засадах.

3. Розуміння ролей суб'єктів координації у сфері кібербезпеки

У частині взаємодії з іншими учасниками системи кібербезпеки більшість респондентів зазначили, що вони взаємодіють переважно з основними суб'єктами забезпечення кібербезпеки (понад 70% взаємодіють із Держспецзв'язку та СБУ та близько 50% із НКЦК і Нацполіцією) за такими напрямками: обмін інформацією щодо актуальних загроз (89%), уточнення застосування нормативних вимог (51%), погодження порядку спільних дій щодо кіберінцидентів (40%).

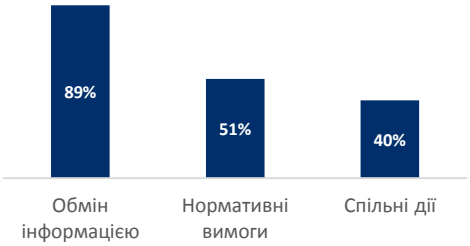


Рисунок 4. Основні напрями взаємодії стейкхолдерів

4. Готовність організації до забезпечення кібербезпеки

Респонденти зазначають, що інформацію щодо кіберзагроз та методів протидії їм отримують переважно завдяки власним зусиллям. 70% респондентів відзначають, що працівники створеного підрозділу отримують інформацію з інших джерел, таких як ЗМІ. 22% зазначили, що отримують інформацію випадково. 46% респондентів зазначили, що вони отримували інформацію від одного або декількох основних суб'єктів системи. При цьому 90% респондентів вважають, що вони мають отримувати інформацію щодо кіберзагроз від основного координаційного органу. При цьому лише 33% респондентів підтвердили, що таку інформацію від нього отримували.

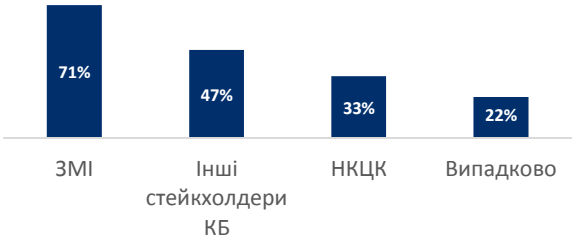


Рисунок 6. Джерела інформації щодо кіберзагроз

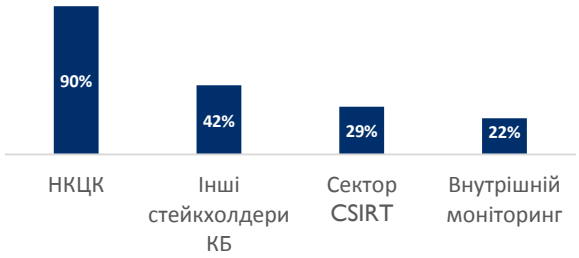


Рисунок 5. Хто має бути джерелом інформації про кіберзагрози

Попри те, що понад 90% респондентів визнали необхідність впровадження системи тренінгів та професійного навчання для працівників, поточна ситуація залишається незадовільною. Наприклад, лише 13% вказали, що їхні працівники беруть участь у навчальних заходах щомісячно, в той час як 31% респондентів вказують, що це відбувається лише раз на квартал. Ще 28% вказали, що підвищення кваліфікації відбувається лише раз на рік, а 27% взагалі не проводять такого навчання.

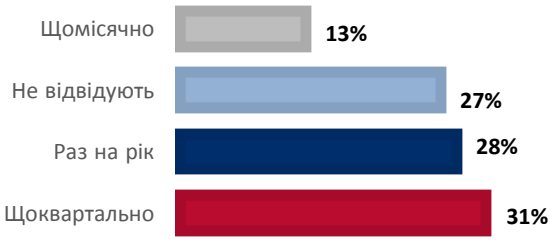


Рисунок 7. Навчання та професійний розвиток співробітників (частота)

Не визначеною є ситуація з проведенням незалежного аудиту. Відповіді респондентів практично розділилися: 51% проводили і 49% не проводили аудит. При цьому лише у 50% висновки аудиту допомогли респондентам у підвищенні рівня кібербезпеки.

На думку більшості респондентів (понад 60%), вимоги щодо організації роботи з кібербезпеки/кіберзахисту в їхніх організаціях визначені, при цьому вони регулюються переважно відомчими актами (понад 30%). Лише 10% респондентів відзначили наявність установлених на законодавчому рівні вимог.

Більшість респондентів відзначили незадовільний рівень забезпечення роботи створеного підрозділу з кібербезпеки: понад 35% респондентів відзначили, що рівень кадрового забезпечення профільного кібербезпекового підрозділу становить менше 20% від потрібного (ще 38% — від 20 до 50% від потреби). 53% вказали, що рівень технічного забезпечення кібербезпекового підрозділу становить менше 20%. При цьому понад 70% респондентів відзначили, що їх працівники (в тому числі вище керівництво) знають, як реагувати на кіберзагрози, знають відповідні процедури.

Рисунок 8. Страхування кіберзагроз

У частині оцінювання ризиків майже 80% респондентів відзначили, що в них відсутні вимоги та практика оцінювання ризиків, пов'язаних із кіберзагрозами, а якщо таке оцінювання і проводиться окремими організаціями, то власними силами (понад 60% випадків). 70% респондентів зазначили, що в них відсутні інструменти підрахунку втрат організації при реалізації кіберзагроз. При цьому понад 60% респондентів вважають за необхідне розвивати систему страхування ризиків у сфері кібербезпеки.

5. Готовність до розслідування кібератак та обміну інформацією

Розслідування кіберінцидентів є важливою складовою процесу здобування досвіду (lessons learning) та відновлення діяльності організації, однак процедури залишаються не визначеними:

56% зазначають відсутність порядку дій та взаємодії з іншими суб'єктами національної системи кібербезпеки при виявленні кіберінциденту;

близько 60% вказують на відсутність вимог щодо забезпечення кібербезпеки/кіберзахисту на рівні їхнього сектору (а ті, хто стверджують, що вони існують, ледь можуть навести приклади їх застосування);

лише 42% вказують, що в їхніх організаціях за результатами кіберінцидентів готують відповідний звіт (але лише 20% зазначають, що подібний звіт складався протягом останнього року).

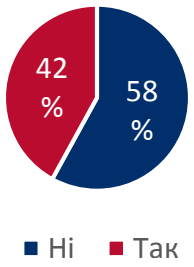


Рисунок 9. Наявність вимог щодо забезпечення кібербезпеки на рівні сектору

Відсутність порядку взаємодії як елемента проведення розслідування тісно пов'язана і з проблемами обміну інформацією про кіберінциденти — респонденти часто не впевнені, кого і як вони мають інформувати. Одна з причин — відсутність чітких і зрозумілих галузевих/секторальних точок взаємодії, яких або не існує, або про які респондентам не відомо (85% не

володіють інформацією про галузеві CSIRT або їх аналоги, а 56% не відомо про плани створення такої структури). Існуючі платформи обміну об'єднують не всіх респондентів — близько 65% опитаних не беруть участі у функціонуванні платформи MISP-UA. При цьому серед тих, хто є учасниками цієї платформи, 90% задоволені ефективністю співпраці. Брак обміну інформацією про кіберінциденти можна пояснити слабкою обізнаністю стейкхолдерів про наявні інструменти або недовірою до них.

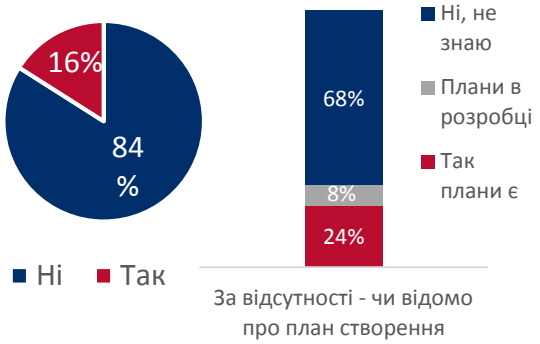


Рисунок 10. Наявність у відомстві CSIRT або його аналога

Також до негативних факторів можна віднести відсутність регламентів обміну інформацією на рівні секторів (70% відповідей). Так, лише у половини респондентів (53%) визначена процедура невідкладного інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA та/або Ситуаційного центру забезпечення кібербезпеки СБУ про кіберінциденти та кібератаки. 70% із тих, хто має визначені процедури інформування, не застосовували їх жодного разу протягом останнього року, хоча в тих же 70% є постійно оновлюванні контактні дані правоохоронних або уповноважених органів, яких потрібно сповістити після виявлення події[1]. Слід підкреслити, що 80% визнають, що протоколи взаємодії вкрай необхідні.

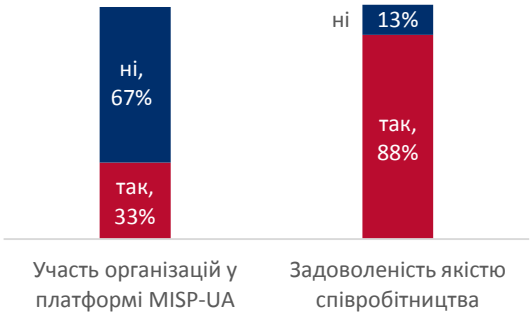


Рисунок 11. Участь у платформі MISP-UA

6. Готовність до реагування

Лише 53% відзначають, що в їхніх організаціях існує план реагування на кібератаку, і близько 20% стверджують, що його застосовували хоча би раз. Там, де такий план існує, він затверджений внутрішнім документом.

Не впорядкованою залишається співпраця з недержавним сектором. На запитання «Чи запроваджено вашою організацією порядок взаємодії з неурядовими організаціями, приватним сектором, громадськістю?» 74% вказали на його відсутність (або не впровадження) у формі формальних документів. Хоча близько 10% респондентів відзначили, що мають такі протоколи для заходів із попередження або розслідування кіберінцидентів.

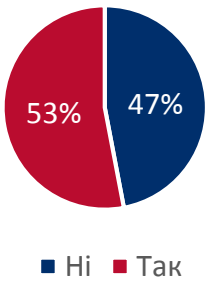


Рисунок 12. Наявність планів реагування на кібератаки

[1] Переважно Держспецзв'язку, СБУ, Департамент кіберполіції України і, трохи менше, НКЦК.

Менше половини організацій впровадили внутрішньовідомчі протоколи щодо дій підрозділів та працівників у разі кіберінциденту (53% не мають таких протоколів). Позитивним є те, що ці протоколи застосовують — 20% респондентів стверджують, що застосовували їх принаймні раз протягом останнього року.

Відповідно до Закону України «Про основі засади кібербезпеки України» (п.4 ст.6) власники/керівники ОКІ мають інформувати CERT-UA про інциденти кібербезпеки. На сьогодні порядок такого інформування частково визначений у документі «Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», однак лише 9% респондентів заявили про те, що застосували його протягом останнього року (ще 2% застосовували Порядок десять та більше разів).

Рисунок 13. Застосування "Порядку координації діяльності ... з запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів ..." протягом останнього року

7. Отримання допомоги від інших учасників системи щодо кібератак/кіберінцидентів

Близько 60% респондентів впевнені в тому, що їхня організація має можливість отримати належну допомогу в реагуванні на кібератаку, однак фактичні дані щодо випадків такої допомоги ставлять таку впевненість під сумнів.

Так, 80% респондентів вказують, що інші суб'єкти кібербезпеки ніколи не зверталися до них по допомогу для реагування на кіберінциденти (відповідно, організації не мають практики опрацювання таких звернень, не знають, що робити в таких випадках та яку допомогу організація може надати).

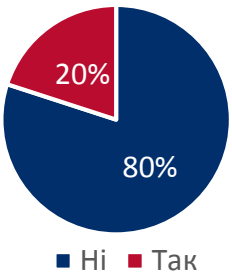


Рисунок 14. Практика звернень організацій до інших суб'єктів по допомогу під час кіберінцидентів

Лише 31% респондентів вказали, що мали позитивний досвід звернення по допомогу до представників основних суб'єктів забезпечення кібербезпеки. 78% ніколи не зверталися по допомогу до секторальних суб'єктів (вочевидь не очікуючи на практичну допомогу), хоча 20% зверталися, і таке звернення було вдалим (водночас характер запитань робить неможливим ідентифікувати, до кого саме були спрямовані ці звернення і кого респонденти вважали в такому випадку «секторальними суб'єктами»). 90% не мають визначених процедур

Рисунок 15. Чи була практика звернення по допомогу з питань кібербезпеки до секторальних суб'єктів

державно-приватної взаємодії щодо отримання допомоги в разі кіберінцидентів.

Ще менше випадків, коли ОКІ зверталися до інших ОКІ по допомогу: 85% ніколи не зверталися, але 12% кажуть про позитивний досвід. Низькі відсотки звернень можуть бути додатково пояснені таким чинником: у 74% опитаних не визначено жодних зобов'язань щодо забезпечення нерозкриття отриманих відомостей про суб'єкта, який звернувся із запитом (знеособлення та забезпечення конфіденційності при подальшому опрацюванні інформації про кіберінцидент), що є однією з вимог NIS Директиви ЄС. Це не забезпечує належного рівня довіри між суб'єктами кібербезпеки та зменшує готовність до горизонтальної взаємодії.

Це засвідчує брак ефективної координації з питань надання допомоги, передусім на горизонтальному рівні.

8. Відновлення функціонування

Більшість респондентів вважають, що їхня організація загалом має належний план відновлення після кібератак. Але при цьому лише 56% стверджують, що він існує у вигляді формального документа. Із них лише 20% відповіли, що існує практика його застосування. При цьому 98% респондентів відзначають брак механізмів взаємодії між центральними органами виконавчої влади на етапі відновлення порушеної функції внаслідок кіберінциденту/кібератаки на критичну інфраструктуру.

Рисунок 16. Статус планів відновлення

9. Інформування про кіберінциденти

56% опитаних вказують на необхідність інформування про кіберінциденти, однак при цьому 89% із тих, хто зазнавав кібератак, вказали, що вони не інформували громадськість про такі ситуації (не випускали прес-реліз, не робили заяви тощо). Незважаючи на це, 67% опитаних вважають, що таке інформування має відбуватися в режимі «єдиного голосу», тобто на підставі узгодженої позиції всіх зацікавлених суб'єктів. При цьому майже та сама кількість респондентів (64%) вказали, що процедура такого узгодження позицій жодним чином не врегульована.

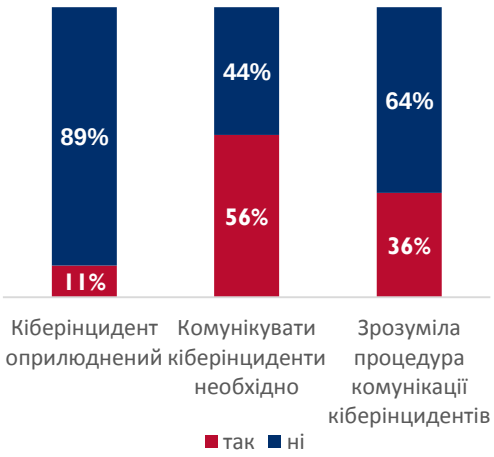


Рисунок 17. Оприлюднення інформації про кібератаки або кіберінциденти

Відтак можна говорити про певну амбівалентність ставлення до процесів інформування про кіберінциденти, яка призводить до браку комунікації. Така практика закритості може бути пов'язана як із браком навичок у відповідних спеціалістів, так і з переконаністю організацій у тому, що будь-який прояв відкритості може становити загрозу для організації. Наприклад, 87% респондентів вважають, що якщо громадськості стане відомо про такі інциденти, це зашкодить репутації організації. Показово, що майже така

сама кількість — 73% — вважають, що поширення такої інформації зашкодить національним інтересам, вочевидь суб'єктивно сприймаючи репутаційні ризики як національні інтереси держави.

10. Спроможність «засвоювати уроки» після кібератак

Засвоєння уроків за результатами кіберінцидентів залишається однією з найменш реалізованих функцій і демонструє відчутну прогалину між оцінкою самих респондентів такої спроможності та фактичним станом речей. Переважна більшість організацій вважають, що знають, як отримувати користь від досвіду кіберінцидентів. Так, 71% опитаних відповіли, що кібератаки вплинули на їхню установу в частині зміни підходів до кібербезпеки/кіберзахисту, а 56% кажуть про наявність практики ґрунтовного вивчення кіберінцидентів для посилення кібербезпеки організації. У 53% вимога щодо аналізу інцидентів та розробки пропозицій/рекомендацій із посилення кібербезпеки прямо прописана у внутрішніх документах. 42% відзначили збільшення інвестицій у сферу кібербезпеки організації після кібератаки (або кіберінциденту).

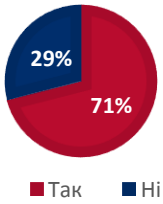


Рисунок 19. Досвід кіберінциденту застосовується (на організаційному рівні)

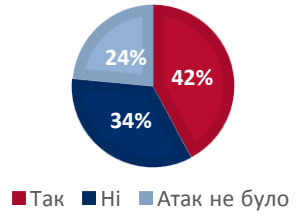


Рисунок 18. Збільшення інвестицій в кібербезпеку після кібератак

Однак, незважаючи на це, 73% визнають, що не готують жодних формальних звітів щодо розслідування кібератаки, а 69% не знають, чи змінювали основні суб'єкти національної системи кібербезпеки вимоги до забезпечення кібербезпеки/кіберзахисту після проведеного аналізу кіберінциденту/кібератаки.

Відсутність практики чіткого документування результатів внутрішніх перевірок може вкрай ускладнити процес удосконалення власної системи кібербезпеки (в тому числі через відсутність чіткого переліку проблем, які потребують вирішення, а відтак і контролю за їх вирішенням). 69% зазначають, що в питаннях відновлення після кібератак організація може покладатися виключно на себе, що свідчить про сумніви щодо можливості отримання допомоги від інших суб'єктів кібербезпеки (в тому числі державних, на яких готові покластися лише 18% опитаних).

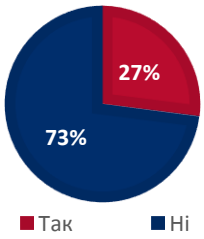


Рисунок 21. Проведено аналіз або розслідування кібератаки

Рисунок 20. На кого ви покладаєтесь у випадку кібератаки?

11. Сприйняття ефективності комунікації

Результати кількісного оцінювання, що мало на меті визначити індекс сприйняття респондентами поточного рівня координації в сфері кібербезпеки, дали змогу дійти низки принципових висновків.

Загальне сприйняття респондентами якості (ефективності) співпраці та комунікації (в широкому розумінні цих понять) у секторі кібербезпеки становить 5,8 із 10 балів (де 10 — найвища оцінка).

Найнижчий рівень сприйняття (4,8) демонструють міністерства та відомства. Респонденти з групи «інші державні установи» (яка охоплювала лише частину основних суб'єктів, а загалом відомчий рівень організацій: переважно служби та агентства) продемонстрували вищі показники — 5,5. Більш оптимістичне сприйняття поточного рівня координації продемонстрували опитані ОКІ — зокрема респонденти з енергетичного сектору в середньому дали оцінку 6,8.

Рисунок 22. Сприйняття респондентами якості (ефективності) співпраці та комунікації, за стейкхолдерами (максимальний бал: 10)

НАПРЯМКИ ПОКРАЩЕННЯ

Ці рекомендації стосуються базового комплексу заходів, які можуть бути вжиті учасниками опитування для вирішення проблемних питань та реалізації потенціалу для покращення ефективності національної системи кібербезпеки. До першочергових заходів належать такі:

Рекомендувати профільним міністерствам і відомствам спільно з ОКІ, що входять до сферу їх відповідальності, виробити порядок взаємодії під час кіберінцидентів/кібератак та визначити можливі форми взаємодопомоги під час таких подій. Забезпечити відпрацювання протоколів взаємодії, в т.ч. секторальних. Загальним стратегічним пріоритетом діяльності всіх суб'єктів має стати покращення координації діяльності на всіх рівнях.

Рекомендувати ОКІ розпочати практику проведення тематичних галузевих заходів із аналогічними об'єктами (круглих столів, дискусій тощо) щодо обговорення спільних проблем кібербезпеки. Одним з напрямків такої діяльності має стати опрацювання можливості впровадження практики кіберстрахування та потрібних для цього нормативно-правових змін.

Секторальним суб'єктам сприяти створенню галузевих CSIRT/SOC, залучивши до цього процесу представників ОКІ відповідних секторів. Запропонувати тим секторальним суб'єктам, що вже мають досвід участі у створенні секторальних CSIRT/SOC узагальнити та поширити свій досвід (в частині розв'язання проблем нормативно-правового, організаційного, кадрового характеру) з метою врахування його при розвитку таких центрів в інших секторах.

Залучити фахівців приватного сектору до консультацій з кібербезпеки. Це має стати однією з форм практичної реалізації концепції державно-приватного партнерства в сфері кібербезпеки та сприяти виробленню типових форматів такого співробітництва.

Рекомендувати респондентам впровадити рекомендації, надані їм за результатами проведення незалежного аудиту кібербезпеки (в тих організаціях, де такий проводився).

Встановити практику щоквартального підвищення кваліфікації співробітників профільних кібербезпекових підрозділів, а також щонайменше раз на півроку проведення заходів з підвищення рівня обізнаності в сфері кібербезпеки для інших категорій працівників. Базою такого навчання може виступати НКЦК РНБО України, як в межах вже розпочатих навчальних програм, так і в контексті запровадження нових (галузево- та секторально орієнтованих).

Проводити періодичні оперативні навчання для співробітників організацій з розвитку навичок готовності до кіберінцидентів, в т.ч. із залученням до їх проведення представників основних суб'єктів національної системи кібербезпеки.

Звернутись до підпорядкованих (якщо такі є) або партнерських освітніх закладів з метою розробки і проведення на їх базі короткострокових спеціалізованих кібербезпекових курсів для підвищення обізнаності і професійної кваліфікації співробітників ОКІ та секторальних суб'єктів.

Апарат РНБО України

НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ