АНАЛІЗ ЗА РЕЗУЛЬТАТАМИ ОНЛАЙН ОПИТУВАННЯ

Київ 2021

ОЦІНКА СТАНУ РОЗВИТКУ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Розробка нової Стратегії кібербезпеки України передбачає реальну оцінку стану розвитку національної системи кібербезпеки. З цією метою для комплексного і всебічного дослідження з цього питання було запропоновано провести онлайн опитування основних суб'єктів кібербезпеки, об'єктів критичної інфраструктури, підприємств реального сектора економіки, фінансової сфери, сфери послуг тощо.

Даний опитувальник підготовлено за ініціативою робочої групи з розроблення концептуальних засад проєкту Стратегії кібербезпеки України (2021-2025 роки), створеною при Національному координаційному центрі РНБО України.

Формат, структура та основні розділи опитувальника адаптовані до довідкової моделі формування інтегральної оцінки глобального індексу кібербезпеки (GCI) Міжнародного союзу електрозв'язку (ITU) департаменту розвитку (Development) (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf) і враховують національні особливості економічного укладу та нормативно-правової бази в Україні.

Проведення опитування було реалізовано через членів робочої групи, підписантів Меморандумів про співпрацю та взаємодію із НКЦК, мережу партнерів з числа вендорів IT-продукції та Київську торгово-промислову палату (http://kiev-chamber.org.ua/uk/17/2333.html).

Загальна кількість респондентів становить 1904, із них 616 повністю відповіли на питання анкети. При обробці результатів опитування враховувались лише повністю заповнені анкети.

Серед організацій, які повністю заповнили анкету, 508 (83%) мають державну форму власності, 75 (12%) є приватними підприємствами, 33 (5%) ідентифікували себе як міжнародні, громадські організації, комунальні підприємства.

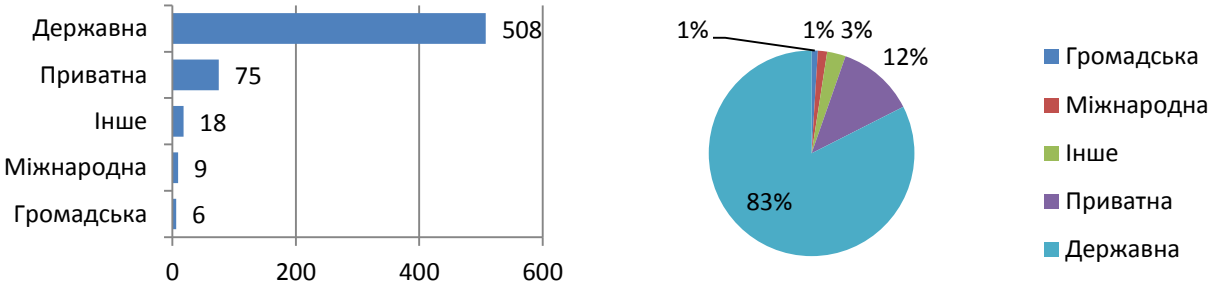


Рис.1

Розподіл учасників опитування за напрямами діяльності та секторами економіки представлений в таблиці 1.

Таблиця 1

Державне управління	240
Кібербезпека	57
Фінанси	56
Інформаційні технології	53
Телекомунікації	22
Соціальні послуги	18
Наукова, технічна діяльність	16
Енергетика	15
Транспорт	15
Охорона здоров’я	12
Комунальні послуги	8
Мистецтво, спорт, розваги	6
Будівництво	5
Торгівля	5
Авіаційна промисловість	4
Харчування	4
Обслуговування	3
Туризм	3
Газова промисловість	2
Засоби масової інформації	2
Металургійна промисловість	2
Нафтова промисловість	2
Оборонна промисловість	2
Хімічна промисловість	2
Ядерна енергетика	2
Космічна промисловість	1
Поштовий зв’язок	1
Інше	58

Для оцінки готовності організацій до сучасних кібератак респонденти за шкалою від 1 до 10 оцінювали рівень готовності за різними напрямами. Оцінки від 1 до 4 були визначені як низький рівень, від 5 до 7 – як середній рівень, від 8 до 10 – як високий рівень. Узагальнені результати наведені на рис. 2

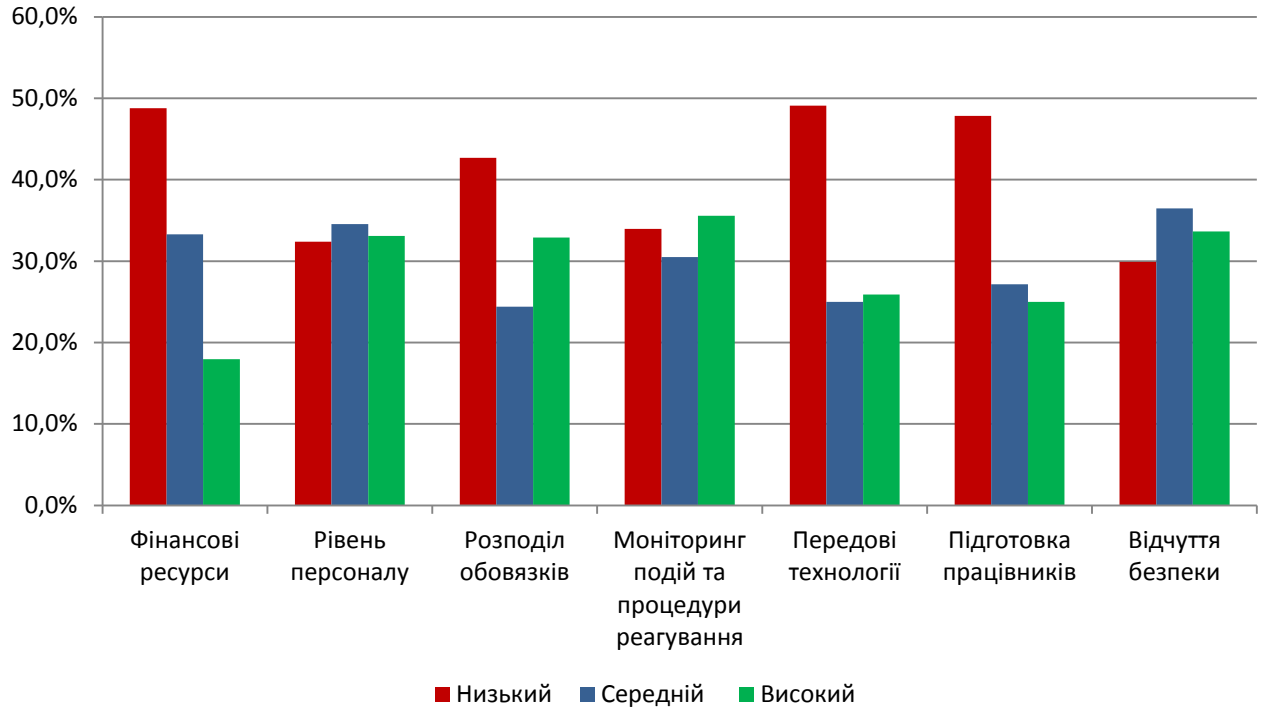
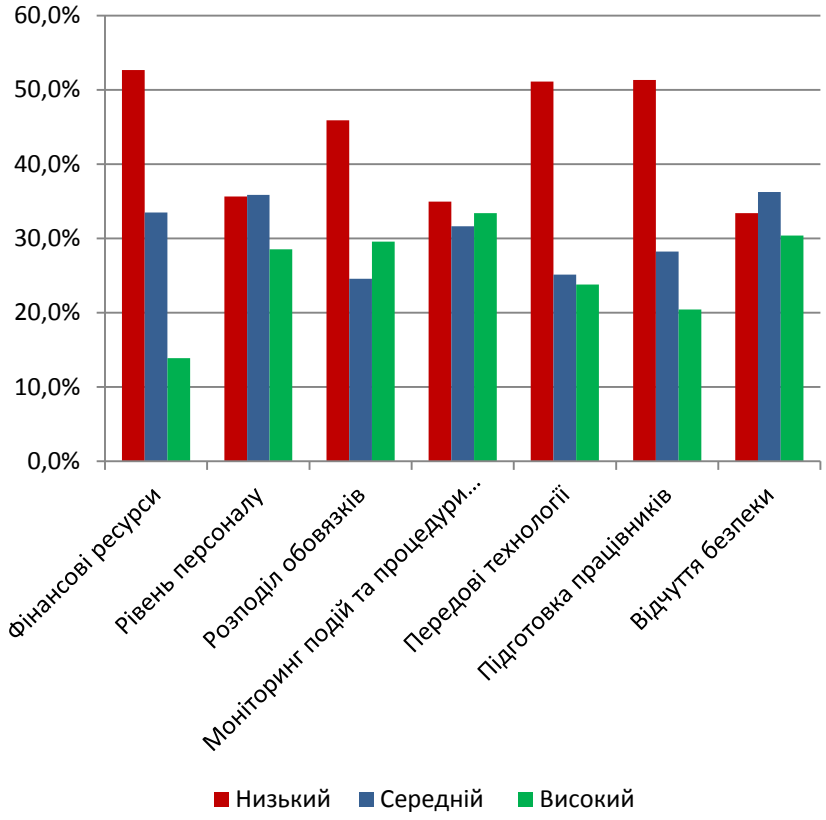


Рис. 2

Найнижче респонденти оцінюють готовність своїх організацій з точки зору впровадження передових технологій у сфері кібербезпеки, достатності фінансових ресурсів та зусиль організацій з підвищення кваліфікації працівників у напрямі кібербезпеки. При цьому рівень компетенцій фахівців з інформаційної безпеки та кібербезпеки цих організацій в цілому оцінюється як високий і більшість респондентів відчувають себе в безпеці. Переважна кількість респондентів вказують, що в їх організаціях здійснюється моніторинг подій безпеки та визначені процедури реагування на кіберінциденти. При цьому у більшості респондентів до сього часу не здійснено формалізоване розділення та не закріплено в розпорядчих документах функції підрозділів інформаційної безпеки (ІБ) та інформаційних технологій (ІТ).

Респонденти з державного та з приватного секторів по різному оцінюють рівень готовності власних організацій за визначеними напрямами. В державному секторі (Рис.3) найнижче оцінюються рівень фінансового забезпечення, відсутність підвищення кваліфікації працівників, відсутність програм впровадження передових технологій в сфері кібербезпеки та відсутність розподілу функцій ІТ та ІБ підрозділів. В той же час в приватному секторі найнижчу оцінку отримали відсутність програм впровадження передових технологій в сфері кібербезпеки, за іншими напрямами рівень готовності оцінюється як високий або середній (Рис. 4).


60,0%
50,0%
40,0%
30,0%
20,0%
10,0%
0,0%
Фінансові ресурси
Рівень персоналу
Розподіл обовязків
Моніторинг подій та процедури...
Передові технології
Підготовка працівників
Відчуття безпеки
Низький
Середній
Високий

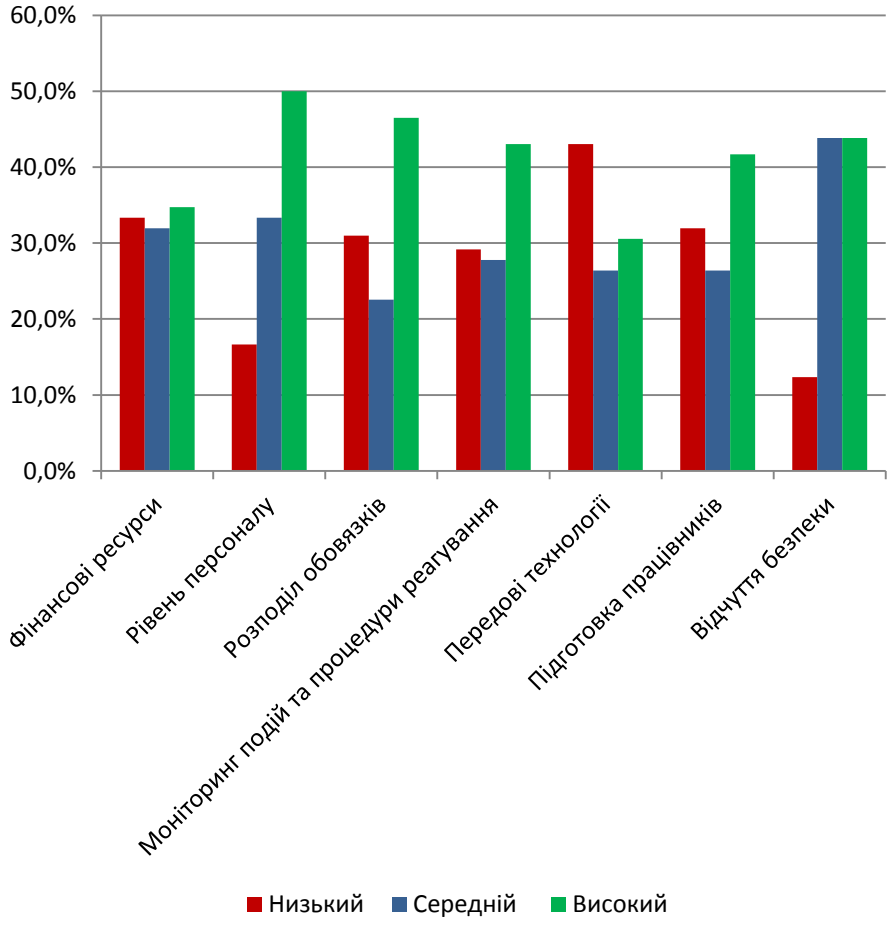

60,0%
50,0%
40,0%
30,0%
20,0%
10,0%
0,0%
Фінансові ресурси
Рівень персоналу
Розподіл обовязків
Моніторинг подій та процедури реагування
Передові технології
Підготовка працівників
Відчуття безпеки
Низький
Середній
Високий

Рис. 3, 4

Узагальнена оцінка рівня готовності складає 53%, в державному секторі – 51%, в приватному секторі – 63%. Дані щодо оцінок рівня готовності за різними напрямами наведені в таблиці 2 та на графіку нижче (Рис.5).

Таблиця 2

	Фінансові ресурси	**Рівень персоналу**	**Розподіл обов'язків**	**Моніторинг подій та процедури реагування**	**Передові технології**	**Підготовка працівникі в**	**Відчуття безпеки**
Загальна	47%	58%	53%	58%	49%	49%	59%
Державний сектор	44%	55%	51%	57%	47%	46%	56%
Приватний сектор	58%	71%	62%	63%	54%	61%	68%

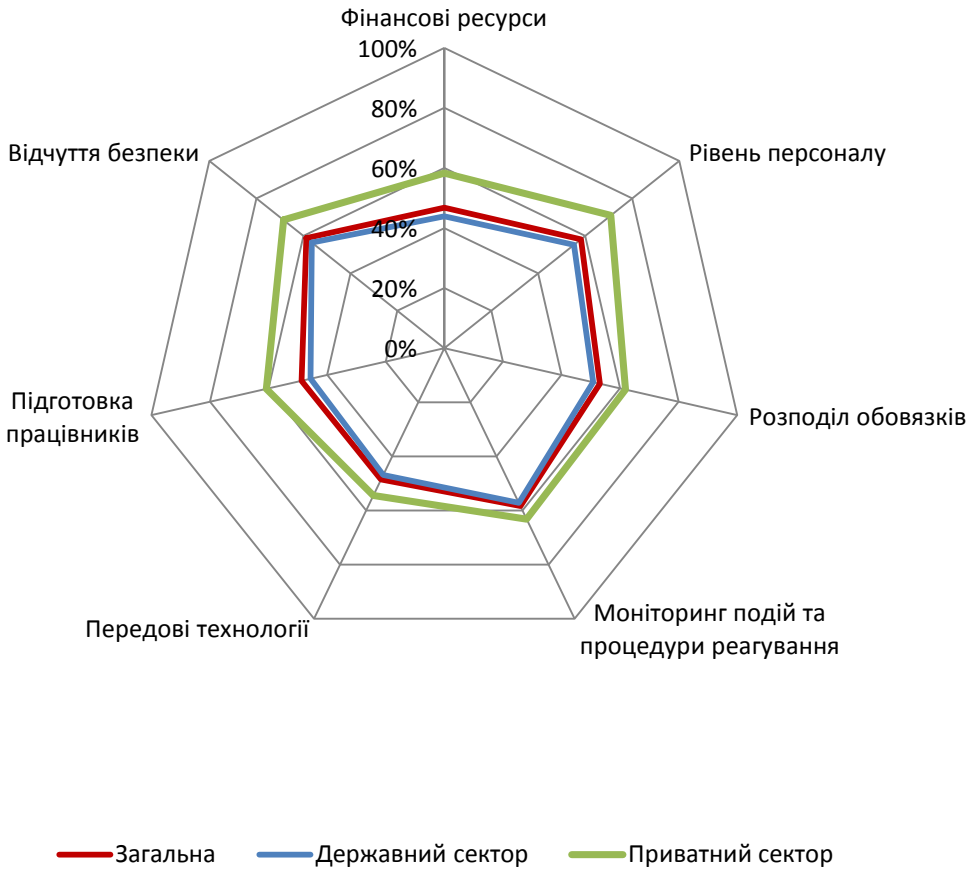


Рис.5

Для оцінки рівня спроможності організацій до протидії кібератакам респонденти за шкалою від 1 до 10 оцінювали рівень спроможності за різними напрямами. Оцінки від 1 до 4 були визначені як низький рівень, від 5 до 7 – як середній рівень, від 8 до 10 – як високий рівень. Узагальнені результати наведені на рис.6.

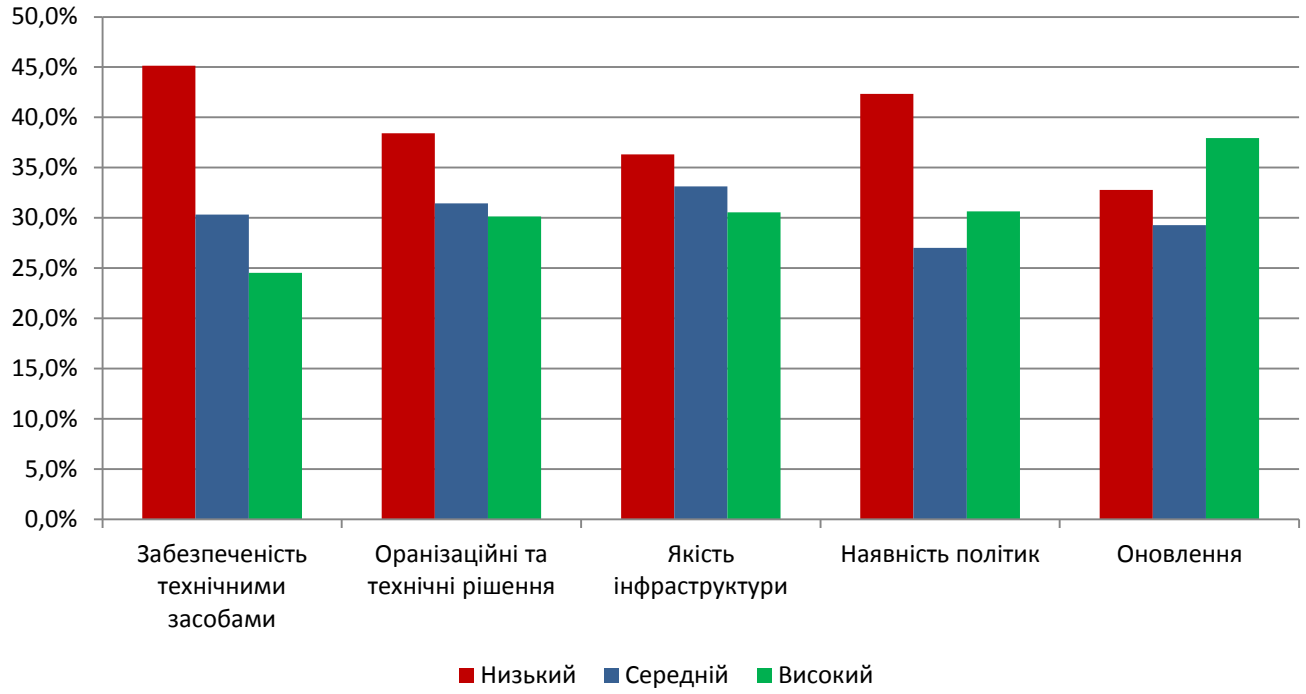


Рис.6

Майже за всіма напрямами респонденти низько оцінюють спроможність їх організацій протидіяти кіберзагрозам. Високо оцінюється тільки спроможність встановлювати оновлення та змінювати конфігурації технічних засобів для усунення виявлених вразливостей.

Приватні організації набагато вище (рівень 62 %) оцінюють свої спроможності протистояти кіберзагрозам, ніж організації державного сектору (рівень 45 %), при загальній оцінці усіх респондентів на рівні 55 %, що наведено в таблиці 3 та на рисунках 7 і 8.

Таблиця 3

	Забезпеченість технічними засобами	**Організаційні та технічні рішення**	**Якість інфраструктури**	**Наявність політик**	**Оновлення**
Загальна	50%	55%	56%	53%	59%
Державний сектор	40%	46%	45%	42%	50%
Приватний сектор	57%	65%	63%	61%	65%

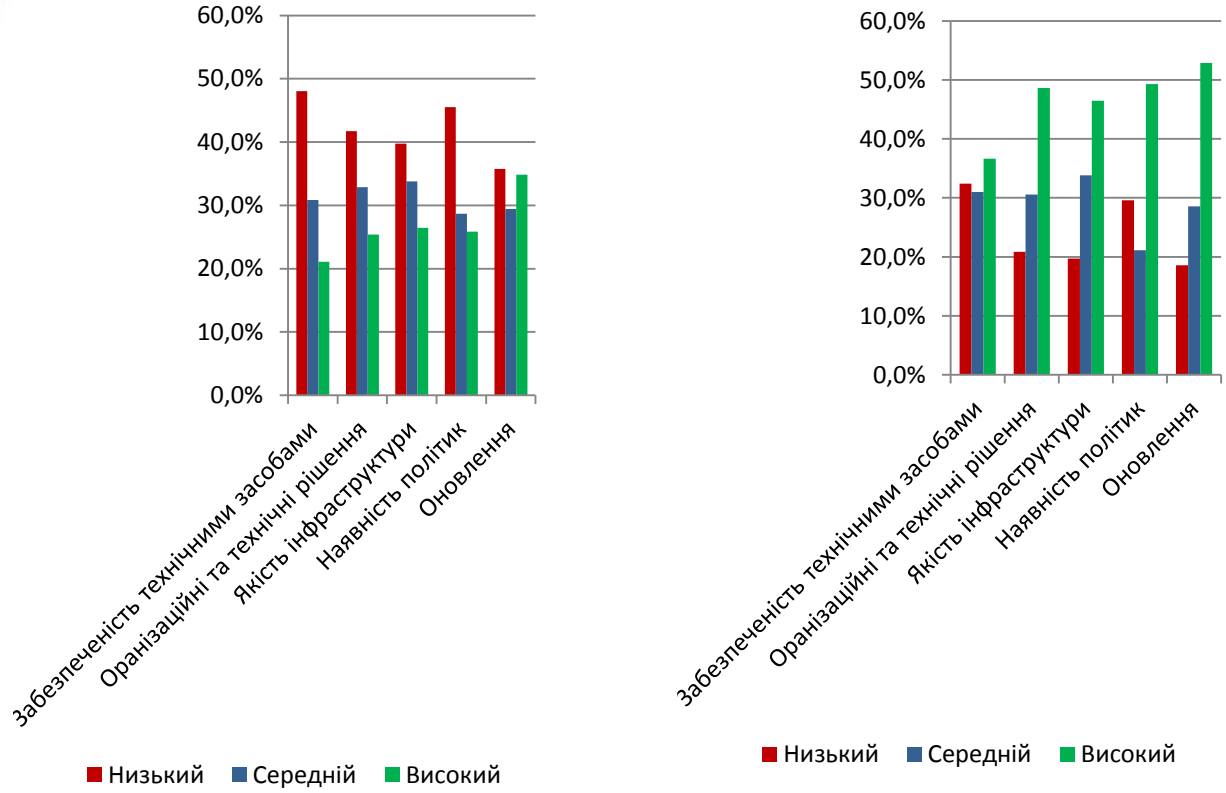

60,0%
50,0%
40,0%
30,0%
20,0%
10,0%
0,0%
Забезпеченість технічними засобами
Оранізаційні та технічні рішення
Якість інфраструктури
Наявність політик
Оновлення
Низький
Середній
Високий

Рис.7

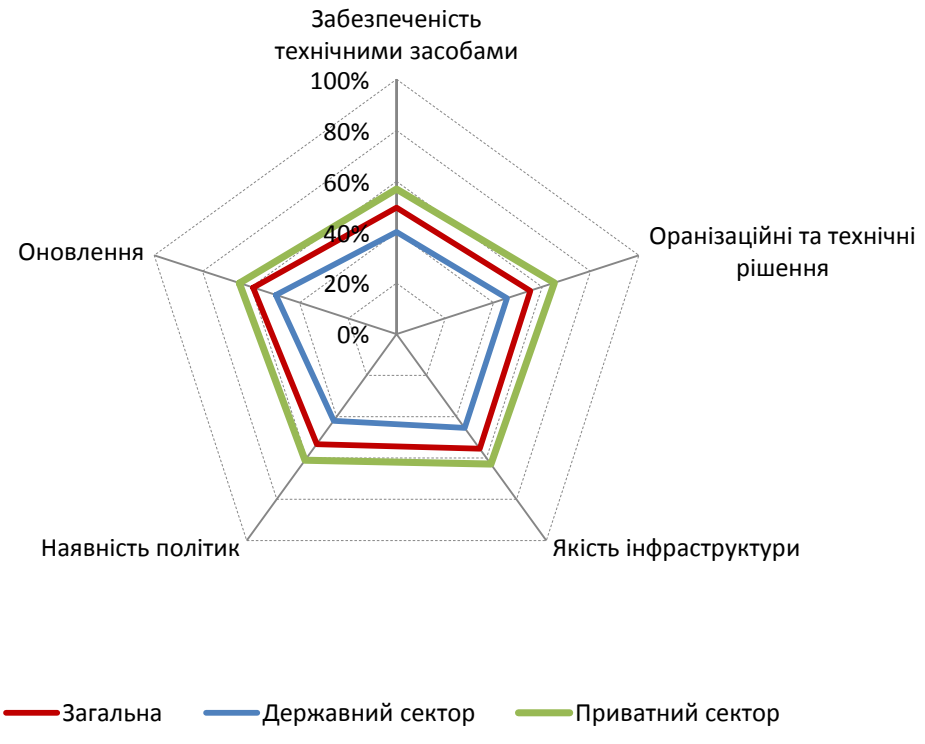

Забезпеченість технічними засобами
100%
80%
60%
40%
20%
0%
Оранізаційні та технічні рішення
Якість інфраструктури
Наявність політик
Оновлення
Загальна
Державний сектор
Приватний сектор

Рис.8

Для оцінки планування впродовж 2016-2020 р.р. діяльності організації з урахуванням необхідності реалізації пріоритетів, визначених Стратегією кібербезпеки України респонденти за шкалою від 1 до 10 оцінювали рівень планування за різними категоріями. Оцінки від 1 до 4 були визначені як низький рівень, від 5 до 7 – як середній рівень, від 8 до 10 – як високий рівень. Узагальнені результати наведені на рис.9

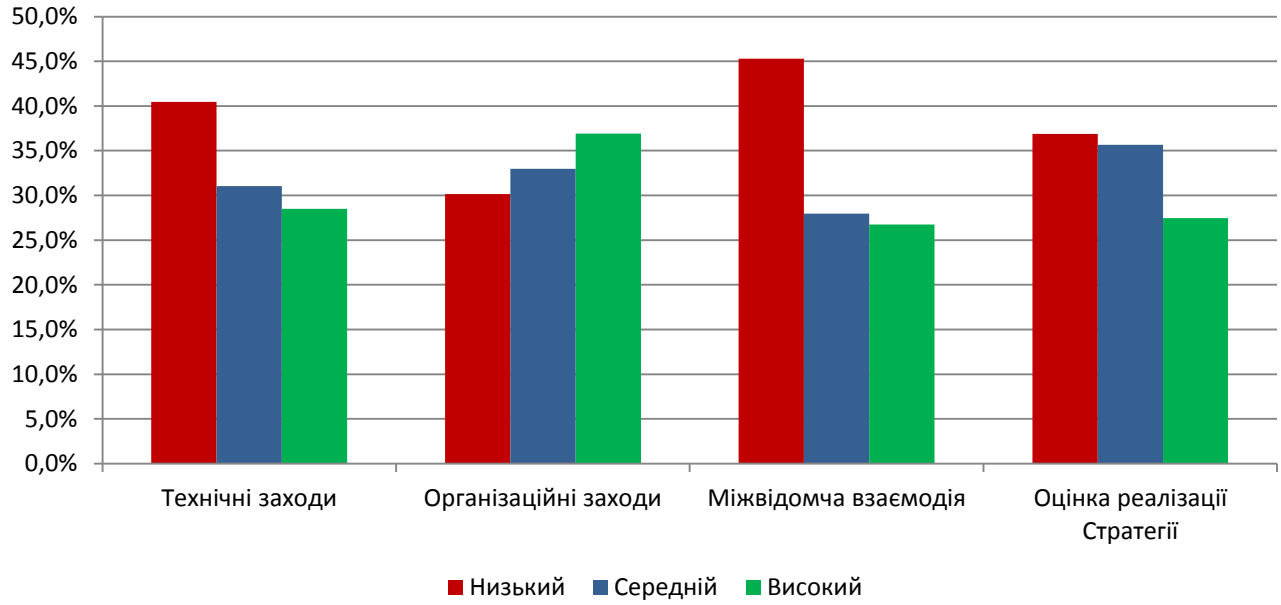


Рис.9

Узагальнена оцінка якості планування та реалізації заходів при виконанні попередньої Стратегії кібербезпеки складає 45 %, що в цілому збігається з даними іншого дослідження – 46 %. Найнижче оцінюється рівень міжвідомчої взаємодії – всього на рівні 41 %, найвище – здійснення організаційних заходів з дотримання вимог нормативних актів в сфері кібербезпеки (52 %).

На питання, чи стикалися ваша організація або ви особисто з негативними наслідками інцидентів в кіберпросторі впродовж минулого 2020 року, позитивно відповіли 22 % респондентів. При цьому в державному секторі цей показник склав 19 %, в приватному секторі – 35 %. *Низькі значення в державному секторі насамперед свідчать про низький рівень виявлення інцидентів.*

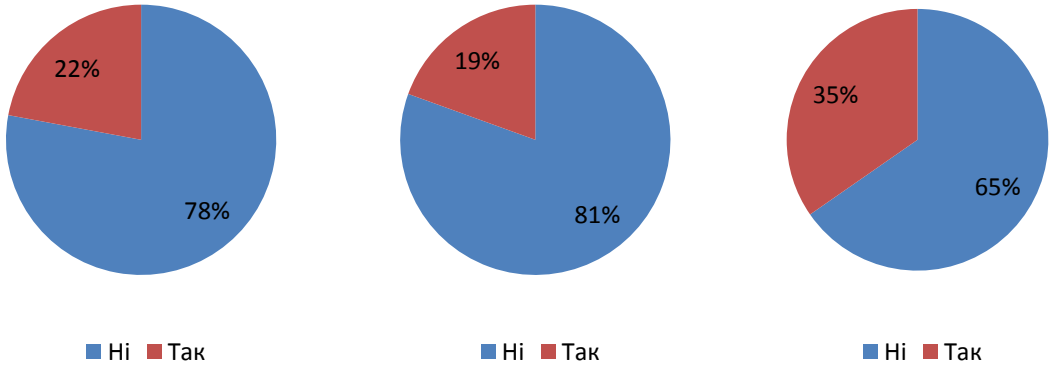


Рис.10

В середньому на вирішення одного інциденту організації витрачали 60,5 годин, найбільше – близько 3 місяців. Деякі з респондентів зазначили, що вирішити інцидент не вдалося. Загалом 128 організацій, що надали відповідь на питання про витрати часу на вирішення інциденту, витратили понад 7700 годин.

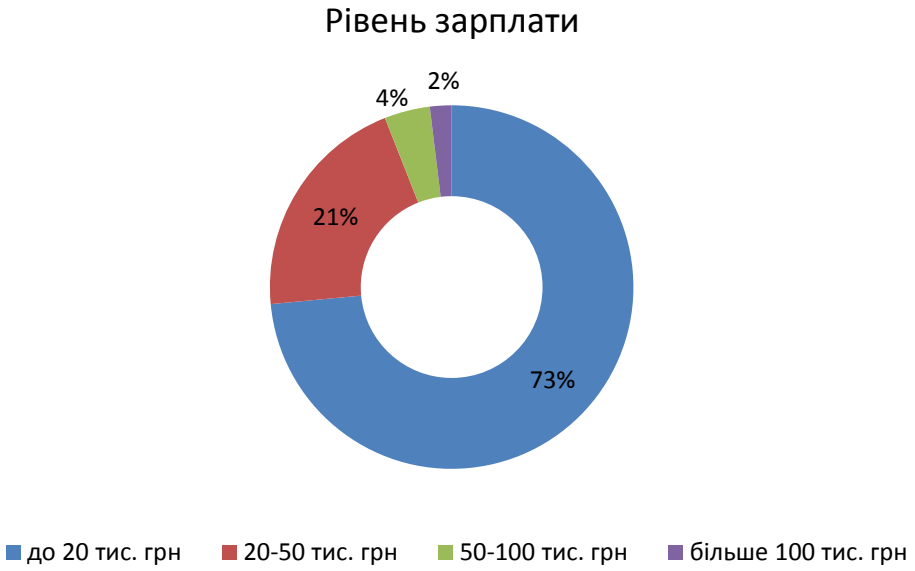


Рис.11

В цілому організації досить низько оцінюють ризики кіберзагроз за результатами 2020 року – середня оцінка 30%.

На рис. 12 наведено загрози високого рівня.

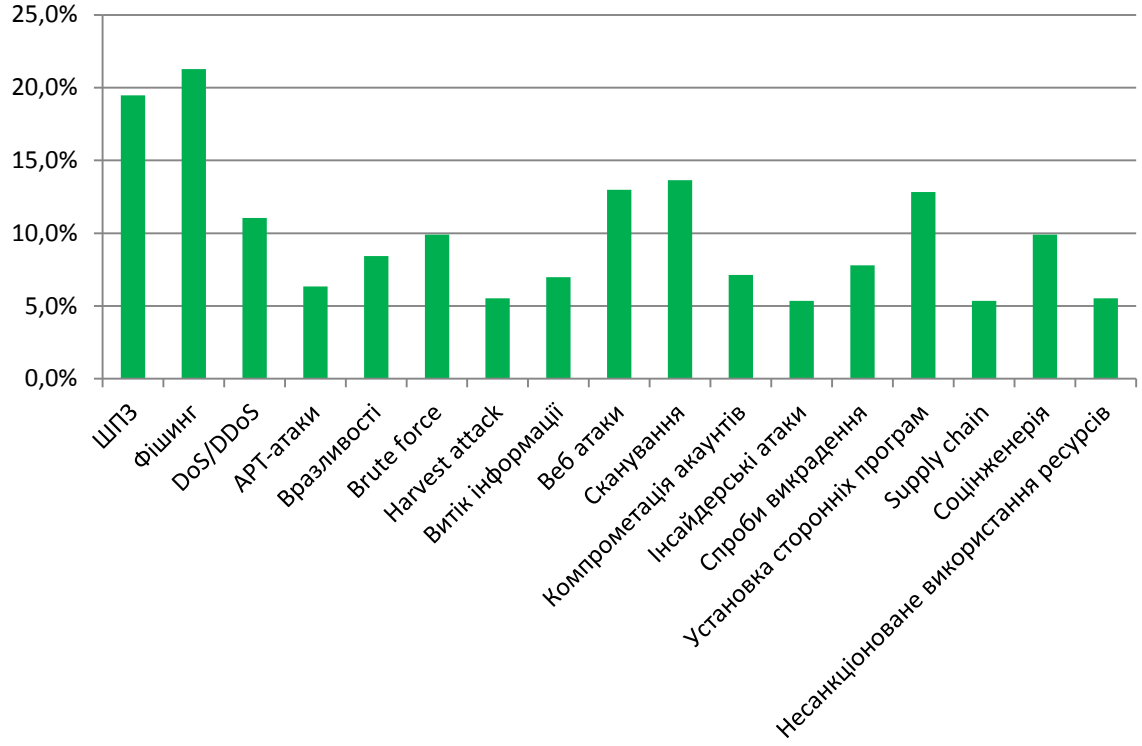


Рис.12

На найближчі 3 роки організації передбачають збільшення ризиків за всіма типами загроз, середня оцінка – 41%.

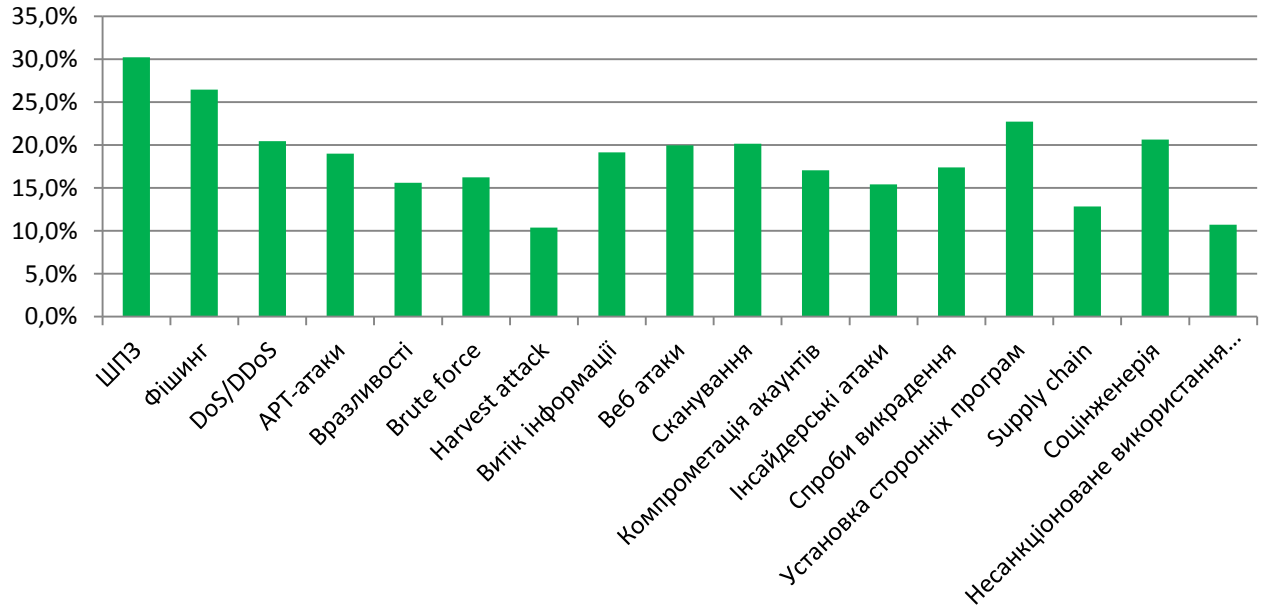


Рис.13

Порівняння оцінки ризиків за минулий 2020 рік та планованих на 2021-2023 р.р. представлено на рисунку 14.

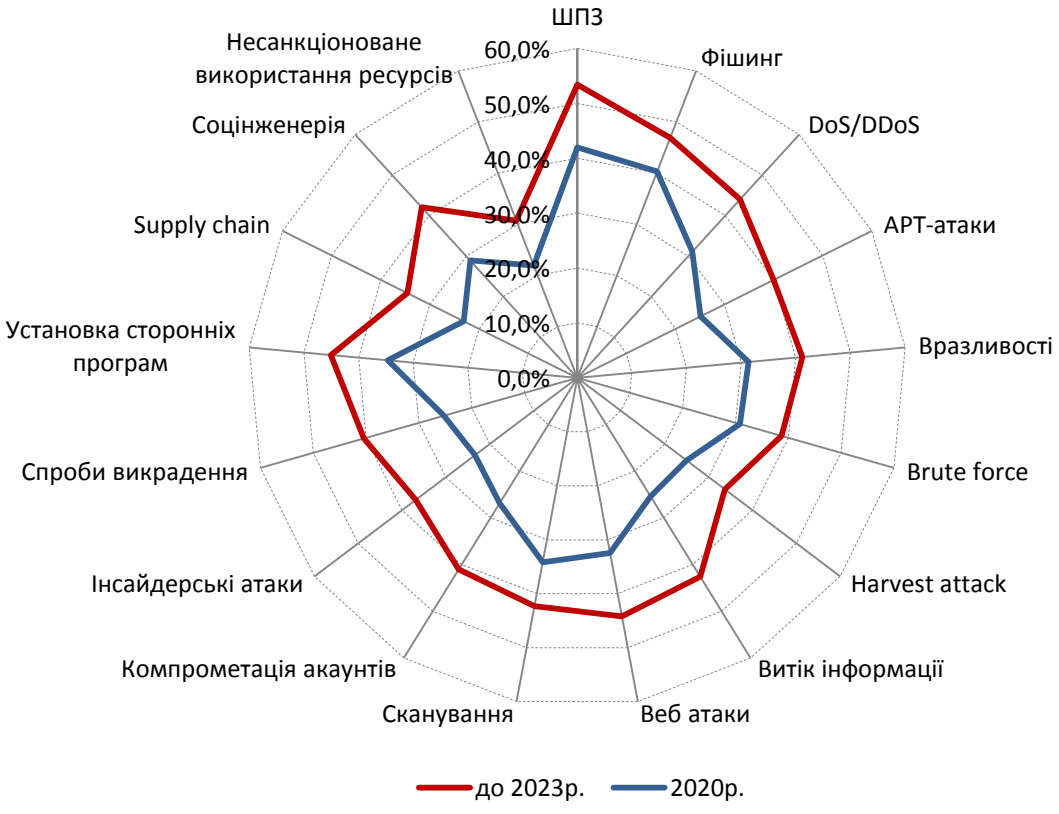


Рис.14

В середньому організації оцінюють діяльність ході забезпечення режиму віддаленої роботи співробітників під час впровадження обмежувальних заходів через COVID-19 на рівні 57%.

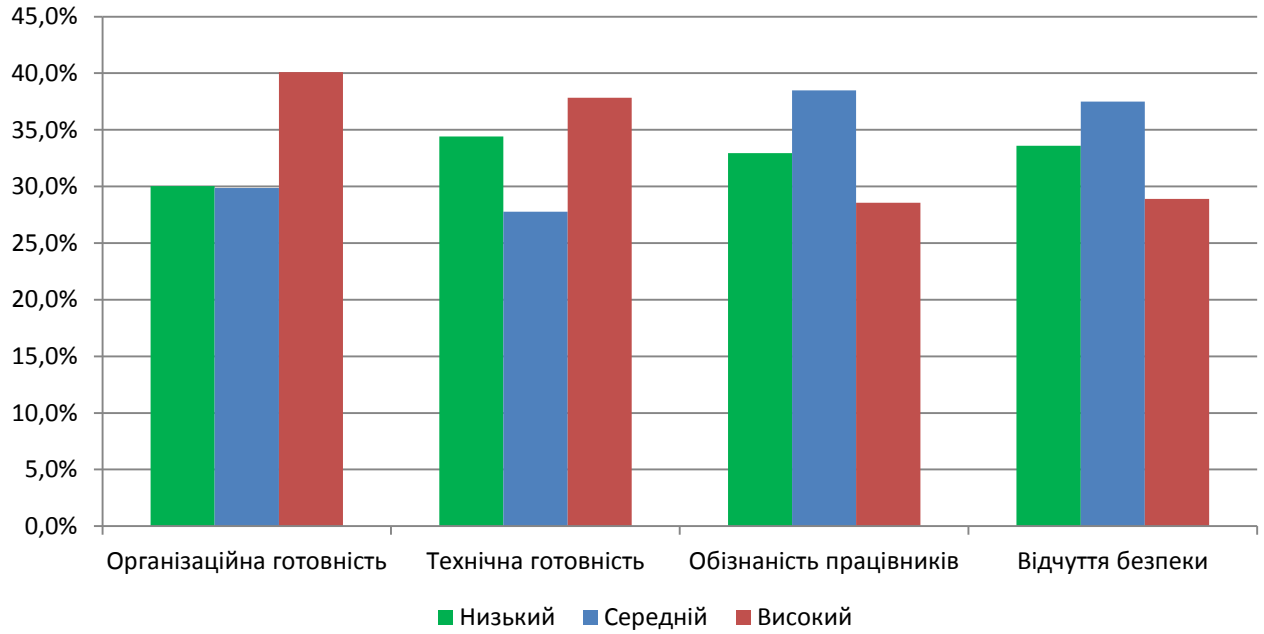


Рис.15

Респонденти досить низько оцінюють залученість міжнародних партнерів до реалізації проектів з кібербезпеки – на середньому рівні 30%, результативність взаємодії на рівні 27 % (рисунок 16).

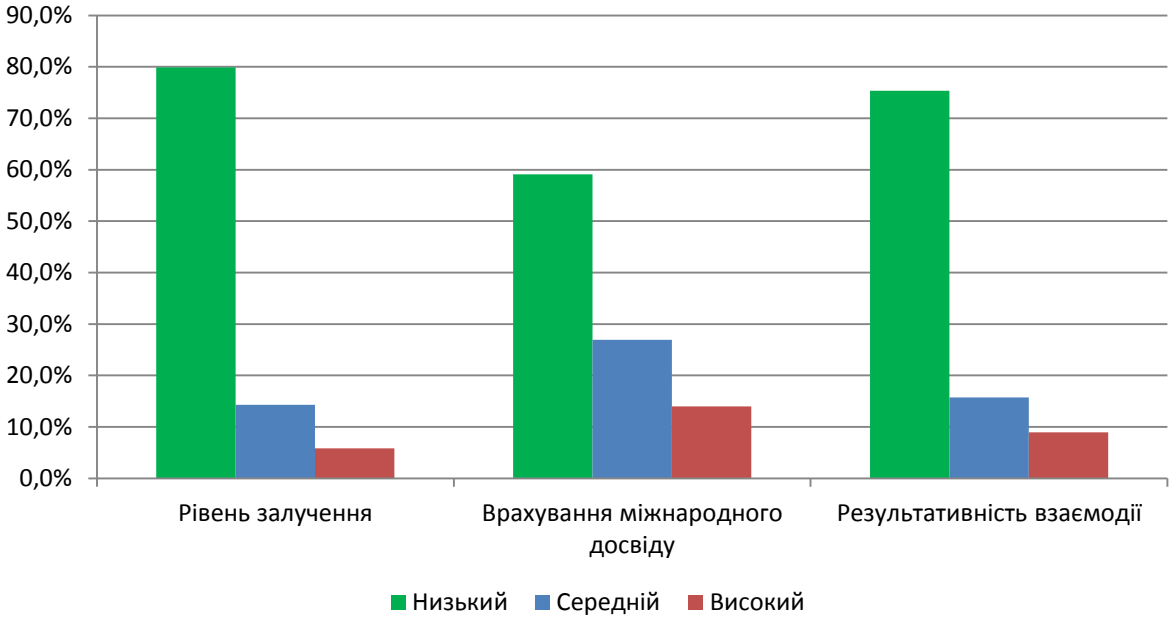


Рис.16

В найближчі 3 роки організації планують насамперед дотримуватися принципів реалізації державної політики в сфері кібербезпеки (63 %), практично не передбачається залучення експертів приватного сектору (40 %).

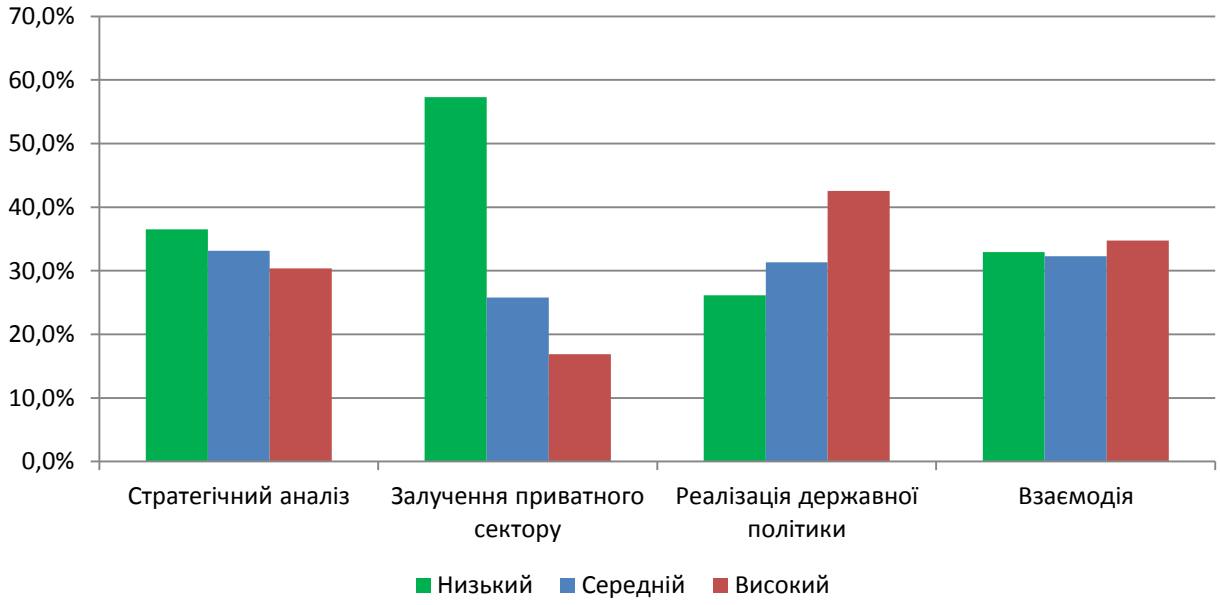


Рис.17

Респонденти в цілому негативно оцінюють рівень розвитку нормативно-правової бази в сфері кібербезпеки: лише 34 % вважають, що рівень достатній.

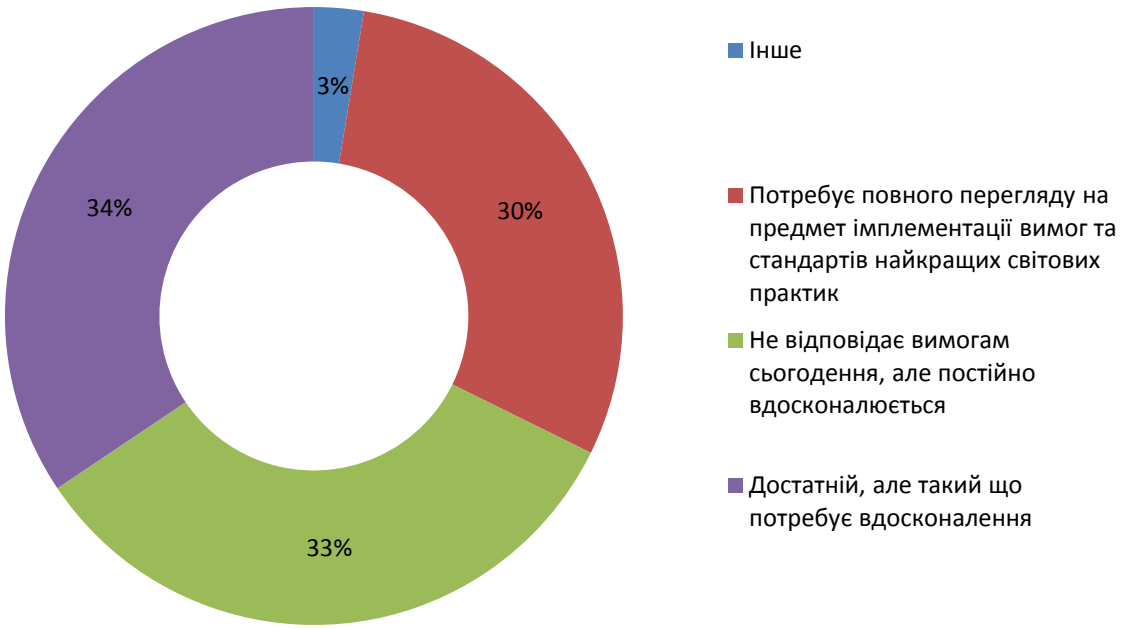


Рис.18

Поточний рівень, що було досягнуто за останні 5 років Україною, для реалізації безпечного функціонування національного кіберпростору, респонденти оцінюють на рівні 42 %.

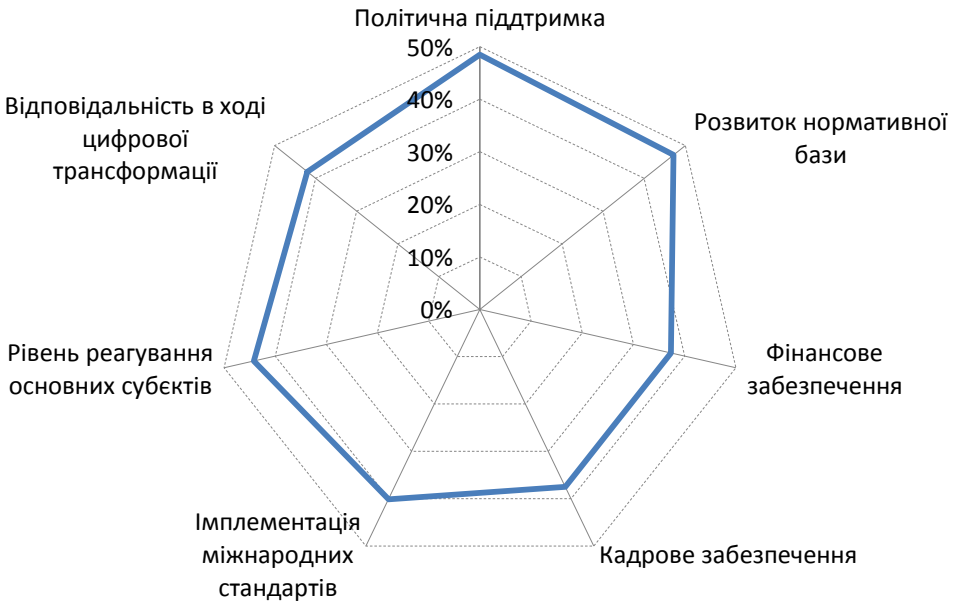


Рис.19

На графіку наведено оцінку основних напрямів діяльності державних органів на наступні 5 років.

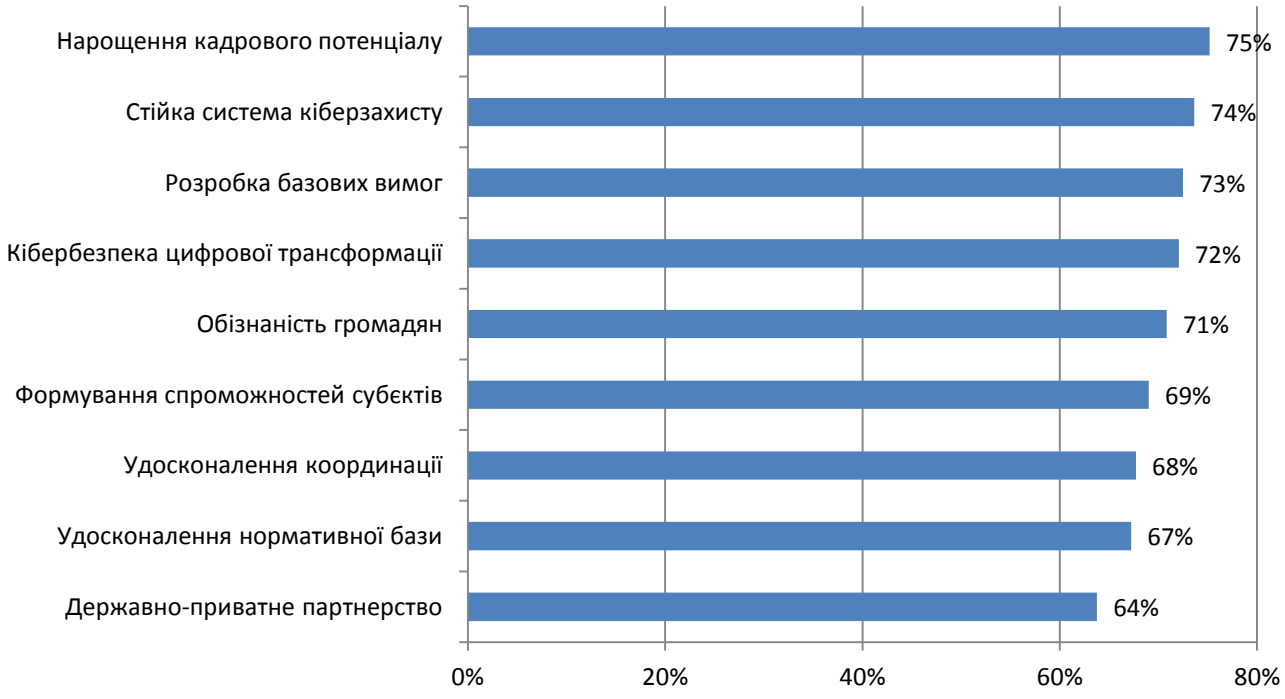


Рис.20

ВИСНОВКИ

Проведені опитування в межах отриманих результатів дозволяють зробити наступні висновки:

1. Загальний рівень безпечного функціонування національного кіберпростору респонденти оцінюють на рівні 42 %, що в цілому підтверджує висновки експертів основних суб'єктів кібербезпеки.

2. Стійкою тенденцію розвитку сфери кібербезпеки можна вважати високий рівень кореляції між державним та приватним секторами.

3. Опитувані організації державного сектору найбільш високими ризиками щодо функціонування національної системи кібербезпеки вважають:

- недостатній рівень фінансового забезпечення;
- відсутність систематичного планового підвищення кваліфікації працівників сфери кібербезпеки;
- відсутність розподілу функцій ІТ та ІБ підрозділів.

4. Опитувані організації приватного сектору найбільш високими ризиками щодо розвитку сфери кібербезпеки вважають:

- відсутність програм впровадження передових технологій в сфері кібербезпеки;
- недостатній рівень фінансового забезпечення.

5. Рівень спроможності суб'єктів кібербезпеки протидіяти кіберзагрозам в державному секторі оцінюється як низький (на рівні 36 %), а для приватного сектора ця оцінка становить близько 62 %. При цьому головним недоліком в державному і в приватному секторах вважається їх недостатня забезпеченість технічними засобами.

6. Проведений аналіз доводить, що ландшафт загроз за останні роки суттєво не змінився і загрозами високого рівня залишаються: шкідливе програмне забезпечення, фішинг та інші прояви соціальної інженерії, DoS/DDoS-атаки та APT-атаки. На найближчі 3 роки очікується збільшення ризиків за всіма типами загроз на рівні 41 %.

7. В умовах COVID-19 організації оцінюють результативність своєї діяльності щодо забезпечення режиму віддаленої роботи співробітників під час впровадження обмежувальних заходів в середньому на рівні 57 %.

8. Зафіксовано низький рівень (близько 30 %) залученості міжнародних партнерів до реалізації проєктів з кібербезпеки.

9. Визначені нагальні проблеми в сфері кібербезпеки і надані пропозиції щодо перспективних шляхів їх реалізації. Серед них основними є:

- вдосконалення нормативно-правової бази;
- нарощування кадрового потенціалу;
- створення стійкої системи кіберзахисту через побудову ефективної організаційно-технічної моделі національної системи кібербезпеки;
- підвищення ролі кібербезпеки в процесі цифрової трансформації держави.