

Функціональний орган у сфері захисту критичної інфраструктури з кіберзахисту у підсекторі електронних довірчих послуг та електронної ідентифікації

Роль, завдання, вимоги та взаємодія з ОКІ

Данило МЯЛКОВСЬКИЙ

Директор Департаменту кіберзахисту
Адміністрації Державної служби
спеціального зв'язку та захисту
інформації України

Кандидат наук з державного управління



Державна служба спеціального зв'язку
та захисту інформації України

Нормативно-правове забезпечення

Закони України

- 1) «Про основні засади забезпечення кібербезпеки України»;
- 2) «Про національну безпеку України»;
- 3) «Про Державну службу спеціального зв'язку та захисту інформації України»;
- 4) «Про критичну інфраструктуру»;
- 5) «Про правовий режим воєнного стану»
- 6) «Про електронні довірчі послуги»

Укази Президента України

- 1) від 15.03.2016 № 96 «Про рішення РНБО України від 27 січня 2016 року «Про Стратегію кібербезпеки України»;
- 2) від 13.02.2017 № 32 «Про рішення РНБО України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»;
- 3) від 30.08.2017 № 254 «Про рішення РНБО України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32»;
- 4) від 01.05.2014 № 449 «Про рішення РНБО України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»;
- 5) від 14.03.2016 № 92 «Про рішення РНБО України від 4 березня 2016 року «Про концепцію розвитку сектору безпеки і оборони України»;
- 6) від 26.08.2021 № 447 «Про рішення РНБО України від 14 травня 2021 року «Про Стратегію кібербезпеки України»;
- 7) від 1.02.2022 № 37 «Про рішення РНБО від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України».

Постанови та розпорядження Кабінету Міністрів України

- 1) від 03.09.2014 № 411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України»;
- 2) від 19.06.2019 № 518 «Про затвердження загальних вимог з кіберзахисту об'єктів критичної інфраструктури»;
- 3) від 09.10.2020 № 934 «Деякі питання об'єктів критичної інформаційної інфраструктури»;
- 4) від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури»;
- 5) від 11.11.2020 № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом»;
- 6) від 23.12.2020 № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»;
- 7) від 23.12.2020 № 1363 «Про реалізацію експериментального проекту щодо запровадження комплексу організаційно-технічних заходів з виявлення вразливостей і недоліків у налаштуванні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в яких обробляються державні інформаційні ресурси»;
- 8) від 08.02.2021 № 94 «Про реалізацію експериментального проекту щодо функціонування Національного центру резервування державних інформаційних ресурсів»;
- 9) від 29.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту».
- 10) від 24.06.2016 № 440-р «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України»;
- 11) від 10.03.2017 № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України»;
- 12) від 11.07.2018 № 481-р «Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України»;

Укази Президента України

- 1) від 15.03.2016 № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»;
- 2) від 13.02.2017 № 32 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»;
- 3) від 30.08.2017 № 254 «Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32»;
- 4) від 01.05.2014 № 449 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»;
- 5) від 14.03.2016 № 92 «Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про концепцію розвитку сектору безпеки і оборони України»;
- 6) від 26.08.2021 № 447 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»;
- 7) від 1.02.2022 № 37 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України».

Накази Адміністрації Держспецзв'язку

- 1) від 02.12.2014 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», зареєстрований в Міністерстві юстиції України 28 січня 2015 року за № 90/26535;
- 2) від 15.01.2016 № 20 «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті», зареєстрований в Міністерстві юстиції України 05 лютого 2016 року за № 196/28326;
- 3) від 15.01.2021 № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури»;
- 4) від 10.09.2021 № 550 «Про утворення Міжвідомчої робочої групи з питань проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом», зареєстрований в Міністерстві юстиції України 28 вересня 2021 за № 1264/36886;
- 5) від 06.10.2021 № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури»;
- 6) від 28.10.2021 № 640 «Про внесення змін до Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті», зареєстровано в Міністерстві юстиції України 07 грудня 2021 р. за № 1576/37198;
- 7) від 24.06.2022 № 284 «Про затвердження Порядку передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об'єктів кіберзахисту», зареєстровано в Міністерстві юстиції України 11 липня 2022 року за № 758/38094;
- 8) від 10.07.2022 № 343 «Про внесення змін до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури»



Завдання Адміністрації Держспецзв'язку як функціонального органу

формування та забезпечення реалізації державної політики

державний контроль за станом кіберзахисту ДІР та ОКІІ

забезпечення впровадження аудиту інформаційної безпеки на ОКІ

технічне регулювання у сферах кіберзахисту ОКІ





***Нововведення щодо
електронних довірчих
послуг відповідно до
NIS2***

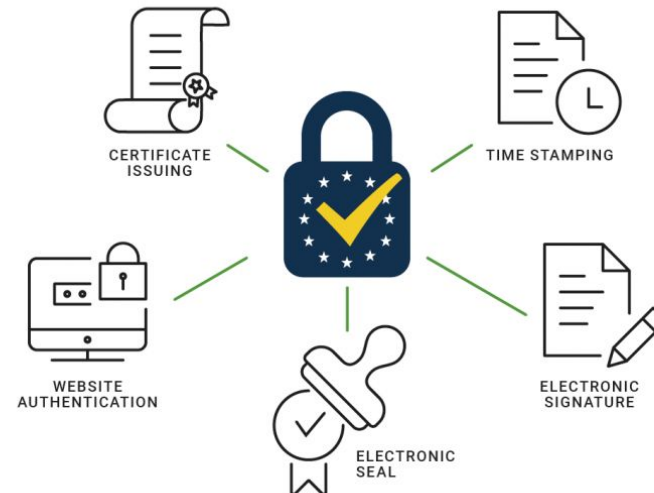


eiDAS та NIS2

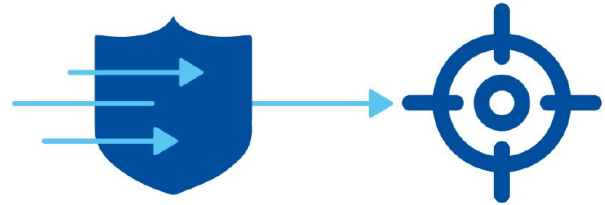
Вимоги NIS2:

- QTSP/none QTSP мають вживати заходів для управління ризиками;
- QTSP/none QTSP мають повідомляти **CSIRT**;
- використання європейських схем сертифікації кібербезпеки за European Cybersecurity Act .

Стаття ~~19~~ Регламенту (ЄС) № 910/2014.

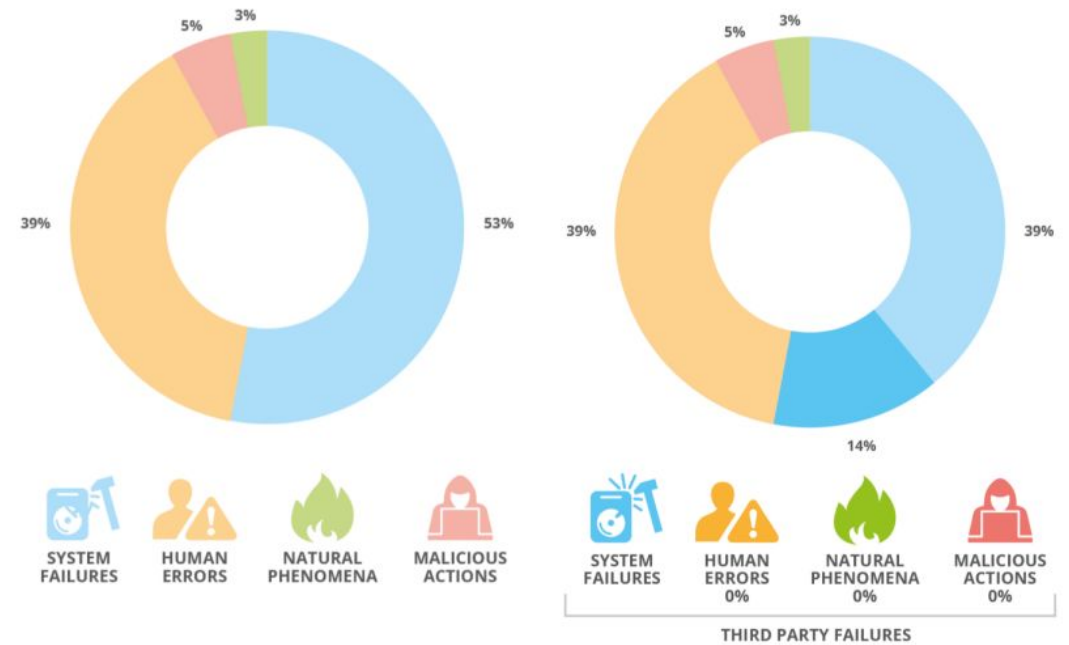
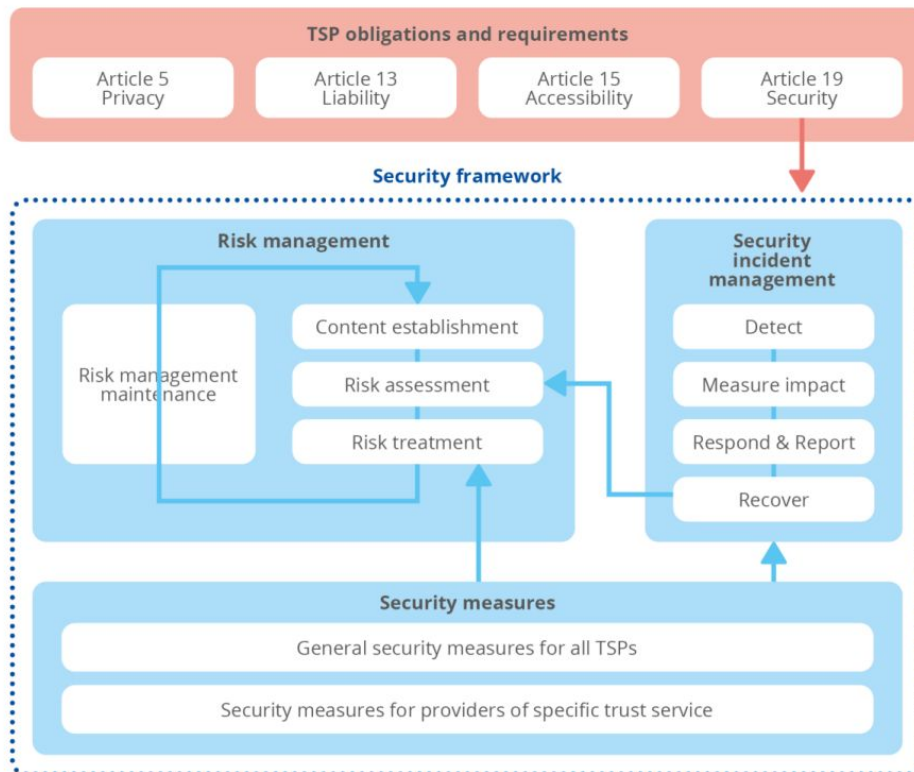


SECURITY MEASURES



RISK MANAGEMENT
Prevent security incidents

SECURITY INCIDENT MANAGEMENT
Minimise the impact of security incidents and inform stakeholders



Загальні організаційні вимоги до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації

1. У регламенті роботи надавача в положеннях політики сертифіката та/або в положеннях з опису процедур і процесів повинно бути визначено необхідність встановлення вимог до процедур з управління ризиками, персоналом, операційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними користувачів, процедур встановлення заявника, затвердженими наказом Державного агентства з питань електронного урядування від 27 листопада 2018 року № 86, зареєстрованими Міністерством юстиції України 26 грудня 2018 року за N 1462/32914.
2. Надавач повинен захищати свої активи відповідно до проведеної оцінки ризиків. Процедури з управління ризиками повинні передбачати виконання заходів з оцінки ризиків з урахуванням цих Вимог.
3. Процедури з управління персоналом повинні передбачати:
 - 1) наявність у надавача щонайменше двох посад адміністратора безпеки та аудиту;
 - 2) щорічне проходження адміністратором безпеки та аудиту практичних навчань з інформаційної безпеки;
 - 3) заборону суміщення посадових обов'язків адміністратора безпеки та аудиту з іншими посадовими обов'язками;
 - 4) встановлення відповідних вимог щодо кваліфікації персоналу.



ЕТАПИ РЕАГУВАННЯ

на різні види подій у кіберпросторі (кіберінциденти/кібератаки)

за етапами:

- підготовка;
- виявлення та аналіз;
- стримування;
- усунення;
- відновлення;
- аналіз ефективності заходів реагування на кіберінциденти/кібератаки).





***ПКМУ від 09.10.2020р. №1109 (в редакції постанови
Кабінету Міністрів України від 16 грудня 2022 р. №
1384)***



Перелік секторів основних послуг критичної інфраструктури держави, затверджений зазначеною постановою:

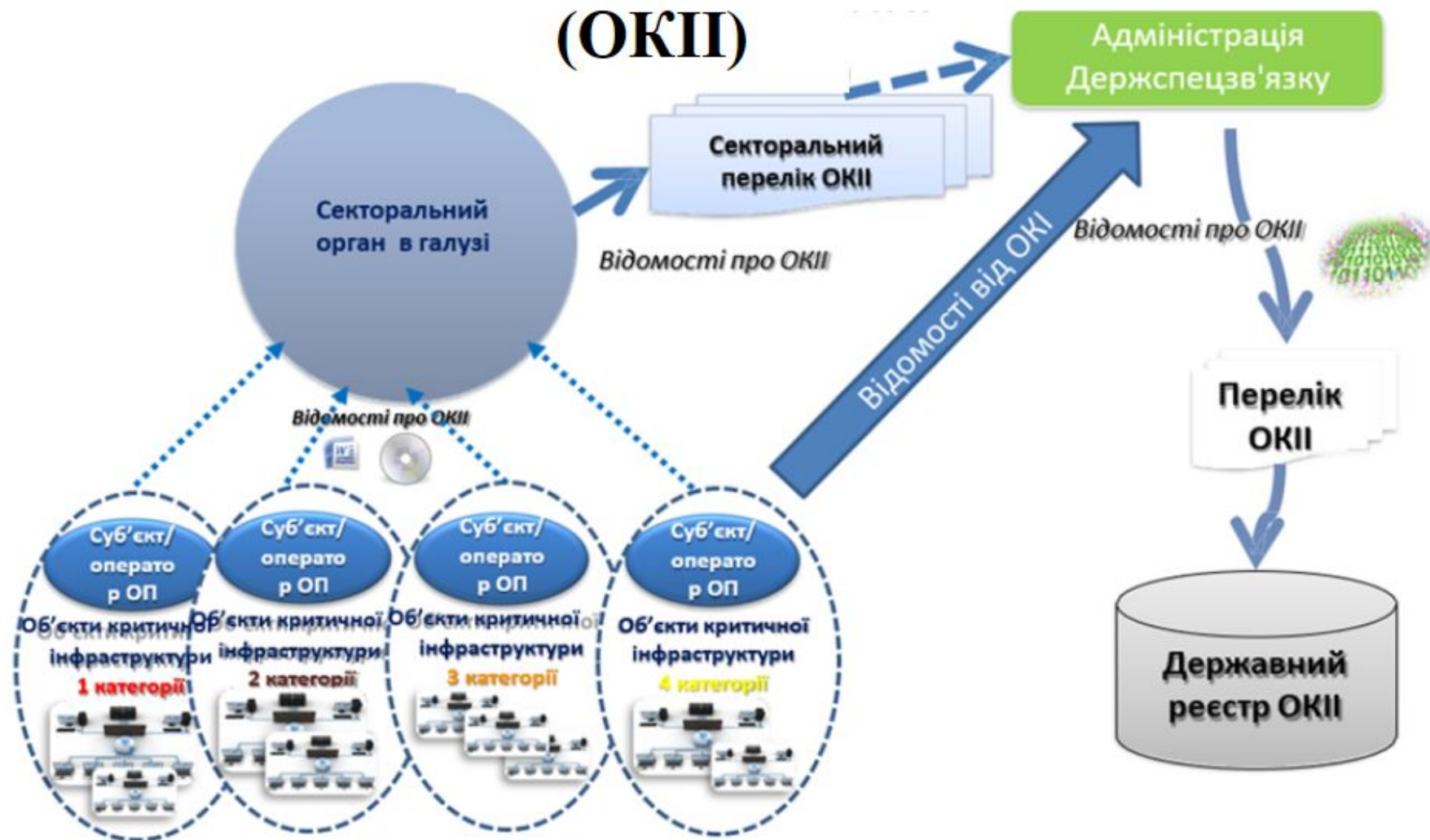
Було
11

Секторальний орган – Мінцифри.
Сектор – інформаційний сектор.
Підсектор - інформаційні технології.
Основна послуга - **надання електронних довірчих послуг.**

Стало
25

Секторальний орган – Мінцифри.
Сектор – цифрові технології.
Підсектор - електронні довірчі послуги та електронна ідентифікація.
Основна послуга - **надання електронних довірчих послуг**, електронної ідентифікації та автентифікації.

Порядок формування переліку об'єктів критичної інформаційної інфраструктури (ОКІІ)



Рівень кіберзахисту ОКІІ

Організаційно - технічна модель кіберзахисту є комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем.

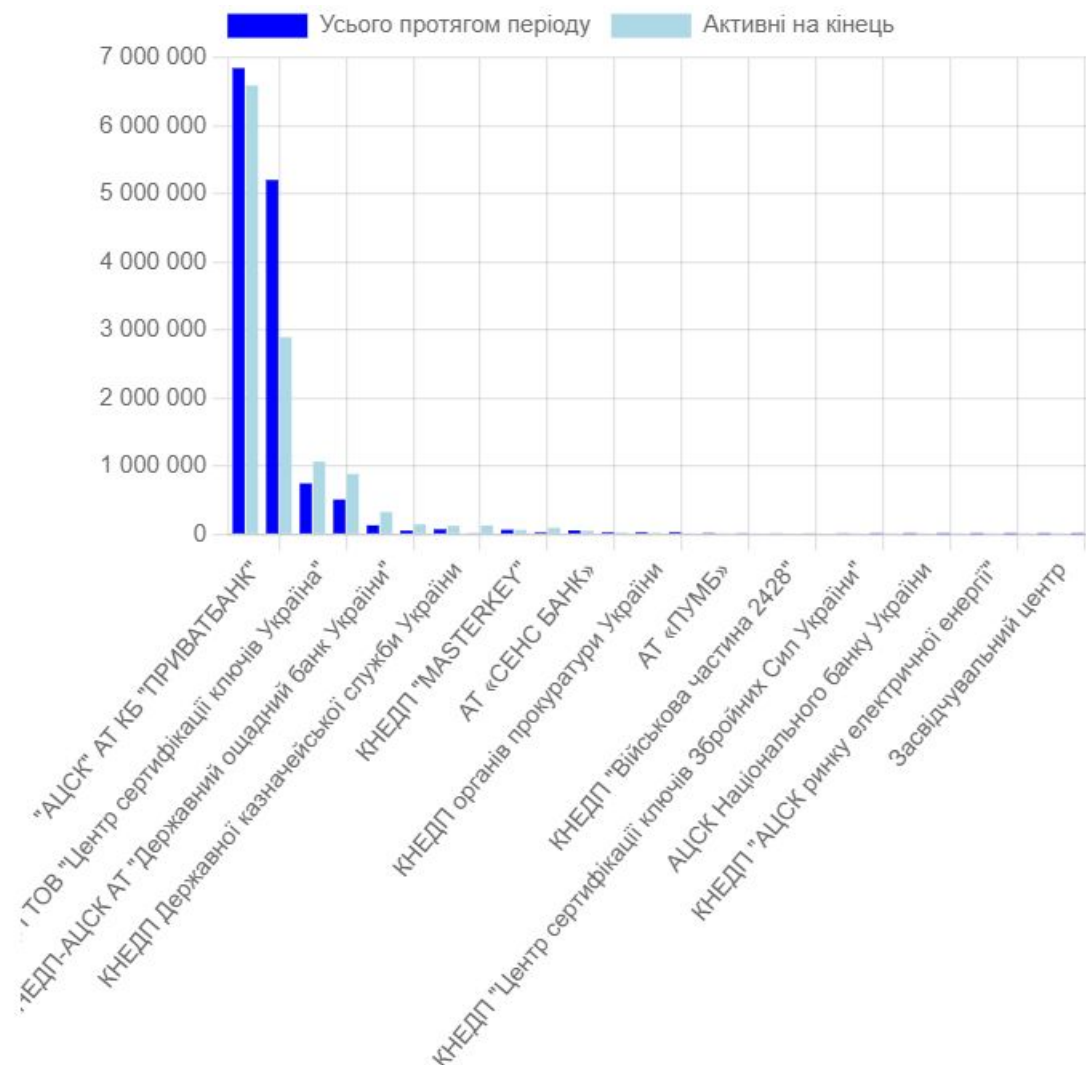
Методичні рекомендації щодо визначення профілю та підвищення рівня кіберзахисту критичної інформаційної інфраструктури розроблено відповідно до **Закону України** «Про основні засади забезпечення кібербезпеки України», Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою **Кабінету Міністрів України від 19 червня 2019 року № 518**, з метою підвищення рівня кіберзахисту критичної інформаційної інфраструктури.

Рекомендації розроблено з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity¹), виданої Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology).



Кваліфіковані надавачі електронних довірчих послуг з найбільшою кількістю сертифікатів

Назва	Усього	Активні
АЦСК АТ КБ «ПРИВАТБАНК»	6 849 563	6 592 641
КНЕДП «ДІЯ»	5 205 525	2 896 064
КНЕДП ТОВ «Центр сертифікації ключів Україна»	748 717	1 068 675
КНЕДП ДПС	511 364	887 668
КНЕДП-АЦСК АТ «Державний ощадний банк України»	132 506	327 257
КНЕДП АТ "УКРСИББАНК«	74 509	125 295
КНЕДП Державної казначейської служби України КНЕДП ДП «УСС»	67 540	64 479



Огляд стану кіберзахисту секторів критичної інфраструктури

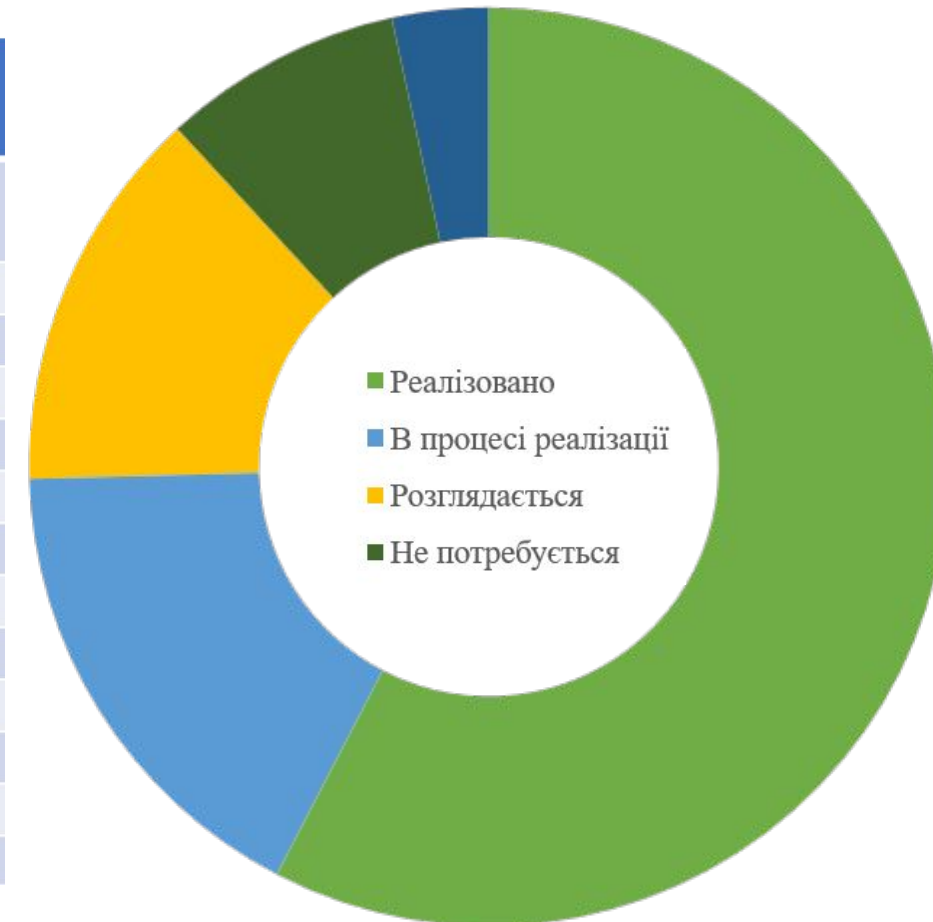
Завдання огляду:

- визначення поточного та цільового профілю кіберзахисту об'єктів критичної інформаційної інфраструктури;
- розробка конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки секторальних цільових профілів кіберзахисту функціонування критичної інфраструктури;
- формування пропозицій щодо вдосконалення законодавства у сфері захисту інформації та кібербезпеки та визначення напрямів розвитку системи в частині кіберзахисту;
- формування пропозицій щодо вдосконалення суб'єктами огляду заходів з кіберзахисту;
- планування заходів щодо забезпечення кіберстійкості операторів критичної інформаційної інфраструктури, об'єктів критичної інфраструктури.



Приклад подання звіту про виконання Загальних вимог до кіберзахисту об'єктів критичної інфраструктури

Клас заходів кіберзахисту	Всього підкатегорій заходів кіберзахисту	Статус (кількість та відсоток заходів за кожною категорією)			
		Реалізовано	В процесі реалізації	Розглядається	Не потребується
Ідентифікація ризиків кібербезпеки (ID)	29	10 34%	9 31%	5 17%	5 17%
Кіберзахист (PR)	39	10 26%	10 26%	10 26%	9 23%
Виявлення кіберінцидентів (DE)	18	8 44%	5 28%	5 28%	0 0%
Реагування на кіберінциденти (RS)	16	5 31%	5 31%	3 19%	3 19%
Відновлення стану кібербезпеки (RC)	6	2 33%	2 33%	1 17%	1 17%
Всього:	108	35 32%	31 29%	24 22%	18 17%



Дякую за увагу!



Державна служба спеціального зв'язку та захисту інформації України