ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
___ _____ 20___ року № ____

Форма

Відомості про об’єкт критичної інформаційної інфраструктури

№ з/п	Абзац пункту 6 Порядку	Призначення поля	Тип поля (т - текстовий; ч – числовий, д - дата)	Наявність словника	Примітка	Значення
1	2	3	4	5	6	7
		Загальні відомості про об’єкт критичної інформаційної інфраструктури (ОКІІ)				
1.	2	Код згідно з ЄДРПОУ юридичної особи, у власності (розпорядженні) якої перебуває ОКІІ	ч			
2.		Унікальний ідентифікатор	ч		Генерується Адміністратором Реєстру	
3.	3	Повна назва ОКІІ	т			
4.	3	Скорочена назва ОКІІ	т			

1	2	3	4	5	6	7
5.	3	Призначення ОКІІ	т			
6.	3	Категорія критичності ОКІІ	т	Словник (І категорія; ІІ категорія)		
7.	5	Секторальний орган у сфері захисту критичної інфраструктури, до сектору (підсектору) якого належить ОКІ	т	Перелік секторів критичної інфраструктури, затверджений постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109		
		Перелік основних послуг				
8.	4	Послуга, надання якої забезпечує об’єкт критичної інформаційної інфраструктури	т	Перелік секторів критичної інфраструктури, затверджений постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109		
		Вид інформації за порядком доступу, яка обробляється або планується для оброблення на об’єкті критичної інформаційної інфраструктури (ОКІІ)				

1	2	3	4	5	6	7
9.	6	Вид інформації	т	Словник (відкрита; службова; державна таємниця, що має ступінь секретності "таємно"; державна таємниця, що має ступінь секретності "цілком таємно"; державна таємниця, що має ступінь секретності "особливої важливості"; конфіденційна інформація про фізичну або юридичну особу (персональні дані); інша таємниця, яка не належить до державної таємниці (лікарська, банківська, тощо); технологічна інформація об’єкта критичної інформаційної інфраструктури; інша інформація, вимога щодо захисту якої визначена законом (необхідно вказати))		

1	2	3	4	5	6	7
10.	6	Інша інформація, вимога щодо захисту якої визначена законом	т		Вказується у випадку вибору значення «інша інформація, вимога щодо захисту якої визначена законом» в пункті 9	
		Адреса фізичного місця розташування об'єкта критичної інформаційної інфраструктури (ОКІІ)				
11.	7	Поштовий індекс	ч			
12.	7	Назва області	т			
13.	7	Назва району	т			
14.	7	Назва населеного пункту	т			
15.	7	Тип вулиці	т			
16.	7	Назва вулиці	т			
17.	7	Номер будинку	т			
18.	7	Корпус будинку	т			
19.	7	Офіс будинку	т			
		Наявність підключення об'єкта критичної інформаційної інфраструктури (ОКІІ) до Інтернету, інших інформаційно-комунікаційних систем, які не входять до його складу				

1	2	3	4	5	6	7
20.	8	Мережа до якої ОКІІ має підключення	т	Словник (Глобальна мережа, Міська мережа, локальна мережа, VPN)		
21.	8	Фізичний тип підключення	т	Словник (телефонна мережа загального користування, вита пара, волоконно-оптична мережа, радіоканал, інший)		
22.	8	Інший фізичний тип підключення	т		Вказується у випадку вибору значення «інший» в пункті 21	
		Діапазон IP-адрес, що використовуються об'єктом критичної інформаційної інфраструктури (ОКІІ)				
23.	8	Версія протоколу IP-адрес	т	Словник (IPv4-Internet Protocol Version 4, IPv6-Internet Protocol Version 6)		

1	2	3	4	5	6	7
24.	8	IP-адреса або діапазон	т			
		Постачальники електронних комунікаційних мереж та/або послуг				
25.	9	Повне найменування юридичної особи постачальника (постачальників) електронних комунікаційних мереж та/або послуг, що надає (надають) послуги з доступу до Інтернету для об'єкта критичної інформаційної інфраструктури	т			
		Місцезнаходження юридичної особи (юридичних осіб), що надає (надають) послуги з доступу до Інтернету для об'єкта критичної інформаційної інфраструктури (ОКІІ)				
26.	9	Поштовий індекс	ч			
27.	9	Назва області	т			
28.	9	Назва району	т			
29.	9	Назва населеного	т			
30.	9	Тип вулиці	т			
31.	9	Назва вулиці	т			
32.	9	Номер будинку	т			
33.	9	Корпус будинку	т			
34.	9	Офіс будинку	т			
		Взаємодія об'єкта критичної інформаційної інфраструктури (ОКІІ) з іншими ОКІІ та/або залежність функціонування ОКІІ від інших таких об'єктів				
35.	10	Наявність взаємодії ОКІІ з іншими ОКІІ та/або щодо залежності функціонування ОКІІ від інших таких об'єктів	т	Словник (так, ні)		

1	2	3	4	5	6	7
36.	10	Повна назва ОКІІ, з яким існує взаємодія	т			
37.	10	Повна назва ОКІ, до складу якого входить ОКІІ, який взаємодіє з ОКІІ	т			
		Атестат відповідності комплексної системи захисту інформації об'єкта критичної інформаційної інфраструктури (ОКІІ) або результатів незалежного аудиту інформаційної безпеки об'єкта критичної інфраструктури (ОКІ)				
38.	11	Наявність атестата відповідності комплексної системи захисту інформації ОКІІ або результатів незалежного аудиту інформаційної безпеки ОКІ	т	Словник (так, ні)		
39.	11	Тип документа	т	Словник (атестат відповідності комплексної системи захисту інформації ОКІІ, результати незалежного аудиту інформаційної безпеки ОКІІ)		
40.	11	Номер документа	т			
41.	11	Дата документа	д			
42.	11	Термін дії документа	д			

1	2	3	4	5	6	7
		Відомості про осіб та/або підрозділ, що відповідають за стан захисту інформації (забезпечення інформаційної безпеки) та кіберзахисту об'єкта критичної інформаційної інфраструктури (ОКІІ), у тому числі тих, на яких покладено функції служби захисту інформації				
43.	12	Наявність осіб та/або підрозділу, що відповідають за стан захисту інформації (забезпечення інформаційної безпеки) та кіберзахисту ОКІІ, у тому числі тих, на яких покладено функції служби захисту інформації	т	Словник (так, ні)		
44.	12	Тип документа	т			
45.	12	Номер документа	т			
46.	12	Дата документа	д			
		Особи та/або підрозділ, що відповідають за стан захисту інформації				
47.	12	Прізвище	т			
48.	12	Власне ім'я	т			
49.	12	По батькові (за наявності)	т			
50.	12	Посада	т			
51.	12	Підрозділ, відповідальний за стан захисту інформації	т			
52.	12	Телефон підрозділу/особи, відповідальної за стан захисту інформації	т			
53.	12	Адреса електронної пошти підрозділу/особи, відповідальної за стан захисту інформації	т			

1	2	3	4	5	6	7
		Відомості про виконання Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 р. № 518, на об'єкті критичної інформаційної інфраструктури (ОКІІ)				
54.	13	Під час визначення відповідальних за інформаційну безпеку перевага надається особам, які мають фахову освіту та досвід роботи у сфері технічного захисту інформації або інформаційної безпеки	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
55.	13	Підрозділ або посадова особа з інформаційної безпеки, підпорядкована безпосередньо керівнику ОКІ	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
56.	13	Функції підрозділу або посадової особи з інформаційної безпеки покладено на службу захисту інформації підприємства, установи, організації	т	Словник (так, ні)		
57.	13	Права та обов'язки всіх категорій користувачів та адміністраторів ОКІІ визначені та задокументовані	т	Словник (так, ні)		
58.	13	Права та обов'язки всіх категорій користувачів та адміністраторів ОКІІ оформлено рішенням з підписом власника та/або керівника ОКІ	т	Словник (так, ні, інше)		

1	2	3	4	5	6	7
		Інше	т		Вказується у випадку вибору значення «інше»	
59.	13	Призначені відповідальні за функціонування та інформаційну безпеку критичних бізнес/операційних процесів із числа керівників ОКІ, працівники яких забезпечують функціонування цих критичних процесів	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
60.	13	На ОКІ визначено перелік інформаційних, програмних та апаратних ресурсів ОКІІ	т	Словник (так, ні)		
61.	13	На ОКІ визначено рівень критичності інформаційних, програмних та апаратних ресурсів ОКІІ для об’єкта критичної інфраструктури та/або функціонування ОКІІ	т	Словник (так, ні)		
62.	13	На ОКІ визначено можливий рівень наслідків у випадку порушення конфіденційності, цілісності та доступності інформації, недоступності служб (функцій) ОКІІ, порушення функціонування компонентів ОКІІ	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
63.	13	На ОКІ затверджено політику управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення	т	Словник (так, ні)		

1	2	3	4	5	6	7
64.	13	На ОКІ не рідше одного разу на рік проводиться обстеження ОКІІ з метою оновлення даних щодо програмно-апаратного складу ОКІІ, технології обробки інформації на ОКІІ, переліку критичних інформаційних ресурсів та компонентів ОКІІ, які підлягають захисту, тощо	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
65.	13	Проводиться перегляд переліку загроз ОКІІ, ризиків інформаційної безпеки та рівня прийнятного ризику, якщо за результатами обстеження ОКІІ виявлено, що на ОКІІ ОКІ змінено технологію обробки інформації, впроваджено нові програмні або апаратні компоненти, змінено перелік критичних інформаційних ресурсів та компонентів об’єкта, які підлягають захисту, тощо	т	Словник (так, ні)		
66.	13	У випадку виявлення нових загроз та/або ризиків здійснюється оновлення технічного завдання на створення комплексної системи захисту інформації ОКІІ (в захищеній від модифікації формі, зокрема електронній) з обов’язковим описом реалізованих в ІКС організаційних та технічних заходів безпеки інформації	т	Словник (так, ні)		
67.	13	Мінімальний перелік документації ОКІІ визначено в технічному завданні на створення комплексної системи захисту інформації ОКІІ	т	Словник (так, ні, інше)		

1	2	3	4	5	6	7
		Інше	т		Вказується у випадку вибору значення «інше»	
68.	13	Програмні та апаратні компоненти ОКІІ налаштовані відповідно до затвердженої політики інформаційної безпеки та технічної, проектної та іншої документації на комплексну систему захисту інформації ОКІІ	т	Словник (так, ні)		
		Політика інформаційної безпеки				
69.	13	На об’єкті критичної інфраструктури розроблена та затверджена окремим рішенням за підписом власника та/або керівника ОКІ політика інформаційної безпеки	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
70.	13	Затверджена політика інформаційної безпеки доведена під підпис або в інший спосіб до відома всіх працівників ОКІ	т	Словник (так, ні)		
71.	13	На ОКІ визначена відповідальність його співробітників за порушення встановленої політики інформаційної безпеки	т	Словник (так, ні)		
72.	13	Встановлено порядок внесення змін до Політики інформаційної безпеки	т	Словник (так, ні)		
73.	13	Затверджена політика інформаційної безпеки визначає мету та основні принципи забезпечення захисту інформаційних ресурсів, критичних бізнес/ операційних процесів тощо на ОКІ	т	Словник (так, ні)		

1	2	3	4	5	6	7
74.	13	Затверджена політика інформаційної безпеки визначає опис критичних бізнес/операційних процесів, який містить схему кожного критичного бізнес-процесу з описом компонентів та користувачів ОКІІ ОКІ, які задіяні в цьому процесі	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
75.	13	Затверджена політика інформаційної безпеки визначає вимоги до порядку визначення, надання, зміни та скасування прав доступу користувачів та адміністраторів до служб (функцій), інформації та компонентів об’єкта та порядок контролю (аудиту) використання прав доступу користувачами та адміністраторами	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
76.	13	Затверджена політика інформаційної безпеки визначає політику фізичної безпеки та захисту ОКІІ ОКІ від навколишнього природного середовища	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
77.	13	Затверджена політика інформаційної безпеки визначає вимоги до забезпечення інформаційної безпеки під час взаємодії з постачальниками	т	Словник (так, ні, інше)		

1	2	3	4	5	6	7
		Інше	т		Вказується у випадку вибору значення «інше»	
78.	13	Затверджена політика інформаційної безпеки визначає політику управління обліковими записами в програмному та апаратному забезпеченні ОКІІ, що визначає в свою чергу порядок створення, блокування та зупинення облікових записів користувачів та адміністраторів в компонентах об’єкта	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
79.	13	Затверджена політика інформаційної безпеки визначає вимоги до порядку формування, надання, скасування та контролю (аудиту) за використанням автентифікаційних атрибутів користувачів та адміністраторів, у тому числі зовнішніх носіїв автентифікаційних даних, для доступу до служб (функцій), інформації та компонентів ОКІІ	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
80.	13	Визначені вимоги до складності паролів, періодичності їх зміни, блокування роботи користувача за певної кількості спроб підбору пароля, порядок поводження із зовнішніми носіями автентифікаційних даних тощо	т	Словник (так, ні, інше)		

1	2	3	4	5	6	7
		Інше	т		Вказується у випадку вибору значення «інше»	
81.	13	Затверджена політика інформаційної безпеки визначає політику забезпечення безперебійної роботи ОКІІ, зокрема порядок резервування даних та компонентів об’єкта, зберігання резервних копій даних, відновлення даних з резервних копій та заміни компонентів об’єкта у випадку виходу їх з ладу тощо	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
82.	13	Затверджена політика інформаційної безпеки визначає порядок дій персоналу ОКІІ у випадках відмов або збоїв ОКІІ ОКІ в цілому або окремих його компонентів	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
83.	13	Затверджена політика інформаційної безпеки визначає порядок використання змінних (зовнішніх) пристроїв та носіїв інформації на ОКІІ	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	

1	2	3	4	5	6	7
84.	13	Затверджена політика інформаційної безпеки визначає політику мережевого захисту, зокрема щодо сегментації мережі ОКІІ, захисту від вірусів, зловмисного коду, шкідливого програмного забезпечення, встановлення та налаштування засобів мережевого захисту тощо	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
85.	13	Затверджена політика інформаційної безпеки визначає політику проведення модернізації (оновлення) компонентів об’єкта, внесення змін до складу та в налаштування компонентів об’єкта	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
86.	13	На ОКІ визначені відповідальні особи, які мають право проводити роботи з модернізації (оновлення) компонентів об’єкта, внесення змін до складу та в налаштування компонентів об’єкта	т	Словник (так, ні)		
87.	13	На ОКІ визначено порядок дотримання політики безпеки, яка прийнята на ОКІ, під час проведення робіт з модернізації (оновлення) компонентів об’єкта, внесення змін до складу та в налаштування компонентів об’єкта	т	Словник (так, ні)		

1	2	3	4	5	6	7
88.	13	Затверджена політика інформаційної безпеки визначає опис критичних бізнес/операційних процесів, який повинен містити схему кожного критичного бізнес-процесу з описом компонентів та користувачів ОКІІ, які задіяні в цьому процесі	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
89.	13	Затверджена політика інформаційної безпеки визначає політику управління оновленнями (порядок отримання, перевірки, розповсюдження та застосування оновлень програмного забезпечення компонентів об’єкта)	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
90.	13	Затверджена політика інформаційної безпеки визначає політику реєстрації та аудиту подій, що реєструються компонентами об’єкта, яка містить перелік подій, що реєструються кожним компонентом об’єкта, параметри ведення журналів (логів) реєстрації подій та їх архівування, порядок та періодичність аудиту журналів (логів) реєстрації подій адміністраторами ОКІІ ОКІ на предмет виявлення ознак кібератак або кіберінцидентів	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	

1	2	3	4	5	6	7
91.	13	Затверджена політика інформаційної безпеки визначає політику управління інцидентами кібербезпеки, яка повинна містити перелік подій, що кваліфікуються як кіберінциденти, описи дій користувачів та адміністраторів у разі їх виникнення, порядок інформування посадових осіб ОКІ, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності галузевої команди реагування на комп'ютерні надзвичайні події)	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
92.	13	Затверджена політика інформаційної безпеки визначає політику використання електронної пошти користувачами ОКІІ	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
93.	13	Затверджена політика інформаційної безпеки визначає політику проведення внутрішнього аудиту інформаційної безпеки ОКІ	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	

1	2	3	4	5	6	7
94.	13	На ОКІ впроваджено програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечено щорічний контроль рівня обізнаності	т	Словник (так, ні)		
95.	13	У підрозділі або посадової особи з інформаційної безпеки ОКІ створений та підтримується в актуальному стані перелік програмного та апаратного забезпечення, що використовується на ОКІІ в захищеній від модифікації формі	т	Словник (так, ні)		
		Управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури (ОКІІ)об'єкта критичної інфраструктури				
96.	13	Механізм розподілу прав доступу до ОКІІ охоплює всі інформаційні ресурси ОКІІ (інформацію, яка зберігається та обробляється на ОКІІ, технологічну інформацію програмного та апаратного забезпечення ОКІІ, журнали реєстрації подій тощо)	т	Словник (так, ні)		
97.	13	Механізм розподілу прав доступу до ОКІІ визначає права на виконання операцій для всіх користувачів та адміністраторів (за необхідності також активних процесів) над інформаційними ресурсами ОКІІ (читання, модифікація, створення, видалення тощо)	т	Словник (так, ні)		
98.	13	Механізм розподілу прав доступу до ОКІІ визначає права доступу користувачів та адміністраторів до служб (функцій) ОКІІ	т	Словник (так, ні)		

1	2	3	4	5	6	7
99.	13	На ОКІІ реалізовано централізоване поширення налаштувань прав та атрибутів доступу, параметрів реєстрації подій, інших параметрів безпеки та системних налаштувань компонентів ОКІІ	т	Словник (так, ні)		
		Ідентифікація та автентифікація користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури (ОКІІ)				
100.	13	Користувачі та адміністратори ОКІІ (за необхідності також активні процеси) отримують доступ до служб (функцій), інформації та компонентів об'єкта в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) користувача і деякої інформації, що вводиться користувачем (пароль), та/або фізичного ідентифікатора, що надається користувачем (ключ, сертифікат, токен тощо)	т	Словник (так, ні)		
101.	13	Засоби ОКІІ надають можливість ідентифікації кожної операції користувача та адміністратора на ОКІІ та їх протоколювання в журналах реєстрації подій	т	Словник (так, ні)		
102.	13	Для надання доступу до служб (функцій) та інформації ОКІІ використовується багатофакторна автентифікація користувачів та адміністраторів	т	Словник (так, ні)		
103.	13	Для надання доступу до служб (функцій) та інформації ОКІІ використовується двофакторна автентифікація, якщо програмне забезпечення не підтримує багатофакторну автентифікацію	т	Словник (так, ні)		

1	2	3	4	5	6	7
104.	13	На ОКІІ заблоковані або змінені облікові записи адміністраторів та їх паролів, встановлені за замовчуванням, у всіх компонентах об’єкта	т	Словник (так, ні)		
105.	13	На ОКІІ видалені або заблоковані неперсоналізовані і гостьові облікові записи користувачів і адміністраторів та використовуватися виключно персоналізовані облікові записи користувачів і адміністраторів у всіх компонентах об’єкта	т	Словник (так, ні)		
106.	13	Під час звільнення з посади працівника його обліковий запис негайно блокується або видаляється в усіх компонентах об’єкта	т	Словник (так, ні)		
107.	13	Обладнання, яке підключається до системи управління технологічними процесами ОКІ, ідентифіковане (наприклад, за IP-адресою, MAC-адресою тощо), вжито заходів, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації.	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
		Реєстрація подій компонентами об’єкта критичної інформаційної інфраструктури (ОКІІ)				

1	2	3	4	5	6	7
108.	13	Компоненти ОКІІ забезпечують реєстрацію, збереження в електронних журналах та захист від модифікації інформації про доступ та дії з інформацією, яка зберігається та обробляється на ОКІІ, а також з налаштуваннями програмного та апаратного забезпечення ОКІІ, журналами реєстрації подій тощо (читання, модифікація, створення, видалення тощо)	т	Словник (так, ні)		
109.	13	Компоненти ОКІІ забезпечують реєстрацію, збереження в електронних журналах та захист від модифікації інформації про реєстрацію подій, пов’язаних із встановленням та зміною прав доступу до служб (функцій), інформації та компонентів об’єкта	т	Словник (так, ні)		
110.	13	Компоненти ОКІІ забезпечують реєстрацію, збереження в електронних журналах та захист від модифікації інформації про вхід/вихід користувачів та адміністраторів в/із компонентів об’єкта	т	Словник (так, ні)		
111.	13	Компоненти ОКІІ забезпечують реєстрацію, збереження в електронних журналах та захист від модифікації інформації про невдалі спроби входу користувачів та адміністраторів на ОКІІ та перевищення граничної кількості спроб введення пароля	т	Словник (так, ні)		
112.	13	Компоненти ОКІІ забезпечують реєстрацію, збереження в електронних журналах та захист від модифікації інформації про реєстрацію, видалення (блокування) облікових записів користувачів та адміністраторів у компонентах ОКІІ	т	Словник (так, ні)		

1	2	3	4	5	6	7
113.	13	Компоненти ОКІІ забезпечують реєстрацію, збереження в електронних журналах та захист від модифікації інформації про зміну пароля користувача в компонентах ОКІІ	т	Словник (так, ні)		
114.	13	Компоненти ОКІІ забезпечують реєстрацію, збереження в електронних журналах та захист від модифікації інформації про реєстрацію подій, пов’язаних із зміною конфігураційних налаштувань компонентів ОКІІ	т	Словник (так, ні)		
115.	13	Компоненти ОКІІ забезпечують реєстрацію, збереження в електронних журналах та захист від модифікації інформації про спроби здійснення несанкціонованого доступу до ресурсів ОКІІ	т	Словник (так, ні)		
116.	13	Компоненти ОКІІ забезпечують реєстрацію, збереження в електронних журналах та захист від модифікації інформації про негативні результати перевірок цілісності даних та програмного і апаратного забезпечення ОКІІ	т	Словник (так, ні)		
117.	13	Компоненти ОКІІ забезпечують реєстрацію, збереження в електронних журналах та захист від модифікації інформації про всі дії адміністратора з журналами реєстрації подій компонентів ОКІІ та налаштування ним параметрів реєстрації	т	Словник (так, ні)		
118.	13	Журнали реєстрації подій компонентів ОКІІ містять інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	

1	2	3	4	5	6	7
119.	13	Журнали реєстрації подій компонентів містять інформацію, достатню для встановлення користувача, процесу і мережевого об’єкта, що мали відношення до кожної зареєстрованої події	т	Словник (так, ні)		
120.	13	Забезпечений захист журналів реєстрації подій компонентів ОКІІ від несанкціонованого доступу, модифікації або руйнування. Електронні журнали реєстрації подій зберігаються не менше ніж один рік з дати реєстрації останньої події	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
121.	13	На ОКІ впроваджено систему збору та аналізу журналів реєстрації подій програмного та апаратного забезпечення ОКІІ, що має можливість встановлення фільтрів, які дозволяють робити вибірку і аналіз журналів та подій за різними критеріями та за потреби мати інтерфейси обміну з іншими системами	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
122.	13	На ОКІІ забезпечена можливість роботи з архівними журналами реєстрації подій за попередні періоди шляхом завантаження журналів на ОКІІ із зовнішнього джерела	т	Словник (так, ні)		
123.	13	Архівні журнали реєстрації подій, що завантажуються на ОКІІ, лише доповнюють існуючі журнали, без затирання або зміни інформації, що вже зберігається в них	т	Словник (так, ні)		

1	2	3	4	5	6	7
124.	13	Архівні журнали реєстрації подій зберігаються на фізично відокремленому компоненті ОКІІ або окремому носії даних не менше року з дати їх утворення	т	Словник (так, ні)		
		Забезпечення мережевого захисту компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури (ОКІІ)				
125.	13	На ОКІІ використовуються засоби захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів	т	Словник (так, ні)		
126.	13	На ОКІІ забезпечене централізоване управління засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів	т	Словник (так, ні)		
127.	13	Доступ адміністраторам до компонентів ОКІІ надається виключно з IP-адрес (робочих станцій), які визначені для адміністрування ОКІІ	т	Словник (так, ні)		
128.	13	Можливе фізичний розподіл зовнішньої мережі та ОКІІ ОКІ на межі (периметрі) між зовнішніми мережами, іншими інформаційно-комунікаційними системами, що обслуговують ОКІ, та ОКІІ ОКІ	т	Словник (так, ні)		
		Наявні функції захисту засобів мережевого захисту, встановлених у випадку неможливості фізичного розподілу зовнішньої мережі та об'єкта критичної інформаційної інфраструктури (ОКІІ) об'єкта критичної інфраструктури на межі (периметрі) між зовнішніми мережами, іншими інформаційно-комунікаційними системами, що обслуговують об'єкт критичної інфраструктури та об'єкт критичної інформаційної інфраструктури об'єкта критичної інфраструктури				

1	2	3	4	5	6	7
129.	13	Захист від атак «нульового дня» (вразливості програмного забезпечення, які ще невідомі користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту), виявлення зловмисного коду та шкідливого програмного забезпечення	т	Словник (так, ні)		
130.	13	Фільтрація трафіка та розмежування доступу між мережею об’єкта кричної інфраструктури та зовнішніми мережами за критеріями дозволених та заборонених служб, протоколів, портів, мережевих адрес, мережевих з’єднань, небажаних вебсайтів тощо. Блокування трафіка та з’єднань, які не відповідають визначеним критеріям	т	Словник (так, ні)		
131.	13	Фільтрація та аналіз трафіка за визначеними відповідно до політики безпеки критеріями	т	Словник (так, ні)		
132.	13	Моніторинг трафіка на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та за іншими визначеними відповідно до політики безпеки критеріями	т	Словник (так, ні)		
133.	13	Виявлення та запобігання атакам та вторгненням, спрямованим на програмні та апаратні компоненти та інформацію ОКІІ	т	Словник (так, ні)		
134.	13	Захист від атак типу «відмова в обслуговуванні»	т	Словник (так, ні)		
135.	13	Захист від несанкціонованого доступу через Інтернет	т	Словник (так, ні)		
136.	13	Балансування навантаження	т	Словник (так, ні)		
137.	13	Маскування структури і мережевих адрес мережі	т	Словник (так, ні)		
138.	13	Завершення з’єднання з вузлом у разі атаки	т	Словник (так, ні)		
139.	13	Реєстрація подій, що мають відношення до безпеки	т	Словник (так, ні)		

1	2	3	4	5	6	7
		Мережева архітектура об'єкта критичної інформаційної інфраструктури (ОКІІ)				
140.	13	Проведено розподіл ОКІІ на фізичному та/або логічному рівні (сегментація мережі) і обмежено доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту	т	Словник (так, ні)		
		Наявні частини/зони мережі об'єкта критичної інформаційної інфраструктури (ОКІІ)				
141.	13	Зовнішня зона (DMZ-zone): зона із зовнішніми діапазонами адресації мережі для розміщення зовнішніх (публічних) інформаційних ресурсів та сервісів ІКС	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
142.	13	Зона прикладних застосувань ІКС (APP-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення серверів застосувань, доступна для виконання функціональних запитів користувачів інформаційних сервісів	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
143.	13	Зона сховищ даних ІКС (DB-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення баз даних, для доступу за запитами прикладних застосувань зони (APP-zone)	т	Словник (так, ні, інше)		

1	2	3	4	5	6	7
		Інше	т		Вказується у випадку вибору значення «інше»	
144.	13	Зона прикладних застосувань системи безпеки (Security-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення сервісів та служб захисту інформації	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
145.	13	Тестова зона (Test-zone): захищена внутрішня зона з внутрішньою адресацією, призначена для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення ІКС перед впровадженням їх у промислову експлуатацію в ІКС	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
146.	13	Сервери та обладнання, що забезпечують функціонування сервісів та віддалений доступ клієнтів/користувачів ОКІІ із зовнішніх мереж, розміщені в зовнішній зоні ОКІІ	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
147.	13	З’єднання серверів та обладнання, які розміщені в зовнішній зоні, із серверами та обладнанням внутрішньої мережі ОКІІ захищаються міжмережевим екраном	т	Словник (так, ні, інше)		

1	2	3	4	5	6	7
		Інше	т		Вказується у випадку вибору значення «інше»	
148.	13	Робочі станції, з яких виконуються дії щодо адміністрування програмного та апаратного забезпечення ОКІІ, а також серверні частини засобів захисту інформації розміщено в зоні прикладних застосувань системи безпеки (Security-zone) мережі, захищеної за допомогою міжмережевого екрана	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
149.	13	Сегмент інформаційної інфраструктури ОКІ, в якому перебуває система керування технологічними процесами, відокремлений від інших систем ОКІ	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
150.	13	У випадку логічного відокремлення системи керування технологічними процесами на межі сегмента встановлено міжмережевий екран	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
151.	13	Визначені та відключені (заблоковані) програмні порти компонентів ОКІІ, які є небезпечними для забезпечення кібербезпеки	т	Словник (так, ні)		

1	2	3	4	5	6	7
152.	13	Виконується перевірка ефективності заходів щодо захисту ОКІІ від зовнішнього проникнення шляхом виконання періодичних (не рідше одного разу на рік) тестів на проникнення (Penetration test)	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
153.	13	У разі отримання негативних результатів після проведення тестів на проникнення вживаються заходи для усунення їх причин	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
154.	13	На ОКІІ передача даних бездротовими мережами здійснюється виключно захищеними з’єднаннями із забезпеченням їх конфіденційності та цілісності	т	Словник (так, ні)		
155.	13	На ОКІІ заборонено використання технологій Wi-Fi та Bluetooth	т	Словник (так, ні)		
156.	13	Для захисту даних, які передаються через незахищене середовище між віддаленими користувачами, адміністраторами та ОКІІ, між компонентами об’єкта (поза контрольованою територією об’єкта критичної інфраструктури), між ОКІІ та іншими (зовнішніми) інформаційно-комунікаційними системами, використовуються захищені з’єднання із забезпеченням конфіденційності та цілісності цих даних	т	Словник (так, ні, інше)		

1	2	3	4	5	6	7
		Інше	т		Вказується у випадку вибору значення «інше»	
157.	13	Системи управління технологічними процесами структури не підключені до глобальних мереж передачі даних, зокрема до Інтернету	т	Словник (не підключені, підключені)		
158.	13	Системи управління технологічними процесами об’єкта інфраструктури підключені до глобальних мереж передачі даних, зокрема до Інтернету, з упровадженням заходів мережевого захисту (тільки у випадку неможливості функціонування технологічного процесу без підключення до Інтернету та за умови впровадження всіх заходів захисту відповідно до Загальних вимог до кіберзахисту ОКІ або конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування ОКІ, що належить до відповідної сфери управління)	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
159.	13	До глобальних мереж передачі даних, зокрема до Інтернету, ОКІІ підключені через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних зі створеними комплексними системами захисту інформації з підтвердженою відповідністю	т	Словник (так, ні)		

1	2	3	4	5	6	7
160.	13	До глобальних мереж передачі даних, зокрема до Інтернету, ОКІІ підключаються через власні системи захищеного доступу до Інтернету структури зі створеними комплексними системами захисту інформації з підтвердженою відповідністю	т	Словник (так, ні)		
		Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури (ОКІІ)				
161.	13	ОКІІ будується на базі відмовостійкого підходу	т	Словник (так, ні)		
		Заходи для забезпечення відмовостійкості об'єкта критичної інформаційної інфраструктури (ОКІІ)				
162.	13	Здійснюється періодичне створення резервних копій інформаційних ресурсів ОКІІ та критичних бізнес/операційних процесів ОКІ, включаючи інформацію, яка зберігається на ОКІІ, технологічну інформацію компонентів об'єкта та образів серверів ОКІІ, а також їх відновлення у випадку втрати або пошкодження	т	Словник (так, ні)		
163.	13	Проводиться резервування критичних для функціонування ОКІІ та бізнес/операційних процесів ОКІ програмних та апаратних компонентів для забезпечення його сталого функціонування у випадку виходу з ладу одного з критичних компонентів	т	Словник (так, ні)		
164.	13	Здійснюється резервування віртуальних серверів ОКІІ	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	

1	2	3	4	5	6	7
165.	13	Проводиться дублювання (кластеризація) критичних для функціонування ОКІІ та бізнес/операційних процесів ОКІ програмних та апаратних компонентів об’єкта для забезпечення його сталого функціонування, зниження навантаження та збільшення продуктивності	т	Словник (так, ні)		
166.	13	Використовуються засоби балансування навантаження	т	Словник (так, ні)		
167.	13	Використовуються джерела безперебійного живлення для критичних компонентів ОКІІ	т	Словник (так, ні)		
168.	13	Зв’язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами) для об’єктів критичної інфраструктури, які надають свої послуги через Інтернет	т	Словник (так, ні)		
169.	13	Під час розроблення, модернізації або оновлення компонентів системи управління технологічними процесами ОКІ використовується тестова програмно-апаратна платформа, яка підключена до окремого (тестового) виділеного сегмента його мережі для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення перед впровадженням їх у промислову експлуатацію	т	Словник (так, ні)		
		Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури (ОКІІ)				

1	2	3	4	5	6	7
170.	13	На ОКІІ проводиться перевірка всіх змінних (зовнішніх) пристроїв та носіїв інформації перед кожним їх використанням на ОКІІ засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів	т	Словник (так, ні)		
171.	13	На ОКІІ проводиться ідентифікація всіх змінних (зовнішніх) пристроїв та носіїв інформації за допомогою унікального ідентифікатора	т	Словник (так, ні, інше)		
		Інше	т		Вказується у випадку вибору значення «інше»	
172.	13	На ОКІІ унеможливлено використання змінних (зовнішніх) пристроїв та носіїв інформації, які не зареєстровані на ОКІІ	т	Словник (так, ні)		
173.	13	На ОКІІ відключено автоматичний запуск програм зі змінних (зовнішніх) пристроїв та носіїв інформації	т	Словник (так, ні)		
174.	13	Порти компонентів мережевого обладнання, робочих станцій та серверів, які не використовуються, заблоковані адміністраторами ОКІІ	т	Словник (так, ні)		
		Визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури (ОКІІ)				
175.	13	На ОКІІ проводитися перевірка на цілісність та автентичність оновлень компонентів об'єкта	т	Словник (так, ні)		
176.	13	У разі порушення цілісності або не підтвердження автентичності оновлення воно відхиляється і не застосовується, а ця подія протоколюється в журналі подій	т	Словник (так, ні)		

1	2	3	4	5	6	7
177.	13	У складі ОКІІ використовується програмне та апаратне забезпечення, для якого не припинено підтримку виробника	т	Словник (так, ні)		
178.	13	У складі ОКІІ використовуються офіційні стабільні версії прикладного програмного забезпечення та драйверів	т	Словник (так, ні)		
179.	13	На ОКІІ перевага надається програмному забезпеченню, яке має більш вищий рівень гарантій відповідно до нормативного документа системи технічного захисту інформації 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”, за результатами державної експертизи у сфері технічного захисту інформації	т	Словник (так, ні)		
180.	13	На ОКІІ блокується самостійне встановлення або видалення користувачами програмного забезпечення	т	Словник (так, ні)		
181.	13	Право на встановлення або видалення програмного забезпечення на ОКІІ має тільки уповноважений адміністратор	т	Словник (так, ні)		
182.	13	Засоби ОКІІ забезпечують неприйняття файлу/повідомлення в обробку у разі отримання негативного результату перевірки електронного підпису файлу/повідомлення, що надійшов/надійшло. Ця подія відображається в журналі реєстрації подій	т	Словник (так, ні)		

1	2	3	4	5	6	7
183.	13	Програмні та апаратні засоби, які використовуються у складі ОКІІ, не мають походження з іноземної держави, до якої застосовано санкції згідно із Законом України «Про санкції», чи бути розроблені/виготовлені юридичною особою-резидентом такої іноземної держави або юридичною особою, частка статутного капіталу якої перебуває у власності зазначеної іноземної держави, або юридичною особою, яка перебуває під контролем юридичної особи такої іноземної держави	т	Словник (так, ні)		
		Визначення умов розміщення компонентів об'єкта критичної інформаційної інфраструктури (ОКІІ)				
184.	13	Компоненти та/або інформація ОКІІ перебувають у власному центрі обробки даних	т	Словник (так, ні)		
185.	13	Компоненти та/або інформація ОКІІ, крім систем управління технологічними процесами, перебувають у сторонньому (не власному) центрі обробки даних	т	Словник (так, ні)		
186.	13	Сторонній центр обробки даних, у якому розташовані компоненти та/або інформація ОКІІ, знаходиться на території України (за винятком тимчасово окупованих територій України)	т	Словник (так, ні)		
187.	13	Власником стороннього центру обробки даних, у якому розташовані компоненти та/або інформація ОКІІ, є резидент України	т	Словник (так, ні)		
188.	13	Компоненти та інформація системи управління технологічними процесами структури перебувають у власному центрі обробки даних. Їх заборонено розміщати в сторонньому центрі обробки даних	т	Словник (так, ні)		

1	2	3	4	5	6	7
189.	13	Розпорядник ОКІІ використовує основний і резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту для створення резервних копій своїх інформаційних ресурсів та їх оперативного відновлення у разі пошкодження або знищення	т	Словник (так, ні)		
190.	13	Компоненти ОКІІ розміщуються у приміщеннях, які унеможливлюють несанкціонований фізичний доступ до них сторонніх осіб	т	Словник (так, ні)		
191.	13	Забезпечений контрольований фізичний доступ до приміщень та/або комутаційних шаф, де розташовані робочі станції, сервери, мережеві компоненти та комутаційні вузли структурованої кабельної системи ОКІІ	т	Словник (так, ні)		
192.	13	Заборонено підключення робочі місця адміністраторів та операторів ОКІІ до інших інформаційно-комунікаційних систем	т	Словник (так, ні)		
193.	13	Схеми (креслення) розміщення обладнання структурованої кабельної системи та кабельних каналів ОКІІ, схеми підключення обладнання, таблиці маркування кабелів структурованої кабельної системи та кабельних з’єднань зберігаються в актуальному стані	т	Словник (так, ні)		

Директор Департаменту кіберзахисту
Адміністрації Держспецзв’язку Данило МЯЛКОВСЬКИЙ