Прим. № __

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

м. Київ

_____ _____ 2023 року № _____

Про затвердження форми Плану захисту об’єкта критичної інфраструктури за проєктною загрозою національного рівня «кібератака/кіберінцидент»

Відповідно до пункту 5 Порядку розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 04 серпня 2023 року № 818, пункту 10 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, наказу Адміністрації Держспецзв’язку від 28 липня 2023 року № 219/ДСК «Про затвердження Проектних загроз критичній інфраструктурі національного рівня»

НАКАЗУЮ:

1. Затвердити форму Плану захисту об’єкта критичної інфраструктури за проєктною загрозою національного рівня «кібератака/кіберінцидент», що додається.

2. Відділу інформаційних комунікацій Адміністрації Держспецзв’язку забезпечити розміщення цього наказу на офіційному вебсайті Держспецзв’язку.

3. Контроль за виконанням цього наказу покласти на заступника Голови Державної служби спеціального зв’язку та захисту інформації України відповідно до розподілу обов’язків.

Голова Служби
бригадний генерал Юрій ЩИГОЛЬ

UB
Адміністрація Держспецзв’язку
№877 від 04.10.2023
КЕП: Щиголь Ю. Ф. 04.10.2023 12:21
30703531AC072D0C04000000BB86080011B21B00
Сертифікат дійсний з 17.02.2023 00:00 до 17.02.2025 00:00

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
__ жовтня 2023 року № ___

ФОРМА ПЛАНУ
ЗАХИСТУ ОБ’ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА ПРОЄКТНОЮ ЗАГРОЗОЮ НАЦІОНАЛЬНОГО РІВНЯ «КІБЕРАТАКА/КІБЕРІНЦИДЕНТ»

Гриф обмеження доступу (зазначається після заповнення)

ЗАТВЕРДЖЕНО

_____

(найменування посади керівника або уповноваженої особи оператора критичної інфраструктури)

_____

(підпис) (власне ім’я, прізвище)

___ _____ 20__ р.

МП (у разі наявності)

ПЛАН

ЗАХИСТУ ОБ’ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА ПРОЄКТНОЮ ЗАГРОЗОЮ НАЦІОНАЛЬНОГО РІВНЯ «КІБЕРАТАКА/КІБЕРІНЦИДЕНТ»

_____

(найменування об’єкта критичної інфраструктури/унікальний реєстровий номер об’єкта критичної інфраструктури)

ПОГОДЖЕНО

Керівник підрозділу функціонального органу у сфері кіберзахисту/його регіонального органу/підрозділу

_____

(найменування підрозділу функціонального органу)

_____

(посада, підпис, власне ім’я, прізвище)

___.___.20__

1. Загальні відомості про об’єкт критичної інформаційної інфраструктури (далі – ОКІІ)

Таблиця 1 – Назва ОКІІ

Унікальний ідентифікатор *(для ОКІ I та II категорій критичності)*	
Повна назва	
Скорочена назва	

Таблиця 2 – Подання відомостей до державного реєстру ОКІІ *(для ОКІ I та II категорій критичності)*

Відомості про стан кіберзахисту ОКІІ (Форма 1, Форма 2) подано до державного реєстру об’єктів критичної інформаційної інфраструктури	Так □	Дата подання відомостей: ___.___.20___	Дата внесення до державного реєстру ОКІІ: ___.___.20___
	Ні □	Запланований термін подання відомостей: ___.___.20___	Відповідальна особа: _____

Таблиця 3 – План виконання Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518

Вимоги до кіберзахисту об’єктів критичної інфраструктури	Відповідальна особа: _____	
	Стан виконання вимог (__ %) станом на: ___.___.20___	Встановлений термін виконання вимог на 100 %: ___.___.20___

Таблиця 4 – Відомості про особу та/або підрозділ, що відповідає за стан захисту інформації (забезпечення інформаційної безпеки) та кіберзахисту ОКІІ, забезпечення постійного зв'язку з відповідними суб'єктами національної системи кібербезпеки

Прізвище, власне ім'я, по батькові (у разі наявності)	
Посада	

Назва підрозділу		
Контактні дані	поштова адреса	
	номер телефону	
	e-mail адреса	

2. Опис об’єкта критичної інформаційної інфраструктури

Таблиця 5 – Опис ОКІІ

Життєво важлива послуга, надання якої забезпечує ОКІІ	*[вказати життєво важливу послугу, що надає ОКІ, яка підтримується ОКІІ та збігається з послугою, що вказана в паспорті ОКІ та у постанові Кабінету Міністрів України від 09 жовтня 2020 року № 1109 «Деякі питання об’єктів критичної інфраструктури»]*	
Вид інформації за порядком доступу, яка обробляється або планується для оброблення на ОКІІ	Відкрита	☐
	Службова (ДСК)	☐
	Державна таємниця	☐
	Конфіденційна інформація про фізичну особу (персональні дані)	☐
	Технологічна	☐
	Інша таємниця, що не належить до державної таємниці (банківська, лікарська тощо)	☐
	Інша (зазначити)	
Підключення до мережі Інтернет або до інших інформаційно-комунікаційних систем, які не входять до його складу	Так ☐ Ні ☐	
	Повне найменування постачальників електронних комунікаційних мереж та/або послуг	
	Чи має постачальник електронних комунікаційних мереж та/або послуг захищені вузли доступу до глобальних мереж передачі даних зі створеними комплексними системами захисту інформації з підтвердженою відповідністю?	Так ☐ Ні ☐

	IP-адреса, що використовується	
	Номер телефону	
	e-mail адреса	
	Повне найменування інших інформаційно-комунікаційних систем, що не входять до складу ОКІІ (у разі підключення)	
Взаємодія ОКІІ з іншими ОКІІ та системами при наданні послуги *[отримання ОКІІ життєво важливих послуг від інших ОКІІ, ненадання яких вплине на функціонування ОКІІ. Надання ОКІІ життєво важливих послуг іншим ОКІІ, неотримання яких вплине на функціонування інших ОКІІ]*	Опис взаємодії	
	Повне найменування іншого ОКІІ	
	Унікальний ідентифікатор ОКІІ	
	Номер телефону	
	e-mail адреса	
Атестат відповідності комплексної системи захисту інформації ОКІІ або результати незалежного аудиту ОКІ	Так ☐ Ні ☐	
	Атестат відповідності КСЗІ ОКІІ або елемента ОКІІ (зазначити який)	
	Сертифікат відповідності (номер, дата) або звіт за результатами незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури	
	Інше	
Взаємодія з платформою (платформами) обміну інформацією щодо шкідливого програмного забезпечення (MISP-	Так ☐ Ні ☐	
	MISP CERT-UA	☐
	MISP-UA	☐

UA, MISP CERT-UA)	MISP-NBU		□
	MISP Національного координаційного центру кібербезпеки (НКЦК) при Раді національної безпеки і оборони України		□
	Інше:		
Взаємодія з командою (командами) реагування на кіберінциденти (CERT, CSIRT)	Так □ Ні □		
	Найменування команди реагування на кіберінциденти		
	Тип за формою власності	Державна	□
		Приватна	□
	Тип за належністю	Національна	□
		Регіональна	□
		Секторальна	□
		Об’єктова	□
	Контактна інформація		
Взаємодія із центрами управління безпекою (SOC)	Так □ Ні □		
	Найменування центру управління безпекою		
	Тип за належністю	Національний	□
		Регіональний	□
		Секторальний	□
		Об’єктовий	□
	Контактна інформація		

Рисунок 1 – Загальна функціональна схема системи (мережі) ОКІІ

ОПИС ЗАГАЛЬНОЇ ФУНКЦІОНАЛЬНОЇ СХЕМИ СИСТЕМИ (МЕРЕЖІ) ОКІІ ТА ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ

[у цьому розділі надається стислий опис роботи системи (мережі) ОКІІ (не має перевищувати двох аркушів). Мають бути описані основні функції, завдання, принципи функціонування, технології обробки інформації, вплив на надання життєво важливої послуги]

3. Проєктні загрози

Таблиця 6 – Проєктні загрози

Рівень	Загрози	Властивості загрози
Національний рівень	Кіберінцидент/кібератака	Порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту
Секторальний (галузевий) та регіональний рівень		
Об’єктовий рівень		

4. Загальний порядок реагування на кіберінциденти/кібератаки

5. План кіберзахисту ОКІІ

Провести оцінку ризиків, сформувати звіт за результатами оцінки ризиків *[методичною основою для оцінки ризиків на об'єкті критичної інфраструктури є стандарт ДСТУ ISO/IEC 27005]*

Таблиця 7 – План кіберзахисту ОКІІ за класом «Ідентифікація ризиків кібербезпеки» (ID)

	№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
ID	**1.**	**«Ідентифікація ризиків кібербезпеки» (ID)**					
	1.	**Провести інвентаризацію активів**					
	2.	**Призначити керівну посадову особу, відповідальну за кібербезпеку на всьому ОКІ, в т.ч. систем управління технологічними процесами, а також систем, що впливають на безпеку функціонування ОКІ**					
	3.	**Забезпечити належну**					

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
	взаємодію підрозділів IT та кіберзахисту					
4.	**Опрацювати вплив відомих вразливостей**					
5.	**Залучити сторонню організацію для проведення незалежного аудиту інформаційної безпеки**					
6.	**Забезпечити реагування на інформування постачальниками про визначені ними інциденти**					
7.	**Забезпечити реагування на інформування постачальниками про виявлені ними вразливості**					

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
8.	**Затвердити вимоги щодо кібербезпеки до постачальників ІКТ або послуг**					

Таблиця 8 – План кіберзахисту ОКІІ за класом «Кіберзахист» (PR)

	№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
PR	**2.**	**«Кіберзахист» (PR)**					
	1.	**Провести зміну паролів, встановлених за замовчуванням**					
	2.	**Забезпечити використання надійних паролів**					
	3	**Забезпечити унікальність облікових даних**					
	4.	**Затвердити процедуру вчасного видалення облікових даних звільнених працівників**					
	5.	**Унеможливити отримання зловмисником прав доступу до**					

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
	привілейованих облікових даних адміністраторів або користувачів					
6.	**Провести сегментацію мережі**					
7.	**Забезпечити виявлення невдалих спроб входу в систему**					
8.	**Впровадити стійку до фішингу багатофакторну автентифікацію**					
9.	**Запровадити базове навчання з кібербезпеки для всіх співробітників**					
10.	**Запровадити додаткове навчання з кібербезпеки для**					

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
	персоналу підрозділу кіберзахисту					
11.	**Забезпечити шифрування при обміні інформацією про активи між підрозділами ІТ та кіберзахисту**					
12.	**Забезпечити захист інформації з обмеженим доступом**					
13.	**Забезпечити захищеність електронної пошти від спуфінгу, фішингу та перехоплення повідомлень**					
14.	**Вимкнути встановлені за замовчуванням макроси та інший програмний код**					

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
15.	**Забезпечити документування конфігураційних файлів ІКТ, що обробляють активи**					
16.	**Забезпечити документування схеми розміщення та з'єднання обладнання мереж**					
17.	**Затвердити процедури інсталяції ІКТ**					
18.	**Забезпечити регулярне створення резервних копій конфігураційних файлів**					
19.	**Затвердити, регулярно тестувати та вносити зміни до планів реагування на**					

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
	кіберінциденти					
20.	**Забезпечити збір журналів подій**					
21.	**Забезпечити безпечне зберігання журналів подій**					
22.	**Забезпечити заборону підключення неавторизованих пристроїв**					
23.	**Забезпечити виявлення та обмеження використання Інтернет-послуг**					
24.	**Забезпечити обмеження підключення ОКІІ до мережі Інтернет**					

Таблиця 9 – План кіберзахисту ОКІІ за класом «Виявлення кіберінцидентів» (DE)

	№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
DE	**3**	**«Виявлення кіберінцидентів» (DE)**					
	1.	**Визначити порядок проведення моніторингу загроз та застосування відповідних тактик, технік і процедур**					

Таблиця 10 – План кіберзахисту ОКІІ за класом «Реагування на кіберінциденти» (RS)

	№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
RS	**4**	**«Реагування на кіберінциденти» (RS)**					
	1.	**Забезпечити інформування про кіберінциденти**					
	2.	**Забезпечити використання результатів досліджень щодо вразливостей**					
	3.	**Забезпечити розміщення файлів security.txt та опрацювання отриманої завдяки їм інформації**					

Таблиця 11 – План кіберзахисту ОКІІ за класом «Відновлення стану кібербезпеки» (RC)

	№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання та наявні ресурси	Заплановані заходи для виконання завдання	Відповідальна особа	Запланований термін виконання	Додаткові ресурси для виконання завдання
RC	**5**	**«Відновлення стану кібербезпеки» (RC)**					
	1.	**Затвердити плани відновлення після інцидентів**					

6. Відомості про моніторинг рівня безпеки об’єкта критичної інфраструктури щодо нейтралізації загрози національного рівня «кібератака/кіберінцидент»

Зведені відомості щодо результатів моніторингу рівня безпеки

Відомості про внесення змін

Таблиця 12 – Відомості про внесення змін до плану захисту ОКІ за проєктною загрозою «кібератака/кіберінцидент», які не потребують погодження

№ з/п	Дата внесення змін	Короткий опис та підстава внесення змін, які не підлягають погодженню	ПІБ та підпис відповідальної особи за стан захисту інформації та кіберзахисту ОКІІ

Директор Департаменту кіберзахисту
Адміністрації Держспецзв’язку Данило МЯЛКОВСЬКИЙ