

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»



UB  
Адміністрація Держспецзв'язку  
№05/05-9018/ВН від 03.10.2023  
КЕП: Мялковський Данило Владиславович 03.10.2023 08:05  
0D1B2B  
Сертифікат дійсний з 26.07.2022 14:28 до 25.07.2024 14:28

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 <input type="checkbox"/>	Дата подання відомостей: ____.____.20__	Дата внесення до державного реєстру ОКІІ: ____ . ____ .20__
	Ні <input type="checkbox"/>	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	<i>[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»]</i>	
Вид інформації за порядком доступу, яка обробляється або планується для оброблення на ОКІІ	Відкрита	<input type="checkbox"/>
	Службова (ДСК)	<input type="checkbox"/>
	Державна таємниця	<input type="checkbox"/>
	Конфіденційна інформація про фізичну особу (персональні дані)	<input type="checkbox"/>
	Технологічна	<input type="checkbox"/>
	Інша таємниця, що не належить до державної таємниці (банківська, лікарська тощо)	<input type="checkbox"/>
	Інша (вказати)	
Підключення до мережі Інтернет або до інших інформаційно-комунікаційних систем, які не входять до його складу	Так <input type="checkbox"/> Ні <input type="checkbox"/>	
	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 підтверженою відповідністю?	Так <input type="checkbox"/> Ні <input type="checkbox"/>

	IP-адреса, що використовується	
	Номер телефону	
	e-mail адреса	
	Повне найменування інших інформаційно-комунікаційних систем, що не входять до складу ОКП (у разі підключення)	
Взаємодія ОКП з іншими ОКП та системами при наданні послуги <i>[отримання ОКП життєво важливих послуг від інших ОКП, ненадання яких вплине на функціонування ОКП. Надання ОКП життєво важливих послуг іншим ОКП, неотримання яких вплине на функціонування інших ОКП]</i>	Опис взаємодії	
	Повне найменування іншого ОКП	
	Унікальний ідентифікатор ОКП	
	Номер телефону	
	e-mail адреса	
Атестат відповідності комплексної системи захисту інформації ОКП або результати незалежного аудиту ОКП	Так <input type="checkbox"/> Ні <input type="checkbox"/>	
	Атестат відповідності КСЗІ ОКП або елемента ОКП (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 <input type="checkbox"/> Ні <input type="checkbox"/>	
	MISP CERT-UA	<input type="checkbox"/>
	MISP-UA	<input type="checkbox"/>

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



Рисунок 1 – Загальна функціональна схема системи (мережі) ОКІІ





### 3. Проектні загрози

Таблиця 6 – Проектні 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		



## 5. План кіберзахисту ОКП

Провести оцінку ризиків, сформувавши 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 ОКП 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
<b>ID</b>	<b>1.</b>	<b>«Ідентифікація ризиків кібербезпеки» (ID)</b>				
	<b>1.</b>	<b>Провести інвентаризацію активів</b>				
	<b>2.</b>	<b>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</b>				
	<b>3.</b>	<b>Забезпечити належну</b>				

№ 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
	<b>взаємодію підрозділів ІТ та кіберзахисту</b>					
4.	<b>Опрацювати вплив відомих вразливостей</b>					
5.	<b>Залучити сторонню організацію для проведення незалежного аудиту інформаційної безпеки</b>					
6.	<b>Забезпечити реагування на інформування постачальниками про визначені ними інциденти</b>					
7.	<b>Забезпечити реагування на інформування постачальниками про виявлені ними вразливості</b>					

№ 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.	<b>Затвердити вимоги щодо кібербезпеки до постачальників ІКТ або послуг</b>					

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
<b>PR</b>	<b>2.</b>	<b>«Кіберзахист» (PR)</b>				
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 багатofакторну 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 ОКП 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
<b>DE</b>	<b>3</b>	<b>«Виявлення кіберінцидентів» (DE)</b>				
	<b>1.</b>	<b>Визначити порядок проведення моніторингу загроз та застосування відповідних тактик, технік і процедур</b>				

Таблиця 10 – План кіберзахисту ОКП 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
<b>RS</b>	<b>4</b>	<b>«Реагування на кіберінциденти» (RS)</b>				
	<b>1.</b>	<b>Забезпечити інформування про кіберінциденти</b>				
	<b>2.</b>	<b>Забезпечити використання результатів досліджень щодо вразливостей</b>				
	<b>3.</b>	<b>Забезпечити розміщення файлів security.txt та опрацювання отриманої завдяки їм інформації</b>				

Таблиця 11 – План кіберзахисту ОКП 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				



