ЗАТВЕРДЖЕНО

Наказ Служби безпеки України і Адміністрації Державної служби спеціального зв’язку та захисту інформації України
19 грудня 2024 року № 627 / 772

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

Гриф обмеження доступу (зазначається після заповнення)

ЗАТВЕРДЖЕНО

_____

(найменування посади керівника оператора критичної інфраструктури

або особи, що його заміщає)

_____

(підпис) (власне ім’я, прізвище)

___ _____ 20__ р.

МП (у разі наявності)

ПЛАН

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

_____

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

ПОГОДЖЕНО
Керівник/заступник керівника функціонального підрозділу Центрального управління/ регіонального органу Служби безпеки України

_____

(найменування підрозділу функціонального органу)

_____

_____

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

___.___.20__

ПОГОДЖЕНО
Керівник/заступник керівника структурного підрозділу/ територіального органу Адміністрації Держспецзв’язку

_____

(найменування підрозділу функціонального органу)

_____

_____

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

___.___.20__

1. Загальні відомості про об’єкт(и) інформаційної інфраструктури (далі – ОІІ) об’єкта критичної інфраструктури (далі – ОКІ)*

Таблиця 1. Ідентифікація ОІІ

Повна назва ОІІ	
Скорочена назва ОІІ	
Унікальний ідентифікатор об’єкта критичної інформаційної інфраструктури (далі – ОКІІ) *(для ОКІ І або ІІ категорії критичності)*	

Таблиця 2. Подання та внесення відомостей до державного реєстру ОКІІ *(для ОКІ І та ІІ категорії критичності)*

Відомості про ОКІІ *(Форма 1, Форма 2)* подано та внесено до державного реєстру ОКІІ	Так ☐	Дата подання відомостей: ___.___.20___	Дата внесення до державного реєстру ОКІІ: ___.___.20___
	Ні ☐	Запланований термін подання відомостей: ___.___.20___	Відповідальна особа: _____

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

Виконання Загальних вимог до кіберзахисту ОКІ	Відповідальна особа: _____	
	Виконано ___ % вимог станом на: ___.___.20___	Встановлений термін виконання вимог на 100 %: ___.___.20___

---

* До Плану захисту вносяться відомості про всі ОІІ *(ОКІІ та інші автоматизовані, інформаційні, електронні комунікаційні, інформаційно-комунікаційні системи, автоматизовані системи управління технологічними процесами)* ОКІ, окрім автоматизованих систем класу «1» *(окремих ПЕОМ)*.

Таблиця 4. Відомості про підрозділ або призначених осіб, на яких покладається забезпечення захисту інформації та контроль за станом кіберзахисту ОКІ

Прізвище, власне ім'я, по батькові *(у разі наявності)*		
Посада		
Назва підрозділу		
Контактні дані	номер телефону	
	e-mail адреса	

2. Опис об’єкта(ів) інформаційної інфраструктури ОКІ

Таблиця 5. Опис ОІІ

Життєво важлива функція та/або послуга ОКІ, надання якої забезпечується (підтримується) ОІІ		
Вид інформації за порядком доступу, яка обробляється або планується для оброблення на ОІІ	Відкрита	☐
	Службова (для службового користування)	☐
	Державна таємниця	☐
	Конфіденційна інформація про фізичну особу (персональні дані)	☐
	Технологічна	☐
	Інша таємниця, що не належить до державної таємниці (банківська, лікарська тощо)	☐
	Інша (зазначити)	
Використання незахищеного середовища для передачі інформації в межах ОІІ	Так ☐ Ні ☐	
Підключення до мережі Інтернет або до інших інформаційно-комунікаційних систем, які не входять до складу ОІІ	Так ☐ Ні ☐	
	Повне найменування постачальника 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 постачальника	
	e-mail адреса	
	Повне найменування інших інформаційно-комунікаційних систем, які не входять до складу ОІІ, але мають фізичне підключення до нього *(за наявності)*	
Використання бездротових технологій (Wi-Fi, Bluetooth тощо)	Так ☐	Ні ☐
	Wi-Fi ☐ Bluetooth ☐	

	Інша (зазначити):		
Взаємодія ОІІ з іншими ОІІ *(отримання ОІІ життєво важливих послуг від інших ОІІ (ОКІІ), ненадання яких вплине на функціонування ОІІ.* *Надання ОІІ життєво важливих послуг іншим ОІІ (ОКІІ), неотримання яких вплине на їх функціонування)*	Опис взаємодії		
	Повне найменування іншого ОІІ		
	Унікальний ідентифікатор ОКІІ *(за наявності)*		
	Номер телефону		
	e-mail адреса		
Атестат відповідності комплексної системи захисту інформації ОІІ, результати незалежного аудиту ОКІ	Так ☐ Ні ☐		
	Атестат відповідності КСЗІ ОІІ та/або складової частини ОІІ *(зазначити всі чинні атестати відповідності)*		
	Сертифікат відповідності та/або звіт за результатами незалежного аудиту інформаційної безпеки на ОКІ *(зазначити реквізити наявних документів, висновок за результатами аудиту)*		
	Інше (зазначити)		
Взаємодія з платформами обміну інформацією щодо шкідливого програмного забезпечення (MISP-UA, MISP CERT-UA тощо)	Так ☐ Ні ☐		
	MISP CERT-UA		☐
	MISP-UA		☐
	MISP-NBU		☐
	MISP Національного координаційного центру кібербезпеки (НКЦК) при Раді національної безпеки і оборони України		☐
	Інша (зазначити)		
Взаємодія з командами реагування на кіберінциденти (CERT, CSIRT тощо)	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		
Використання програмних та/або апаратних засобів: а) що мають походження або виготовлені державою-агресором; б) виготовлених фізичними або юридичними особами, щодо яких застосовано персональні спеціальні економічні та інші обмежувальні заходи (санкції) згідно із Законом України «Про санкції»; в) отриманих на безоплатній основі від фізичних або юридичних осіб	Так ☐ Ні ☐		
	Назва програмних та/або апаратних засобів		
	Назва компанії-розробника такого(их) засобів		
	Назва компанії-постачальника такого(их) засобів		
	Назва компанії, що здійснює підтримку такого(их) засобів		
	Наявність плану по заміщенню такого(их) засобів *(для підпунктів а і б)*	Так ☐ Ні ☐	
	Орієнтовні терміни заміщення такого(их) засобів *(для підпунктів а і б)*	__.__.20__	
Перевірка ефективності заходів щодо захисту ОІІ від зовнішнього проникнення шляхом виконання тестів на проникнення (Penetration test)	Так ☐ Ні ☐		
	Стислий опис проведених заходів та результатів:		
Використання механізму здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (Bug Bounty)	Так ☐ Ні ☐		
	Стислий опис проведених заходів та результатів. Зазначити посилання на публічну пропозицію, де виставляється повна інформація *(відповідно до пункту 6 Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого постановою Кабінету Міністрів України від 16 травня 2023 року № 497)*		

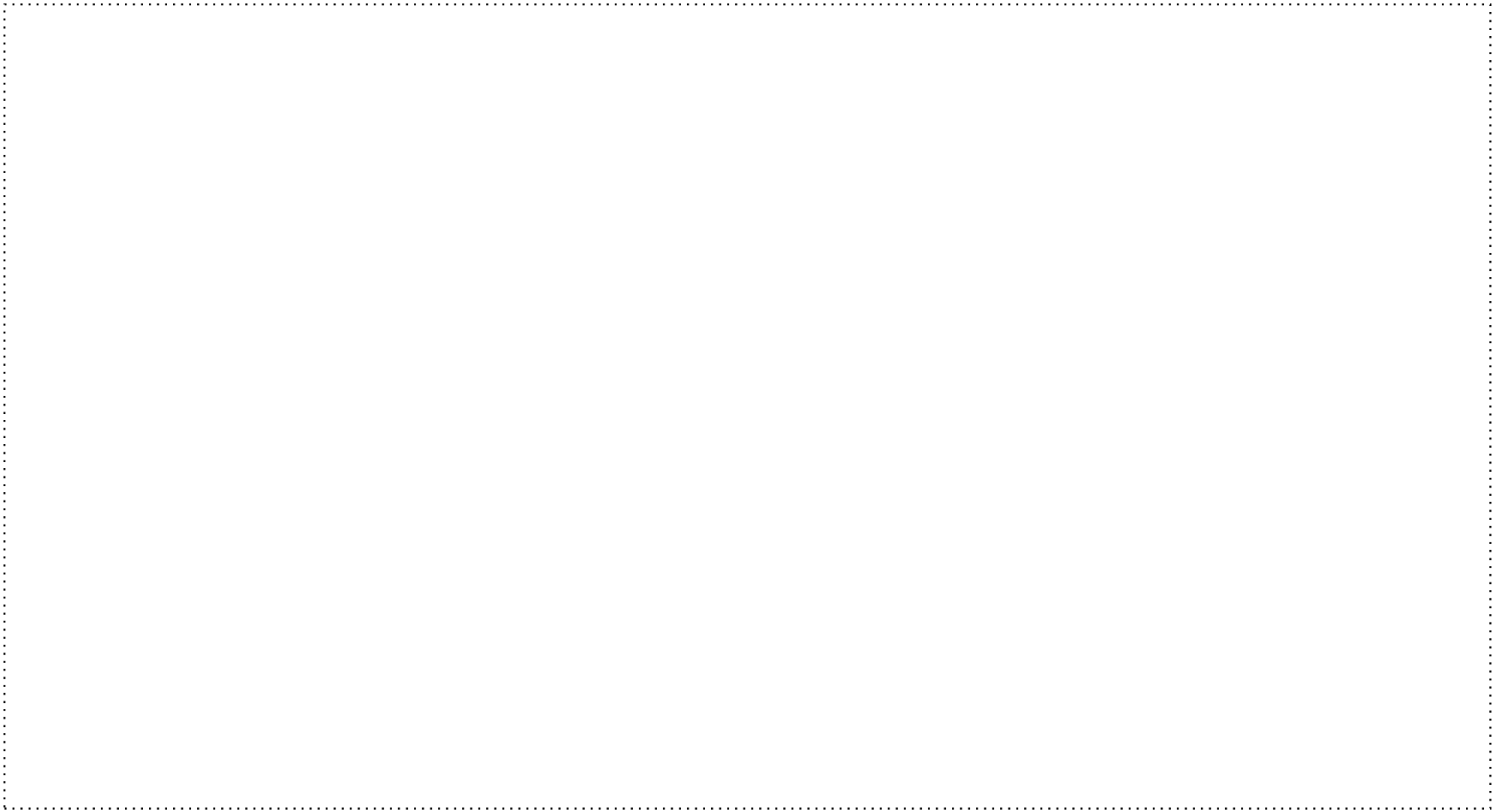

Рисунок 1. Загальна функціональна схема системи (мережі) ОКІ

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

(У цьому розділі надається стислий опис роботи системи (мережі) ОКІ. Мають бути описані основні функції, завдання, принципи функціонування, технології обробки інформації, вплив на надання життєво важливої(их) функції(й) та/або послуги(г). Не має перевищувати двох аркушів)

3. Проектні загрози

Таблиця 6. Проектні загрози

Рівень	Загрози	Властивості загрози
Національний рівень	Кібератака/кіберінцидент	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 рівень		
Об’єктовий рівень		

4. Загальний порядок реагування на кібератаки/кіберінциденти

5. План кіберзахисту ОКІ

_____

(вказати назву ОІІ)

План кіберзахисту ОКІ має містити мінімальний набір завдань, які в першу чергу *(але не обмежуючись ними надалі в діяльності з підвищення рівня кіберзахисту критичної інформаційної інфраструктури)* мають бути впроваджені або заплановані для впровадження на ОКІ.

Таблиця 7. План кіберзахисту ОКІ за класом «Ідентифікація ризиків кібербезпеки» (ID)

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальна особа	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
1	**«Ідентифікація ризиків кібербезпеки» (ID)**					
1	**Провести ідентифікацію інформаційних, програмних та апаратних ресурсів (програмних та апаратних компонентів, змінних (зовнішніх) пристроїв та носіїв інформації тощо)**					
2	**Створити підрозділ (або призначити посадову особу) з інформаційної безпеки, що відповідає за політику інформаційної безпеки, прийняту на ОКІ, та контроль за її дотриманням. Підрозділ**					

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальна особа	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
	або посадова особа повинні бути підпорядковані безпосередньо керівнику ОКІ.					
3	**Забезпечити належну взаємодію підрозділів ІТ та кіберзахисту**					
4	**Опрацювати вплив відомих вразливостей**					
5	**Залучити сторонню організацію для проведення незалежного аудиту інформаційної безпеки**					
6	**Затвердити політику управління інцидентами кібербезпеки**					
7	**Забезпечити реагування на інформування постачальниками про виявлені ними вразливості**					
8	**Затвердити вимоги до забезпечення інформаційної безпеки під час взаємодії з постачальниками**					

Таблиця 8. План кіберзахисту ОКІ за класом «Кіберзахист» (PR)

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано / не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальна особа	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
2	**«Кіберзахист» (PR)**					
1	**Затвердити процедуру ідентифікації та багатофакторної автентифікації користувачів та адміністраторів (парольна політика)**					
2	**Забезпечити використання надійних паролів**					
3	**Забезпечити унікальність облікових даних**					
4	**Затвердити процедуру вчасного видалення облікових записів звільнених працівників**					
5	**Унеможливити отримання зловмисником прав доступу до привілейованих облікових даних адміністраторів або користувачів**					
6	**Здійснити розподіл мережі на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту**					
7	**Забезпечити виявлення невдалих спроб входу в систему**					

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано / не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальна особа	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
	та перевищення граничної кількості спроб введення пароля					
8	**Впровадити багатофакторну автентифікацію**					
9	**Впровадити програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечити щорічний контроль рівня обізнаності**					
10	**Запровадити додаткове навчання з кібербезпеки для персоналу підрозділу кіберзахисту**					
11	**Забезпечити шифрування при обміні інформацією про активи між підрозділами IT та кіберзахисту**					
12	**Забезпечити захист інформації з обмеженим доступом (за наявності), створення (модернізація) комплексної системи захисту інформації**					
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 (реалізовано / не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальна особа	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
15	**Описати конфігураційні файли критичних програмних та апаратних компонентів**					
16	**Забезпечити документування та актуалізацію схем (креслень) обладнання структурованої кабельної системи та кабельних каналів, схеми підключення обладнання, таблиці маркування кабелів структурованої кабельної системи та кабельних з'єднань**					
17	**Затвердити процедури інсталяції ІКТ Затвердити політики встановлення засобів мережевого захисту, встановлення або видалення користувачами програмного забезпечення**					
18	**Забезпечити регулярне створення та зберігання резервних копій інформаційних ресурсів**					
19	**Затвердити, регулярно тестувати та вносити зміни до планів реагування на кіберінциденти**					
20	**Забезпечити збір журналів (логів) реєстрації подій**					
21	**Забезпечити безпечне**					

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано / не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальна особа	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
	зберігання журналів (логів) реєстрації подій					
22	**Забезпечити ідентифікацію обладнання та вжиття заходів, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації**					
23	**Забезпечити контрольоване використання послуг через мережу Інтернет, виявлення аномальної взаємодії та створити необхідні обмеження**					
24	**Забезпечити підключення ОІІ до мережі Інтернет через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю, та тільки у випадку неможливості функціонування без підключення до мережі Інтернет**					

Таблиця 9. План кіберзахисту ОКІ за класом «Виявлення кіберінцидентів» (DE)

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано / не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальна особа	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
3	**«Виявлення кіберінцидентів» (DE)**					
	Визначити порядок проведення моніторингу загроз та застосування відповідних тактик, технік і процедур					

Таблиця 10. План кіберзахисту ОКІ за класом «Реагування на кіберінциденти» (RS)

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано / не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальна особа	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
4	**«Реагування на кіберінциденти» (RS)**					
1	**Забезпечити інформування про кіберінциденти**					
2	**Забезпечити використання результатів досліджень щодо вразливостей**					
3	**Забезпечити розміщення файлів security.txt (стандарт безпеки веб-сайтів, в рамках програми Bug Bounty) та опрацювання отриманої завдяки їм інформації**					

Таблиця 11. План кіберзахисту ОКІ за класом «Відновлення стану кібербезпеки» (RC)

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано / не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальна особа	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
5	**«Відновлення стану кібербезпеки» (RC)**					
	Затвердити плани відновлення після інцидентів					

6. Відомості про моніторинг рівня безпеки ОКІ 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 проектною 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 ОКІ

Відповідальна особа за заповнення форми:
Посада ПІБ
__.__.20__

Т.в.о. начальника Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України

Володимир КАРАСТЕЛЬОВ

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

Ігор МАЛЬЧЕНЮК