ЗАТВЕРДЖЕНО

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

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

ЗАТВЕРДЖУЮ

Т.в.о. Генерального директора
КНП «ОПЛ №4»ООР
_____ Ірина ГАДЗАЛО
«__» _____ 2025 року

ПЛАН
КІБЕРЗАХИСТУ ОБ'ЄКТА ІНФОРМАЦІЙНІХ, ЕЛЕКТРОННИХ ТА ІНФОРМАЦІЙНО-КОМУНІКАТИВНИХ СИСТЕМ

КНП «ОПЛ №4№»ООР»

код 01998684

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

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

Таблиця 1. Ідентифікація ОІІ

Повна назва ОІІ	Комунальне некомерційне підприємства "Обласна психіатрична лікарня 4 "Одеської обласної ради "
Скорочена назва ОІІ	КНП"ОПЛ 4"ООР"
Унікальний ідентифікатор об'єкта критичної інформаційної інфраструктури (далі – ОКІІ) *(для ОКІ I або II категорії критичності)*	01998684 ОІІ

Таблиця 2. Відомості про підрозділ або призначених осіб, на яких покладається забезпечення захисту інформації та контроль за станом кіберзахисту ОКІ

Прізвище, власне ім'я, по батькові		Галат Ігор Володимирович
Посада		Відповідальна особа за забезпечення кібербезпеки
Назва підрозділу		Відповідальна особа за забезпечення кібербезпеки
Контактні дані	номер телефону	+380-67-486-14-54
	e-mail адреса	opl4oor@gmail.com

2. Опис об'єкта(ів) інформаційної інфраструктури ОІІ

Таблиця 3. Опис ОІІ

Життєво важлива функція та/або послуга ОКІ, надання якої забезпечується (підтримується) ОІІ	КВЕД-2010 клас 86.10 Діяльність лікарняних закладів	
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	ТОВ «БІСНЕТ» (інтернет) Код ЄДРПОУ 35131343
	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	Адмінвідділ: (098)624-31-49
	e-mail адреса	E-mail:info.bisnet@regiontv.com.ua
	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	1. Водопостачання та водовідведення 2. Розподіл газу 3. Розподіл електроенергії 4. Постачання електроенергії 5. Постачання газу 6. Вивіз ТПВ
	Повне найменування іншого ОІІ	1. Комунальне підприємство «Білгород-Дністровськводоканал» 2. АТ «Одесагаз» 3. АТ «ДТЕК Одеські електромережі» 4. ТОВ «ОПЕРАТОР ЕНЕРГІЇ» 5. ТОВ «Газопостачальна компанія «Нафтогаз Трейдинг» 6. Комунальне підприємство «Автотранссервіс»
	Унікальний ідентифікатор ОКІІ *(за наявності)*	1. 20937068 2. 03351208 3. 00131713 4. 43418783 5. 42399676 6. 32018333
	Номер телефону	1. (04849)3-50-23 2. (048)705-36-28 3. (048)705-22-59 4. (073)130-30-33 5. (044)222-24-46 6. (067)-009-93-80
	e-mail адреса	3. Kanc-ooe@dtek-oem.com.ua 4.info@operator.in.ua 5. E-mail:ngt@naftogaztrading.com.ua 6. e-mail:kpats@bdmr.gov.ua
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)*	Аудит не проводився	
	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 ☑	

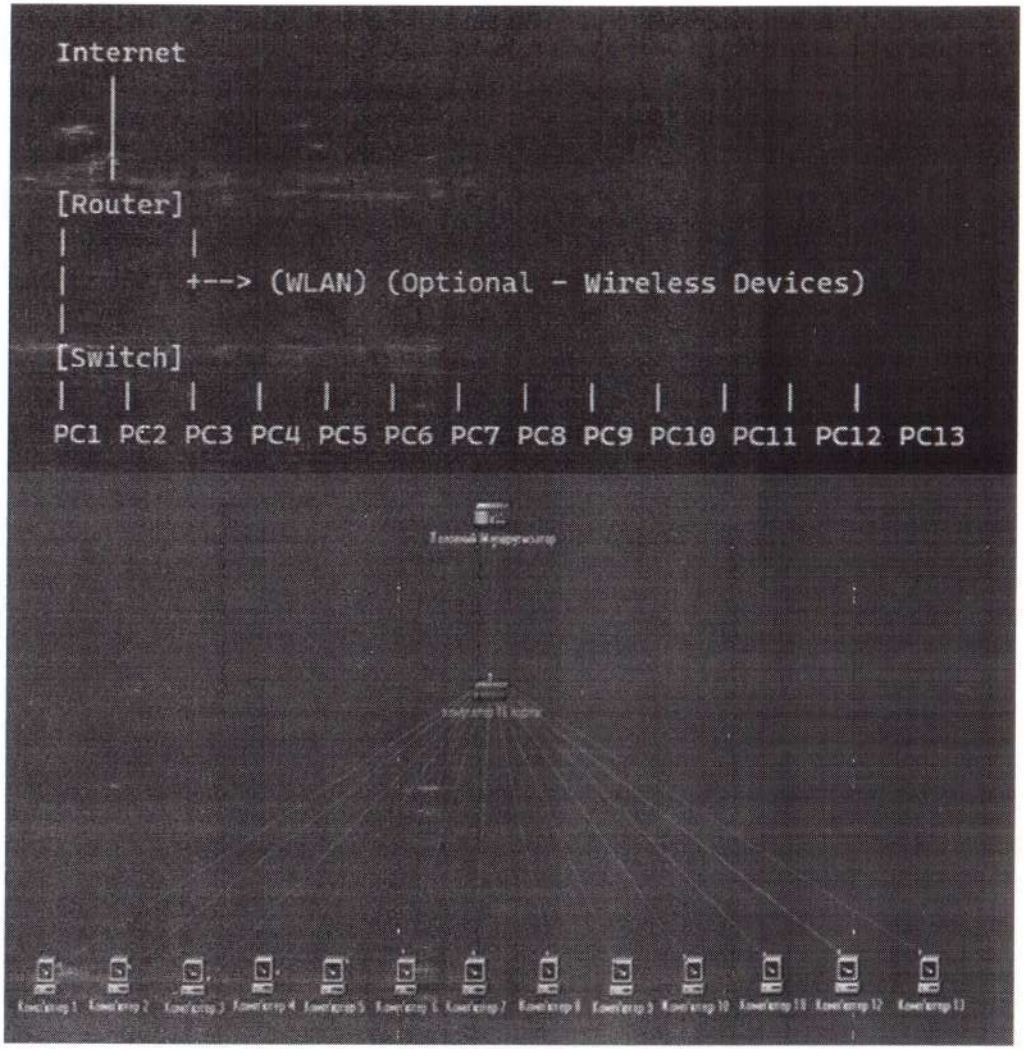

Рисунок 1. Загальна функціональна схема системи (мережі) ОІІ

9

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

(У цьому розділі надається стислий опис роботи системи (мережі) ОІІ. 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)

Маршрутизатор є центральним вузлом, а свіч розподіляє з'єднання попри всі пристрої. 13 робочих станцій (комп'ютерів) Всі комутації виконані за допомогою кабелю (вита пара). Маршрутизатор роздає WI-FI мережу в межах робочого кабінету. WI-FI мережа запаролена.

3. Проектні загрози

Таблиця 4. 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	Кіберінцидент	Порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах

4. Загальний порядок реагування на кібератаки/кіберінциденти

Порядок реагування здійснюється відповідно до наказу Держспецзв'язку від 03.07.2023 № 570 «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»

5. План кіберзахисту ОІІ

КНП «ОПЛ №4№»ООР»

(вказати назву ОІІ)

Таблиця 5. План кіберзахисту ОІІ 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 або посадова особа повинні бути підпорядковані безпосередньо керівнику ОКІ.**	Реалізовано	Наказ вид 16 лютого 2023 року № 27 про визначення відповідального за забезпечення кібербезпеки КНП"ОПЛ 4"ООР"	Галат Ігор Володимирович	постійно	-
3	**Забезпечити належну взаємодію**	-	-	-	-	-

№ 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)
	підрозділів ІТ та кіберзахисту					
4	**Опрацювати вплив відомих вразливостей**	Реалізовано	проведено інструктаж серед працівників КНП"ОПЛ 4"ООР"	Галат Ігор Володимирович	постійно	-
5	**Залучити сторонню організацію для проведення незалежного аудиту інформаційної безпеки**	-	-	-	-	-
6	**Затвердити політику управління інцидентами кібербезпеки**	Реалізовано	Відповідно до наказу Держспецзв'язку від 03.07.2023 № 570	Галат Ігор Володимирович	постійно	Відповідно до наказу Держспецзв'язку від 03.07.2023 № 570
7	**Забезпечити реагування на інформування постачальниками про виявлені ними вразливості**	Реалізовано	-	Галат Ігор Володимирович	постійно	-
8	**Затвердити вимоги до забезпечення інформаційної безпеки під час взаємодії з постачальниками**	Реалізовано	-	Остапенко Олександр Вячеславович адміністратор системи	постійно	-

Таблиця 6. 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)**	Реалізовано	-	Остапенко Олександр Вячеславович адміністратор системи	постійно	-
2	**Забезпечити використання надійних паролів**	Реалізовано	-	Остапенко Олександр Вячеславович адміністратор системи	постійно	-
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**	Реалізовано	-	Остапенко Олександр Вячеславович адміністратор системи	постійно	-

	функціональністю засобів мережевого захисту					
7	**Забезпечити виявлення невдалих спроб входу в систему 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**	Реалізовано	-	Галат Ігор Володимирович	постійно	-
10	**Запровадити додаткове навчання з кібербезпеки для персоналу підрозділу кіберзахисту**	Реалізовано		Галат Ігор Володимирович	постійно	-
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**	Реалізовано	-	Остапенко Олександр Вячеславович адміністратор системи	постійно	-
13	**Забезпечити захищеність електронної пошти від спуфінгу, фішингу та перехоплення повідомлень**	**Реалізовано**	-	Остапенко Олександр Вячеславович адміністратор системи	постійно	-
14	**Вимкнути встановлені за замовчуванням макроси та інший програмний код**	-	-	-	-	-

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**	Реалізовано	-	Остапенко Олександр Вячеславович адміністратор системи	постійно	-
19	**Затвердити, регулярно тестувати та вносити зміни до планів реагування на кіберінциденти**	Реалізовано	Відповідно до наказу Держспецзв'язку від 03.07.2023 № 570	Галат Ігор Володимирович	постійно	-
20	**Забезпечити збір журналів (логів) реєстрації подій**	-	-	-	-	-
21	**Забезпечити безпечне 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**	Реалізовано	-	Галат Ігор Володимирович	постi-йно	-

Таблиця 7. План кіберзахисту ОІІ 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 8. План кіберзахисту ОІІ 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**	Реалізовано	Відповідно до наказу Держспецзв'язку від 03.07.2023 № 570	-	постійно	-
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 9. План кіберзахисту ОІІ 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	реалізовано	Відповідно до наказу Держспецзв'язку від 03.07.2023 № 570	Галат Ігор Володимирович	постійно	-

Відповідальна особа за заповнення форми:
Посада Відповідальна особа за забезпечення кібербезпеки

Ігор ГАЛАТ
ПІБ

24. 02.2025 року