ЗАТВЕРДЖЕНО
Наказом ДП "УСС"
від __ _____ 2026 р. № ___
(в редакції наказу ДП "УСС"
від __ _____ 2026 р. № __)

Телекомунікаційна система ERP/1
«Повний набір сервісів»

ЦІЛЬОВИЙ ПРОФІЛЬ БЕЗПЕКИ

UA.47850061.СЗІ.ДП-40

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
1. УПРАВЛІННЯ ДОСТУПОМ (AC)				
1	Управління обліковими записами	a. Визначити та задокументувати типи облікових записів системи, дозволених для використання в ІС для підтримки цілей, завдань, функцій і процесів організації. b. Призначити менеджерів облікових записів для управління системними обліковими записами. c. Створити умови для групового та рольового членства. d. Визначити авторизованих користувачів інформаційної системи, членство в групі та ролі, а також дозволи доступу (наприклад, привілеї) та інші атрибути (за потреби) для кожного облікового запису. e. Вимагати схвалення [Призначення: визначеною організацією відповідальною особою або роллю] запитів на створення облікових записів системи. f. Створювати, активувати, змінювати, деактивувати та видаляти системні облікові записи відповідно до [Призначення: визначених організацією політики, процедур та умов]. g. Впровадити моніторинг використання облікових записів системи. h. Повідомляти адміністраторів облікових записів у межах [Призначення: визначеного організацією часового періоду для кожної ситуації]: 1. коли облікові записи більше не потрібні; 2. коли користувачі звільнені чи переведені; 3. коли використовуються індивідуальні системи або наявні зміни, які потребують нових знань. i. Авторизувати доступ до системи на основі: 1. Дійсної авторизації доступу. 2. Передбачуваного використання системи. 3. Інших атрибутів, що вимагаються організацією. j. Проводити перегляд облікових записів на відповідність вимогам управління обліковими записами з [Призначення: визначеною організацією частотою]. k. Впровадити процес повторного випуску облікових даних спільного/групового облікового запису (якщо він буде розгорнутий), коли особи виходять з групи. l. Узгодити процеси управління обліковими записами з процесами звільнення та переводу (передачі повноважень) персоналу.	AC-2	Система забезпечує створення, активацію, зміну та видалення облікових записів відповідно до політик організації. Права доступу жорстко прив'язані до ідентифікатора працівника ('subject_employee') або ролі. _____ Параметр: account_management Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
2	Примусове застосування доступу (Access Enforcement)	Застосовувати затверджені повноваження для логічного доступу до інформації та ресурсів системи відповідно до чинної політики (правил) управління доступом.	AC-3	Усі запити до ресурсів системи примусово проходять через Policy Decision Point (PDP) модуля ‘abac‘. Прямий доступ до даних в обхід механізмів авторизації заборонено архітектурно. Параметр: access_ enforcement Тип: boolean Значення: true
3	Принцип найменших привілеїв (Least Privilege)	Впровадити принцип мінімізації повноважень, який дозволяє користувачам (або процесам, що діють від імені користувачів) здійснювати лише такі авторизовані звернення, які необхідні для виконання визначених завдань відповідно до цілей (призначення, місії) організації та функцій.	AC-6	Профілі безпеки і ролі конфігуруються таким чином, що користувачам надаються лише ті привілеї, які необхідні для виконання їхніх посадових обов’язків. Механізм дозволів ‘abac‘ працює за принципом ’Default-Deny’. Параметр: least_ privilege Тип: boolean Значення: true
4	Блокування сеансу	a. Заборонити подальший доступ до системи шляхом ініціювання блокування пристрою після [Призначення: визначеного організацією періоду] бездіяльності або після отримання запиту від користувача. b. Зберігати блокування пристрою, поки користувач не відновить доступ, використовуючи встановлені процедури ідентифікації та автентифікації.	AC-11	Сеанс користувача автоматично блокується системою (‘synrc/n2o‘ session expiry) після визначеного періоду бездіяльності, вимагаючи повторної автентифікації. Параметр: session_ lock_timeout Тип: integer Значення: 900
5	Завершення сеансу	Сеанс користувача має завершуватися автоматично після [Призначення: визначених організацією умов або тригерних подій, що вимагають припинення сеансу].	AC-12	Користувач може ініціювати завершення сеансу (logout). Крім того, система примусово завершує сеанси при досягненні максимального часу життя токена або зміни контексту безпеки. Параметр: session_ termination Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
6	Дозволені дії без ідентифікації чи автентифікації	a. Визначити [Призначення: дозволені організацією дії користувачів], які можуть виконуватися в системі без ідентифікації або автентифікації відповідно до завдань та функцій організації. b. Документувати та визначити відповідне обґрунтування в плані безпеки системи дій користувача, які не потребують ідентифікації або автентифікації.	AC-14	Система явно визначає перелік відкритих сторінок та API-ендпойнтів (наприклад, портал входу або публічний довідник), доступних без автентифікації. Будь-які інші дії суворо заборонені. --- Параметр: permitted_ unauthenticated_ actions Тип: boolean Значення: true
7	Віддалений доступ	a. Встановити та задокументувати обмеження на використання, вимоги до конфігурації/підключення та рекомендації щодо здійснення кожного типу віддаленого доступу. b. Авторизувати віддалений доступ до системи, перш ніж будуть дозволені такі підключення.	AC-17	Віддалений доступ до системи керується додатковими політиками (наприклад, перевірка IP-адреси, VPN, mTLS), які інтегруються з ‘synrc/ca‘ та ‘abac‘ для забезпечення безпеки доступу за межами захищеного периметра. --- Параметр: remote_ access_control Тип: boolean Значення: true
8	АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ	a. Визначити засоби для асоціювання (пов’язання) [Призначення: визначених організацією типів атрибутів безпеки та приватності], що приймають [Призначення: визначені організацією значення атрибутів безпеки та приватності] з інформацією, яка зберігається, обробляється та/або передається. b. Пов’язані атрибути безпеки та приватності мають створюватися і зберігатися разом з інформацією. c. Встановити дозволені [Призначення: визначені організацією атрибути безпеки та приватності] для [Призначення: систем, визначених організацією]. d. Визначити дозволені [Призначення: визначені організацією значення або діапазони] для кожного з встановлених атрибутів безпеки та приватності. e. Проводити аудит змін атрибутів. f. Переглядати атрибути безпеки та приватності на відповідність з [Призначення: визначеною організацією частотою].	AC-16	Інформаційна система повинна підтримувати та динамічно пов’язувати визначені атрибути безпеки (мітки конфіденційності, ролі, посади, структурні підрозділи) з суб’єктами та об’єктами інформаційної взаємодії. Бібліотека ABAC реалізує стандарти ISO/IEC 29146:2016 та NIST SP 800-162, гарантуючи політику Zero Trust.

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
9	Динамічне пов'язання атрибутів (заборона кешування)		AC-16(1)	ABAC через компонент PIP (Policy Information Point) динамічно завантажує актуальні атрибути з контексту (наприклад, стан об'єкта 'object_process' чи профіль 'subject_employee' з KVS) безпосередньо в момент виконання запиту ('request'). Це гарантує, що рішення приймається на базі поточного, а не закешованого стану безпеки. --- Параметр: dynamic_binding Тип: boolean Значення: true
10	Зміна значень атрибутів авторизованими особами через PAP		AC-16(2)	Точка адміністрування PAP дозволяє уповноваженим адміністраторам (які пройшли перевірку PDP) змінювати правила ('rule'), політики ('policy') та кадрові атрибути співробітників, гарантуючи, що лише особи з належними повноваженнями можуть керувати системою доступу. --- Параметр: authorized_changes Тип: boolean Значення: true
11	Підтримка системою пов'язання атрибутів (KVS)		AC-16(3)	Інфраструктура бази даних 'synrc/kvs' нативно інтегрована з моделями 'abac.hrl'. Система зберігає зв'язки між суб'єктами та атрибутами на рівні записів (records), що не підлягають несанкціонованому перезапису. --- Параметр: attribute_binding_support Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
12	Пов'язання атрибутів авторизованими особами		AC-16(4)	Тільки уповноважені особи (з відповідними атрибутами безпеки) можуть створювати або делегувати повноваження (наприклад, призначати ролі 'assistant' або 'delegate' в моделі 'subject_employee'). --- Параметр: binding_ by_authorized_ individuals Тип: boolean Значення: true
13	Відображення атрибутів на пристроях виведення (nitro)		AC-16(5)	Завдяки інтеграції з 'synrc/nitro', рівні конфіденційності та безпекові атрибути об'єктів чітко рендеряться на інтерфейсі клієнта (веб-сторінках) у вигляді візуальних міток. --- Параметр: display_ attributes Тип: boolean Значення: true
14	Підтримка пов'язання атрибутів організацією (org, branch)		AC-16(6)	В 'subject_employee' підтримуються специфічні атрибути для ієрархічної структури (поля 'org', 'branch'), що дозволяє обчислювати доступ на основі приналежності до організаційної одиниці. --- Параметр: org_ binding_support Тип: boolean Значення: true
15	Послідовна інтерпретація атрибутів (XACML algorithms)		AC-16(7)	Використання стандартизованих алгоритмів комбінування політик XACML (алгоритми 'all' або 'any') у PDP гарантує строгу та несуперечливу математичну інтерпретацію безпекових обмежень по всій системі. --- Параметр: consistent_ interpretation Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
16	Техніки та технології пов'язання атрибутів (Pattern Matching, CA)		AC-16(8)	Механізми Pattern Matching платформи Erlang/OTP використовуються для швидкого та безпомилкового порівняння атрибутів. Інтеграція криптографічних підписів ('synrc/ca') у структуру об'єкта підтверджує автентичність його міток. --- Параметр: binding_ techniques Тип: boolean Значення: true
17	Перепризначення атрибутів згідно з життєвим циклом		AC-16(9)	Політики можуть передбачати логіку перепризначення атрибутів у процесі життєвого циклу об'єкта (наприклад, після підписання документа його атрибут статусу змінюється, що автоматично змінює правила доступу до нього). --- Параметр: attribute_ reassignment Тип: boolean Значення: true
18	Конфігурація атрибутів уповноваженими особами (PAP API)		AC-16(10)	Інфраструктура PAP надає API для гнучкого налаштування нових типів атрибутів і політик, гарантуючи, що ці налаштування виконуються тільки згідно встановлених процедур адміністрування. --- Параметр: authorized_ configuration Тип: boolean Значення: true
19	УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ	Застосувати затверджені повноваження для управління потоком інформації всередині системи та між пов'язаними системами на основі [Призначення: визначеними організацією політиками управління інформаційним потоком].	AC-4	Інформаційна система повинна забезпечувати виконання дозволів та заборон щодо передачі (руху) інформації. Бібліотека BPE (Business Process Engine) реалізує це через моделювання інформаційних потоків у стандарті BPMN 2.0.

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
20	Атрибути безпеки об'єкту		AC-4(1)	BPE перед будь-яким переходом до наступного кроку (‘bpe:next‘) аналізує атрибути (метадані, документи), прив'язані до процесу. Шлюзи перевіряють ці мітки для ухвалення рішень маршрутизації. --- Параметр: object_ security_attributes Тип: boolean Значення: true
21	Домени обробки (ізольовані процеси Erlang)		AC-4(2)	Кожен BPMN-процес виконується як окремий ізольований процес віртуальної машини Erlang (Actor). Ці процеси створюють незалежні безпекові домени обробки інформації без спільної пам'яті. --- Параметр: processing_domains Тип: boolean Значення: true
22	Управління інформаційним потоком (SequenceFlow)		AC-4(3)	Сутність ‘sequenceFlow‘ (ребра графу BPMN) математично обмежує єдині можливі шляхи передачі інформації між задачами. --- Параметр: enforce_ sequence_flow Тип: boolean Значення: true
23	Управління потоком зашифрованої інформації		AC-4(4)	BPE здатний маршрутизувати зашифровані payload-дані як непрозорі (opaque) структури, залишаючи розшифрування авторизованим клієнтам або конкретним сервісним завданням (‘serviceTask‘). --- Параметр: encrypted_payloads Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
24	Вбудовування типів даних (Erlang Records)		AC-4(5)	Об'єкти інформаційного потоку строго типізовані через структури ‘record‘ (наприклад, ‘#userTask{}‘, ‘#messageEvent{}‘). Це запобігає переміщенню невідомих форматів. --- Параметр: embedded_data_types Тип: boolean Значення: true
25	Метадані (список docs у BPE)		AC-4(6)	BPE керує метаданими документів, використовуючи внутрішній список ‘docs‘ (API ‘bpe:docs/1‘, ‘bpe:amend/2‘), що невідривно супроводжує потік процесу. --- Параметр: metadata_management Тип: boolean Значення: true
26	Механізми одностороннього потоку (DAG)		AC-4(7)	Направлені ациклічні графи (DAG) BPMN природно реалізують односторонню передачу даних від ‘beginEvent‘ до ‘endEvent‘ без можливості повернення (якщо це не передбачено схемою). --- Параметр: one_way_flow Тип: boolean Значення: true
27	Політики безпеки (Gateways)		AC-4(8)	Логічні шлюзи (‘gateway‘) виступають інтегрованими фільтрами, які застосовують політики безпеки на розгалуженнях потоку. --- Параметр: security_policies Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
28	Перевірки, що проводить персонал (UserTask)		AC-4(9)	Використання ‘#userTask{}‘ зупиняє автоматичний потік інформації та вимагає ручної перевірки (Human-in-the-loop) і підтвердження для продовження маршруту. ——— Параметр: personnel_ checks Тип: boolean Значення: true
29	Активація та деактивація фільтрів політики (BoundaryEvent)		AC-4(10)	Використання подій, як-от ‘boundaryEvent‘ (Boundary Events), дозволяє динамічно активувати обхідні гілки політик в залежності від виникнення інцидентів або таймаутів. ——— Параметр: filter_ activation Тип: boolean Значення: true
30	Конфігурація фільтрів політики безпеки (XML)		AC-4(11)	Правила маршрутизації (фільтри) завантажуються декларативно з BPMN XML файлів та транслюються у незмінні правила Erlang (‘bpe:load/1‘). ——— Параметр: filter_ configuration Тип: boolean Значення: true
31	Ідентифікатори типу даних (MessageEvent)		AC-4(12)	Система розрізняє вхідні повідомлення через обробку ‘messageEvent‘ з відповідними ідентифікаторами повідомлень, ігноруючи нерозпізнані сигнали. ——— Параметр: data_ type_identifiers Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
32	Декомпозиція на субкомпоненти (Call Activity)		AC-4(13)	BPE підтримує виклик підпроцесів (‘Call Activity‘), що дозволяє розбити складні потоки на ізольовані субкомпоненти зі своїми власними політиками. _____ Параметр: subcomponent_ decomposition Тип: boolean Значення: true
33	Обмеження фільтра політики (conditions)		AC-4(14)	Можливості маршрутизації обмежені набором умов ‘condition()‘, які дозволяють математично гарантувати неперетин потоків. _____ Параметр: policy_ filter_constraints Тип: boolean Значення: true
34	Виявлення несанкціонованої інформації		AC-4(15)	При спробі передати процесу повідомлення, яке не відповідає поточній стадії потоку (unauthorized message), система автоматично відкидає його або фіксує в лог як невалідний event. _____ Параметр: unauthorized_info_ detection Тип: boolean Значення: true
35	Передача інформації про взаємопов’язані системи (ServiceTask)		AC-4(16)	Компонент ‘#serviceTask{}‘ дозволяє інтегрувати механізми перевірки даних, перш ніж передати інформаційний потік до інших ІТС (наприклад, через API REST або RPC). _____ Параметр: interconnected_ systems_transfer Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
36	Прив'язка атрибуту безпеки (Process ID)		AC-4(18)	Інформація в рамках потоку жорстко прив'язується до Process ID (Id інстанції). Усі документи успадковують обмеження доступу поточного процесу. --- Параметр: security_attribute_binding Тип: boolean Значення: true
37	Перевірка метаданих (BPMN compare)		AC-4(19)	BPMN-умови підтримують функції типу '{compare, Field, ConstCheckAgainst}', що перевіряють значення конкретних метаданих об'єкта під час прийняття рішення про маршрут. --- Параметр: metadata_validation Тип: boolean Значення: true
38	Затверджені рішення (Default-Deny)		AC-4(20)	Erlang Match Specifications та XACML гарантують, що лише явно затверджені алгоритми маршрутизації виконуються (Default-Deny принцип). --- Параметр: approved_decisions Тип: boolean Значення: true
39	Фізичне та логічне відділення інформаційних потоків		AC-4(21)	Логічне відділення гарантується механізмом процесів OTP VM. Можливість виконання різних процесів на різних фізичних нодах Erlang-кластера забезпечує фізичне відділення потоків. --- Параметр: physical_logical_separation Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
40	Єдиний доступ (bpe:next)		AC-4(22)	Централізований компонент контролю ‘bpe:next‘ слугує єдиною точкою (Choke Point) доступу та маршрутизації для всіх інформаційних потоків. --- Параметр: single_ access_point Тип: boolean Значення: true
41	Модифікована інформація, яка не підлягає оприлюдненню (scrubbing)		AC-4(23)	При поверненні історії та статусів через API клієнту, BPE може відфільтровувати та очищати внутрішні атрибути (‘scrubbing‘), не допускаючи витоку чутливої інформації. --- Параметр: scrub_ hidden_fields Тип: boolean Значення: true
42	Нормалізований формат (BPE Record)		AC-4(24)	Весь внутрішній потік конвертується в уніфікований стандартизований формат (‘BPE Record Format‘), незалежно від того, як дані надійшли на вході. --- Параметр: normalized_format Тип: boolean Значення: true
43	Очищення даних (Garbage Collection, End Event)		AC-4(25)	Вбудовані механізми Garbage Collection віртуальної машини Erlang та знищення об’єктів пам’яті ізольованого процесу після завершення (‘End Event‘) забезпечують очищення даних з ОЗУ. --- Параметр: data_ sanitization Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
44	Дії з фільтрації аудиту (hist у KVS)		AC-4(26)	Кожен крок і зміна маршруту фіксується у вигляді об'єкта ‘hist‘ у ‘kvs‘, створюючи прозорий ланцюг подій, де шлюзи та фільтри залишають свій слід. ——— Параметр: audit_ filter_actions Тип: boolean Значення: true
45	Незалежні фільтруючі механізми (ABAC + BPE)		AC-4(27)	Дозвіл на доступ (ABAC) та перевірка логіки процесу (BPE) працюють як архітектурно незалежні механізми, підсилюючи концепцію "Defense-in-depth". ——— Параметр: independent_filtering Тип: boolean Значення: true
46	Лінійні фільтрувальні канали (Linear Pipeline)		AC-4(28)	BPE підтримує лінійну маршрутизацію (Linear Pipeline), коли ‘SequenceFlow‘ гарантовано не має відгалужень, забезпечуючи послідовне виконання політик без ризику обходу. ——— Параметр: linear_ pipelines Тип: boolean Значення: true
47	Механізми оркестровки		AC-4(29)	Ядро BPE виступає єдиним централізованим механізмом оркестровки інформаційного обміну в рамках системи. ——— Параметр: orchestration_ mechanisms Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
48	Фільтрація з використанням кількох процесів (Parallel Gateway)		AC-4(30)	Компонент ‘Parallel Gateway‘ (‘#gateway{type=parallel}‘) створює декілька паралельних потоків, кожен з яких може мати власні незалежні правила фільтрації. _____ Параметр: multi_ process_filtering Тип: boolean Значення: true
49	Запобігання передачі вмісту		AC-4(31)	Якщо інформаційний об’єкт не відповідає політиці (фільтр на Gateway відхилив вміст), процес переривається або спрямовується на подію помилки (Error Event). _____ Параметр: content_ transfer_prevention Тип: boolean Значення: true
50	Вимоги до процесу передачі інформації (Receive/Send Task)		AC-4(32)	Механізми ‘Receive Task‘ та ‘Send Task‘ строго декларують вимоги до структури payload-повідомлень перед тим, як дозволити зовнішній чи внутрішній обмін. _____ Параметр: transfer_ process_requirements Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
2. ОБІЗНАНІСТЬ ТА НАВЧАННЯ (AT)				
51	Навчання з обізнаності щодо безпеки	Впровадити базові тренінги з підвищення обізнаності у сфері безпеки та приватності для користувачів системи (включно з менеджерами, керівниками компаній і підрядниками): a. Забезпечити навчання грамотності з питань безпеки та конфіденційності для користувачів системи (включаючи менеджерів, керівників вищої ланки та підрядників): 1. як частину початкового навчання для нових користувачів і [Призначення: частота, визначена організацією] після цього; 2. якщо цього потребують системні зміни або наступні [Призначення: події, визначені організацією]. b. Використовувати наведені нижче методи, щоб підвищити рівень безпеки та конфіденційності користувачів системи [Завдання: визначені організацією методи поінформованості]; c. Оновлювати навчання грамотності та зміст обізнаності [Завдання: частота, визначена організацією] і наступні [Завдання: події, визначені організацією]; d. Включити уроки, отримані з внутрішніх або зовнішніх інцидентів безпеки або порушень, у навчання грамотності та методи підвищення обізнаності.	AT-2	Програми навчання та інструктажі (див. розділ AT у digital-profile.pdf). _____ Параметр: security_ awareness_training_ ref Тип: string Значення: digital-profile.pdf
52	Навчання з питань безпеки, залежне від ролі	a. Забезпечити проведення навчання з питань безпеки та приватності на основі ролей для працівників з ролями та обов'язками: [Призначення: визначені організацією ролі та обов'язки]: 1. перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків і [Призначення: частота, визначена організацією] після цього; 2. коли цього потребують системні зміни. b. Оновити навчальний контент на основі ролей [Призначення: частота, визначена організацією] і наступні [Призначення: події, визначені організацією]; c. Включіть у рольове навчання, інформацію, отриману з внутрішніх або зовнішніх інцидентів та порушень безпеки.	AT-3	Спеціалізоване навчання для адміністраторів (див. розділ AT у digital-profile.pdf). _____ Параметр: role_ based_training_ref Тип: string Значення: digital-profile.pdf
3. АУДИТ ТА ПІДЗВІТНІСТЬ (AU)				
53	Узагальнення записів про аудит з декількох джерел (feeds)		AU-2(1)	BPMN підтримує паралельні ланцюги (feeds, streams), що дозволяє агрегувати записи про аудит з декількох джерел у єдиний потік журналу. _____ Параметр: audit_ aggregation Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
54	Перегляд та оновлення (індексація hist)		AU-2(3)	Записи аудиту періодично індексуються, що дозволяє швидко витягувати всю історію (наприклад, через ‘bpe:hist/1‘). Параметр: audit_review_update Тип: boolean Значення: true
55	Зміст записів аудиту (метадані, Permit/Deny)	Переконатися, що записи аудиту містять інформацію, яка встановлює наступне: a. який тип події стався; b. коли відбулася подія; c. де відбулася подія; d. джерело події; e. наслідки події; f. результат події та ідентифікатор будь-яких осіб або суб’єктів, пов’язаних з подією.	AU-3	Інформація в логах BPMN (особливо при збереженні об’єктів BPE/ABAC) містить вичерпні метадані: тип події, суб’єкт, цільовий об’єкт, результат операції (Permit/Deny) та позначку часу, що повністю закриває вимоги AU-3. Параметр: audit_content_metadata Тип: boolean Значення: true
56	Місткість сховища записів аудиту (розподілені бекенди)	Розподіляти місткість сховища записів аудиту у відповідності до [Призначення: визначених організацією вимог до зберігання записів аудиту].	AU-4	BPMN може використовувати розподілені бекенди (Riak KV, розподілена Mnesia, KAI), що дозволяє горизонтально масштабувати місткість сховища логів (AU-4) без зупинки системи. Параметр: audit_storage_capacity Тип: boolean Значення: true
57	Позначка часу (erlang:system_time)		AU-8(1)	Усі ідентифікатори та події, що генеруються в BPMN (наприклад, через генератор ‘id_seq‘), прив’язані до високоточного системного часу Erlang (‘erlang:system_time/1‘). Це забезпечує надійну прив’язку подій до точного часу (AU-8(1)). Параметр: sync_time_source Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
58	Апаратні носії одноразового запису (Append-Only)		AU-9(1)	Архітектура Append-Only гарантує, що записи не оновлюються (no UPDATE). Це створює ефект апаратного "Write-Once-Read-Many" (AU-9(1)). Видалити запис без порушення криптографічної чи логічної цілісності ланцюга посилань практично неможливо. --- Параметр: append_only_enforced Тип: boolean Значення: true
59	Неспростовність (Ланцюжок збереження доказів)		AU-10(3)	Журнали BPMN слугують доказовою базою (Ланцюжок збереження доказів AU-10(3)). У комбінації з ‘synrc/ca‘ записи можуть підписуватися ЕЦП (AU-10(5)), що гарантує 100% неспростовність дій автора транзакції. --- Параметр: non_repudiation Тип: boolean Значення: true
60	Довгострокова можливість отримання записів аудиту		AU-11(1)	Сховища типу RocksDB (в якості бекенда BPMN) оптимізовані для довгострокового зберігання петабайтів даних (Long-Term Storage) із забезпеченням швидкого доступу до історичних записів (AU-11(1)). --- Параметр: log_retention_days Тип: integer Значення: 1825

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
61	Огляд, аналіз та звітність про аудит	a. Переглядати та аналізувати записи системного аудиту [Призначення: з визначеною організацією частотою] для виявлення [Призначення: визначеної організацією неналежної або незвичайної діяльності]. b. Відправляти звіт про аудит [Призначення: визначеним організацією персоналу або посадам]. c. Налаштувати рівні огляду аудиту, аналізу та звітності в рамках системи, коли змінюється рівень ризику на основі інформації від правоохоронних органів, розвідувальної інформації або від інших достовірних джерел інформації.	AU-6	Аналіз аудиту відбувається за допомогою консольних інструментів платформи (наприклад, ‘kvs:hist/1‘ або інтерфейсів Erlang Shell). Також доступний експорт журналів для SIEM. _____ Параметр: audit_analysis_tools Тип: boolean Значення: true
62	Генерація аудиту	a. Забезпечити генерацію даних аудиту для типів подій, що перевіряються в AU-2a в [Призначення: визначених організацією компонентах системи]. b. Дозволити [Призначення: визначеному організацією персоналу або посадам] вибирати, які типи подій, що перевіряються, повинні перевірятися окремими компонентами системи; c. Генерувати записи аудиту для типів подій, визначених в AU-2c. з вмістом згідно з AU-3.	AU-12	KVS забезпечує генерацію записів аудиту для всіх операцій створення, оновлення (через створення нової ревізії) та видалення, гарантуючи фіксацію критичних подій безпеки. _____ Параметр: audit_generation Тип: boolean Значення: true
4. УПРАВЛІННЯ КОНФІГУРАЦІЄЮ (CM)				
63	Базова конфігурація (Baseline Configuration)	a. Розробити, задокументувати та підтримувати за допомогою заходів конфігурації поточні базові налаштування системи. b. Переглядати та оновлювати базові налаштування системи: 1. з [Призначення: визначеною організацією частотою]; 2. за потреби внаслідок [Призначення: визначених організацією обставин]; 3. коли встановлені нові або оновлені компоненти системи.	CM-2	Файл ‘erpuno.ex‘ фіксує єдину базову конфігурацію (Baseline) безпеки для всієї системи. Зміни в конфігурації застосовуються виключно через оновлення коду, що забезпечує строгий контроль та аудит змін. _____ Параметр: baseline_configuration_code Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
64	Контроль змін конфігурації	a. Визначити типи змін у системі, які контролюються конфігурацією. b. Переглядати запропоновані зміни в конфігурації, контрольовані системою, і схвалити або відхилити ці зміни з явним урахуванням аналізу наслідків безпеки. c. Документувати рішення зі зміни конфігурації системи. d. Впровадити схвалені зміни конфігурації в систему. e. Зберігати записи змін конфігурації системі впродовж [Призначення: певного періоду часу, визначеного організацією]. f. Здійснювати моніторинг і аналіз дій, пов'язаних зі змінами конфігурації системи. g. Координувати та впроваджувати нагляд за діяльністю з управління змінами конфігурації за допомогою [Призначення: елементу управління змінами конфігурації, визначеного організацією], який викликається [Вибір (один або кілька): [Призначення: з визначеною організацією частотою]; [Призначення: визначені організацією умови зміни конфігурації]].	CM-3	Оскільки CMDB є частиною вихідного коду (Elixir модуль), всі зміни проходять через стандартний процес розробки (Code Review, CI/CD, контроль версій Git), унеможливлюючи несанкціоноване втручання в налаштування на "живій" системі. --- Параметр: configuration_ change_control Тип: boolean Значення: true
65	Налаштування конфігурації	a. Встановити та задокументувати параметри конфігурації компонентів, які застосовуються в системі, які відображають найбільш обмежений режим, що відповідає експлуатаційним вимогам, використовуючи [Призначення: визначені організацією загальні безпечні конфігурації]. b. Реалізувати конфігураційні установки. c. Визначити, задокументувати та затвердити будь-які відхилення від встановлених конфігураційних параметрів конфігурації для [Призначення: визначених організацією компонентів системи] на основі [Призначення: визначених організацією експлуатаційних вимог]. d. Відстежувати та керувати змінами конфігураційних параметрів відповідно до організаційної політики та процедур.	CM-6	Параметри політик безпеки та їхні значення за замовчуванням жорстко зашиті в ‘erpuno.ex‘. Компілятор генерує незмінний об'єктний файл, який гарантує виконання затверджених налаштувань під час роботи. --- Параметр: compile_ time_config Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
66	Інвентаризація компонентів ІТС	a. b. Розробити та задокументувати процес інвентаризації компонентів системи, який: 1. точно описує поточну систему; 2. охоплює всі компоненти в межах акредитації системи; 3. не включає повторний облік компонентів або компонентів, будь-якої іншої системи; 4. визначає рівень деталізації, який є необхідним для відстеження та звітування; 5. включає інформацію для досягнення підзвітності компонентів системи: [Призначення: визначена організацією інформація, необхідна для досягнення ефективної підзвітності компонентів системи]. Переглядати та оновлювати опис компонентів системи з [Призначення: визначеною організацією частотою].	CM-8	Профіль автоматично фіксує перелік використовуваних компонентів системи (бібліотеки ‘synrc/kvs‘, ‘synrc/ca‘ тощо) та їхні параметри, забезпечуючи інтегральну інвентаризацію модулів захисту. ——— Параметр: component_inventory Тип: boolean Значення: true
67	План управління конфігурацією	Унікально ідентифікувати та автентифікувати користувачів або процеси, що діють від імені користувачів.	CM-9	Профіль ‘ERPUNO.Profile‘ слугує самодокументованим планом управління конфігураціями, здатним автоматично генерувати актуальну документацію (через метод ‘generate_md/0‘). ——— Параметр: auto_generate_documentation Тип: boolean Значення: true
5. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (IA)				
68	Ідентифікація та автентифікація (організаційні користувачі)	Користувачі унікально ідентифіковані та автентифіковані;.	IA-2	Система однозначно ідентифікує та автентифікує (перевіряє справжність) організаційних користувачів та процеси, що діють від їх імені, перед тим, як дозволити їм доступ до захищених ресурсів. ——— Параметр: org_user_auth Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
69	Ідентифікація та автентифікація (неорганізаційні користувачі)	Унікально ідентифіку ються та автентифікуються користувачі, що не належать до організації або процеси (що не належать організації), які діють від імені користувачів.	IA-8	Зовнішні користувачі, що підключаються з публічних мереж, проходять сувору автентифікацію (наприклад, за допомогою mTLS або інтеграції з КЕП) для запобігання анонімному або підробленому доступу. --- Параметр: non_org_ user_auth Тип: boolean Значення: true
70	Автентифікація на основі пароля (хешування)		IA-5(1)	Для паролів чи PING-кодів (наприклад, для розблокування контейнерів PKCS#12) використовуються криптостійкі функції хешування з сіллю для запобігання атакам. --- Параметр: password_ based_auth Тип: boolean Значення: true
71	Автентифікація на основі відкритого ключа		IA-5(2)	Є основним профілем бібліотеки ‘ca‘. Вона генерує, перевіряє (validate) та керує життєвим циклом інфраструктури відкритих ключів (X.509), забезпечуючи строгу автентифікацію. --- Параметр: pki_ enabled Тип: boolean Значення: true
72	Зміна автентифікаторів до доставки (CSR)		IA-5(5)	Система підтримує протоколи, за яких приватний ключ генерується на пристрої клієнта, а до CA відправляється лише Certificate Signing Request (CSR). Це гарантує зміну/встановлення ключів ще до факту доставки готового сертифіката користувачу. --- Параметр: pre_ delivery_change Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
73	Захист автентифікаторів (PEM/PKCS#12)		IA-5(6)	Приватні ключі (автентифікатори) зберігаються в захищеному зашифрованому вигляді (наприклад, контейнери формату PEM з паролем або PKCS#12), що унеможливлює використання ключів без знання пароля доступу. --- Параметр: authenticator_ protection Тип: boolean Значення: true
74	Відсутність вбудованих незашифрованих статичних автентифікаторів		IA-5(7)	Бібліотека заохочує динамічну генерацію ключів під час ініціалізації середовища (Root CA), що виключає необхідність зберігання "hardcoded" секретів у вихідному коді системи. --- Параметр: no_ unencrypted_static Тип: boolean Значення: true
75	Багатосистемні облікові записи (mTLS/SSO)		IA-5(8)	Сертифікати X.509, видані ‘synrc/ca‘, можуть використовуватись як багатосистемний засіб автентифікації (на кшталт mTLS/SSO) для доступу до різноманітних мікросервісів та ERP-компонентів, розгорнутих у спільному домені довіри. --- Параметр: multi_ system_accounts Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
76	Управління об'єднанням автентифікаторів (Intermediate CA)		IA-5(9)	Підтримується архітектура федерації ключів (Federation) за рахунок використання ланцюгів сертифікатів (Intermediate CAs) та можливості перевіряти крос-сертифікаційні підписи (Cross-Certification). --- Параметр: federation_ management Тип: boolean Значення: true
77	Динамічне зв'язування мандатів		IA-5(10)	Бібліотека дозволяє видавати короткострокові сертифікати, що динамічно зв'язуються з конкретною сесією, IP-адресою чи атрибутами користувача (Dynamic Credential Binding). --- Параметр: dynamic_ credential_binding Тип: boolean Значення: true
78	Автентифікація на основі апаратних токенів		IA-5(11)	'synrc/ca' прозоро підтримує роботу з підписами, згенерованими на апаратних захищених носіях (Hardware Tokens, HKI, e-Токени, PKCS#11). Серверній частині потрібен лише відкритий ключ для валідації. --- Параметр: hardware_ token_auth Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
79	Ефективність біометричної автентифікації (Secure Enclave)		IA-5(12)	Хоча ‘ca‘ працює з криптографією, будь-яка біометрична автентифікація (наприклад, TouchID, FaceID) на клієнті конвертується в криптографічний підпис (наприклад, через Secure Enclave), який успішно валідується модулями ‘synrc/ca‘. --- Параметр: biometric_ efficiency Тип: boolean Значення: true
80	Закінчення терміну дії автентифікаторів (NotBefore/NotAfter)		IA-5(13)	Жорстко перевіряються поля ‘NotBefore‘ та ‘NotAfter‘ в сертифікатах X.509. Сертифікати зі строком дії, що минув, автоматично відхиляються без можливості оскарження. --- Параметр: authenticator_ expiration Тип: boolean Значення: true
81	Управління змістом довірчих сховищ (Trust Stores)		IA-5(14)	На рівні сервера бібліотека керує сховищем довірених кореневих сертифікатів (Trust Store, ‘priv/cacerts‘). Оновлення або відкликання (через CRL) довіри до Root CA автоматично реплікується на політику доступу. --- Параметр: trust_ store_management Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
82	Продукти та послуги, затверджені уповноваженим органом (ДСТУ 4145-2002)		IA-5(15)	Завдяки абстракції криптографічних примітивів, ‘synrc/ca‘ підтримує державні криптографічні стандарти (наприклад, алгоритм цифрового підпису ДСТУ 4145-2002), необхідні для побудови систем, затверджених Державною службою спеціального зв’язку та захисту інформації (ДССЗЗІ). ——— Параметр: approved_ products Тип: boolean Значення: true
83	Передача довірчої автентифікації зовнішньої сторони (АЦСК)		IA-5(16)	‘synrc/ca‘ здатна перевіряти підписи, накладені зовнішніми Акредитованими центрами сертифікації ключів (АЦСК), забезпечуючи довірчу автентифікацію зовнішніх сторін. ——— Параметр: external_ auth_transfer Тип: boolean Значення: true
84	Менеджер паролів (KeyStores)		IA-5(18)	Незважаючи на те, що ‘synrc/ca‘ не є менеджером паролів у звичному розумінні, механізми захисту ключів (KeyStores, PKCS#12) виступають у ролі захищених криптографічних сейфів, які можна відкрити лише спеціалізованими засобами із дотриманням секретності. ——— Параметр: password_ manager Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
6. РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR)				
85	Навчання з реагування на інциденти	a. Забезпечити навчання користувачів щодо системи реагування на інциденти, відповідно до призначених ролей та обов'язків: 1. у рамках [Призначення: визначеного організацією періоду часу], впродовж якого авторизована роль або відповідальність за реагування на інциденти; 2. у разі внесення змін у систему; 3. з визначеною [Призначення: визначена організацією частота] у подальшому. b. Переглядайте та оновлюйте навчальний контент із реагування на інциденти [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією].	IR-2	Інтерфейс 'erpuno/itsm' надає контекстні підказки та інструкції безпосередньо у формах обробки інцидентів, що виконує функцію інтерактивного навчання та підтримки персоналу в кризових ситуаціях. _____ Параметр: incident_response_training Тип: boolean Значення: true
86	Тестування реагування на інциденти	Перевіряти ефективність реагування системи на інциденти [Призначення: з визначеною організацією частотою] за допомогою [Призначення: визначених організацією тестів].	IR-3	Можливості BPE-движка дозволяють запускати симуляції інцидентів у тестовому середовищі 'itsm' для регулярного тестування планів реагування без впливу на продуктивну систему. _____ Параметр: incident_testing_simulation Тип: boolean Значення: true
87	Обробка інцидентів	a. Впровадити можливості обробки інцидентів безпеки та приватності, включно з підготовкою, виявленням і аналізом, локалізацією, ліквідацією та відновленням. b. Координувати діяльність з обробки інцидентів із заходами із забезпечення безперервності функціонування. c. Включити засвоєні уроки від поточних дій з обробки інцидентів до процедур реагування, навчання та перевірки інцидентів і реалізувати відповідні зміни. d. Встановлюйте строгість заходів з обробки інцидентів у порівнянній та передбачуваній формі в межах всієї організації.	IR-4	Будь-який інцидент безпеки автоматично реєструється як тикет у модулі 'itsm'. Процес обробки ('incident_management_process') гарантує, що інцидент пройде всі необхідні етапи: виявлення, ізоляція, усунення, відновлення. _____ Параметр: incident_handling Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
88	Моніторинг інцидентів	Відстежувати та документувати інциденти безпеки та приватності.	IR-5	Статуси інцидентів у реальному часі відображаються на дашбордах ‘erpuno/itsm‘. BPE-движок дозволяє призначати SLA-таймаути (Boundary Events) для ескалації інцидентів, якщо час реакції перевищено. _____ Параметр: incident_ monitoring Тип: boolean Значення: true
89	Звітність про інциденти	a. Вимагати від персоналу повідомляти про підозрілі інциденти з безпеки та приватності відповідно до організаційної спроможності реагування на інциденти впродовж [Призначення: визначеного організацією періоду часу]. b. Звітувати про інциденти безпеки, приватності та ланцюжки постачання в [Призначення: визначений організацією уповноважений орган].	IR-6	Система ‘erpuno/itsm‘ автоматично формує звіти про інциденти, надаючи вичерпну інформацію про порушені сервіси, час простою (SLA) та дії команди, що закриває вимоги внутрішньої та зовнішньої звітності. _____ Параметр: automated_incident_ reporting Тип: boolean Значення: true
90	Допомога у реагуванні на інциденти	Надавати ресурси для підтримки реагування на інциденти, що є невіддільною частиною спроможностей організації реагування на інциденти, які являють собою поради та допомогу користувачам інформаційної системи для обробки та формування звітності про інциденти безпеки та приватності.	IR-7	Вбудовані засоби комунікації в рамках тикету (коментарі, призначення експертів, інтеграція з базою знань) забезпечують оперативну допомогу та координацію групи безпеки під час інциденту. _____ Параметр: incident_ assistance Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
91	План реагування на інциденти	a. Розробити план реагування на інциденти, який: 1. надає організації дорожню карту для впровадження її можливостей реагування на інциденти; 2. описує структуру та організацію спроможності реагування на інциденти; 3. надає високорівневий підхід до того, як здатність реагування на інциденти вписується в загальну практику організації; 4. відповідає вимогам керівництва організації; 5. визначає інциденти, що вимагають звітування, а також метрики для їх вимірювання в організації; 6. визначає ресурси й керівні принципи управління, необхідні для ефективного функціонування та підтримки спроможності реагування на інциденти. b. Розповсюдити копії плану реагування на інциденти [Призначення: серед визначеного організацією персоналу або ролей]. c. Переглядати план реагування на інциденти [Призначення: з визначеною організацією частотою]. d. Оновлювати план реагування на інциденти для розв'язання проблем із системою й організацією під час перевірок та реагування. e. Повідомляти про зміни у плані реагування на інциденти [Призначення: визначеному організацією персоналу або ролям]. f. Захищати план реагування на інциденти від несанкціонованого розголошення та зміни.	IR-8	Сам конфігураційний код процесів 'erpuno/itsm' виступає в ролі актуального та виконуваного плану реагування на інциденти (Executable Incident Response Plan), усуваючи розбіжність між документацією та реальністю. --- Параметр: executable_ir_plan Тип: boolean Значення: true
92	Реагування на витік інформації (Information Spillage)	<IR-09_ODP[01] персонал або ролі> призначено відповідальним за реагування на витоки інформації;.	IR-9	Спеціалізовані BPMN-схеми в 'itsm' передбачені для обробки витоків інформації. Вони включають обов'язкові кроки ідентифікації скомпрометованих даних, блокування доступу ('abac') та сповіщення регулятора. --- Параметр: information_spillage_response Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
7. ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ (MP)				
93	Доступ до носіїв інформації (через Erlang VM)		MP-2(1)	Прямий доступ до файлів БД (RocksDB/Mnesia) на носіях закритий на рівні ОС. Весь логічний доступ здійснюється виключно через інтерфейс KVS всередині віртуальної машини Erlang, яка діє як обмежений шлюз доступу (MP-2(1)). --- Параметр: os_level_access_control Тип: boolean Значення: true
94	Криптографічний захист носіїв (Data-at-Rest)		MP-4(1)	KVS підтримує політики постійного збереження даних на диск (Disk Persistence). Захист інформації в стані спокою (Data-at-Rest) реалізується через інтеграцію з шифруванням файлової системи (LUKS) або шифруванням значень (MP-4(1)). --- Параметр: encryption_at_rest Тип: boolean Значення: true
95	Транспортування носіїв інформації (TLS-реплікація)		MP-5(1)	В розподіленому кластері KVS реплікує дані (переміщує їх) між нодами. Цей процес транспортування інформації захищається за допомогою TLS (Erlang Distribution over TLS), запобігаючи перехопленню даних поза контрольованими зонами (MP-5(1), MP-5(4)). --- Параметр: tls_replication Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
96	Знищення інформації на носіях (Tombstones)		MP-6(8)	Хоча KVS є системою Append-Only, він надає чіткі API (‘kvs:delete‘) для виконання процедур очищення даних (наприклад, для забезпечення вимог GDPR "Право на забуття"). Під час видалення запису, бекенд RocksDB гарантовано помічає блоки як видалені (Tombstones), які під час подальшої компресії фізично стираються з носія без можливості відновлення (MP-6(8)). _____ Параметр: tombstone_deletion_enabled Тип: boolean Значення: true
97	Використання носіїв інформації (марковані томи)		MP-7(1)	KVS може конфігуруватись на використання виключно заздалегідь визначених (іменованих) просторів таблиць на авторизованих томах зберігання, забороняючи використання невідомих чи немаркованих баз даних (MP-7(1)). _____ Параметр: authorized_volumes_only Тип: boolean Значення: true
8. ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ (CP)				
98	Резервне копіювання інформаційної системи	Резервне копіювання інформації кор истувача, що міститься в.	CP-9	Система здійснює автоматичне створення резервних копій бази даних KVS. Бекапи можуть зберігатися локально або відправлятися до хмарних сховищ, гарантуючи відновлення даних відповідно до RTO/RPO. _____ Параметр: system_backup Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
99	Відновлення інформаційної системи	Відновлення системи до відомого стану забезпечується протягом.	CP-10	KVS забезпечує механізми швидкого відновлення з резервних копій (‘kvs:restore/1‘), дозволяючи адміністраторам відновити працездатність вузла з гарантією логічної цілісності журналу транзакцій. _____ Параметр: system_recovery Тип: boolean Значення: true
9. ФІЗИЧНИЙ ЗАХИСТ ТА ЗАХИСТ НАВКОЛИШНЬОГО СЕРЕДОВИЩА (PE)				
100	Фізичний доступ	Розроблено перелік осіб, які мають право авторизованого доступу до об’єкта, де перебуває система;.	PE-2	Регламентується інструкціями з режиму ЦОД (див. розділ PE у digital-profile.pdf). _____ Параметр: physical_access_doc_ref Тип: string Значення: digital-profile.pdf
101	Контроль фізичного доступу	Авторизація фізичного доступу забезпечується в <PE-03_ODP[01] пунктах входу і виходу> шляхом перевірки індивідуальних дозволів доступу;.	PE-3	Регламентується системами СКУД будівлі (див. розділ PE у digital-profile.pdf). _____ Параметр: physical_access_control_ref Тип: string Значення: digital-profile.pdf
10. ОЦІНКА РИЗИКІВ (RA)				
102	Оцінка ризиків	Частота> або коли відбуваються значні зміни в системі, середовищі її функціонування або інших умовах, які можуть вплинути на стан безпеки або приватності системи.	RA-3	Всі ідентифіковані вразливості або загрози фіксуються в реєстрі ‘itsm‘, де їм присвоюється рівень критичності. На базі цього рівня розраховується пріоритет та призначаються відповідальні особи. _____ Параметр: risk_assessment Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
103	Сканування вразливостей	Здійснюється моніторинг систем та розміщених застосунків на наявність вразливостей <RA-05_ ODP[01] частота та/або випадковість відповідно до визначеного організацією процесу>, а також коли виявляються та повідомляються нові вразливості, що потенційно можуть вплинути на систему;.	RA-5	Система передбачає можливість інтеграції зовнішніх сканерів вразливостей, звіти яких автоматично перетворюються на тикети усунення ризиків в системі ‘itsm‘. --- Параметр: vulnerability_ scanning Тип: boolean Значення: true
11. ЗАХИСТ СИСТЕМ ТА КОМУНІКАЦІЙ (SC)				
104	Ізоляція функції безпеки	Розділяти функціональність користувача, включно зі службами, що призначені для користувача інтерфейсу, від функціональності системного управління.	SC-2	Функції безпеки (шифрування, авторизація) виконуються в ізольованих процесах Erlang VM, окремо від бізнес-логіки системи. Ця архітектура Actor Model унеможливлює втручання несанкціонованих процесів у роботу механізмів безпеки. --- Параметр: security_ function_isolation Тип: boolean Значення: true
105	Інформація в загальних ресурсах системи	Запобігати несанкціонованій та ненавмисній передачі інформації через спільні системні ресурси.	SC-4	Erlang VM не використовує спільну пам’ять (shared memory) між процесами сесій N2O. Пам’ять звільняється автоматично (Garbage Collection) після обробки запиту, запобігаючи витоку залишкової інформації між різними користувачами. --- Параметр: shared_ resource_protection Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
106	Захист від атак «відмова в обслуговуванні» (DoS)	a. [Призначення: захистити від; Обмежити] наслідки наступних типів подій відмови в обслуговуванні (DoS): [Призначення: визначені організацією типи подій відмови в обслуговуванні]; b. Застосувати наступні заходи захисту для досягнення мети відмови обслуговування [Призначення: заходи захисту визначені організацією, за типом події відмови в обслуговуванні].	SC-5	Інфраструктура N2O/Cowboy обробляє сотні тисяч конкурентних WebSocket-з'єднань завдяки легкості Erlang-процесів. Вбудовані механізми rate-limiting, обмеження розміру payload та таймаути захищають від атак на виснаження ресурсів (Slowloris, Flood). --- Параметр: dos_ protection Тип: boolean Значення: true
107	Захист периметра (Boundary Protection)	a. Контролювати та управляти зв'язком на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи. b. Реалізувати підмережі для загальнодоступних компонентів системи, які є [Вибір: фізично; логічно] відділені від внутрішніх мереж організації. c. Підключатися до зовнішніх мереж або систем тільки через керовані інтерфейси, що складаються з пристроїв захисту периметру, і розташованих відповідно до архітектури безпеки та приватності організації.	SC-7	Всі зовнішні підключення приймаються виключно через єдиний порт (керований інтерфейс), що обробляється веб-сервером (Cowboy). Доступ до внутрішніх API і вузлів кластера блокується правилами мережевого екранування за замовчуванням (Default Deny). --- Параметр: boundary_ protection Тип: boolean Значення: true
108	Захист цілісності та конфіденційності під час передачі	Забезпечити [Вибір (один або кілька): конфіденційність; цілісність] інформації, що передається.	SC-8	Передача інформації між клієнтом і сервером здійснюється виключно через зашифровані канали (WSS/TLS), що унеможливлює перехоплення (Man-in-the-Middle) або несанкціоновану модифікацію даних на льоту. --- Параметр: transmission_ confidentiality Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
109	Розрив мережевого з'єднання	Завершити з'єднання з мережею, яке пов'язане із сеансом зв'язку в кінці сеансу або після [Призначення: визначений організацією період часу] бездіяльності.	SC-10	Протокол N2O автоматично розриває мережеве з'єднання після завершення комунікаційного сеансу або перевищення часу очікування (Inactivity Timeout), звільняючи ресурси та сесію. Параметр: network_ disconnect_timeout Тип: integer Значення: 3600
110	Криптографічне управління ключами	Встановити та управляти криптографічними ключами для криптографічних засобів, які використовуються в системі відповідно до [Призначення: визначені організацією вимоги до генерації, поширення, зберігання, доступу та знищення ключів].	SC-12	Керування ключами та сертифікатами для встановлення захищених з'єднань делегується бібліотеці 'synrc/ca' та інтегрованим механізмам TLS ОС, що відповідають чинним криптографічним стандартам. Параметр: cryptographic_key_ management Тип: boolean Значення: true
111	Криптографічний захист	a. Визначити [Призначення: використання криптографічних засобів, визначених організацією]; b. Впровадити [Завдання: визначені організацією види криптографії для кожного визначеного криптографічного використання].	SC-13	Система підтримує використання схвалених криптографічних алгоритмів (AES-GCM, SHA-256/512, ДСТУ 4145-2002 через відповідні модулі), які забезпечують необхідний рівень стійкості. Параметр: cryptographic_ protection Тип: boolean Значення: true
112	Автентичність сеансу зв'язку	Забезпечити автентифікацію сеансів зв'язку.	SC-23	Автентичність WebSocket-сесій N2O захищається токенами з криптографічним підписом (HMAC). Це гарантує, що повідомлення в рамках сесії не можуть бути підроблені або інжектовані сторонньою особою. Параметр: session_ authenticity Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
12. ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ (SI)				
113	ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ	Перевіряти дійсність [Призначення: визначена організацією введена інформація].	SI-10	Система повинна перевіряти вхідну інформацію перед тим, як її обробляти та зберігати, щоб захиститись від ін'єкцій та забезпечити логічну цілісність. Екосистема Synrc (Nitro, Form) використовує архітектуру Server-Side Rendering (через N2O WebSockets) та декларативну серверну валідацію, що усуває цілі класи вразливостей.
114	Перевірка вводу перевизначення (лише серверна валідація)		SI-10(1)	Клієнтська сторона (браузер) в ‘synrc/nitro‘ не містить логіки валідації, яку можна було б обійти чи перевизначити (override) через маніпуляції з DOM або JS. Уся перевірка жорстко зашита у виконуваний код Erlang (‘synrc/form‘). Жодне клієнтське перевизначення не здатне змінити правила серверної валідації. --- Параметр: server_ side_validation_only Тип: boolean Значення: true
115	Перевірка вводу інформації помилок (екранування HTML)		SI-10(2)	Повідомлення про помилки валідації генеруються на сервері (Erlang) і передаються клієнту через WebSocket як готові безпечні HTML-фрагменти (екрановані ‘nitro‘), запобігаючи виникненню XSS під час відображення помилкового вводу користувачу. --- Параметр: escape_ html_output Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
116	Передбачувана поведінка (декларативні Records)		SI-10(3)	Оскільки валідація описана декларативно (Record-структурами з типами полів, як-от ‘integer‘, ‘string‘, ‘date‘), реакція системи на некоректні дані завжди є 100% передбачуваною (Predictable Behavior). Відсутні приховані клієнтські скрипти, що можуть реагувати непередбачувано на специфічний ввід. --- Параметр: predictable_behavior Тип: boolean Значення: true
117	Часові взаємодії (таймаути N2O)		SI-10(4)	Оскільки ввід передається через сталий WebSocket-зв’язок (N2O), система має вбудований контроль тайм-аутів з’єднання та захист від перевантажень (Rate-limiting). Довгі запити або неповний ввід просто ігноруються після завершення вікна сесії, блокуючи атаки типу Slowloris. --- Параметр: timing_interactions Тип: boolean Значення: true
118	Обмеження вводу довіреними джерелами і форматами		SI-10(5)	Бібліотека ‘form‘ пропускає дані лише для тих полів, які явно задекларовані в схемі форми (Approved Formats). Pattern Matching платформи Erlang автоматично відкидає будь-які JSON/BERT payload-пакети, які містять незадекларовані поля (унеможливлюючи Mass Assignment Vulnerability) або походять з неавторизованого джерела (Trust Zone). --- Параметр: strict_type_checking Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
119	Профілактика вводу даних (блокування через ABAC)		SI-10(6)	Комбінація ‘nitro‘ та ‘abac‘ дозволяє здійснювати профілактику (Prevention): якщо користувач не має права вносити дані в певне поле, це поле взагалі не рендериться на стороні клієнта або рендериться в стані ‘readonly/disabled‘, а бекенд-валідатор автоматично блокує будь-яку спробу його програмно передати (Data Input Prevention at source). --- Параметр: data_ input_prevention Тип: boolean Значення: true
13. РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR)				
120	Політика та процедури реагування на інциденти	a. Розробити, задокументувати та поширити [Призначення: серед визначеного організацією персоналу або ролей]: 1. 2. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики реагування на інциденти, яка: (a) містить мету, сферу застосування, ролі, обов’язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам; процедури, що забезпечують реалізацію політики реагування на інциденти та пов’язані з нею заходи реагування на інциденти. b. Призначити [Призначення: визначену організацією посадову особу вищого керівництва] для управління, документування і розповсюдження політики та процедур реагування на інциденти. c. Переглядати та оновлювати поточні: 1. політику реагування на інциденти [Призначення: з визначеною організацією частотою] і наступні [Призначення: події, визначені організацією]; 2. процедури реагування на інциденти [Призначення: з визначеною організацією частотою] та наступні [Призначення: події, визначені організацією].	IR-1	Політика реагування на інциденти закодована безпосередньо у бізнес-процесах (BPMN) ‘erpuno/itsm‘, забезпечуючи неухильне виконання процедур на кожному кроці життєвого циклу інциденту. --- Параметр: incident_ policy_enforcement Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
14. ПЛАНУВАННЯ (PL)				
121	План безпеки системи	Розроблено план захисту інформації, який відповідає архітектурі підприємства організації;.	PL-2	Система підтримує автоматичну генерацію актуального Плану безпеки системи на основі цього профілю (CM). План чітко визначає всі технічні та організаційні контролі (AC, AU, SC, CM тощо), середовище функціонування та архітектуру. --- Параметр: system_ security_plan Тип: boolean Значення: true
122	Правила поведінки	Встановлені правила, які описують обов'язки та очікувану поведінку щодо використання інформації та системи, безпеки та конфіденційності для осіб, яким потрібен доступ до системи;.	PL-4	Для всіх користувачів платформи (організаційних та зовнішніх) визначаються правила поведінки. Згода з правилами (наприклад, Terms of Service, NDA) фіксується в базі даних KVS під час онбордингу, перед наданням доступу до ERP/1. --- Параметр: rules_of_ behavior Тип: boolean Значення: true
123	Архітектура безпеки	Описує архітектура безпеки системи те, як вона інтегрована в архітектуру підприємства та підтримує її;.	PL-8	Архітектура безпеки платформи (Actor Model, ізоляція процесів, Zero Dependencies, Append-Only логування) розробляється інтегровано з загальною архітектурою підприємства. Вона регулярно переглядається на відповідність державним стандартам (НД ТЗІ, NIST SP 800-53). --- Параметр: security_ architecture Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
15. УПРАВЛІННЯ РИЗИКАМИ В ЛАНЦЮГУ ПОСТАЧАННЯ (SR)				
124	План управління ризиками ланцюга постачання	a. Розробіть план управління ризиками ланцюга постачання, пов'язаними з дослідженнями та розробкою, проектуванням, виробництвом, придбанням, доставкою, інтеграцією, експлуатацією та обслуговуванням, а також утилізацією таких систем, компонентів системи або послуг для системи: [Призначення: системи, визначені організацією, системні компоненти або системні служби]; b. Перегляньте та оновіть план управління ризиками ланцюга постачання [Призначення: частота, визначена організацією] або за потреби для усунення загроз; c. Захистіть план управління ризиками ланцюга постачання від несанкціонованого розголошення та модифікації.	SR-2	План управління базується на принципі відмови від стороннього коду. Замість інтеграції сотень неперевірених бібліотек, команда розробляє всі необхідні компоненти (веб-сервер N2O, KVS, CA) самостійно в єдиному монорепозиторії. Параметр: zero_dependency_policy Тип: boolean Значення: true
125	Контроль та захист ланцюга постачання	a. Встановлення процесу або процесів для виявлення та усунення слабких місць або недоліків в елементах і процесах ланцюга постачання [Призначення: визначена організацією система або компонент системи] у координації з [Завдання: персонал ланцюга постачання, визначений організацією]; b. Використовуйте такі заходи захисту, щоб захистити систему, компонент системи або системну службу від ризиків ланцюга постачання та обмежити шкоду чи наслідки від подій, пов'язаних із ланцюгом постачання: [Призначення: заходи захисту ланцюга постачання, визначені організацією]; c. Задокументуйте обрані та впроваджені процеси та заходи захисту ланцюгом постачання у [Вибір: плани безпеки та приватності; план управління ризиками ланцюга постачання; [Призначення: документ, визначений організацією]].	SR-3	Заборонено використання автоматичних менеджерів пакетів для завантаження коду під час збірки. Весь вихідний код системи та модулів міститься безпосередньо в репозиторії проекту, що гарантує 100% контроль над кожним рядком коду, який компілюється. Параметр: strict_code_vendoring Тип: boolean Значення: true
126	Аудит та огляди постачальників	Оцініть і перегляньте ризики ланцюга постачання, пов'язані з постачальниками або підрядниками, системою, системним компонентом або системною послугою, яку вони надають [Призначення: частота, визначена організацією].	SR-6	Єдиним зовнішнім «постачальником» є розробник платформи Erlang/OTP (компанія Ericsson та спільнота). Оновлення версій OTP проходять жорстку перевірку перед їх застосуванням на продуктивних серверах. Параметр: erlang_otp_supplier_review Тип: boolean Значення: true

№	Вимога з безпеки інформації	Вимога ГПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
127	Автентичність компонентів	a. Розробити та впровадити політику та процедури боротьби з підробками, які включають засоби для виявлення та запобігання потраплянню підроблених компонентів у систему; b. Повідомляти про підроблені системні компоненти [Вибір (один або кілька): джерело підробленого компонента; [Призначення: зовнішні звітні організації, визначені організацією]; [Призначення: персонал або ролі, визначені організацією]].	SR-11	Будь-які оновлення або патчі самої системи передаються виключно через захищені канали із застосуванням криптографічних підписів (‘synrc/ca‘), що виключає можливість підміни бінарних файлів під час розгортання. _____ Параметр: component_ authenticity Тип: boolean Значення: true