

ЗАТВЕРДЖУЮ

Директор технічний

ТОВ НВП ХАРТРОН-ІНКОР ЛТД

В.В. Горбенко

2026 р.



Звіт

Реалізація плану кіберзахисту КТЗ ПМ РЗА «Діамант»

ЗВ-17010-15/2026

Аркушів 9

Харків

2026

1. Вступ

Мета: підтвердити достатність та коректності реалізованих заходів кіберзахисту ПМ РЗА згідно з реалізацією «ПЛАНУ КІБЕРЗАХИСТУ ПЛ-17020 - 4/2024» і вимогами НП 306.2.237-2022.

2. Об'єкт перевірки

Об'єктом перевірки є «Комплекс технічних засобів приладових модулів релейного захисту та автоматики (КТЗ ПМ РЗА) "Діамант"» призначений для реалізації функцій релейного захисту та автоматики керування електротехнічним обладнанням.

Відповідно до НП 306.2.202-2015 «Вимоги з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки АС» ПМ РЗА виконують функції категорії В і С.

Відповідно до НП 306.2.237-2022 «Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки» для ПМ РЗА встановлюється рівень кіберзахисту К2.

3. Методи та інструменти

Для підтвердження достатності реалізованих заходів кіберзахисту ПМ РЗА використані наступні методи:

- 1) Статичний аналіз вихідного коду, з метою підтвердження відсутності прихованих функцій;
- 2) Динамічне тестування на стендовому обладнанні;
- 3) Аудит технічних і організаційних заходів кіберзахисту на підприємстві.

4. Результати перевірки

Результати перевірки реалізації плану кіберзахисту КТЗ ПМ РЗА приведені в таблиці 1.

Таблиця 1 - Результати перевірки реалізації плану кіберзахисту КТЗ ПМ РЗА

№	Заходи з кіберзахисту	Пункт ПК	Пункт ПМК	Метод перевірки	Результат	Статус
1	Захист від несанкціонованого фізичного доступу	3.1	7.1.1	Перевірка засобів захисту у КД.	Підтверджено використання засобів захисту від несанкціонованого фізичного доступу у КД КТЗ ПМ РЗА (ТУ).	Відповідає
2	Доступ згідно з принципом найменших привілеїв і автентифікація та авторизація користувачів	3.2	7.1.2	Тестування реалізації автентифікації та авторизації користувачів на комплексному стенді.	Реалізацію доступу згідно з принципом найменших привілеїв і підтверджено (протокол випробувань).	Відповідає
3	Запобігання несанкціонованому віддаленому доступу	3.3	7.1.3	Тестування відсутності зв'язку мережевого інтерфейсу LAN ПМ РЗА з ПК за допомогою утиліти ping.	Відсутність зв'язку через інтерфейс LAN з ПК підтверджено (протокол випробувань).	Відповідає
4	Відсутність обхідних облікових записів	3.4	7.1.4	Тестування утиліти керування обліковими записами. Перевірка створення і контролю облікових записів.	Відсутність обхідних облікових записів підтверджено (протокол випробувань).	Відповідає
5	Забезпечення необхідної довжини паролів, їх надійності, складності та періодичності зміни	3.5	7.1.5	Тестування введення валідних і невалідних паролів в облікових записах і на інтерфейсі ПМ РЗА.	Правильність перевірки валідності паролів в ПЗ ПМ РЗА підтверджено (протокол випробувань).	Відповідає
6	Блокування несанкціонованого підключення будь-яких зовнішніх пристроїв	3.6	7.1.6	Перевірка розглядом у КД відсутності безпроводного зв'язку. Тестування неможливості роботи з флеш носіями.	Відсутність безпроводного зв'язку підтверджено (ТУ). Підтверджено неможливість логічного підключення флеш носіїв до ПМ РЗА (протокол випробувань).	Відповідає
7	Заходи для мінімізації прихованих функцій	3.7	7.1.7	Перевірка заходів здійснюється шляхом розгляду документів з верифікації ПМ РЗА (Плану верифікації і звітів з верифікації).	Підтверджена наявність в Плані верифікації інформації про заходи для мінімізації прихованих функцій.	Відповідає

Продовження таблиці 1

№	Заходи з кіберзахисту	Пункт ПК	Пункт ПМК	Метод перевірки	Результат	Статус
8	Заходи проти впровадження шкідливих чи прихованих функцій	3.8.1	7.1.8.1	Статичний аналіз вихідного коду ПЗ. Пошук незадекларованих функцій у коді ПЗ. Тест програмного коду. Динамічне тестування функцій ПМ РЗА на комплексному стенді.	Шкідливих чи прихованих функцій в вихідному коді ПЗ ПМ РЗА не виявлено (Звіт з верифікації № ЗВ-17010-10/2026).	Відповідає
9	Заходи щодо перевірки технічних та програмних засобів розробки, а також тестового обладнання	3.8.2	7.1.8.2	Перевіряння здійснюється шляхом розгляду звіту з верифікації щодо перевірки технічних та програмних засобів розробки.	Підтверджено використання необхідних засобів кіберзахисту на обладнанні для розробки і тестування ПМ РЗА (Звіт № ЗВ-17010-11/2026).	Відповідає
10	Заходи проти перехоплення або викривлення даних, що відображаються за допомогою інтерфейсу "людина-машина"	3.9	7.1.9	Тестування приховування символів на інтерфейсі при введенні пароля. Тестування блокування доступу до функцій за паролем через 20 хвилин (за відсутності роботи користувача з інтерфейсом)	Приховування символів на інтерфейсі при введенні пароля підтверджено. Блокування доступу до функцій за паролем через 20 хвилин підтверджено (протокол випробувань).	Відповідає
11	Реалізація засобів перевірки коректності модифікацій, внесених у ПЗ	3.10	7.1.10	Перевірка інформації щодо засобів перевірки коректності модифікацій, внесених у ПЗ в плані з верифікації.	Наявність у плані з верифікації інформації щодо засобів перевірки коректності модифікацій підтверджено.	Відповідає
12	Унеможливлення зміни ПЗ, що зберігається на носіях даних	3.11	7.1.11	Перевірка у КД процедури зміни ПЗ на карті пам'яті (необхідності демонтажу карти з корпусу приладу для виконання зміни ПЗ). Перевірка використання носіїв CD дисків з копіями ПЗ (що не мають можливості перезапису).	Унеможливлення зміни ПЗ, що зберігається на носіях даних підтверджено (Інструкція з конфігурації. ААВГ. 460644.014 Д).	Відповідає

Продовження таблиці 1

№	Заходи з кіберзахисту	Пункт ПК	Пункт ПМК	Метод перевірки	Результат	Статус
13	Забезпечення антивірусним захистом	4.1	7.1.12	Перевірка забезпечення антивірусного захисту в звіті з аудиту про забезпечення кіберзахисту на підприємстві	За результатами аудиту забезпечення кіберзахисту на підприємстві підтверджено використання антивірусного захисту на усіх ПК (Звіт № 3В-17010-11/2026).	Відповідає
14	Наявності відповідальних осіб, які забезпечують кіберзахист в організації	4.2	7.1.13	Перевірка адміністративної документації підприємства про призначення відповідальних осіб, які забезпечують кіберзахист.	За результатами аудиту забезпечення кіберзахисту наказом на підприємстві призначені відповідальні особи, які забезпечують кіберзахист (Наказ підприємства).	Відповідає
15	Наявність документації з кіберзахисту	4.3	7.1.14	Перевірка наявності документації відповідно до Політики інформаційної безпеки та кіберзахисту, Політики щодо ядерної безпеки, Політики у сфері якості та вимог внутрішніх нормативних документів.	За результатами аудиту забезпечення кіберзахисту, проведена перевірка наявності на підприємстві документації з кіберзахисту. Перелік документів, що стосуються кіберзахисту приведено в Додатку А	Відповідає
16	Розроблення ПМ РЗА, ПЗ в захищеному середовищі	4.4	7.1.15	Перевірка забезпечення умов розроблення ПЗ в захищеному середовищі у відповідному звіті.	За результатами аудиту з кіберзахисту випущений «Звіт № 3В-17010-11/2026 Загальні заходи забезпечення кіберзахисту на підприємстві ТОВ НВП Хартрон-Інкор ЛТД» в якому підтверджується забезпечення умов кіберзахисту середовища розроблення ПМ РЗА, ПЗ.	Відповідає

Продовження таблиці 1

№	Заходи з кіберзахисту	Пункт ПК	Пункт ПМК	Метод перевірки	Результат	Статус
17	Забезпечення запобігання несанкціонованому доступу до ПМ РЗА на стадії розроблення	4.5	7.1.16	Перевірка у відповідному звіті заходів і засобів запобігання несанкціонованому доступу до ПМ РЗА на стадії розроблення..	Заходи запобігання несанкціонованому доступу приведені у «Звіті № ЗВ-17010-11/2026 Загальні заходи забезпечення кіберзахисту на підприємстві ТОВ НВП Хартрон-Інкор ЛТД»	Відповідає
18	Порядок зберігання конфіденційної інформації та документації	4.6	7.1.17	Перевірка в документах підприємства порядку зберігання конфіденційної інформації та документації, умов зберігання носіїв інформації і наявності доступу до документації на сервері за обліковими записами	Інформацію про порядок зберігання документації підтверджено в стандартах підприємства СТП 523.7-191-2003, СТП 523.7-ISO 9001-2018. За результатами аудиту підтверджені умови зберігання носіїв з ПЗ в спеціальному сейфі, а також наявність доступу до електронної документації на сервері за обліковими записами.	Відповідає
19	Наявність обмежень на використання зовнішніх носіїв даних.	4.7	7.1.18	Перевірка у документації підприємства обмежень на використання зовнішніх носіїв даних	Обмеження на використання зовнішніх носіїв даних приведені у «Звіті № ЗВ-17010-11/2026 Загальні заходи забезпечення кіберзахисту на підприємстві ТОВ НВП Хартрон-Інкор ЛТД»	Відповідає
20	Порядок проведення оцінювання кіберзахисту	4.8	7.1.19	Перевірка в документації підприємства порядку проведення оцінювання кіберзахисту	Порядок проведення оцінювання кіберзахисту приведений в СТП 523.7-234-2025 «Забезпечення кіберзахисту»	Відповідає

Продовження таблиці 1

№	Заходи з кіберзахисту	Пункт ПК	Пункт ПМК	Метод перевірки	Результат	Статус
21	Наявність порядку реєстрації та реагування на кіберінциденти	4.9	7.1.20	Перевірка в документації підприємства порядку проведення оцінювання кіберзахисту	Порядок реєстрації та реагування на кіберінциденти приведений в СТП 523.7-234-2025 «Забезпечення кіберзахисту»	Відповідає
22	Заходи кіберзахисту під час розроблення ПМ РЗА, ПЗ	4.10	7.1.21	Перевірка в документації підприємства заходів кіберзахисту під час розроблення ПМ РЗА, ПЗ	Заходи кіберзахисту під час розроблення ПМ РЗА, ПЗ приведені в СТП 523.7-234-2025 «Забезпечення кіберзахисту» і в «Звіті № ЗВ-17010-11/2026 Загальні заходи забезпечення кіберзахисту на підприємстві ТОВ НВП Хартрон-Інкор ЛТД»	Відповідає
23	Відсутність негативного впливу засобів кіберзахисту на виконання функцій	4.11	7.1.22	Тестування функціонування ПМ РЗА відповідно до вимог ТУ на комплексному стенді.	В результаті тестування підтверджено відсутність негативного впливу засобів кіберзахисту на виконання функцій у «Звіті з верифікації № ЗВ-17010-10/2026 (згідно з доповнення №1 до плану верифікації програмного забезпечення ПЛ-17010 - 170/2018)».	Відповідає

Продовження таблиці 1

№	Заходи з кіберзахисту	Пункт ПК	Пункт ПМК	Метод перевірки	Результат	Статус
	Заходи кіберзахисту під час транспортування	4.12	7.1.23	Перевірка виконання вимог до пакування проводять зовнішнім оглядом та у КД.	За результатами аудиту підтвержено виконання вимог до пакування згідно ТУ, що обмежує доступ до ПМ РЗА під час транспортування. Підтверджена наявність пломби на передній ПМ РЗА, що запобігає несанкціонованому доступу всередину приладу.	Відповідає
25	Вхідний контроль усіх виробів сторонньої розробки і тестування ПЗ сторонньої розробки	4.13	7.1.24	Перевірка інформації щодо процедури вхідного контролю виробів сторонньої розробки в документації підприємства.	Процедури вхідного контролю виробів сторонньої розробки описані в СТП 523.7-ISO 9001-2018, СТП 523.7-194-2003.	Відповідає

5. Висновки

Реалізовані заходи згідно «ПЛАНУ КІБЕРЗАХИСТУ ПЛ-17020 - 4/2024» відповідають вимогам стандарту НП 306.2.237-2022 «Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки». Підтверджена достатність та коректність реалізованих заходів кіберзахисту КТЗ ПМ РЗА. Рекомендовано впровадження «Комплексу технічних засобів приладових модулів релейного захисту та автоматики (КТЗ ПМ РЗА) "Діамант"» в експлуатацію.

Підписи

Відповідальний за статичну верифікацію:  М. Ткачов

Відповідальний за динамічну верифікацію:  О. Севостьянова

Дата: 10.07.2026 р.

Додаток А

Перелік документів з кіберзахисту

Позначення	Найменування
ТУ ПМ РЗА	Комплекс технічних засобів приладових модулів релейного захисту та автоматики. Технічні умови. ТУ У 25187880.001-2000 (ААВГ.421453.005 ТУ)
СТП 523.7-191-2003	Система управління якістю. Документація на продукцію. Порядок обліку, зберігання та обігу. Стандарт підприємства.
СТП 523.7-194-2003	Вхідний контроль комплектуючих виробів. Стандарт підприємства.
СТП 523.7-ISO 9001-2018	Настанова щодо якості. Стандарт підприємства.
СТП 523.7-234-2025	Забезпечення кіберзахисту. Стандарт підприємства.
План кіберзахисту ПЛ-17020 - 4/2024	КТЗ ПМ РЗА. План кіберзахисту ПЛ-17020 - 4/2024.
План верифікації ПЗ ПЛ-17010 -170/2018	Модернізація схем РЗА власних потреб 6 кВ АЕС. План верифікації програмного забезпечення. ПЛ-17010 – 170/2018.
ПЛ-17010 -181/2018	Звіт з верифікації програмного забезпечення.
ПЛ-17010 - 170/2018	«Доповнення №1 до плану верифікації програмного забезпечення ПЛ-17010 - 170/2018».
ААВГ.421453.005 НЕ	Настанова з експлуатування ПМ РЗА.
ААВГ.421453.153 34 02	ІНСТРУКЦІЯ ОПЕРАТОРА ААВГ.421453.153 34 02 СЕРВІСНЕ ПЗ ПМРЗА "ДІАМАНТ"
ААВГ.421453.158 34 01	ІНСТРУКЦІЯ ОПЕРАТОРА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ ОБЛІКОВИХ ЗАПИСІВ КОРИСТУВАЧІВ СЕРВІСНОГО ПЗ ПМ РЗА "ДІАМАНТ"
ААВГ. 460644.014 Д	Плати процесорні. Інструкція з конфігурації.
ЗВ-17010-11/2026	«Звіт № ЗВ-17010-11/2026 Загальні заходи забезпечення кіберзахисту на підприємстві ТОВ НВП Хартрон-Інкор ЛТД».
ЗВ-17010-10/2026	«Звіт з верифікації № ЗВ-17010-10/2026 (згідно доповнення №1 до плану верифікації програмного забезпечення ПЛ-17010 - 170/2018)».
ПМ-17020-5/2024	«Програма-методика випробувань комплексу технічних засобів приладових модулів релейного захисту і автоматики «Діамант» на відповідність вимогам НП 306.2.237-2022 до кіберзахисту ІКС АС»