МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

м. Київ

Про внесення змін до наказу Міністерства енергетики України від 31 березня 2026 року № 176

Відповідно до підпунктів «д», «е» пункту 5 Положення про державну реєстрацію нормативно-правових актів міністерств, інших органів виконавчої влади, затвердженого постановою Кабінету Міністрів України від 28 грудня 1992 року № 731, та наказу Міністерства юстиції України від 07 квітня 2026 року № 912/5 «Про визнання акта таким, що не підлягає державній реєстрації»

НАКАЗУЮ:

1. Пункти 2 та 3 наказу Міністерства енергетики України від 31 березня 2026 року № 176 «Про затвердження профілів безпеки системи для паливно-енергетичного комплексу України» виключити.

У зв’язку з чим пункт 4 вважати пунктом 2.

2. Контроль за виконанням цього наказу покласти на заступника Міністра з питань цифрового розвитку, цифрових трансформацій і цифровізації ШУГАЛІЯ Дениса.

Перший віце-прем’єр-міністр України –
Міністр **Денис ШМИГАЛЬ**

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

_____ **м. Київ** _____

Про затвердження профілів безпеки системи для паливно-енергетичного комплексу України

Відповідно до статті 10 Закону України «Про захист інформації в інформаційно-комунікаційних системах», Порядку розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 року № 712, Положення про Міністерство енергетики України, затвердженого постановою Кабінету Міністрів України від 17 червня 2020 року № 507,
НАКАЗУЮ:

1. Затвердити такі, що додаються:

Галузевий профіль безпеки системи, де обробляється відкрита або конфіденційна інформація для паливно-енергетичного комплексу України;

Галузевий профіль безпеки системи, де обробляється службова інформація для паливно-енергетичного комплексу України.

2. Управлінню кібербезпеки та цифрового розвитку забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.

3. Цей наказ набирає чинності з дня його офіційного опублікування.

4. Контроль за виконанням цього наказу покласти на заступника Міністра з питань цифрового розвитку, цифрових трансформацій і цифровізації ШУГАЛІЯ Дениса.

Перший віце-прем’єр-міністр України –
Міністр **Денис ШМИГАЛЬ**

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
31 березня 2026 року № 176

Галузевий профіль
безпеки системи, де обробляється відкрита або конфіденційна інформація
для паливно-енергетичного комплексу України

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту відповідно до НД ТЗІ 3.6-006-24[1]	Мінімальні необхідні параметри налаштування заходів захисту відповідно до НД ТЗІ 3.6-006-24[1]
1	2	3	4	5
Управління доступом (АС)				
1	Управління обліковими записами	Визначити дозволені та заборонені типи облікових записів у системі. Створити, активувати, змінити, деактивувати та видалити облікові записи із системи відповідно до політики, процедур, передумов і критеріїв суб'єкта господарювання паливно-енергетичного комплексу України (далі – ПЕК). Визначити авторизованих користувачів системи, належність до груп і ролей, а також повноваження доступу (тобто привілеї).	АС-2	Повідомляти адміністраторів облікових записів, у межах визначеного суб'єктом господарювання ПЕК часового періоду для кожної ситуації, коли облікові записи

[1] Нормативний документ системи технічного захисту інформації НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30 квітня 2024 року № 234.

1	2	3	4	5
		Авторизувати доступ до системи. Контролювати використання облікових записів у системі. Оповістити користувачів системи або ролі суб'єкта господарювання ПЕК про визначений суб'єктом господарювання ПЕК період часу, коли: облікові записи більше не потрібні; користувачі звільняються або переводяться; у системі наявні зміни, які потребують нових знань. Вимагати, щоб користувачі виходили з системи після визначеного суб'єктом господарювання ПЕК періоду часу або за визначених суб'єктом господарювання ПЕК обставин.		більше не потрібні, працівники звільнені чи переведені та коли використовуються індивідуальні системи або наявні зміни, які потребують нових знань впродовж 24 годин. Проводити перегляд облікових записів на відповідність вимогам управління обліковими записами кожні 90 календарних днів.
			AC-2 (5)	Вимагати від користувачів виходити із системи в кінці кожного робочого дня користувача.
2	Забезпечення доступу	Застосовувати затверджені суб'єктом господарювання ПЕК повноваження користувачів системи або процесів, що діють від імені користувачів системи, для логічного доступу до конфіденційної інформації та ресурсів у системі.	AC-3	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
3	Управління інформаційними потоками	Застосовувати затверджені суб'єктом господарювання ПЕК дії для управління потоками відкритої та конфіденційної інформації всередині системи та між підключеними системами.	AC-4	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
4	Розмежування обов'язків	Визначити обов'язки осіб, які потребують розмежування. Встановити правила авторизації доступу для підтримки розмежування обов'язків осіб, які потребують розмежування.	AC-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
5	Мінімізація повноважень	Надавати користувачам або процесам, що діють від імені користувачів, лише авторизований доступ до системи, необхідний для виконання поставлених завдань суб'єкта господарювання ПЕК. Авторизувати доступ до функції безпеки інформації, визначених суб'єктом господарювання ПЕК, та важливої для безпеки інформації.	AC-6 AC-6 (1) AU-9 (4)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
6	Мінімізація повноважень – доступ до незахищених функцій	Обмежити привілейовані облікові записи в системі для працівників або ролі, що визначається суб'єктом господарювання ПЕК. Вимагати, щоб користувачі або ролі з привілейованими обліковими записами використовували непривілейовані облікові записи для доступу до незахищених функцій або інформації.	AC-6 (2)	Вимагати від користувачів облікових записів системи або ролей, які мають доступ до привілейованих функцій, використовувати непривілейовані облікові записи чи ролі під час доступу до незахищених функцій.

1	2	3	4	5
			AC-6 (5)	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
7	Мінімізація повноважень – заборона користувачам виконувати привілейовані функції	Заборонити непривілейованим користувачам виконувати привілейовані функції.	AC-6 (10)	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
8	Невдалі спроби входу в систему	Встановити обмеження на кількість, яка визначена суб’єктом господарювання ПЕК, невдалих спроб входу в систему протягом певного часу, який визначений суб’єктом господарювання ПЕК. Автоматично заблокувати обліковий запис або комунікаційний вузол на період часу, визначений суб’єктом господарювання ПЕК. Заблокувати обліковий запис або комунікаційний вузол до зняття адміністратором. Відкласти наступний запит на вхід. Повідомити системного адміністратора. Вжити інших заходів, коли перевищено максимальну кількість невдалих спроб входу в систему.	AC-7	Повідомити відповідального адміністратора коли перевищено максимальну кількість невдалих спроб входу в систему.
9	Попередження про використання системи	Відображати повідомлення в системі з попередженнями про конфіденційність і безпеку відповідно до застосованих нормативно-правових актів у сфері кібербезпеки та захисту інформації для відкритої та	AC-8	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.

1	2	3	4	5
		конфіденційної інформації перед тим, як надати доступ до системи.		
10	Управління паралельною сесією	Встановити обмеження на кількість, яка визначена суб'єктом господарювання ПЕК, одночасних сеансів для працівників або ролі, що визначається суб'єктом господарювання ПЕК.	АС-10	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
11	Блокування пристрою	Заборонити доступ до системи за допомогою дій: ініціювання блокування пристрою після періоду часу, визначеного суб'єктом господарювання ПЕК. Вимагати від користувача ініціювати блокування пристрою перед тим, як залишити систему без нагляду. Зберігати блокування пристрою до відновлення користувачем доступу за допомогою встановлених процедур ідентифікації та автентифікації. Приховати за допомогою блокування пристрою інформацію, яку раніше було виведено на дисплей, за допомогою публічно доступного зображення.	АС-11	Заборонити подальший доступ до системи шляхом ініціювання блокування пристрою через період, що не перевищує 30 хвилин бездіяльності або після отримання запиту від користувача. Користувачі ініціюють блокування пристрою перед тим, як залишити систему без нагляду.
			АС-11 (1)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
12	Припинення сеансу	Автоматично завершувати сеанс користувача після умови або події, що вимагають відключення сеансу, які визначені суб'єктом господарювання ПЕК.	АС-12	Налаштування заходів захисту визначаються

1	2	3	4	5
				суб’єктом господарювання ПЕК.
13	Віддалений доступ	Встановити обмеження на використання, дії до конфігурації та підключення для кожного типу допустимого віддаленого доступу до системи. Авторизувати кожен тип віддаленого доступу до системи перед встановленням таких з’єднань. Виконувати маршрутизацію всього віддаленого доступу до системи через авторизовані та керовані точки контролю управління доступом до мережі. Авторизувати віддалене виконання привілейованих команд і віддалений доступ до інформації, важливої для безпеки.	АС-17 АС-17 (3) АС-17 (4)	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
14	Бездротовий доступ	Встановити обмеження на використання, дії до конфігурації та підключення для кожного типу бездротового доступу до системи. Авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення.	АС-18	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
15	Контроль доступу для мобільних пристроїв	Встановити обмеження на використання, дії до конфігурації та підключення для мобільних пристроїв. Авторизувати підключення мобільних пристроїв до системи. Застосувати повне шифрування носія інформації пристрою або шифрування на підставі шифрування сховищ інформації (контейнерів).	АС-19 АС-19 (5)	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК. Суб’єкт господарювання ПЕК має застосувати повне шифрування пристроїв та шифрування сховищ інформації для

1	2	3	4	5
				захисту конфіденційності та цілісності інформації на всіх мобільних комп'ютерах та пристроях, які обробляють дані суб'єкта господарювання ПЕК.
16	Використання зовнішніх систем	Заборонити використання зовнішніх систем, крім систем дозволених суб'єктом господарювання ПЕК. Встановити такі положення, умови та дії щодо безпеки, які повинні бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованим користувачам за умов, положення та дії, які визначаються суб'єктом господарювання ПЕК. Дозволити авторизованим користувачам використовувати зовнішню систему для доступу до системи суб'єкту господарювання ПЕК або для обробки, зберігання чи передачі відкритої та конфіденційної інформації, лише після: перевірки реалізації дій безпеки на зовнішній системі, як зазначено в планах суб'єкта господарювання ПЕК. Обмежити використання портативних пристроїв зберігання даних авторизованими особами на зовнішніх системах.	AC-20 AC-20 (1) AC-20 (2)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
17	Публічно доступний контент	Навчати авторизованих осіб щодо нерозголошення відкритої та конфіденційної інформації в загальнодоступних системах.	AC-22	Переглядати вміст загальнодоступної системи на предмет

1	2	3	4	5
		Періодично переглядати вміст загальнодоступних систем на предмет наявності відкритої та конфіденційної інформації та видаляти таку інформацію, якщо її виявлено.		наявності інформації з обмеженим доступом кожні 90 календарних днів або в міру надходження нової інформації. Зазначена інформація має бути видалена в разі її виявлення.
Обізнаність та навчання (AT)				
18	Політика та процедури підвищення обізнаності та навчання	Розробити, задокументувати та розповсюдити серед працівників суб'єкта господарювання ПЕК або ролей політики та процедури у сфері кібербезпеки та захисту інформації, необхідні для виконання підвищення обізнаності та навчання. Періодично переглядати та оновлювати політики та процедури з частотою, визначеною суб'єктом господарювання ПЕК.	AT-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
19	Навчання з підвищення обізнаності	Забезпечити навчання користувачів системи з питань безпеки: як частину початкового навчання для нових користувачів і періодично після цього; якщо цього потребують зміни в системі або наступні події, визначені суб'єктом господарювання ПЕК; щодо розпізнавання та повідомлення про індикатори внутрішньої загрози, соціальної інженерії, та соціального шпіонажу. Оновлювати зміст тренінгу з безпекової обізнаності з періодичністю, визначеною суб'єктом господарювання	AT-2	Забезпечити навчання з питань безпеки та конфіденційності для користувачів системи, як частину початкового навчання для нових користувачів і один раз кожен календарний рік після цього.

1	2	3	4	5
		ПЕК та після подій, визначених суб'єктом господарювання ПЕК.	AT-2 (2)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
20	Рольове навчання	Провести тренінги з безпеки для працівників суб'єкту господарювання ПЕК на основі покладених обов'язків: перед авторизацією доступу до системи або відкритої та конфіденційної інформації, перед виконанням призначених обов'язків, а також після цього з частотою, визначеною суб'єктом господарювання ПЕК; коли цього вимагають зміни в системі або після події, визначеної суб'єктом господарювання ПЕК. Оновлювати зміст тренінгів з частотою, визначеною суб'єктом господарювання ПЕК на основі покладених обов'язків, а також після події, визначеної суб'єктом господарювання ПЕК.	AT-3	Забезпечити проведення навчання з питань безпеки та приватності на основі ролей для працівників з ролями та обов'язками перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків і кожен календарний рік після цього.
Аудит та підзвітність (AU-1)				
21	Події аудиту	Визначити перелік подій, які реєструються в системі. Переглядати та оновлювати, з частотою, визначеною суб'єктом господарювання ПЕК, типи подій, обрані для реєстрації.	AU-2	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
22	Зміст записів аудиту	Записи аудиту повинні містити таку інформацію: який тип події стався; коли відбулася подія; де відбулася подія; джерело події;	AU-3 AU-3 (1)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
		наслідки події; результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією. За потреби надавати додаткову інформацію для записів аудиту.		
23	Збереження записів аудиту	Згенерувати записи аудиту для вибраних типів подій згідно з вмістом записів аудиту, вказаних в пунктах 23–24 цього Профілю. Зберігати записи аудиту протягом періоду часу, який відповідає політиці зберігання записів аудиту.	AU-11	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
			AU-12	Забезпечити генерацію даних аудиту для типів подій, що перевіряються в AU-2, у всіх інформаційних системах та мережевих компонентах.
24	Реагування на відмови обробки даних аудиту	Сповіщати працівників або ролі суб'єкту господарювання ПЕК в межах періоду часу, визначеного суб'єктом господарювання ПЕК, у разі збою обробки даних аудиту. Виконати додаткові дії, визначені суб'єктом господарювання ПЕК.	AU-5	Виконати визначені суб'єктом господарювання ПЕК дії, які необхідно зробити, майже в реальному часі.
25	Огляд, аналіз і звітність аудиту	Переглядати та аналізувати з частотою, визначеною суб'єктом господарювання ПЕК, записи аудиту системи на предмет виявлення ознак і потенційного впливу не властивої або незвичної діяльності.	AU-6	Переглядати та аналізувати записи системного аудиту кожні 7 календарних

1	2	3	4	5
		Повідомляти про результати аудиту працівників суб'єкту господарювання ПЕК. Аналізувати та зіставляти записи аудиту в різних сховищах задля забезпечення ситуативної обізнаності в масштабах суб'єкта господарювання ПЕК.		днів для виявлення визначеної суб'єктом господарювання ПЕК неналежної або незвичайної діяльності.
			AU-6 (3)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
26	Скорочення записів аудиту та формування звіту	Впровадити функцію скорочення записів аудиту і створення звітів, яка підтримує перегляд записів аудиту, аналіз, дії до звітності. Зберігати оригінальний зміст і часовий порядок записів аудиту.	AU-7	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
27	Позначка часу	Використовувати внутрішній годинник у системі для створення позначок часу для записів аудиту. Застосовувати позначки часу, які відповідають деталізації вимірювання часу, визначеній суб'єктом господарювання ПЕК, і використовують: всесвітній координований час (UTC); фіксоване зміщення місцевого часу відносно UTC або зміщення місцевого часу як частину позначки часу.	AU-8	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
28	Захист інформації аудиту	Захистити інформацію аудиту та інструментів журналювання аудиту від несанкціонованого доступу, зміни та видалення. Надавати доступ до управління функціями аудиту тільки підмножині привілейованих користувачів або ролей.	AU-9 AU-9 (4)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
Управління конфігурацією (CM)				

1	2	3	4	5
29	Базова конфігурація	Розробляти та підтримувати під контролем налаштування поточної базової конфігурації системи. Переглядати та оновлювати з частотою, визначеною суб'єктом господарювання ПЕК, базову конфігурацію системи, а також при встановленні або модифікації компонентів системи.	СМ-2	Переглядати та оновлювати базові налаштування системи кожен календарний рік.
30	Налаштування конфігурації	Встановити, задокументувати та впровадити параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним діям та налаштуванням конфігурації, які визначені суб'єктом господарювання ПЕК. Визначити, задокументувати та затвердити будь-які відхилення від встановлених налаштувань конфігурації.	СМ-6	Визначити, задокументувати та затвердити будь-які відхилення від встановлених конфігураційних параметрів конфігурації для всіх конфігурованих компонентів системи на основі визначених суб'єктом господарювання ПЕК експлуатаційних вимог.
31	Управління змінами конфігурації	Визначити типи змін у конфігурації системи, які необхідно контролювати. Переглядати запропоновані зміни в конфігурації системи, схвалювати або відхиляти такі зміни, враховуючи вплив на безпеку. Упровадити та задокументувати затверджені зміни конфігурації системи.	СМ-3	Зберігати записи змін конфігурації системи впродовж 1 календарного року.

1	2	3	4	5
		Відстежувати та переглядати дії, пов’язані зі змінами в конфігурації системи, які необхідно контролювати.		
32	Аналіз впливу на безпеку та приватність	Проаналізувати вплив змін у системі на безпеку перед їх впровадженням.	СМ-4	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
33	Обмеження доступу до змін	Визначити, задокументувати, затвердити та впровадити фізичні та логічні обмеження доступу, пов’язані зі змінами в системі.	СМ-5	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
34	Мінімально необхідна функціональність	Налаштувати систему так, щоб вона надавала лише необхідні для виконання завдань функції. Заборонити або обмежити використання функцій, портів, протоколів, підключень і служб, визначених суб’єктом господарювання ПЕК. Переглядати з частотою, визначеною суб’єктом господарювання ПЕК, систему, щоб виявити непотрібні або небезпечні функції, порти, протоколи, з’єднання та служби. Вимкнути або видалити функції, порти, протоколи, з’єднання та служби, які є непотрібними або небезпечними.	СМ-7	Заборонити або обмежити використання всіх функцій, портів, протоколів, програмного забезпечення та послуг в системі, які були визначені як непотрібні та/або незахищені.
			СМ-7 (1)	Проводити перегляд системи, щонайменше, раз на рік або в міру внесення змін до системи чи виникнення інцидентів для

1	2	3	4	5
				виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг. Вимкнути всі функції, порти, протоколи, програмне забезпечення та послуги в системі, визначені як непотрібні та/або незахищені.
Планування безперервної роботи (CP)				
35	Політика та процедури планування безперервної роботи	Розробити, задокументувати та розповсюдити серед працівників суб'єкта господарювання ПЕК або ролей політики та процедури у сфері кібербезпеки та захисту інформації, необхідні для планування безперервної роботи. Періодично переглядати та оновлювати політики та процедури з частотою, визначеною суб'єктом господарювання ПЕК.	CP-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
36	План безперервної роботи та відновлення функціонування	Розробити план забезпечення безперервної роботи та відновлення функціонування системи на випадок надзвичайної ситуації, який: визначає основні завдання, функції та пов'язані з ними вимоги щодо безперервної роботи; забезпечує цілі, пріоритети та відповідні показники відновлення функціонування;	CP-2	Поширити копії плану забезпечення безперервної роботи та відновлення функціонування серед працівників,

1	2	3	4	5
		визначає ролі, обов'язки та відповідальних осіб з контактною інформацією; спрямований на підтримку основних завдань і функції, попри системні збої, компрометації або помилки; спрямований на повне відновлення функціонування системи без погіршення запланованих і реалізованих заходів захисту інформації. Розповсюдити копії плану забезпечення безперервної роботи та відновлення функціонування системи на випадок надзвичайної ситуації серед визначених працівників, відповідального за реагування на випадок надзвичайної ситуації (ідентифікованого за іменами та/або за ролями), та елементів суб'єкта господарювання ПЕК. Оновлювати план забезпечення безперервної роботи та відновлення функціонування системи на випадок надзвичайної ситуації з урахуванням змін в системі та суб'єкта господарювання ПЕК або проблем, що виникли під час впровадження, виконання або тестування плану. Захистити план забезпечення безперервної роботи та відновлення функціонування від несанкціонованого розголошення.		визначених суб'єктом господарювання ПЕК. Переглядати план забезпечення безперервної роботи та відновлення функціонування кожен календарний рік.
37	Навчання із забезпечення безперервної роботи	Проводити навчання із забезпечення безперервної роботи для користувачів системи відповідно до призначених ролей та обов'язків: протягом періоду часу, визначеного суб'єктом господарювання ПЕК, з моменту прийняття на себе ролі чи відповідальності за реагування на випадок надзвичайної ситуації або отримання доступу до системи;	СР-3	Проводити навчання користувачів системи на випадок надзвичайних ситуацій відповідно до визначених суб'єктом

1	2	3	4	5
		коли цього вимагають зміни в системі; надалі з частотою, визначеною суб'єктом господарювання ПЕК. Переглядати та оновлювати зміст навчання із забезпечення безперервної роботи з періодичністю, визначеною суб'єктом господарювання ПЕК, та наступні події, визначені суб'єктом господарювання ПЕК.		господарювання ПЕК ролей і обов'язків. Переглядати та оновлювати зміст тренінгів на випадок надзвичайних ситуацій кожен календарний рік.
Ідентифікація та автентифікація (ІА)				
38	Ідентифікація та автентифікація (користувачів суб'єкта господарювання ПЕК)	Унікально ідентифікувати та автентифікувати користувачів суб'єкта господарювання ПЕК і пов'язувати цю унікальну ідентифікацію з процесами, що діють від імені цих користувачів.	ІА-2	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
39	Ідентифікація та автентифікація пристроїв	Унікально ідентифікувати та автентифікувати пристрої перед встановленням з'єднання з системою.	ІА-3	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
40	Ідентифікація та автентифікація – багатофакторна автентифікація привілейованих облікових записів	Впровадити багатофакторну автентифікацію для доступу до облікових записів системи.	ІА-2 (1) ІА-2 (2)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
41	Ідентифікація та автентифікація (користувачів	Впровадити механізми автентифікації, стійкі до повторного відтворення, для доступу до облікових записів у системі.	ІА-2 (8)	Реалізувати стійкі до відтворення механізми

1	2	3	4	5
	суб’єкта господарювання ПЕК) – доступ до облікових записів – стійкість до відтворення			автентифікації для доступу до привілейованих облікових записів.
42	Управління ідентифікацією	Отримати дозвіл від працівників або ролей суб’єкта господарювання ПЕК на призначення ідентифікатора особи, групи, ролі, служби або пристрою. Вибрати та призначити ідентифікатор, який ідентифікує особу, групу, роль, службу або пристрій. Запобігати повторному використанню ідентифікаторів за період часу, визначений суб’єктом господарювання ПЕК.	ІА-4	Запобігання повторному використанню ідентифікаторів впродовж 1 календарного року для окремих осіб, груп, ролей.
43	Автентифікація на основі пароля	Вести перелік часто використовуваних, очікуваних або скомпрометованих паролів і періодично оновлювати його. Перевіряти, коли користувачі створюють або оновлюють паролі, чи не містяться вони у списку загальновживаних, очікуваних або скомпрометованих паролів. Передавати паролі тільки криптографічно захищеними каналами. Зберігати паролі в криптографічно захищеному вигляді. Встановити новий пароль при першому використанні після відновлення облікового запису. Впровадити правила складу та складності паролів, визначені суб’єктом господарювання ПЕК.	ІА-5 (1)	Вести список часто використовуваних, очікуваних або скомпрометованих паролів та оновлювати його кожні 90 календарних днів, а також при підозрі, що паролі суб’єкта господарювання ПЕК скомпрометовані. Застосовувати такі правила складу та складності:

1	2	3	4	5
				Дванадцяти символьний набір з великих, малих літер, цифр та спеціальних символів, що включає принаймні по одному символу кожного регістру та змінювати принаймні 50 процентів символів при створенні нових паролів.
44	Зворотний зв’язок автентифікатора	Забезпечити прихований зворотний зв’язок автентифікаційної інформації під час процесу автентифікації.	IA-6	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
45	Управління автентифіка-тором	Перевіряти ідентичність особи, групи, ролі, служби або пристрою, які отримують автентифікатор під час початкового розповсюдження автентифікатора. Встановити початковий вміст автентифікатора для всіх автентифікаторів, виданих суб’єктом господарювання ПЕК. Створити та впровадити адміністративні процедури для початкового розподілу автентифікаторів для втрачених, скомпрометованих або пошкоджених автентифікаторів, а також для відкликання автентифікаторів. Змінити автентифікатори за замовчуванням під час першого використання.	IA-5	Зміни/оновлення автентифікаторів не більше 180 календарних днів для паролів або коли відбуваються події, визначені суб’єктом господарювання ПЕК.

1	2	3	4	5
		Змінювати або оновлювати автентифікатори періодично або коли відбуваються події, визначені суб'єктом господарювання ПЕК. Захистити вміст автентифікатора від несанкціонованого розкриття та модифікації.		
Реагування на інциденти (IR)				
46	Обробка інциденту	Впровадити систему реагування на інциденти, яка відповідає плану реагування на інциденти і передбачає підготовку, виявлення та аналіз, локалізацію, ліквідацію та відновлення інцидентів.	IR-4	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
47	Моніторинг інциденту	Відстежувати та документувати інциденти, пов'язані з безпекою системи. Повідомляти про підозрілі інциденти до служби реагування на інциденти в суб'єкті господарювання ПЕК протягом часу, визначеного суб'єктом господарювання ПЕК. Повідомити інформацію про інцидент працівникам, визначеним суб'єктом господарювання ПЕК. Забезпечити ресурс підтримки реагування на інциденти, який пропонує поради та допомогу користувачам системи щодо обробки та звітування про інциденти.	IR-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
			IR-6	Вимагати від працівників повідомляти про підозрілі інциденти з безпеки та приватності впродовж 2 годин.
			IR-7	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
48	Перевірка реагувань на інциденти	Перевіряти ефективність спроможності реагування на інциденти з частотою, визначеною суб'єктом господарювання ПЕК.	IR-3	Перевіряти ефективність реагування системи на інциденти кожен

1	2	3	4	5
				календарний рік за допомогою визначених суб’єктом господарювання ПЕК тестів.
49	Навчання з реагування на інциденти	Проводити навчання з реагування на інциденти для користувачів системи відповідно до призначених ролей та обов’язків: протягом період часу, визначеного суб’єктом господарювання ПЕК, з моменту прийняття на себе ролі чи відповідальності за реагування на інцидент або отримання доступу до системи; коли цього вимагають зміни в системі; надалі з частотою, визначеною суб’єктом господарювання ПЕК. Переглядати та оновлювати зміст програм навчання з реагування на інциденти з періодичністю, визначеною суб’єктом господарювання ПЕК та наступні події, визначені суб’єктом господарювання ПЕК.	IR-2	Забезпечити навчання користувачів щодо системи реагування на інциденти, відповідно до призначених ролей та обов’язків в рамках 30 робочих днів, впродовж яких авторизована роль або відповідальність за реагування на інциденти. Надалі кожен календарний рік. Переглядати та оновлювати навчальний контент із реагування на інциденти кожен календарний рік.
50	План реагування на інциденти	Розробити план реагування на інцидент, який: надає суб’єкту господарювання ПЕК план дій для реалізації його можливостей реагування на інциденти, описує структуру та організацію системи реагування на	IR-8	Поширити копії плану реагування на інциденти серед працівників,

1	2	3	4	5
		інциденти, забезпечує високорівневий підхід до того, як спроможність реагування на інциденти вписується в загальну структуру суб'єкта господарювання ПЕК, визначає інциденти, про які необхідно повідомляти, вирішує питання обміну інформацією про інциденти, і розподіляє обов'язки між структурними підрозділами, працівниками або ролями. Розповсюдити копії плану реагування на інцидент серед визначених працівників, відповідального за реагування на інцидент (ідентифікованого за іменами та/або за ролями), та елементів суб'єкта господарювання ПЕК. Оновлювати план реагування на інциденти з урахуванням змін в системі та суб'єкті господарювання ПЕК або проблем, що виникли під час впровадження, виконання або тестування плану. Захистити план реагування на інциденти від несанкціонованого розголошення.		визначених суб'єктом господарювання ПЕК. Повідомляти про зміни плану реагування на інциденти працівників, визначених суб'єктом господарювання ПЕК.
Технічне обслуговування (МА)				
51	Інструменти для технічного обслуговування системи	Визначеній суб'єктом господарювання ПЕК особі або працівниками з кібербезпеки: затверджувати, контролювати та відстежувати використання інструментів для технічного обслуговування системи; перевіряти інструменти для технічного обслуговування на наявність неналежних або несанкціонованих модифікацій.	МА-3	Переглядати раніше затверджені інструменти технічного обслуговування системи кожен календарний рік.
			МА-3 (1) МА-3 (2)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
52	Віддалене обслуговування системи	Визначеній суб’єктом господарювання ПЕК особі або працівниками з кібербезпеки: затверджувати та контролювати віддалені сеанси з технічного обслуговування та діагностики; впровадити багатофакторну автентифікацію та стійкість до повторного відтворення при створенні віддалених сеансів технічного обслуговування та діагностики; забезпечити завершення сеансу та мережевих з’єднань після завершення віддаленого технічного обслуговування.	МА-4	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
53	Працівники з технічного обслуговування системи	Встановити процес авторизації працівників з технічного обслуговування системи. Вести список уповноважених суб’єктів господарювання або працівників з технічного обслуговування системи. Переконатися, що працівники суб’єкта господарювання ПЕК без супроводу, які виконують технічне обслуговування системи, мають необхідні дозволи на доступ. Призначити працівників суб’єкта господарювання ПЕК з необхідними повноваженнями доступу та технічною компетентністю для нагляду за діяльністю працівників з технічного обслуговування, які не мають необхідних повноважень доступу.	МА-5	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
Захист носіїв інформації (МР)				
54	Зберігання носіїв інформації	Фізично контролювати та безпечно зберігати носії інформації, що містять відкриту та конфіденційну інформацію.	МР-4	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.

1	2	3	4	5
55	Доступ до носіїв інформації	Обмежити доступ до конфіденційної інформації на носіях інформації.	MP-2	Обмежити доступ до всіх типів цифрових та/або нецифрових носіїв, що містять інформацію, не дозволену для публічного оприлюднення.
56	Знищення інформації на носіях інформації	Очистити носії інформації, що містять відкриту та конфіденційну інформацію, перед утилізацією, випуском з-під контролю суб'єкта господарювання ПЕК або повторним використанням.	MP-6	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
57	Маркування носіїв інформації	Маркувати носії інформації, що містять відкриту та конфіденційну інформацію, для позначення обмежень щодо розповсюдження, застережень стосовно поводження з ними та позначок безпеки.	MP-3	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
58	Переміщення носіїв інформації	Захистити і контролювати носії інформації, що містять відкриту та конфіденційну інформацію, під час транспортування за межі контрольованих територій. Вести облік носіїв інформації, що містять відкриту та конфіденційну інформацію, під час транспортування за межі контрольованих територій. Документувати дії, пов'язані з транспортуванням системних носіїв, які містять відкриту та конфіденційну інформацію.	MP-5 SC-28	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
59	Використання носіїв інформації	Обмежити або заборонити використання типів носіїв інформації, визначених суб'єктом господарювання ПЕК. Заборонити використання знімних носіїв інформації без ідентифікованого власника.	MP-7	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
60	Резервне копіювання	Захистити конфіденційність резервної копії, що розміщена на типах носіїв інформації, визначених суб’єктом господарювання ПЕК.	CP-9	Проводити резервне копіювання інформації користувачів, що міститься на системних компонентах, визначених суб’єктом господарювання ПЕК, кожні 7 календарних днів або як визначено в плані дій у надзвичайних ситуаціях, затвердженому суб’єктом господарювання ПЕК. Проводити резервне копіювання системної інформації на системному рівні, що міститься в системі, кожні 7 календарних днів або як визначено в плані дій у надзвичайних ситуаціях, затвердженому

1	2	3	4	5
				суб’єктом господарювання ПЕК. Проводити резервне копіювання системної документації, включно з документацією, пов’язаною із забезпеченням безпеки та приватності при створенні, отриманні, оновленні або як визначено в плані дій у надзвичайних ситуаціях, затвердженому суб’єктом господарювання ПЕК.
Програма (концепція) інформаційної безпеки (PM)				
61	Політика та процедури інформаційної безпеки	Розробити та поширити на суб’єктному рівні план програми (концепцію) з інформаційної безпеки, яка: містить огляд вимог до програми (концепції) безпеки та описує заходи управління програмою інформаційної безпеки і загальних заходів безпеки; містить визначення та розподіл ролей, обов’язків, заходи з координації діяльності суб’єкта господарювання ПЕК і забезпечення відповідності вимогам законодавства та	PM-1	Переглядати та оновлювати план програми (концепцію) інформаційної безпеки суб’єкта господарювання ПЕК кожен календарний рік та у випадках,

1	2	3	4	5
		іншим нормативно-правовим актам у сфері кібербезпеки та захисту інформації; відображає координацію між елементами суб'єкта господарювання ПЕК, що відповідають за інформаційну безпеку; затверджена вищою посадовою особою, що відповідає та підзвітна за управління ризиками, пов'язаними з діяльністю суб'єкта господарювання ПЕК (включно з завданнями (місією), функціями, активами, фізичними особами, іншими суб'єктами господарювання).		визначених суб'єктом господарювання ПЕК.
62	Інвентаризація системи	Розробити та оновити в період часу, визначений суб'єктом господарювання ПЕК, перелік систем суб'єкта господарювання ПЕК.	PM-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
63	Стратегія управління ризиками	Розробити комплексну стратегію управління: ризиками безпеки для операцій та активів суб'єкта господарювання ПЕК, фізичних осіб, інших суб'єктів господарювання і держави, пов'язаних з експлуатацією та використанням систем суб'єкта господарювання ПЕК. Реалізувати стратегію управління ризиками в масштабах суб'єкта господарювання ПЕК.	PM-9	Переглядати й оновлювати стратегію управління ризиками, кожен календарний рік або, якщо потрібно, у разі змін в суб'єкті господарювання ПЕК.
64	Програма інформування про загрози	Запровадити програму інформування про загрози, яка містить можливості спільного обміну інформацією між суб'єктами господарювання для аналізу загроз.	PM-16	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
65	Оцінка ризиків	Визначити та задокументувати: припущення, що впливають на оцінку ризиків, реагування на ризики та моніторинг ризиків;	PM-28	Переглядати та оновлювати підходи щодо визначення

1	2	3	4	5
		обмеження, що впливають на оцінку ризиків, реагування на ризики та моніторинг ризиків; пріоритети та компроміси, які розглядаються суб'єктом господарювання ПЕК для здійснення управління ризиками; стійкість суб'єкта господарювання ПЕК до ризиків. Інформувати працівників, що визначається суб'єктом господарювання ПЕК, про результати визначення ризиків.		ризиків кожен календарний рік.
66	План управління ризиками ланцюга постачання	Розробити план управління ризиками ланцюга постачання, пов'язаного з розробкою, придбанням, обслуговуванням та утилізацією систем, компонентів системи та послуг для системи. Реалізувати план управління ризиками ланцюга постачання послідовно в масштабах суб'єкта господарювання ПЕК.	PM-30	Переглядати та оновлювати план управління ризиками ланцюга постачання кожен календарний рік або, якщо потрібно, у разі змін в суб'єкті господарювання ПЕК.
Кадрова безпека (PS)				
67	Перевірка працівників	Перевіряти осіб перед тим, як надавати їм доступ до системи. Проводити повторні перевірки осіб відповідно до умов, що потребують повторної перевірки, визначених суб'єктом господарювання ПЕК.	PS-3	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
68	Звільнення працівників. Переведення працівників	Коли припиняється індивідуальна трудова діяльність: заборонити доступ до системи протягом період часу, визначеного суб'єктом господарювання ПЕК. Припинити дію або відкликати автентифікатори та облікові записи, пов'язані з особою. Відновити властивості системи, пов'язані з безпекою. Коли працівників призначають або переводять на інші посади суб'єкта господарювання ПЕК: переглянути та підтвердити поточну оперативну потребу в логічних і фізичних дозволах доступу до системи та об'єкта; ініціювати дії з переведення або призначення, визначені суб'єктом господарювання ПЕК, протягом період часу після дії з переведення або призначення, визначеного суб'єктом господарювання ПЕК; змінювати авторизацію доступу відповідно до будь-яких змін в оперативних потребах.	PS-4	Відключити доступ до системи у разі добровільного звільнення – якомога швидше, але не більше ніж за 5 календарних днів, у разі примусового звільнення – у той самий день, що й припинення трудових відносин.
			PS-5	Ініціювати дії з перепризначення, щоб забезпечити видалення або вимкнення всіх системних доступів, які більше не потрібні.
Фізичний захист і захист робочого середовища (PE)				
69	Авторизація фізичного доступу до місця розташування системи	Розробити, затвердити та підтримувати список осіб, які мають право доступу до фізичного місця розташування системи. Надавати повноваження для доступу до фізичного місця розташування системи. Періодично перевіряти список фізичного доступу до фізичного місця розташування системи. Переглядати список доступу до фізичного місця розташування	PE-2	Переглядати список доступу, у якому закріплений перелік працівників або ролей, яким дозволений санкціонований доступ до фізичного місця розташування

1	2	3	4	5
		системи з частотою, визначеною суб'єктом господарювання ПЕК. Видаляти осіб зі списку фізичного доступу до місця розташування системи, коли доступ більше не потрібен.		системи, кожен календарний рік.
70	Моніторинг фізичного доступу до місця розташування системи	Перевіряти фізичний доступ до місця розташування системи, щоб виявляти та реагувати на інциденти фізичної безпеки. Переглядати журнали фізичного доступу до місця розташування системи з частотою, визначеною суб'єктом господарювання ПЕК, та при виникненні подій, визначених суб'єктом господарювання ПЕК.	PE-6	Переглядати журнали фізичного доступу, кожні 90 календарних днів на предмет наявності подій, визначених суб'єктом господарювання ПЕК.
71	Альтернативне робоче місце розташування системи	Визначити альтернативні робочі місця, які дозволено використовувати працівникам. Застосовувати дії безпеки, визначені суб'єктом господарювання ПЕК, на альтернативних робочих місцях.	PE-17	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
72	Керування фізичним доступом до місця розташування системи	Контролювати фізичний доступ до місця, де знаходиться система: перевіряти індивідуальні фізичні дозволи на доступ перед наданням доступу; контролювати вхід і вихід за допомогою систем/пристроїв фізичного контролю доступу або охоронців. Вести журнали контролю фізичного доступу для точок входу та виходу. Супроводжувати відвідувачів і контролювати їх діяльність. Забезпечити захист ключів, кодів доступу та інших пристроїв фізичного доступу.	PE-3 PE-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
73	Контроль доступу до ліній електропередач. Контроль доступу до пристроїв виведення інформації	Контролювати фізичний доступ до розподільчих ліній системи і ліній електропередач на об’єктах суб’єкта господарювання ПЕК.	PE-4	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
Оцінювання ризику (RA)				
74	Оцінювання ризику	Оцінити ризик несанкціонованого розголошення в результаті обробки, зберігання або передачі конфіденційної інформації.	RA-3	Переглядати результати оцінювання ризиків та оновлювати оцінювання ризику кожен календарний рік.
75	Сканування вразливостей	Перевіряти та сканувати систему на наявність вразливостей з частотою, визначеною суб’єктом господарювання ПЕК та при виявленні нових вразливостей, що можуть вплинути на систему. Усунути вразливості системи протягом часу на реагування, визначеного суб’єктом господарювання ПЕК.	RA-5	Сканувати на наявність вразливостей в системі, щонайменше, кожні 30 днів та коли виявляються нові вразливості, які потенційно впливають на систему.
Оцінювання, акредитація та моніторинг безпеки (CA)				
76	Оцінювання безпеки	Оцінювати дії з частотою, визначеною суб’єктом господарювання ПЕК до безпеки системи та середовища	CA-2	Оцінювати заходи захисту в системі та в

1	2	3	4	5
		її функціонування, щоб визначити, чи були ці дії виконані.		її середовищі функціонування кожен календарний рік.
77	План усунення недоліків та контрольні показники	Розробити план дій і контрольні показники для системи: задокументувати заплановані заходи з виправлення слабких місць або недоліків, виявлених під час оцінювання безпеки; зменшити або усунути відомі недоліки системи. Оновити існуючий план дій і показників на основі результатів оцінки безпеки, незалежних аудитів або оглядів, а також безперервного моніторингу.	CA-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
78	Безперервний моніторинг	Розробити та впровадити стратегію безперервного моніторингу на рівні системи, що передбачає постійний моніторинг та оцінку безпеки.	CA-7	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
79	Взаємодія систем	Затвердити та керувати обміном конфіденційної інформації між системою та іншими системами. Документувати характеристики інтерфейсу, дії до безпеки та обов'язки для кожної системи. Переглядати та оновлювати договори про обмін з частотою, визначеною суб'єктом господарювання ПЕК.	CA-3	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
Захист інформаційної системи та комунікацій (SC)				
80	Захист периметра	Контролювати та управляти зв'язком на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи. Реалізувати підмережі для загальнодоступних компонентів системи, які фізично або логічно відділені від внутрішніх мереж.	SC-7	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
		Підключатися до зовнішніх мереж тільки через керовані інтерфейси, що складаються з пристроїв захисту периметра, розташованих відповідно до архітектури безпеки суб'єкта господарювання ПЕК.		
81	Інформація в загальних ресурсах системи	Запобігати несанкціонованій і ненавмисній передачі інформації за допомогою загальних ресурсів системи.	SC-4	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
82	Захист периметра – відмова за замовчуванням – дозвіл за винятком	Заборонити трафік мережевих комунікацій за замовчуванням і дозволити трафік мережевих комунікацій за винятком.	SC-7 (5)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
83	Цілісність передачі. Захист інформації у стані спокою	Реалізувати механізми криптографічного захисту для запобігання несанкціонованому розкриттю конфіденційної інформації під час передачі та зберігання.	SC-8	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
			SC-8 (1)	Запобігати несанкціонованому розголошенню інформації та виявляти зміни в ній.
			SC-28	Забезпечити конфіденційність та цілісність всієї інформації в стані спокою.

1	2	3	4	5
			SC-28 (1)	Впровадити криптографічні механізми для запобігання несанкціонованому розкриттю та модифікації всієї інформації у стані спокою на всі компоненти системи та носії інформації.
84	Відключення мережі	Завершити з'єднання з мережею, яке пов'язане із сеансом зв'язку в кінці сеансу або після періоду бездіяльності.	SC-10	Завершити з'єднання з мережею, яке пов'язане із сеансом зв'язку в кінці сеансу або після не більше ніж 15 хвилин бездіяльності.
85	Криптографічні ключі	Встановити криптографічні ключі в системі та керувати ними відповідно діям до встановлення та управління ключами, визначених суб'єктом господарювання ПЕК.	SC-12	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
86	Захист інформації	Впровадити типи криптографічного захисту, визначені суб'єктом господарювання ПЕК, при використанні системи для захисту конфіденційності відкритої та конфіденційної інформації.	SC-13	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
87	Спільні обчислювальні	Заборонити віддалену активацію спільних обчислювальних пристроїв і програмного забезпечення з	SC-15	Заборонити віддалену активацію спільних обчислювальних

1	2	3	4	5
	пристрої та застосунки	винятками, визначеними суб'єктом господарювання ПЕК. Надавати чіткі вказівки щодо використання користувачам, які фізично наявні біля пристроїв.		пристроїв (хмар) та застосунків з такими виключеннями: спеціальні апартаменти, розташовані в затверджених керівником суб'єкта господарювання ПЕК місцях.
88	Мобільний код	Визначити прийнятний мобільний код і технології мобільного коду. Авторизувати, відстежувати та контролювати використання мобільного коду.	SC-18	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
89	Автентифікація сесії	Захистити автентифікацію сеансів зв'язку.	SC-23	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
Цілісність системи та інформації (SI)				
90	Виправлення дефектів	Виявляти, повідомляти та виправляти недоліки системи. Встановлювати оновлення програмного забезпечення та вбудованих програм, що стосуються безпеки, протягом період часу після виходу оновлень, визначеного суб'єктом господарювання ПЕК.	SI-2	Інсталювати оновлення програмного забезпечення та оновлення вбудованого програмного забезпечення в межах 30 календарних днів.

1	2	3	4	5
91	Захист від шкідливого коду	Впровадити механізми захисту від шкідливого коду у визначених місцях системи для виявлення та знищення шкідливого коду. Оновлювати механізми захисту від шкідливого коду в міру виходу нових версій відповідно до політики та процедур управління конфігурацією, затверджених суб'єктом господарювання ПЕК. Налаштувати механізми захисту від шкідливого коду на: виконання сканування системи з частотою, визначеною суб'єктом господарювання ПЕК, та сканування файлів із зовнішніх джерел у реальному часі на кінцевих точках або точках входу та виходу з мережі під час завантаження, відкриття або виконання файлів; блокування шкідливого коду, поміщення шкідливого коду в карантин або інші дії у відповідь на виявлення шкідливого коду.	SI-3	Виконання періодичного сканування системи кожні 7 календарних днів і сканування файлів у реальному часі із зовнішніх джерел кінцевих точок та точок входу/виходу з мережі. Блокування та карантин шкідливого коду відповідальним адміністратором, визначеним суб'єктом господарювання ПЕК, у відповідь на виявлення шкідливого коду.
92	Попередження, рекомендації та директиви з безпеки	Отримувати попередження, рекомендації та директиви щодо безпеки системи від зовнішніх суб'єктів господарювання на постійній основі. Створювати та розповсюджувати внутрішні попередження системи, рекомендації та директиви щодо безпеки у разі потреби. Впроваджувати директиви з безпеки відповідно до часових рамок, встановлених суб'єктом господарювання ПЕК.	SI-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
93	Моніторинг системи	Проводити моніторинг системи для виявлення: атак та індикаторів потенційних атак; неавторизованих підключень. Виявляти неавторизоване використання системи. Проводити моніторинг вхідного та вихідного комунікаційного трафіка для виявлення незвичних або несанкціонованих дій чи умов.	SI-4	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
			SI-4 (4)	Проводити моніторинг вхідного та вихідного комунікаційного трафіку безперервно для виявлення незвичайних або несанкціонованих дій чи умов.
Планування безпеки (PL)				
94	Політика та процедури планування безпеки	Розробити, задокументувати та розповсюдити серед працівників суб'єкта господарювання ПЕК або ролей політики та процедури у сфері кібербезпеки та захисту інформації, необхідні для виконання дій безпеки. Періодично переглядати та оновлювати політики та процедури з частотою, визначеною суб'єктом господарювання ПЕК.	AC-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			AU-1	Розробити, задокументувати та поширити для всіх працівників. Переглядати та оновлювати поточну політику та процедури кожен календарний рік.

1	2	3	4	5
			CA-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			CM-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			IA-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			IR-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			MA-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			MP-1	Переглядати та оновлювати поточну політику та процедури

1	2	3	4	5
				кожен календарний рік.
			PE-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			PL-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			PS-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			RA-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			SA-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			SC-1	Переглядати та оновлювати поточну

1	2	3	4	5
				політику та процедури кожен календарний рік.
			SI-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			SR-1	Розробити, задокументувати та поширити серед призначених осіб або працівників з кібербезпеки. Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
95	Плани захисту інформації та персональних даних	Розробити план захисту інформації, який: визначає складові компоненти системи; описує робоче середовище системи; описує конкретні загрози для системи; надає огляд дій до безпеки системи; визначає з'єднання з іншими системами; визначає осіб, які виконують ролі та обов'язки в системі;	PL-2	Включає дії, пов'язані з безпекою та конфіденційністю, які впливають на систему, виконання яких вимагає планування та координацію з призначеною особою

1	2	3	4	5
		містить іншу інформацію, необхідну для захисту відкритої та конфіденційної інформації. Періодично переглядати та оновлювати план захисту інформації з частотою, визначеною суб'єктом господарювання ПЕК. Захистити план захисту інформації від неавторизованого розголошення.		або працівниками з кібербезпеки. Поширити копії планів захисту інформації та персональних даних і повідомляти про подальші зміни планів серед призначених осіб або працівників з кібербезпеки. Переглядати плани захисту інформації та персональних даних, щонайменше, щороку.
Придбання систем та послуг (SA)				
96	Компоненти системи, що не підтримуються	Замінювати компоненти системи, якщо розробник, постачальник або виробник більше не надає їх підтримку. Надати варіанти зменшення ризиків або альтернативні джерела для продовження підтримки компонентів, що не підтримуються, якщо їх неможливо замінити.	SA-22	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
Управління ризиками ланцюга постачання (SR)				
97	План управління ризиками ланцюга постачання	Розробити план управління ризиками ланцюга постачання, пов'язаними з дослідженнями та розробкою, проєктуванням, виробництвом, придбанням, доставленням (постачанням), інтеграцією, експлуатацією та обслуговуванням, а також утилізацією таких систем,	SR-2	Переглядати та оновлювати план управління ризиками ланцюга постачання, щонайменше, щороку.

1	2	3	4	5
		компонентів системи або послуг для системи, визначеною суб’єктом господарювання ПЕК. Періодично переглядати та оновлювати план управління ризиками ланцюга постачання з частотою, визначеною суб’єктом господарювання ПЕК. Захистити план управління ризиками ланцюга постачання від несанкціонованого розголошення та модифікації.		

Виконувач обов’язків начальника Управління кібербезпеки
та цифрового розвитку **Олександр ГУМЕНЮК**

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
31 березня 2026 року № 176

Галузевий профіль
безпеки системи, де обробляється службова інформація
для паливно-енергетичного комплексу України

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту відповідно до НД ТЗІ 3.6-006-24[1]	Мінімальні необхідні параметри налаштування заходів захисту відповідно до НД ТЗІ 3.6-006-24[1]
1	2	3	4	5
Управління доступом (АС)				
1	Управління обліковими записами	Визначити дозволені та заборонені типи облікових записів у системі. Створити, активувати, змінювати, деактивувати та видаляти облікові записи із системи відповідно до політики, процедур, передумов і критеріїв суб'єкта господарювання паливно-енергетичного комплексу України (далі – ПЕК). Визначити авторизованих користувачів системи, належність до груп і ролей, а також повноваження доступу (тобто привілеї).	АС-2	Повідомляти адміністраторів облікових записів, у межах визначеного суб'єктом господарювання ПЕК часового періоду для кожної ситуації, коли облікові записи більше не потрібні,

[1] Нормативний документ системи технічного захисту інформації НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем», затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30 квітня 2024 року № 234.

1	2	3	4	5
		Авторизувати доступ до системи на основі діючого дозволу на доступ та цілей використання системи. Контролювати використання облікових записів у системі. Вимкнути системні облікові записи, коли: термін дії облікових записів закінчився; облікові записи були неактивні протягом періоду часу, визначеного суб'єктом господарювання ПЕК; облікові записи більше не пов'язані з користувачем або особою; облікові записи порушують політику суб'єкта господарювання ПЕК, або виявлено значні ризики, пов'язані з фізичними особами. Оповістити працівників або ролі суб'єкта господарювання ПЕК про визначений суб'єктом господарювання ПЕК період часу, коли: облікові записи більше не потрібні; користувачі звільняються або переводяться; у системі наявні зміни, які потребують нових знань. Вимагати, щоб користувачі виходили з системи після визначеного суб'єктом господарювання ПЕК періоду часу очікуваної бездіяльності або за визначених суб'єктом господарювання ПЕК обставин.		працівники звільнені чи переведені та коли використовуються індивідуальні системи або наявні зміни, які потребують нових знань впродовж 24 годин. Проводити перегляд облікових записів на відповідність вимогам управління обліковими записами кожні 90 календарних днів.
			AC-2 (3)	Автоматично деактивувати облікові записи не пізніше 72 годин. Автоматично деактивувати облікові записи коли вони були неактивними впродовж 90 календарних днів.
			AC-2 (5)	Вимагати від користувачів виходити із системи в кінці кожного

1	2	3	4	5
				робочого дня користувача.
			AC-2 (13)	Деактивувати облікові записи користувачів, які становлять значний ризик, впродовж 30 хвилин після виявлення ризику.
2	Забезпечення доступу	Застосовувати затверджені суб'єктом господарювання ПЕК повноваження для логічного доступу до службової інформації та ресурсів у системі.	AC-3	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
3	Управління інформаційними потоками	Застосовувати затверджені суб'єктом господарювання ПЕК дії для управління потоками службової інформації всередині системи та між підключеними системами.	AC-4	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
4	Розмежування обов'язків	Визначити обов'язки осіб, які потребують розмежування. Встановити правила авторизації доступу для підтримки розмежування обов'язків.	AC-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
5	Мінімізація повноважень	Надавати користувачам або процесам, що діють від імені користувачів лише авторизований доступ до системи, необхідний для виконання поставлених завдань суб'єкта господарювання ПЕК. Авторизувати доступ до функцій безпеки, визначених суб'єктом господарювання ПЕК, та важливої для безпеки інформації.	AC-6 AC-6 (1) AC-6 (7) AU-9 (4)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
		Переглянути повноваження, надані користувачам з періодичністю, визначеною суб'єктом господарювання ПЕК, щоб підтвердити необхідність таких повноважень. Повторно призначити або видалити повноваження користувачів, за необхідності.		
6	Мінімізація повноважень – непривілейований доступ до незахищених функцій	Обмежити привілейовані облікові записи в системі для працівників або ролей, що визначаються суб'єктом господарювання ПЕК. Вимагати, щоб користувачі або ролі з привілейованими обліковими записами використовували непривілейовані облікові записи для доступу до незахищених функцій або інформації.	АС-6 (2)	Вимагати від користувачів облікових записів системи або ролей, які мають доступ до привілейованих функцій, використовувати непривілейовані облікові записи чи ролі під час доступу до незахищених функцій.
			АС-6 (5)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
7	Мінімізація повноважень – заборона непривілейованим	Заборонити непривілейованим користувачам виконувати привілейовані функції. Ведення журналу виконання привілейованих функцій.	АС-6 (9) АС-6 (10)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
	користувачам виконувати привілейовані функції			
8	Невдалі спроби входу в систему	Встановити обмеження на кількість, яка визначена суб'єктом господарювання ПЕК, невдалих спроб входу в систему протягом певного проміжку часу, визначеного суб'єктом господарювання ПЕК. Автоматично: заблокувати обліковий запис або комунікаційний вузол на період часу, визначений суб'єктом господарювання ПЕК; заблокувати обліковий запис або комунікаційний вузол до зняття адміністратором; відкласти наступний запит на вхід; повідомити системного адміністратора; вжити інших заходів, коли перевищено максимальну кількість невдалих спроб входу в систему.	AC-7	Повідомити відповідального адміністратора коли перевищено максимальну кількість невдалих спроб входу в систему.
9	Попередження про використання системи	Відображати повідомлення в системі з попередженнями про конфіденційність і безпеку відповідно до застосовних нормативно-правових актів у сфері кібербезпеки та захисту інформації для службової інформації перед тим, як надати доступ до системи.	AC-8	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
10	Управління паралельною сесією	Встановити обмеження на кількість, яка визначена суб'єктом господарювання ПЕК, одночасних сеансів для працівників або ролей, що визначаються суб'єктом господарювання ПЕК.	AC-10	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
11	Блокування пристрою	Заборонити доступ до системи за допомогою дій: ініціювання блокування пристрою після періоду часу бездіяльності, визначеного суб'єктом господарювання ПЕК; вимагати від користувача ініціювати блокування пристрою перед тим, як залишити систему без нагляду; зберігати блокування пристрою до відновлення користувачем доступу за допомогою встановлених процедур ідентифікації та автентифікації; приховати за допомогою блокування пристрою інформацію, яку раніше було видно на дисплеї, за допомогою публічно доступного зображення.	AC-11	Заборонити подальший доступ до системи шляхом ініціювання блокування пристрою через період, що не перевищує 30 хвилин бездіяльності або після отримання запиту від користувача. Користувачу ініціювати блокування пристрою перед тим, як залишити систему без нагляду.
			AC-11 (1)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
12	Припинення сеансу	Автоматично завершувати сеанс користувача після умови або події, що вимагають відключення сеансу, визначених суб'єктом господарювання ПЕК.	AC-12	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
13	Віддалений доступ	Встановити обмеження на використання, дії до конфігурації та підключення для кожного типу допустимого віддаленого доступу до системи. Авторизувати кожен тип віддаленого доступу до системи перед встановленням таких з'єднань.	AC-17 AC-17 (3) AC-17 (4)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
		Виконувати маршрутизацію всього віддаленого доступу до системи через авторизовані та керовані точки контролю управління доступом до мережі. Авторизувати віддалене виконання привілейованих команд і віддалений доступ до інформації, важливої для безпеки.		
14	Бездротовий доступ	Встановити обмеження на використання, дії до конфігурації та підключення для кожного типу бездротового доступу до системи. Авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення. Вимкнути можливості бездротового доступу, якщо вони не призначені для використання, перед їх запуском та розгортанням. Захистити бездротовий доступ до системи за допомогою автентифікації та шифрування.	AC-18	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
			AC-18 (1)	Забезпечити захист бездротового доступу до системи за допомогою автентифікації користувачів та пристроїв і шифрування.
			AC-18 (3)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
15	Контроль доступу для мобільних пристроїв	Встановити обмеження на використання, дії до конфігурації та підключення для мобільних пристроїв. Авторизувати підключення мобільних пристроїв до системи.	AC-19	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
			AC-19 (5)	Суб'єкт господарювання ПЕК має застосувати повне

1	2	3	4	5
		Застосувати повне шифрування носія інформації пристрою або шифрування на основі шифрування сховищ інформації (контейнерів).		шифрування пристроїв та шифрування сховищ інформації для захисту конфіденційності та цілісності інформації на всіх мобільних комп'ютерах та пристроях, які обробляють дані суб'єкта господарювання ПЕК.
16	Використання зовнішніх систем	Заборонити використання зовнішніх систем, крім систем, дозволених суб'єктом господарювання ПЕК. Встановити такі положення, умови та дії щодо безпеки, визначені суб'єктом господарювання ПЕК, які повинні бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованим особам. Дозволити авторизованим особам використовувати зовнішню систему для доступу до системи суб'єкта господарювання ПЕК або для обробки, зберігання чи передачі службової інформації, лише після перевірки реалізації дій безпеки на зовнішній системі, як зазначено в планах безпеки суб'єкта господарювання ПЕК. Обмежити використання портативних пристроїв зберігання даних авторизованими особами на зовнішніх системах.	AC-20 AC-20 (1) AC-20 (2)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
17	Публічно доступний контент	Навчати авторизованих осіб щодо нерозголошення службової інформації в загальнодоступних системах. Періодично переглядати вміст загальнодоступних систем на предмет наявності службової інформації та видаляти таку інформацію, якщо її виявлено.	АС-22	Переглядати вміст загальнодоступної системи на предмет наявності інформації з обмеженим доступом кожні 90 календарних днів або в міру надходження нової інформації. Зазначена інформація має бути видалена в разі її виявлення.
Обізнаність та навчання (АТ)				
18	Політика та процедури підвищення обізнаності та навчання	Розробити, задокументувати та розповсюдити серед визначених працівників суб'єкта господарювання ПЕК або ролей політики та процедури у сфері кібербезпеки та захисту інформації, необхідні для виконання підвищення обізнаності та навчання. Періодично переглядати та оновлювати політики та процедури з частотою, визначеною суб'єктом господарювання ПЕК.	АТ-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
19	Навчання з підвищення обізнаності	Забезпечити навчання користувачів системи з питань безпеки: як частину початкового навчання для нових користувачів і періодично після цього; якщо цього потребують зміни в системі або наступні події, визначені суб'єктом господарювання ПЕК;	АТ-2	Забезпечити навчання з питань безпеки та конфіденційності для користувачів системи, як частину початкового навчання для нових

1	2	3	4	5
		щодо розпізнавання та повідомлення про індикатори внутрішньої загрози, соціальної інженерії, та соціального шпіонажу. Оновлювати зміст тренінгу з безпекової обізнаності з визначеною суб'єктом господарювання ПЕК періодичністю та після визначеної суб'єктом господарювання ПЕК події.		користувачів і, один раз кожен календарний рік після цього.
			AT-2 (2) AT-2 (3)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
20	Рольове навчання	Провести тренінги з безпеки для працівників суб'єкту господарювання ПЕК на основі покладених обов'язків: перед авторизацією доступу до системи або службової інформації та перед виконанням призначених обов'язків, а також з частотою визначеною суб'єктом господарювання ПЕК після цього; коли цього вимагають зміни в системі або після події, визначеної суб'єктом господарювання ПЕК. Оновлювати зміст тренінгів з частотою, визначеною суб'єктом господарювання ПЕК на основі покладених обов'язків, а також після події, визначеної суб'єктом господарювання ПЕК.	AT-3	Забезпечити проведення навчання з питань безпеки та приватності на основі ролей для працівників з ролями та обов'язками перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків і кожен календарний рік після цього.
Аудит та підзвітність (AU)				
21	Події аудиту	Визначити перелік подій, які реєструються в системі. Переглядати та оновлювати типи подій, обрані для реєстрації з частотою, визначеною суб'єктом господарювання ПЕК.	AU-2	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
22	Зміст записів аудиту	Записи аудиту повинні містити таку інформацію: який тип події стався; коли відбулася подія; де відбулася подія; джерело події; наслідки події; результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією. За потреби надавати додаткову інформацію для записів аудиту.	AU-3 AU-3 (1)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
23	Збереження записів аудиту	Згенерувати записи аудиту для вибраних типів подій згідно з вмістом записів аудиту, вказаних в пунктах 23–24 цього Профілю. Зберігати записи аудиту протягом періоду часу, який відповідає політиці зберігання записів аудиту.	AU-11	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
			AU-12	Забезпечити генерацію даних аудиту для типів подій, що перевіряються в AU-2, у всіх інформаційних системах та мережевих компонентах.
24	Реагування на відмови обробки даних аудиту	Сповіщати працівників або ролі суб'єкта господарювання ПЕК у разі збою обробки даних аудиту в межах періоду часу, визначеного суб'єктом господарювання ПЕК.	AU-5	Виконати визначені суб'єктом господарювання ПЕК дії, які необхідно

1	2	3	4	5
		Виконати додаткові дії, визначені суб'єктом господарювання ПЕК.		зробити, майже в реальному часі.
25	Огляд, аналіз і звітність аудиту	Переглядати та аналізувати з частотою, визначеною суб'єктом господарювання ПЕК, записи аудиту системи на предмет виявлення ознак і потенційного впливу не властивої або незвичної діяльності. Повідомляти про результати аудиту працівникам суб'єкта господарювання ПЕК. Аналізувати та зіставляти записи аудиту в різних сховищах задля забезпечення ситуативної обізнаності в масштабах суб'єкта господарювання ПЕК.	AU-6	Переглядати та аналізувати записи системного аудиту, кожні 7 календарних днів для виявлення визначеної суб'єктом господарювання ПЕК неналежної або незвичайної діяльності.
			AU-6 (3)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
26	Скорочення записів аудиту та формування звіту	Впровадити функцію скорочення записів аудиту і створення звітів, яка підтримує перегляд записів аудиту, аналіз, дії до звітності. Зберігати оригінальний зміст і часовий порядок записів аудиту.	AU-7	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
27	Позначка часу	Використовувати внутрішній годинник у системі для створення позначок часу для записів аудиту. Застосовувати позначки часу, які відповідають деталізації вимірювання часу, визначеної суб'єктом господарювання ПЕК, і використовують: всесвітній координований час (далі – UTC);	AU-8	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
		фіксоване зміщення місцевого часу відносно UTC або зміщення місцевого часу, як частину позначки часу.		
28	Захист інформації аудиту	Захистити інформацію аудиту та інструментів журналювання аудиту від несанкціонованого доступу, зміни та видалення. Надавати доступ до управління функціями аудиту тільки підмножині привілейованих користувачів або ролей.	AU-9 AU-9 (4)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
Управління конфігурацією (CM)				
29	Базова конфігурація	Розробляти та підтримувати під контролем налаштування поточної базової конфігурації системи. Переглядати та оновлювати з частотою, визначеною суб'єктом господарювання ПЕК, базову конфігурацію системи, а також при встановленні або модифікації компонентів системи.	CM-2	Переглядати та оновлювати базові налаштування системи кожен календарний рік.
30	Налаштування конфігурації	Встановити, задокументувати та впровадити параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним діям та налаштуванням конфігурації, які визначені суб'єктом господарювання ПЕК. Визначити, задокументувати та затвердити будь-які відхилення від встановлених налаштувань конфігурації.	CM-6	Визначити, задокументувати та затвердити будь-які відхилення від встановлених конфігураційних параметрів конфігурації для всіх конфігурованих компонентів системи на основі визначених суб'єктом

1	2	3	4	5
				господарювання ПЕК експлуатаційних вимог.
31	Управління змінами конфігурації	Визначити типи змін у конфігурації системи, які необхідно контролювати. Переглядати запропоновані зміни в конфігурації системи, схвалювати або відхиляти такі зміни, враховуючи вплив на безпеку. Впровадити та задокументувати затверджені зміни конфігурації системи. Відстежувати та переглядати дії, пов'язані зі змінами в конфігурації системи, які необхідно контролювати.	СМ-3	Зберігати записи змін конфігурації системи впродовж 1 календарного року.
32	Аналіз впливу на безпеку та приватність	Проаналізувати вплив змін у системі на безпеку перед їх впровадженням. Переконатися, що дії до безпеки системи продовжують задовольнятися після впровадження змін у системі.	СМ-4 СМ-4 (2)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
33	Обмеження доступу до змін	Визначити, задокументувати, затвердити та впровадити фізичні та логічні обмеження доступу, пов'язані зі змінами в системі.	СМ-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
34	Мінімально необхідна функціональність	Налаштувати систему так, щоб вона надавала лише необхідні для виконання завдань функції. Заборонити або обмежити використання функцій, портів, протоколів, підключень і служб, визначених суб'єктом господарювання ПЕК. Переглядати систему з частотою, визначеною суб'єктом господарювання ПЕК, щоб виявити	СМ-7	Заборонити або обмежити використання всіх функцій, портів, протоколів, програмного забезпечення та

1	2	3	4	5
		непотрібні або небезпечні функції, порти, протоколи, з’єднання та служби. Вимкнути або видалити функції, порти, протоколи, з’єднання та служби, які є непотрібними або небезпечними.		послуг в системі, які були визначені як непотрібні та/або незахищені.
			СМ-7 (1)	Проводити перегляд системи, щонайменше, раз на рік або в міру внесення змін до системи чи виникнення інцидентів для виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг. Вимкнути всі функції, порти, протоколи, програмне забезпечення та послуги в системі, визначені як непотрібні та/або незахищені.
35	Мінімально необхідна функціональність – авторизоване програмне	Визначити програмне забезпечення, дозволене для виконання в системі. Впровадити політику «заборонити все, дозволити за винятком» для виконання дозволеного програмного забезпечення в системі.	СМ-7 (5)	Переглядати та оновлювати список авторизованих програм кожен календарний рік.

1	2	3	4	5
	забезпечення – білий список	Переглянути та оновити список дозволеного програмного забезпечення з частотою, визначеною суб'єктом господарювання ПЕК.		
36	Інвентаризація компонентів системи	Розробити та задокументувати інвентаризацію компонентів системи. Переглядати та оновлювати інвентаризацію компонентів системи з частотою, визначеною суб'єктом господарювання ПЕК. Оновлювати інвентаризацію компонентів системи в рамках встановлення, видалення та оновлення системи.	СМ-8	Включає інформацію для досягнення підзвітності компонентів системи: технічні характеристики обладнання (виробник, тип, модель, серійний номер, фізичне місцезнаходження); програмне забезпечення та інформація про ліцензію на програмне забезпечення; власник інформаційної системи/компонента; для мережевого компонента або пристрою – найменування обладнання. Переглядати та оновлювати опис

1	2	3	4	5
				компонентів системи кожен календарний рік.
			СМ-8 (1)	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
37	Розташування інформації	Визначити та задокументувати місцезнаходження службової інформації та компонентів системи, в яких обробляється та зберігається інформація. Задокументувати зміни в системі або в компонентах системи, де обробляється та зберігається службова інформація.	СМ-12	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
38	Базова конфігурація – конфігурація систем та компонентів для сфер з високим ризиком	Надавати системи або системні компоненти з конфігураціями, визначені суб’єктом господарювання ПЕК, особам, які прямують до зони підвищеного ризику. Застосовувати дії безпеки, визначені суб’єктом господарювання ПЕК, до систем або компонентів, коли особи повертаються зі службового відрядження.	СМ-2 (7)	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
Планування безперервної роботи (СР)				
39	Політика та процедури планування безперервної роботи	Розробити, задокументувати та розповсюдити серед працівників суб’єкта господарювання ПЕК або ролей політики та процедури у сфері кібербезпеки та захисту інформації, необхідні для планування безперервної роботи.	СР-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.

1	2	3	4	5
		Періодично переглядати та оновлювати політики та процедури з частотою, визначеною суб’єктом господарювання ПЕК.		
40	План безперервної роботи та відновлення функціонування	Розробити план забезпечення безперервної роботи та відновлення функціонування системи на випадок надзвичайної ситуації, який: визначає основні завдання, функції та пов’язані з ними вимоги щодо безперервної роботи; забезпечує цілі, пріоритети та відповідні показники відновлення функціонування; визначає ролі, обов’язки та відповідальних осіб з контактною інформацією; спрямований на підтримку основних завдань і функцій, незважаючи на системні збої, компрометації або помилки; спрямований на повне відновлення функціонування системи без погіршення запланованих і реалізованих заходів захисту інформації. Розповсюдити копії плану забезпечення безперервної роботи та відновлення функціонування системи на випадок надзвичайної ситуації серед визначених працівників, відповідального за реагування на випадок надзвичайної ситуації (ідентифікованого за іменами та/або за ролями), та елементів суб’єкта господарювання ПЕК. Оновлювати план забезпечення безперервної роботи та відновлення функціонування системи на випадок надзвичайної ситуації з урахуванням змін	СР-2	Поширити копії плану забезпечення безперервної роботи та відновлення функціонування серед працівників, визначених суб’єктом господарювання ПЕК. Переглядати план забезпечення безперервної роботи та відновлення функціонування кожен календарний рік.

1	2	3	4	5
		в системі та суб’єкті господарювання ПЕК або проблем, що виникли під час впровадження, виконання або тестування плану. Захистити план забезпечення безперервної роботи та відновлення функціонування від несанкціонованого розголошення.		
41	Навчання із забезпечення безперервної роботи	Проводити навчання із забезпечення безперервної роботи для користувачів системи відповідно до призначених ролей та обов’язків: протягом періоду часу, визначеного суб’єктом господарювання ПЕК, з моменту прийняття на себе ролі чи відповідальності за реагування на випадок надзвичайної ситуації або отримання доступу до системи; коли цього вимагають зміни в системі; надалі з частотою, визначеною суб’єктом господарювання ПЕК. Переглядати та оновлювати зміст навчання із забезпечення безперервної роботи з періодичністю, визначеною суб’єктом господарювання ПЕК, та наступні події, визначені суб’єктом господарювання ПЕК.	СР-3	Проводити навчання користувачів системи на випадок надзвичайних ситуацій відповідно до визначених суб’єктом господарювання ПЕК ролей і обов’язків. Переглядати та оновлювати зміст тренінгів на випадок надзвичайних ситуацій кожен календарний рік.
Ідентифікація та автентифікація (ІА)				
42	Ідентифікація та автентифікація користувачів суб’єкта	Унікально ідентифікувати та автентифікувати користувачів суб’єкта господарювання ПЕК і пов’язувати цю унікальну ідентифікацію з процесами, що діють від імені цих користувачів.	ІА-2 ІА-11	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.

1	2	3	4	5
	господарювання ПЕК	Повторно автентифікувати користувачів, коли виникають визначені суб’єктом господарювання ПЕК обставини або ситуації, що вимагають повторної автентифікації.		
43	Ідентифікація та автентифікація пристроїв	Унікально ідентифікувати та автентифікувати пристрої перед встановленням з’єднання з системою.	IA-3	
44	Ідентифікація та автентифікація (користувачів суб’єкта господарювання ПЕК) – багатофакторна автентифікація привілейованих облікових записів	Упровадити багатофакторну автентифікацію для доступу до облікових записів системи.	IA-2 (1) IA-2 (2)	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
45	Ідентифікація та автентифікація (користувачів суб’єкта господарювання ПЕК) – доступ до облікових записів – стійкість до відтворення	Упровадити механізми автентифікації, стійкі до повторного відтворення, для доступу до облікових записів у системі.	IA-2 (8)	Реалізувати стійкі до відтворення механізми автентифікації для доступу до привілейованих облікових записів.

1	2	3	4	5
46	Управління ідентифікацією	Отримати дозвіл від працівників або ролей суб'єкта господарювання ПЕК на призначення ідентифікатора особи, групи, ролі, служби або пристрою. Вибрати та призначити ідентифікатор, який ідентифікує особу, групу, роль, службу або пристрій. Запобігати повторному використанню ідентифікаторів за період часу, визначений суб'єктом господарювання ПЕК. Керувати індивідуальними ідентифікаторами, унікально ідентифікуючи кожну особу за характеристиками, що ідентифікують статус особи, які визначені суб'єктом господарювання ПЕК.	ІА-4	Запобігання повторному використанню ідентифікаторів впродовж 1 календарного року для окремих осіб, груп, ролей.
			ІА-4 (4)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
47	Управління автентифікатором, автентифікація на основі пароля	Вести перелік часто використовуваних, очікуваних або скомпрометованих паролів і періодично оновлювати його. Перевіряти, коли користувачі створюють або оновлюють паролі, чи відсутні вони у списку загальновживаних, очікуваних або скомпрометованих паролів. Передавати паролі тільки криптографічно захищеними каналами. Зберігати паролі в криптографічно захищеному вигляді. Встановити новий пароль при першому використанні після відновлення облікового запису. Впровадити правила складу та складності паролів, визначені суб'єктом господарювання ПЕК.	ІА-5 (1)	Вести список часто використовуваних, очікуваних або скомпрометованих паролів та оновлювати його кожні 90 календарних днів, а також при підозрі, що паролі суб'єкта господарювання ПЕК скомпрометовані. Застосовувати такі правила складу та складності:

1	2	3	4	5
				Дванадцяти символьний набір з великих, малих літер, цифр та спеціальних символів, що включає принаймні по одному символу кожного регістру та змінювати принаймні 50 процентів символів при створенні нових паролів.
48	Зворотний зв’язок автентифікатора	Забезпечити прихований зворотний зв’язок автентифікаційної інформації під час процесу автентифікації.	IA-6	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
49	Управління автентифікатором	Перевіряти ідентичність особи, групи, ролі, служби або пристрою, які отримують автентифікатор під час початкового розповсюдження автентифікатора. Встановити початковий вміст автентифікатора для всіх автентифікаторів, виданих суб’єктом господарювання ПЕК. Створити та впровадити адміністративні процедури стосовно початкового розподілу автентифікаторів для втрачених, скомпрометованих або пошкоджених автентифікаторів, а також для відкликання автентифікаторів. Змінити автентифікатори за замовчуванням під час першого використання.	IA-5	Зміни/оновлення автентифікаторів не більше 180 календарних днів для паролів або коли відбуваються події, визначені суб’єктом господарювання ПЕК.

1	2	3	4	5
		Змінювати або оновлювати автентифікатори періодично або коли відбуваються події, визначені суб'єктом господарювання ПЕК. Захистити вміст автентифікатора від несанкціонованого розкриття та модифікації.		
Реагування на інциденти (IR)				
50	Обробка інциденту	Впровадити систему реагування на інциденти, яка відповідає плану реагування на інциденти і передбачає підготовку, виявлення та аналіз, локалізацію, ліквідацію та відновлення після інцидентів.	IR-4	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
51	Моніторинг інциденту	Відстежувати та документувати інциденти, пов'язані з безпекою системи. Повідомляти про підозрілі інциденти до служби реагування на інциденти суб'єкта господарювання ПЕК протягом часу, визначеного суб'єктом господарювання ПЕК. Повідомити інформацію про інцидент працівникам, які визначені суб'єктом господарювання ПЕК. Забезпечити ресурс підтримки реагування на інциденти, який пропонує поради та допомогу користувачам системи щодо обробки та звітування про інциденти.	IR-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
			IR-6	Вимагати від працівників повідомляти про підозрілі інциденти з безпеки та приватності впродовж 2 годин.
			IR-7	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
52	Перевірка реагувань на інциденти	Перевіряти ефективність спроможності реагування на інциденти з частотою, визначеною суб'єктом господарювання ПЕК.	IR-3	Перевіряти ефективність реагування системи на інциденти, кожен

1	2	3	4	5
				календарний рік за допомогою визначених суб'єктом господарювання ПЕК тестів.
53	Навчання з реагування на інциденти	Проводити навчання з реагування на інциденти для користувачів системи відповідно до призначених ролей та обов'язків: протягом період часу, визначеного суб'єктом господарювання ПЕК, з моменту прийняття на себе ролі чи відповідальності за реагування на інцидент або отримання доступу до системи; коли цього вимагають зміни в системі; надалі з частотою, визначеною суб'єктом господарювання ПЕК. Переглядати та оновлювати зміст програм навчання з реагування на інциденти з періодичністю, визначеною суб'єктом господарювання ПЕК та наступні події, визначені суб'єктом господарювання ПЕК.	IR-2	Забезпечити навчання користувачів щодо системи реагування на інциденти, відповідно до призначених ролей та обов'язків в рамках 30 робочих днів, впродовж яких авторизована роль або відповідальність за реагування на інциденти. Надалі кожен календарний рік. Переглядати та оновлювати навчальний контент із реагування на інциденти кожен календарний рік.
54	План реагування на інциденти	Розробити план реагування на інцидент, який: надає суб'єкту господарювання ПЕК план дій для реалізації його можливостей реагування на інциденти, описує структуру та організацію	IR-8	Поширити копії плану реагування на інциденти серед працівників,

1	2	3	4	5
		системи реагування на інциденти, забезпечує високорівневий підхід до того, як спроможність реагування на інциденти вписується в загальну структуру суб'єкта господарювання ПЕК, визначає інциденти, про які необхідно повідомляти, вирішує питання обміну інформацією про інциденти, і розподіляє обов'язки між структурними підрозділами, працівниками або ролями. Розповсюдити копії плану реагування на інцидент серед визначених працівників, відповідального за реагування на інцидент (ідентифікованого за іменами та/або за ролями), та елементів суб'єкта господарювання ПЕК. Оновлювати план реагування на інциденти з урахуванням змін в системі та суб'єкті господарювання ПЕК або проблем, що виникли під час впровадження, виконання або тестування плану. Захистити план реагування на інциденти від несанкціонованого розголошення.		визначених суб'єктом господарювання ПЕК. Повідомляти про зміни плану реагування на інциденти працівників, визначених суб'єктом господарювання ПЕК.
Технічне обслуговування (МА)				
55	Інструменти для технічного обслуговування системи	Визначеній суб'єктом господарювання ПЕК особі або працівниками з кібербезпеки: затверджувати, контролювати та відстежувати використання інструментів для технічного обслуговування системи; перевіряти інструменти для технічного обслуговування на наявність неналежних або несанкціонованих модифікацій;	МА-3	Переглядати раніше затверджені інструменти технічного обслуговування системи кожен календарний рік.
			МА-3 (1)	

1	2	3	4	5
		запобігати вилученню обладнання для обслуговування системи, що містить службову інформацію, шляхом перевірки відсутності службової інформації на обладнанні, санітарної обробки або знищення обладнання, або утримання обладнання в межах об'єкта.	МА-3 (2) МА-3 (3)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
56	Віддалене обслуговування системи	Визначеній суб'єктом господарювання ПЕК особі або працівниками з кібербезпеки: затверджувати та контролювати віддалені сеанси з технічного обслуговування та діагностики; впровадити багатофакторну автентифікацію та стійкість до повторного відтворення при створенні віддалених сеансів технічного обслуговування та діагностики; забезпечити завершення сеансу та мережевих з'єднань після завершення віддаленого технічного обслуговування.	МА-4	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
57	Працівники з технічного обслуговування системи	Встановити процес авторизації працівників з технічного обслуговування системи. Вести список уповноважених суб'єктів господарювання або працівників з технічного обслуговування системи. Переконатися, що працівники суб'єкта господарювання ПЕК без супроводу, які виконують технічне обслуговування системи, мають необхідні дозволи на доступ. Призначити працівників суб'єкта господарювання ПЕК з необхідними повноваженнями доступу та технічною компетентністю для нагляду за	МА-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
		діяльністю працівників з технічного обслуговування, які не мають необхідних повноважень доступу.		
Захист носіїв інформації (MP)				
58	Зберігання носіїв інформації	Фізично контролювати та безпечно зберігати носії інформації, що містять службову інформацію.	MP-4	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
59	Доступ до носіїв інформації	Обмежити доступ до службової інформації на носіях інформації.	MP-2	Обмежити доступ до всіх типів цифрових та/або нецифрових носіїв, що містять інформацію, не дозволену для публічного оприлюднення.
60	Знищення інформації на носіях інформації	Очистити носії інформації, що містять службову інформацію, перед утилізацією, випуском з-під контролю суб'єкта господарювання ПЕК або повторним використанням.	MP-6	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
61	Маркування носіїв інформації	Маркувати носії інформації, що містять службову інформацію, для позначення обмежень щодо розповсюдження, застережень стосовно поводження з ними та позначок безпеки.	MP-3	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
62	Транспортування носіїв інформації	Захистити і контролювати носії інформації, що містять службову інформацію, під час транспортування за межі контрольованих територій.	MP-5 SC-28	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
		Вести облік носіїв інформації, що містять службову інформацію, під час транспортування за межі контрольованих територій. Документувати дії, пов'язані з транспортуванням системних носіїв, які містять службову інформацію.		
63	Використання носіїв інформації	Обмежити або заборонити використання типів носіїв інформації, визначених суб'єктом господарювання ПЕК. Заборонити використання знімних носіїв інформації без ідентифікованого власника.	MP-7	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
64	Резервне копіювання	Захистити конфіденційність резервної копії. Впровадити криптографічні механізми для запобігання несанкціонованому розкриттю службової інформації в місцях зберігання резервних копій.	CP-9	Проводити резервне копіювання інформації користувачів, що міститься на системних компонентах, визначених суб'єктом господарювання ПЕК, кожні 7 календарних днів або як визначено в плані дій у надзвичайних ситуаціях, затвердженому суб'єктом господарювання ПЕК.

1	2	3	4	5
				Проводити резервне копіювання системної інформації на системному рівні, що міститься в системі, кожні 7 календарних днів або як визначено в плані дій у надзвичайних ситуаціях, затвердженому суб’єктом господарювання ПЕК. Проводити резервне копіювання системної документації, включно з документацією, пов’язаною із забезпеченням безпеки та приватності при створенні, отриманні, оновленні або як визначено в плані дій у надзвичайних ситуаціях, затвердженому

1	2	3	4	5
				суб’єктом господарювання ПЕК.
			СР-9 (8)	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
Програма (концепція) інформаційної безпеки (РМ)				
65	Політика та процедури інформаційної безпеки	Розробити та поширити на суб’єктному рівні план програми (концепцію) з інформаційної безпеки, яка: містить огляд вимог до програми (концепції) безпеки та описує заходи управління програмою інформаційної безпеки і загальних заходів безпеки; містить визначення та розподіл ролей, обов’язків, заходи з координації діяльності суб’єкта господарювання ПЕК і забезпечення відповідності вимогам законодавства та іншим нормативно-правовим актам у сфері кібербезпеки та захисту інформації; відображає координацію між елементами суб’єкта господарювання ПЕК, що відповідають за інформаційну безпеку; затверджена вищою посадовою особою, що відповідає та підзвітна за управління ризиками, пов’язаними з діяльністю суб’єкта господарювання ПЕК (включно з завданнями (місією), функціями, активами, фізичними особами, іншими суб’єктами господарювання).	РМ-1	Переглядати та оновлювати план програми (концепцію) інформаційної безпеки суб’єкта господарювання ПЕК кожен календарний рік та у випадках, визначених суб’єктом господарювання ПЕК.

1	2	3	4	5
66	Інвентаризація системи	Розробити та оновити за період часу, визначений суб'єктом господарювання ПЕК, перелік систем суб'єкта господарювання ПЕК.	РМ-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
67	Стратегія управління ризиками	Розробити комплексну стратегію управління: ризиками безпеки для операцій та активів суб'єкта господарювання ПЕК, фізичних осіб, інших суб'єктів господарювання і держави, пов'язаних з експлуатацією та використанням систем суб'єкта господарювання ПЕК. Реалізувати стратегію управління ризиками в масштабах суб'єкта господарювання ПЕК.	РМ-9	Переглядати й оновлювати стратегію управління ризиками кожен календарний рік або, якщо потрібно, у разі змін в суб'єкті господарювання ПЕК.
68	Програма інформування про загрози	Запровадити програму інформування про загрози, яка містить можливості спільного обміну інформацією між суб'єктами господарювання для аналізу загроз.	РМ-16	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
69	Оцінка ризиків	Визначити та задокументувати: припущення, що впливають на оцінку ризиків, реагування на ризики та моніторинг ризиків; обмеження, що впливають на оцінку ризиків, реагування на ризики та моніторинг ризиків; пріоритети та компроміси, які розглядаються суб'єктом господарювання ПЕК для здійснення управління ризиками; стійкість суб'єкта господарювання ПЕК до ризиків. Інформувати працівників, що визначаються суб'єктом господарювання ПЕК, про результати визначення ризиків.	РМ-28	Переглядати та оновлювати підходи щодо визначення ризиків кожен календарний рік.

1	2	3	4	5
70	План управління ризиками ланцюга постачання	Розробити план управління ризиками ланцюга постачання, пов’язаного з розробкою, придбанням, обслуговуванням та утилізацією систем, компонентів системи та послуг для системи. Реалізувати план управління ризиками ланцюга постачання послідовно в масштабах суб’єкта господарювання ПЕК.	PM-30	Переглядати та оновлювати план управління ризиками ланцюга постачання кожен календарний рік або, якщо потрібно, у разі змін в суб’єкті господарювання ПЕК.
Кадрова безпека (PS)				
71	Перевірка працівників	Перевіряти осіб перед тим, як надавати їм доступ до системи. Проводити повторні перевірки осіб відповідно до умов, що потребують повторної перевірки, визначених суб’єктом господарювання ПЕК.	PS-3	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
72	Звільнення працівників. Переведення працівників	Коли припиняється індивідуальна трудова діяльність: заборонити доступ до системи протягом період часу, визначеного суб’єктом господарювання ПЕК. Припинити дію або відкликати автентифікатори та облікові записи, пов’язані з особою. Відновити властивості системи, пов’язані з безпекою. Коли працівників призначають або переводять на інші посади суб’єкта господарювання ПЕК:	PS-4	Відключити доступ до системи у разі добровільного звільнення – якомога швидше, але не більше ніж за 5 календарних днів, у разі примусового звільнення – у той самий день, що й припинення трудових відносин.

1	2	3	4	5
		переглянути та підтвердити поточну оперативну потребу в логічних і фізичних дозволах доступу до системи та об'єкта; ініціювати дії з переведення або призначення, визначені суб'єктом господарювання ПЕК, протягом період часу після дії з переведення або призначення, визначеного суб'єктом господарювання ПЕК; змінювати авторизацію доступу відповідно до будь-яких змін в оперативних потребах.	PS-5	Ініціювати дії з перепризначення, щоб забезпечити видалення або вимкнення всіх системних доступів, які більше не потрібні.
Фізичний захист і захист робочого середовища (PE)				
73	Авторизація фізичного доступу до місця розташування системи	Розробити, затвердити та підтримувати список осіб, які мають право доступу до фізичного місця розташування системи. Надавати повноваження для доступу до фізичного місця розташування системи. Періодично перевіряти список фізичного доступу. Переглядати список доступу до фізичного місця розташування системи з частотою, визначеною суб'єктом господарювання ПЕК. Видаляти осіб зі списку фізичного доступу до місця розташування системи, коли доступ більше не потрібен.	PE-2	Переглядати список доступу, у якому закріплений перелік працівників або ролей, яким дозволений санкціонований доступ до фізичного місця розташування системи, кожен календарний рік.
74	Моніторинг фізичного доступу до місця розташування системи	Перевіряти фізичний доступ до місця розташування системи, щоб виявляти та реагувати на інциденти фізичної безпеки. Переглядати журнали фізичного доступу до місця розташування системи з частотою, визначеною	PE-6	Переглядати журнали фізичного доступу кожні 90 календарних днів на предмет наявності подій,

1	2	3	4	5
		суб’єктом господарювання ПЕК, та при виникненні подій, визначених суб’єктом господарювання ПЕК.		визначених суб’єктом господарювання ПЕК.
75	Альтернативне робоче місце розташування системи	Визначити альтернативні робочі місця, дозволені для використання працівниками. Застосовувати дії безпеки, визначені суб’єктом господарювання ПЕК, на альтернативних робочих місцях.	РЕ-17	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
76	Керування фізичним доступом до місця розташування системи	Контролювати фізичний доступ до місця, де знаходиться система: перевіряти індивідуальні фізичні дозволи на доступ перед наданням доступу; контролювати вхід і вихід за допомогою систем/пристроїв фізичного контролю доступу або охоронців. Вести журнали контролю фізичного доступу для точок входу та виходу. Супроводжувати відвідувачів і контролювати їх діяльність. Забезпечити захист ключів, кодів доступу та інших пристроїв фізичного доступу до місця розташування системи. Контролювати фізичний доступ до пристроїв виводу, щоб запобігти доступу сторонніх осіб до конфіденційної інформації.	РЕ-3 РЕ-5	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.
77	Контроль доступу до джерел і ліній електроживлення. Контроль доступу до пристроїв	Контролювати фізичний доступ до розподільчих ліній системи і ліній електропередач на об’єктах суб’єкта господарювання ПЕК.	РЕ-4	Налаштування заходів захисту визначаються суб’єктом господарювання ПЕК.

1	2	3	4	5
	виведення інформації			
Оцінювання ризику (RA)				
78	Оцінювання ризику	Оцінити ризик несанкціонованого розголошення в результаті обробки, зберігання або передачі службової інформації. Оновлювати оцінки ризиків з частотою, визначеною суб'єктом господарювання ПЕК.	RA-3	Переглядати результати оцінювання ризиків та оновлювати оцінювання ризику кожен календарний рік.
			RA-3 (1)	Оновлювати оцінювання ризику ланцюга постачання кожен календарний рік коли відбуваються значні зміни у відповідному ланцюгу постачання, або коли зміни в системі, робочому середовищі чи інших умовах можуть вимагати змін у ланцюгу постачання.
			SR-6	Оцінювати і переглядати ризики ланцюга постачання, пов'язані з постачальниками або підрядниками,

1	2	3	4	5
				системою, системним компонентом або системною послугою, яку вони надають, кожен календарний рік або за потребою.
79	Сканування вразливостей	Перевіряти та сканувати систему на наявність вразливостей з частотою, визначеною суб'єктом господарювання ПЕК, та при виявленні нових вразливостей, що впливають на систему. Усунути вразливості системи протягом часу на реагування, визначеного суб'єктом господарювання ПЕК. Оновлювати вразливості системи, що підлягають скануванню з частотою, визначеною суб'єктом господарювання ПЕК, а також при виявленні нових вразливостей і повідомляти про них.	RA-5	Сканувати на наявність вразливостей в системі кожні 30 календарних днів та коли виявляються нові вразливості, які потенційно впливають на систему.
			RA-5 (2)	Оновлювати перелік вразливостей системи, що були просканові протягом 24 годин до запуску сканування.
80	Реагування на ризики	Реагувати на результати оцінок безпеки, моніторингу та аудитів.	RA-7	
Оцінювання, акредитація та моніторинг безпеки (CA)				
81	Оцінювання безпеки	Оцінювати дії з частотою, визначеною суб'єктом господарювання ПЕК, до безпеки системи та середовища її функціонування, щоб визначити, чи були ці дії виконані.	CA-2	Оцінювати заходи захисту в системі та в її середовищі функціонування кожен календарний рік.

1	2	3	4	5
82	План усунення недоліків та контрольні показники	Розробити план дій і контрольні показники для системи: задокументувати заплановані заходи з виправлення слабких місць або недоліків, виявлених під час оцінювання безпеки; зменшити або усунути відомі недоліки системи. Оновити існуючий план дій і показників на основі результатів оцінки безпеки, незалежних аудитів або оглядів, а також безперервного моніторингу.	CA-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
83	Безперервний моніторинг	Розробити та впровадити стратегію безперервного моніторингу на рівні системи, що передбачає постійний моніторинг та оцінку безпеки.	CA-7	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
84	Взаємодія систем	Затвердити та керувати обміном службової інформації між системою та іншими системами. Документувати характеристики інтерфейсу, дії до безпеки та обов'язки для кожної системи.	CA-3	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
Захист інформаційної системи та комунікацій (SC)				
85	Захист периметра	Контролювати та управляти зв'язком на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи. Реалізувати підмережі для загальнодоступних компонентів системи, які фізично або логічно відділені від внутрішніх мереж. Підключатися до зовнішніх мереж тільки через керовані інтерфейси, що складаються з пристроїв захисту периметра, розташованих відповідно до архітектури безпеки суб'єкта господарювання ПЕК.	SC-7	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
86	Інформація в загальних ресурсах системи	Запобігати несанкціонованій і ненавмисній передачі інформації за допомогою загальних ресурсів системи.	SC-4	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
87	Захист периметра – відмова за замовчуванням – дозвіл за винятком	Заборонити трафік мережевих комунікацій за замовчуванням і дозволити трафік мережевих комунікацій за винятком.	SC-7 (5)	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
88	Конфіденційність і цілісність передачі. Захист інформації у стані спокою	Реалізувати механізми криптографічного захисту для запобігання несанкціонованому розкриттю службової інформації під час передачі та зберігання.	SC-8	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
			SC-8 (1)	Запобігати несанкціонованому розголошенню інформації та виявляти зміни в ній.
			SC-28	Забезпечити конфіденційність та цілісність всієї інформації в стані спокою.
			SC-28 (1)	Впровадити криптографічні механізми для запобігання несанкціонованому розкриттю та модифікації всієї

1	2	3	4	5
				інформації у стані спокою на всі компоненти системи та носії інформації.
89	Відключення мережі	Завершити з'єднання з мережею, яке пов'язане із сеансом зв'язку в кінці сеансу або після періоду бездіяльності.	SC-10	Завершити з'єднання з мережею, яке пов'язане із сеансом зв'язку, в кінці сеансу або після не більше ніж 15 хвилин бездіяльності.
90	Встановлення та управління криптографічними ключами	Встановити криптографічні ключі в системі та керувати ними відповідно діям до встановлення та управління ключами, визначених суб'єктом господарювання ПЕК.	SC-12	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
91	Криптографічний захист	Впровадити типи криптографічного захисту, визначені суб'єктом господарювання ПЕК, при використанні системи для захисту конфіденційності відкритої та конфіденційної інформації.	SC-13	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
92	Спільні обчислювальні пристрої та застосунки	Заборонити віддалену активацію спільних обчислювальних пристроїв і програмного забезпечення з винятками, визначеними суб'єктом господарювання ПЕК. Надавати чіткі вказівки щодо використання користувачам, які фізично наявні біля пристроїв.	SC-15	Заборонити віддалену активацію спільних обчислювальних пристроїв (хмар) та застосунків з такими виключеннями: спеціальні апартаменти, розташовані в

1	2	3	4	5
				затверджених керівником суб'єкта господарювання ПЕК місцях.
93	Мобільний код	Визначити прийнятний мобільний код і технології мобільного коду. Авторизувати, відстежувати та контролювати використання мобільного коду.	SC-18	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
94	Автентифікація сесії	Захистити автентифікацію сеансів зв'язку.	SC-23	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
Цілісність системи та інформації (SI)				
95	Виправлення дефектів	Виявляти, повідомляти та виправляти недоліки системи. Встановлювати оновлення програмного забезпечення та вбудованих програм, що стосуються безпеки, протягом період часу після виходу оновлень, визначеного суб'єктом господарювання ПЕК.	SI-2	Інсталювати оновлення програмного забезпечення та оновлення вбудованого програмного забезпечення в межах 30 календарних днів.
96	Захист від шкідливого коду	Впровадити механізми захисту від шкідливого коду у визначених місцях системи для виявлення та знищення шкідливого коду. Оновлювати механізми захисту від шкідливого коду в міру виходу нових версій відповідно до політики та процедур управління конфігурацією, затверджених суб'єктом господарювання ПЕК.	SI-3	Виконання періодичного сканування системи кожні 7 календарних днів і сканування файлів у реальному часі із зовнішніх

1	2	3	4	5
		Налаштувати механізми захисту від шкідливого коду на: виконання сканування системи з частотою, визначеною суб'єктом господарювання ПЕК, та сканування файлів із зовнішніх джерел у реальному часі на кінцевих точках або точках входу та виходу з мережі під час завантаження, відкриття або виконання файлів; блокування шкідливого коду, поміщення шкідливого коду в карантин або інші дії у відповідь на виявлення шкідливого коду.		джерел кінцевих точок та точок входу/виходу з мережі. Блокування та карантин шкідливого коду адміністратором, визначеним суб'єктом господарювання ПЕК, у відповідь на виявлення шкідливого коду.
97	Попередження, рекомендації та директиви з безпеки	Отримувати попередження, рекомендації та директиви щодо безпеки системи від зовнішніх суб'єктів господарювання на постійній основі. Створювати та розповсюджувати внутрішні попередження системи, рекомендації та директиви щодо безпеки у разі потреби. Впроваджувати директиви з безпеки відповідно до часових рамок, встановлених суб'єктом господарювання ПЕК.	SI-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
98	Моніторинг системи	Проводити моніторинг системи для виявлення: атак та індикаторів потенційних атак; неавторизованих підключень. Виявляти неавторизоване використання системи.	SI-4	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
		Проводити моніторинг вхідного та вихідного комунікаційного трафіка для виявлення незвичних або несанкціонованих дій чи умов.	SI-4 (4)	Проводити моніторинг вхідного та вихідного комунікаційного трафіку безперервно

1	2	3	4	5
				для виявлення незвичайних або несанкціонованих дій чи умов.
99	Управління та збереження інформації	Керувати та зберігати службову інформацію в системі та виводити службову інформацію з системи відповідно до норм законодавства України, організаційно-розпорядчих актів, директив, положень, політик, стандартів, інструкцій та операційних дій.	SI-12	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
Планування безпеки (PL)				
100	Політика та процедури планування безпеки	Розробити, задокументувати та розповсюдити серед працівників суб'єкта господарювання ПЕК або ролей політики та процедури у сфері кібербезпеки та захисту інформації, необхідні для виконання дій безпеки. Періодично переглядати та оновлювати політики та процедури з частотою, визначеною суб'єктом господарювання ПЕК.	AC-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			AT-1	Розробити, задокументувати та поширити для всіх працівників. Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			AU-1	Розробити, задокументувати та поширити для всіх працівників.

1	2	3	4	5
				Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			CA-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			CM-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			IA-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			IR-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			MA-1	Переглядати та оновлювати поточну політику та процедури

1	2	3	4	5
				кожен календарний рік.
			MP-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			PE-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			PL-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			PS-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			RA-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			SA-1	Переглядати та оновлювати поточну

1	2	3	4	5
				політику та процедури кожен календарний рік.
			SC-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			SI-1	Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
			SR-1	Розробити, задокументувати та поширити серед призначених осіб або працівників з кібербезпеки. Переглядати та оновлювати поточну політику та процедури кожен календарний рік.
101	Плани захисту інформації та персональних даних	Розробити план захисту інформації, який: визначає складові компоненти системи; описує робоче середовище системи; описує конкретні загрози для системи; надає огляд дій до безпеки системи;	PL-2	Включає дії, пов’язані з безпекою та конфіденційністю, які впливають на систему, виконання яких

1	2	3	4	5
		визначає з’єднання з іншими системами; визначає осіб, які виконують ролі та обов’язки в системі; містить іншу інформацію, необхідну для захисту відкритої та конфіденційної інформації. Періодично переглядати та оновлювати план захисту інформації з частотою, визначеною суб’єктом господарювання ПЕК. Захистити план захисту інформації від неавторизованого розголошення.		вимагає планування та координацію з призначеною особою або працівниками з кібербезпеки. Поширити копії планів захисту інформації та персональних даних і повідомляти про подальші зміни планів серед призначених осіб або працівників з кібербезпеки. Переглядати плани захисту інформації та персональних даних, кожен календарний рік.
102	Правила поведінки	Встановити правила, які описують обов’язки та очікувану поведінку щодо використання системи та захисту службової інформації. Ознайомлювати з правилами осіб, яким потрібен доступ до системи. Отримувати задокументоване підтвердження від осіб, що вони ознайомлені та згодні дотримуватися правил поведінки, перш ніж надавати їм доступ до службової інформації та системи.	PL-4	Переглядати та оновлювати правила поведінки кожен календарний рік. Вимагати від осіб, які підписали попередню версію правил поведінки, перечитати та повторно підписати правила кожен

1	2	3	4	5
				календарний рік або коли правила переглядаються чи оновлюються.
Придбання систем та послуг (SA)				
103	Принципи інженерії безпеки	Застосовувати принципи інженерії безпеки систем, визначені суб'єктом господарювання ПЕК, до розробки або модифікації системи та її компонентів.	SA-8	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
104	Компоненти системи, що не підтримуються	Замінювати компоненти системи, якщо розробник, постачальник або виробник більше не надає їх підтримку. Надати варіанти зменшення ризиків або альтернативні джерела для продовження підтримки компонентів, що не підтримуються, якщо їх неможливо замінити.	SA-22	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
105	Зовнішні послуги для системи	Вимагати від постачальників зовнішніх послуг для системи, що використовуються для обробки, зберігання або передачі службової інформації, дотримання дій безпеки, визначених суб'єктом господарювання ПЕК. Визначити та задокументувати ролі та обов'язки користувачів відносно зовнішніх послуг для системи, включаючи спільні обов'язки із зовнішніми постачальниками. Впровадити процеси, методи та техніки для постійного моніторингу дотримання дій безпеки зовнішніми постачальниками послуг.	SA-9	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

1	2	3	4	5
Управління ризиками ланцюга постачання (SR)				
106	План управління ризиками ланцюга постачання	Розробити план управління ризиками ланцюга постачання, пов'язаними з дослідженнями та розробкою, проєктуванням, виробництвом, придбанням, доставленням (постачанням), інтеграцією, експлуатацією та обслуговуванням, а також утилізацією таких систем, компонентів системи або послуг для системи, визначених суб'єктом господарювання ПЕК. Захистити план управління ризиками ланцюга постачання від несанкціонованого розголошення та модифікації.	SR-2	Переглядати та оновлювати план управління ризиками ланцюга постачання кожен календарний рік.
107	Стратегії придбання, інструменти і методи	Розробляти та впроваджувати стратегії придбання, контрактні інструменти та методи придбання для виявлення, захисту та зменшення ризиків у ланцюгу постачання.	SR-5	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.
108	Контроль ланцюга постачання і процесів	Запровадити процес виявлення та усунення слабких місць або недоліків в елементах та процесах ланцюга постачання. Впровадити дії безпеки, визначені суб'єктом господарювання ПЕК, для захисту від ризиків ланцюга постачання для системи, компонентів системи або послуг для системи, а також для обмеження шкоди або наслідків від подій, пов'язаних з ланцюгом постачання.	SR-3	Налаштування заходів захисту визначаються суб'єктом господарювання ПЕК.

Виконувач обов'язків начальника Управління кібербезпеки
та цифрового розвитку **Олександр ГУМЕНЮК**