Додаток 2
до Методичних рекомендацій щодо
здійснення базових заходів кіберзахисту
(пункт 8 розділу I)

Зіставлення заходів безпеки, визначених в НД ТЗІ 3.6-006-24, застосованих в базовому профілі безпеки інформації, затвердженому наказом Адміністрації Держспецзв'язку від 24.06.2024 № 317 та застосованому в Методичних рекомендаціях щодо здійснення базових заходів кіберзахисту

Таблиця зіставлення[1] заходів безпеки НД ТЗІ 3.6-006-24, застосованих в базову профілі безпеки інформації, затвердженому наказом Адміністрації Держспецзв'язку від 24.06.2024 № 317 та застосованому в Методичних рекомендаціях щодо здійснення базових заходів кіберзахисту.

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
	УПРАВЛІННЯ ДОСТУПОМ (AC)			
AC-1	Політика та процедури управління доступом		+	+
AC-2	Управління обліковими записами	+	+	+
AC-3	Забезпечення доступу	+	+	+
AC-4	Управління інформаційними потоками	+	+	+
AC-5	Розмежування обов’язків	+	+	
AC-6	Мінімізація повноважень	+	+	+
AC-7	Невдалі спроби входу в систему	+	+	+
AC-8	Попередження про використання системи	+	+	+
AC-9	Сповіщення про попередній вхід (доступ)			+
AC-10	Управління паралельною сесією			+

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
AC-11	Блокування пристрою	+	+	+
AC-12	Припинення сеансу	+	+	+
AC-13	Нагляд та огляд — управління доступом			
AC-14	Дозволені дії без ідентифікації або автентифікації			+
AC-15	Автоматизоване маркування			
AC-16	Атрибути безпеки та приватності			+
AC-17	Віддалений доступ	+	+	+
AC-18	Бездротовий доступ	+	+	
AC-19	Контроль доступу для мобільних пристроїв	+	+	+
AC-20	Використання зовнішніх систем	+	+	+
AC-21	Розповсюдження інформації			
AC-22	Публічно доступний контент	+	+	
AC-23	Захист від несанкціонованого інтелектуального аналізу даних			+
AC-24	Рішення щодо управління доступом			+
AC-25	Диспетчер доступу			
	ОБІЗНАНІСТЬ ТА НАВЧАННЯ (AT)			
AT-1	Політика та процедури підвищення обізнаності та навчання		+	
AT-2	Навчання з підвищення обізнаності	+	+	+
AT-3	Рольове навчання	+	+	+

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
AT-4	Навчальні записи			
AT-5	Контакти з групами безпеки та асоціаціями			
AT-6	Відгуки про проведенні навчання			
	АУДИТ ТА ПІДЗВІТНІСТЬ (AU)			
AU-1	Політика та процедури аудиту та підзвітності		+	+
AU-2	Події аудиту	+	+	+
AU-3	Зміст записів аудиту	+	+	
AU-4	Місткість сховища записів аудиту			
AU-5	Реагування на відмови обробки даних аудиту	+	+	
AU-6	Огляд, аналіз і звітність аудиту	+	+	+
AU-7	Скорочення записів аудиту та формування звіту	+	+	+
AU-8	Позначка часу	+	+	
AU-9	Захист інформації аудиту	+	+	
AU-10	Неспростовність			
AU-11	Збереження записів аудиту	+	+	
AU-12	Генерація даних аудиту	+	+	+
AU-13	Моніторинг розкриття інформації			+
AU-14	Аудит сесії			
AU-15	Альтернативна можливість аудиту			
AU-16	Міжорганізаційний аудит			+

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
ОЦІНЮВАННЯ, АКРЕДИТАЦІЯ ТА МОНІТОРИНГ БЕЗПЕКИ (CA)				
CA-1	Політика та процедури оцінювання, акредитації та моніторингу		+	
CA-2	Оцінювання	+	+	+
CA-3	Взаємодія систем	+	+	+
CA-4	Сертифікація безпеки			
CA-5	План усунення недоліків і контрольні показники	+	+	
CA-6	Акредитація			
CA-7	Безперервний моніторинг	+	+	+
CA-8	Тестування на проникнення			+
CA-9	Внутрішні з’єднання системи			+
УПРАВЛІННЯ КОНФІГУРАЦІЄЮ (CM)				
CM-1	Політика та процедури управління конфігурацією		+	
CM-2	Базова конфігурація	+	+	+
CM-3	Управління змінами конфігурації	+	+	+
CM-4	Аналіз впливу на безпеку та приватність	+	+	+
CM-5	Обмеження доступу до змін	+	+	+
CM-6	Налаштування конфігурації	+	+	+
CM-7	Мінімально необхідна функціональність	+	+	+
CM-8	Інвентаризація компонентів системи		+	+

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
CM-9	План управління конфігурацією			+
CM-10	Обмеження використання програмного забезпечення			
CM-11	Встановлене користувачем програмне забезпечення			
CM-12	Розташування інформації			
CM-13	Відображення дій даних			
CM-14	Підписані компоненти			
ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ (CP)				
CP-1	Політика та процедури планування безперервної роботи			
CP-2	План забезпечення безперервної роботи та відновлення функціонування			+
CP-3	Навчання із забезпечення безперервної роботи			+
CP-4	Тестування плану забезпечення безперервної роботи та відновлення функціонування			+
CP-5	Оновлення плану забезпечення безперервної роботи та відновлення функціонування			
CP-6	Альтернативне місце зберігання			
CP-7	Альтернативний майданчик роботи			+
CP-8	Комунікаційні послуги			+
CP-9	Резервне копіювання		+	+
CP-10	Відновлення та відтворення системи			+

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
СР-11	Альтернативні протоколи зв’язку			+
СР-12	Безпечний режим			+
СР-13	Альтернативні механізми безпеки			+
ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (IA)				
IA-1	Політика та процедури ідентифікації та автентифікації		+	+
IA-2	Ідентифікація та автентифікація (користувачів організації)	+	+	+
IA-3	Ідентифікація та автентифікація пристроїв	+	+	+
IA-4	Управління ідентифікацією	+	+	+
IA-5	Управління автентифікатором	+	+	+
IA-6	Зворотний зв’язок автентифікатора	+	+	+
IA-7	Автентифікація криптографічного модуля			+
IA-8	Ідентифікація та автентифікація (користувачі, що не належать до організації)			+
IA-9	Послуги ідентифікації та автентифікації			+
IA-10	Адаптивна автентифікація			+
IA-11	Повторна автентифікація			+
IA-12	Перевірка справжності (ідентичності)			
РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR)				
IR-1	Політика та процедури реагування на інциденти		+	
IR-2	Навчання з реагування на інциденти	+	+	+

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
IR-3	Перевірка реагувань на інциденти	+	+	+
IR-4	Обробка інциденту	+	+	+
IR-5	Моніторинг інциденту	+	+	+
IR-6	Звітність про інциденти	+	+	+
IR-7	Підтримка реагування на інциденти	+	+	+
IR-8	План реагування на інциденти	+	+	+
IR-9	Реагування на витік інформації			+
IR-10	Інтегрована команда аналізу інформаційної безпеки			
	ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ (MA)			
MA-1	Політика та процедури технічного обслуговування		+	
MA-2	Контрольоване обслуговування			+
MA-3	Інструменти для обслуговування	+	+	+
MA-4	Віддалене обслуговування	+	+	+
MA-5	Технічний персонал	+	+	+
MA-6	Своєчасне обслуговування			
MA-7	Технічне обслуговування в польових умовах			
	ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ (MP)			
MP-1	Політика та процедури щодо захисту носіїв інформації		+	

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
MP-2	Доступ до носіїв інформації	+	+	
MP-3	Маркування носіїв інформації	+	+	
MP-4	Зберігання носіїв інформації	+	+	
MP-5	Транспортування носіїв інформації	+	+	
MP-6	Знищення інформації на носіях інформації	+	+	+
MP-7	Використання носіїв інформації	+	+	
MP-8	Зниження категорії безпеки носіїв інформації			+
ФІЗИЧНИЙ ЗАХИСТ І ЗАХИСТ РОБОЧОГО СЕРЕДОВИЩА (PE)				
PE-1	Політика та процедури фізичного захисту та захисту робочого середовища		+	
PE-2	Авторизація фізичного доступу	+	+	+
PE-3	Керування фізичним доступом	+	+	+
PE-4	Контроль доступу до джерел і ліній електроживлення	+	+	+
PE-5	Контроль доступу для пристроїв виведення інформації	+	+	+
PE-6	Моніторинг фізичного доступу	+	+	+
PE-7	Контроль відвідувачів			
PE-8	Реєстр доступу відвідувачів			+
PE-9	Енергетичне обладнання та кабелі			+
PE-10	Аварійне відключення			+

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
PE-11	Аварійне енергозабезпечення			+
PE-12	Аварійне освітлення			+
PE-13	Протипожежний захист			+
PE-14	Контроль температури та вологості			+
PE-15	Захист від пошкодження водою			+
PE-16	Доставлення та видалення			+
PE-17	Альтернативне робоче місце	+	+	+
PE-18	Розташування компонентів системи			+
PE-19	Витік інформації			+
PE-20	Моніторинг і відстеження активів			+
PE-21	Захист від електромагнітного імпульсу			
PE-22	Маркування компонентів			
PE-23	Розташування об’єкта			
	ПЛАНУВАННЯ БЕЗПЕКИ (PL)			
PL-1	Політики та процедури планування безпеки	+	+	
PL-2	Плани захисту інформації та персональних даних	+	+	+
PL-3	Оновлення планів захисту інформації та персональних даних			
PL-4	Правила поведінки		+	
PL-5	Оцінювання впливу на приватність			

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
PL-6	Планування діяльності, пов’язаної з безпекою			
PL-7	Концепція експлуатації			
PL-8	Архітектура безпеки та приватності			+
PL-9	Централізоване управління			
PL-10	Вибір базового профілю безпеки			
PL-11	Налаштування базового профілю безпеки			
МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (PM)				
PM-1	Програма (концепція) інформаційної безпеки			+
PM-2	Ролі програми інформаційної безпеки			+
PM-3	Ресурси забезпечення інформаційної безпеки та приватності			+
PM-4	План дій і етапи			
PM-5	Інвентаризація системи			+
PM-6	Показники продуктивності			
PM-7	Архітектура підприємства			+
PM-8	План захисту критичної інфраструктури			+
PM-9	Стратегія управління ризиками			+
PM-10	Процес авторизації			+
PM-11	Визначення завдань і процесів			+
PM-12	Програма інсайдерської загрози			+
PM-13	Безпека та приватність працівників			+

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
PM-14	Тестування, навчання та моніторинг			+
PM-15	Контакти з групами й асоціаціями з питань безпеки інформації та приватності			+
PM-16	Програма інформування про загрози			+
PM-17	Захист публічної інформації у зовнішніх системах			
PM-18	Програма (концепція) забезпечення приватності			+
PM-19	Керівні ролі програми приватності			
PM-20	Система записів програми приватності			
PM-21	Облік розкриття персональних даних			
PM-22	Управління якістю персональних даних			
PM-23	Орган управління персональними даними			
PM-24	Орган з питань цілісності даних			
PM-25	Мінімізація персональних даних, що використовуються під час тестування, навчання та досліджень			
PM-26	Управління скаргами			
PM-27	Звітність з питань забезпечення приватності			
PM-28	Оцінка ризиків			+
PM-29	Ролі керівників програми управління ризиками			
PM-30	План управління ризиком ланцюга постачання			+
PM-31	План безперевного моніторингу			

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
PM-32	Призначення			
КАДРОВА БЕЗПЕКА (PS)				
PS-1	Політика та процедури кадрової безпеки		+	+
PS-2	Визначення посадового ризику			+
PS-3	Перевірка персоналу	+	+	+
PS-4	Звільнення персоналу		+	+
PS-5	Переведення персоналу	+	+	+
PS-6	Договори про доступ			+
PS-7	Безпека зовнішнього персоналу			+
PS-8	Кадрові санкції			+
PS-9	Опис позицій			
ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ (PT)				
PT-1	Політика та процедури обробки персональних даних			
PT-2	Повноваження на обробку персональних даних			
PT-3	Цілі обробки персональних даних			
PT-4	Згода на обробку персональних даних			
PT-5	Повідомлення про конфіденційність			
PT-6	Система записів повідомлень про конфіденційність			
PT-7	Спеціальні категорії персональних даних			

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
PT-8	Вимоги до відповідності			
ОЦІНЮВАННЯ РИЗИКУ (RA)				
RA-1	Політика та процедури оцінювання ризику		+	
RA-2	Категоріювання безпеки			+
RA-3	Оцінювання ризику	+	+	+
RA-4	Оновлення оцінювання ризику			+
RA-5	Сканування вразливостей	+	+	+
RA-6	Заходи протидії технічній розвідці		+	
RA-7	Реагування на ризик			
RA-8	Оцінювання впливу на приватність			
RA-9	Аналіз критичності			
RA-10	Активний пошук загроз			+
ПРИДБАННЯ СИСТЕМИ ТА ПОСЛУГ (SA)				
SA-1	Політика та процедури придбання системи та послуг		+	
SA-2	Розподіл ресурсів			+
SA-3	Життєвий цикл розробки системи			+
SA-4	Процес закупівель		+	+
SA-5	Системна документація			+
SA-6	Обмеження щодо використання програмного забезпечення			

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
SA-7	Встановлене користувачем програмне забезпечення			
SA-8	Безпека та приватність принципів інжинірингу			+
SA-9	Зовнішні послуги для системи		+	+
SA-10	Управління конфігурацією розробника			+
SA-11	Тестування та оцінювання розробника			+
SA-12	Керування ризиками ланцюга постачання			+
SA-13	Довірчість			
SA-14	Аналіз критичності			+
SA-15	Процеси, стандарти й інструменти розробки			+
SA-16	Навчання, що надається розробниками			+
SA-17	Проєкт і архітектура безпеки та приватності для розробника			+
SA-18	Захист і виявлення підробки			
SA-19	Справжність компонента			
SA-20	Індивідуальна розробка критичних компонентів			
SA-21	Перевірка розробника			+
SA-22	Компоненти системи, що не підтримуються		+	
SA-23	Спеціалізація			
СИСТЕМНИЙ ТА КОМУНІКАЦІЙНИЙ ЗАХИСТ (SC)				
SC-1	Політика та процедури захисту системи та комунікацій		+	

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
SC-2	Розділення функцій			
SC-3	Ізоляція функцій безпеки			
SC-4	Інформація в загальних системних ресурсах	+	+	
SC-5	Захист від атак «Відмова в обслуговуванні»			
SC-6	Доступність ресурсів			
SC-7	Захист периметра	+	+	
SC-8	Конфіденційність і цілісність передачі	+	+	
SC-9	Конфіденційність передачі			
SC-10	Відключення мережі	+	+	
SC-11	Довірений канал зв’язку			+
SC-12	Встановлення та управління криптографічними ключами	+	+	+
SC-13	Криптографічний захист	+	+	+
SC-14	Захист громадського доступу			
SC-15	Спільні обчислювальні пристрої та застосунки	+	+	+
SC-16	Передача атрибутів безпеки та приватності			
SC-17	Сертифікати інфраструктури відкритих ключів			
SC-18	Мобільний код	+	+	
SC-19	Інтернет-протокол голосового зв’язку			
SC-20	Безпечна служба імен/адрес (уповноважене джерело)			

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
SC-21	Безпечна служба імен/адрес (рекурсивний або кешувальний перетворювач)			
SC-22	Архітектура і забезпечення служби імен/адрес			
SC-23	Автентифікація сесії	+	+	
SC-24	Уведення у відомий стан			
SC-25	Тонкі вузли			
SC-26	Приманка для зловмисників (honeypots)			
SC-27	Незалежні від платформи застосунки			
SC-28	Захист інформації в стані спокою		+	+
SC-29	Гетерогенність			
SC-30	Маскування та хибний напрям			
SC-31	Аналіз прихованого каналу			+
SC-32	Поділ системи на частини			+
SC-33	Підготовка цілісності передачі			
SC-34	Незмінювані виконавчі програми			+
SC-35	Розпізнавання приманок для зловмисників (honeyclient)			+
SC-36	Розподілена обробка та зберігання			+
SC-37	Позасмугові канали			
SC-38	Безпека операцій			
SC-39	Ізоляція процесу			+
SC-40	Захист бездротового з’єднання			

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
SC-41	Доступ до портів і пристроїв введення/виведення			
SC-42	Можливості датчика та дані			
SC-43	Обмеження використання			+
SC-44	Екрановані камери			
SC-45	Синхронізація системи з часом			
SC-46	Забезпечення виконання міждоменної політики			
SC-47	Альтернативний шлях зв’язку			
SC-48	Переміщення датчика			
SC-49	Примусове апаратне розділення та політика забезпечення виконання			
SC-50	Примусове програмне розділення та політика забезпечення виконання			
SC-51	Апаратний захист			
ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ (SI)				
SI-1	Політика та процедури цілісності інформації		+	
SI-2	Виправлення дефектів	+	+	
SI-3	Захист від шкідливого коду	+	+	
SI-4	Моніторинг системи	+	+	
SI-5	Попередження, рекомендації та директиви з безпеки	+	+	
SI-6	Перевірка функцій безпеки та приватності			

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
SI-7	Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації			
SI-8	Захист від спаму			
SI-9	Обмеження на введення інформації			
SI-10	Перевірка ведення інформації			
SI-11	Оброблення помилок			
SI-12	Управління та збереження інформації		+	+
SI-13	Запобігання прогнозованим збоям			+
SI-14	Нестійкість			+
SI-15	Фільтрація вихідних даних			
SI-16	Захист пам’яті			+
SI-17	Відмовостійкі процедури			+
SI-18	Операції забезпечення якості даних			
SI-19	Деідентифікація			
SI-20	Псування			
SI-21	Оновленні інформації			
SI-22	Різновиди інформації			
SI-23	Фрагметація інформації			

Продовження додатка 2

Шифр	Назва класу/назва заходу безпеки	Заходи безпеки, визначені у базовому профілі безпеки для відкритої інформації	Заходи безпеки, визначені у базовому профілі безпеки для ДСК	Заходи безпеки, визначені Рекомендаціями (CSF 2.0)
	УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ (SR)			
SR-1	Політика та процедури управління ризиками ланцюга постачання			
SR-2	План управління ризиками ланцюга постачання		+	
SR-3	Контроль ланцюга постачання і процесів		+	
SR-4	Походження			
SR-5	Стратегії придбання, інструменти і методи		+	
SR-6	Оцінка постачальників			
SR-7	Безпека операцій ланцюга постачання			
SR-8	Повідомлення про порушення ланцюга постачання			
SR-9	Захист від злому та виявлення			
SR-10	Перевірка системи і компонентів системи			
SR-11	Автентичність компоненту			
SR-12	Утилізація компоненту			

[1] Залежно від збігів у застосуванні заходів безпеки, визначених в Методичних рекомендаціях, та заходів безпеки, визначеними базовими профілями, в таблиці деякі чарунки позначені кольорами:

блакитним - коли збігаються із заходами безпеки, визначеними у базовому профілі для інформації “ДСК”,

зеленим - коли збігаються із заходами безпеки, визначеними у базовому профілі для відкритої інформації та інформації “ДСК”,

жовтим - коли захід безпеки визначено лише Методичними рекомендаціями.