ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
___ _____20__ року №_____

РЕКОМЕНДАЦІЇ
з оцінювання дотримання вимог цільового профілю безпеки системи

І. Загальні положення

1. Ці Рекомендації описують рекомендований порядок дій щодо процесу перевірки обраних та/або запроваджених методів, заходів, засобів захисту інформації та кіберзахисту в інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних системах (далі – системи) з метою встановлення стану захищеності систем або їх відповідності вимогам законодавства, національним стандартам, нормативним документам у сферах криптографічного та технічного захисту інформації, кіберзахисту.

2. Ці Рекомендації розроблено відповідно до Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 року № 712.

3. Ці Рекомендації не є нормативно-правовим актом, не встановлюють правових норм і враховуються при оцінюванні дотримання вимог цільового профілю безпеки системи та оформлення його результатів.

4. У цих Рекомендаціях терміни вживаються у значенні, наведеному в Законах України «Про Державну службу спеціального зв’язку та захисту інформації України», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про інформацію» та Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженому постановою Кабінету Міністрів України від 18 червня 2025 року № 712.

5. Ці Рекомендації можуть використовуватися під час оцінювання дотримання вимог цільового профілю безпеки системи, зокрема при:

оцінюванні дотримання вимог цільового профілю безпеки системи (далі – ЦПБ) з метою авторизації з безпеки системи, що проводиться юридичними особами, фізичними особами – підприємцями або фізичними особами, які відповідають вимогам затвердженим Адміністрацією Держспецзв'язку відповідно до законодавства;

інших видах перевірок, направлених на оцінювання дотримання вимог ЦПБ (внутрішній аудит, зовнішній аудит, державний контроль тощо).

6. Оцінювання дотримання вимог ЦПБ з метою авторизації системи з безпеки здійснюється юридичними особами, фізичними особами – підприємцями або фізичними особами (далі – суб'єкти оцінювання), вимоги до яких затверджуються Адміністрацією Держспецзв'язку.

7. Власник або розпорядник системи самостійно обирає виконавця робіт для проведення оцінювання дотримання вимог ЦПБ з метою авторизації системи з безпеки.

8. Заходи щодо організації та проведення оцінювання дотримання вимог ЦПБ з метою авторизації системи з безпеки проводяться з дотриманням таких принципів:

незалежність: оцінювачі та організації, що проводять оцінювання, діють незалежно від будь-яких осіб чи обставин, здатних вплинути на об'єктивність оцінювання. Незалежність є ключовою умовою забезпечення достовірності висновків і збереження довіри до результатів оцінювання;

неупередженість у прийнятті рішень: рішення та висновки оцінювання формуються виключно на підставі перевірених доказів. Жоден оцінювач не може допускати впливу особистих інтересів, тиску з боку керівництва, клієнта або третіх осіб;

відсутність конфлікту інтересів: оцінювання не може проводити організація, яка володіє або розпоряджується об'єктом оцінювання або брала участь у його створенні, щоб уникнути будь-якого конфлікту інтересів і забезпечити повну незалежність оцінювання;

об'єктивність доказів: висновки базуються лише на перевірених і задокументованих фактах, отриманих шляхом дослідження, опитування, випробування;

прозорість процесу: усі етапи оцінювання, критерії оцінки, методи та рішення документуються та є доступними для зацікавлених сторін у межах встановлених правил конфіденційності;

відповідальність оцінювача: кожен оцінювач несе персональну відповідальність за дотримання принципів незалежності, професійної етики та об'єктивності.

9. Оцінювання дотримання вимог ЦПБ передбачає такі етапи:

оцінювання ЦПБ;

оцінювання реалізації ЦПБ;

оформлення звіту з оцінювання дотримання вимог ЦПБ.

ІІ. Оцінювання ЦПБ

1. Оцінювання ЦПБ проводиться з метою:

підтвердження відповідності вибору базового профілю безпеки системи (далі – БПБ) або галузевого профілю безпеки системи (далі – ГПБ) для формування ЦПБ (підтвердження вибору);

підтвердження наявності у ЦПБ всіх заходів захисту обраного БПБ або ГПБ (підтвердження повноти);

підтвердження наявності мінімально необхідних параметрів налаштування заходів захисту в ЦПБ відповідно до вибраного БПБ або ГПБ (підтвердження коректності);

підтвердження відповідності ЦПБ вимогам законодавства та стандартів у сфері захисту інформації, нормативних документів системи технічного захисту інформації, галузевих вимог, політик безпеки тощо для визначеної системи (підтвердження відповідності).

2. Оцінювання ЦПБ може проводитися на етапі його розроблення та затвердження власником або розпорядником системи та/або під час проведення внутрішнього аудиту, зовнішній аудиту, державного контролю тощо.

Під час проведення оцінювання дотримання вимог ЦПБ з метою авторизації системи з безпеки роботи з оцінювання ЦПБ оцінювачем не проводяться.

ІІІ. Оцінювання реалізації ЦПБ

1. Оцінювання реалізації ЦПБ проводиться з метою підтвердження реалізації в системі дій з безпеки та/або заходів захисту, передбачених ЦПБ.

2. Рекомендації з оцінювання реалізації ЦПБ, розробленого з використанням БПБ, який затверджено наказом Адміністрації Держспецзв’язку від 30.06.2025 № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація», наведено у додатку 1 до цих Рекомендацій.

3. Рекомендації з оцінювання реалізації ЦПБ, розробленого з використанням БПБ, який затверджено наказом Адміністрації Держспецзв’язку від 02.07.2025 № 419 «Про затвердження базового профілю безпеки системи, де обробляється службова інформація», наведено у додатку 2 до цих Рекомендацій.

4. Оцінювання реалізації ЦПБ у частині заходів захисту, що не входять до БПБ, проводиться відповідно до НД ТЗІ 2.3-025-24 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» (далі – НД ТЗІ 2.3-025-24).

5. Оцінювання реалізації ЦПБ, розробленого з використанням БПБ для систем, де обробляється інформація, що становить державну таємницю, проводиться відповідно до НД ТЗІ 2.3-025-24.

6. Під час проведення оцінювання реалізації ЦПБ визначаються конкретні елементи, що оцінюються:

специфікації – задокументовані об’єкти (плани, політики, процедури, вимоги, функціональні специфікації та специфікації забезпечення, архітектури та проєктна документація, налаштування конфігурацій тощо), пов’язані із системою;

механізми – апаратні, програмні та апаратно-програмні засоби захисту, реалізовані в системі;

дії – пов’язані із захистом дії, що підтримують систему, які передбачають залучення людей (проведення операцій резервного копіювання системи, виконання плану реагування на інциденти, моніторинг мережевого трафіка тощо);

особи – люди, які застосовують специфікації, механізми або дії, зазначені вище.

7. Методи оцінювання реалізації ЦПБ визначають зміст і обсяг дій оцінювача і використовуються для полегшення розуміння, досягнення роз’яснень або отримання доказів.

Потенційні методи оцінювання дій з безпеки та/або заходу захисту передбачають дослідження, опитування та випробування, а саме:

метод дослідження – процес огляду, вивчення, інспектування, спостереження або аналізу елементів оцінювання;

метод опитування – процес проведення співбесід з окремими особами або групами осіб щодо елементів оцінювання;

метод випробування – процес виконання елементами оцінювання (тобто діями, механізмами) певних дій у визначених умовах з метою порівняння фактичної поведінки з очікуваною.

Потенційні об’єкти та методи оцінювання наведено у таблиці 1.

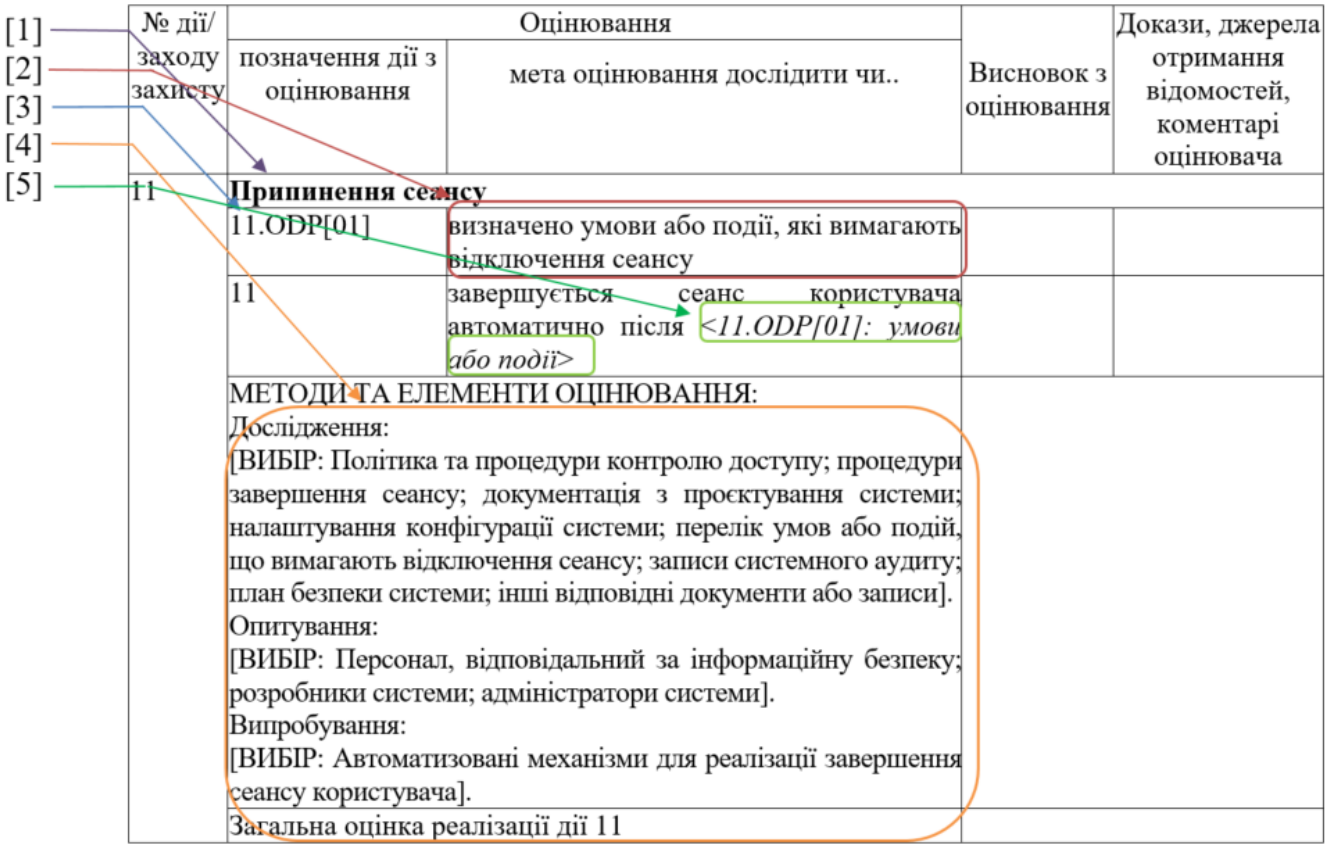
Таблиця 1

Метод оцінювання	Елементи	Опис
Дослідження	Специфікації: політики та процедури, проєктна та супутня документація, налаштування конфігурацій, журнали аудиту тощо	Оцінювач ознайомлюється та вивчає елемент оцінювання та приймає вмотивоване рішення щодо коректності реалізації відповідної вимоги до дії з безпеки або заходу захисту. Рішення відображається у звіті оцінювача
Опитування	Особи: відповідальні посадові особи та уповноважений персонал	Оцінювач може проводити співбесіди із залученими працівниками для кращого розуміння реалій впровадження дії з безпеки або заходів захисту. Рішення за результатами співбесіди відображається у звіті оцінювача

Випробування	Механізми: засоби захисту інформації Дії: пов'язані із захистом дії, що підтримують систему, які передбачають залучення людей	Оцінювач проводить тестові випробування механізмів або дій, впроваджених для забезпечення реалізації дії з безпеки або заходів захисту. Результати випробування відображаються у звіті оцінювача

8. Процедура оцінювання дій з безпеки та/або заходів захисту ЦПБ складається з мети оцінювання та набору потенційних методів і елементів оцінювання, які можуть бути використані для проведення оцінювання. Кожна мета оцінювання передбачає позитивний (П) або негативний (Н) висновок (твердження) про реалізацію вимоги, пов'язаної зі змістом дії з безпеки та/або заходу захисту, визначеного ЦПБ.

9. На рис. 1 наведено приклад структури та змісту оцінювання дії з безпеки «Припинення сеансу»:

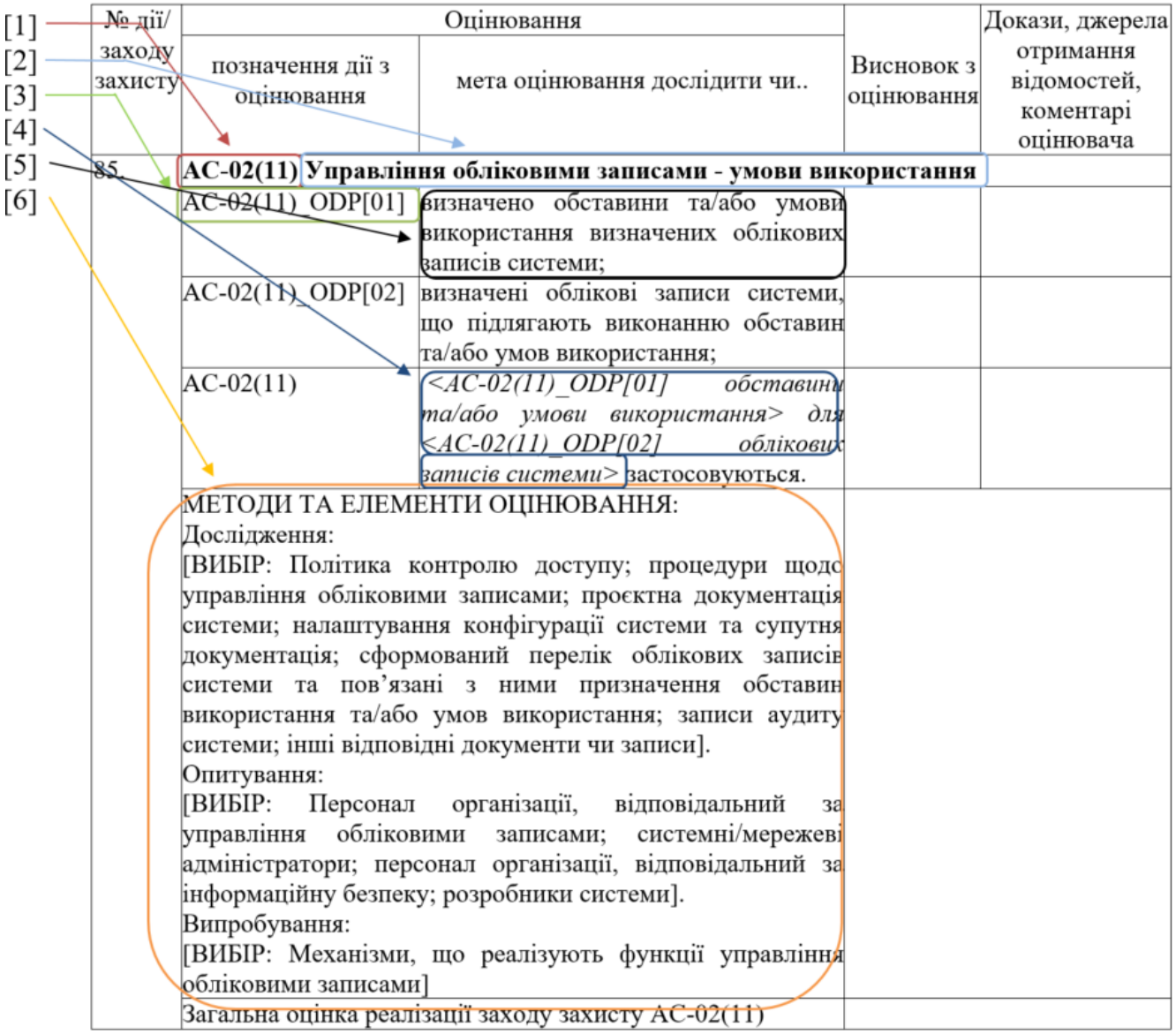


№ дії/ заходу захисту	Оцінювання		Висновок з оцінювання	Докази, джерела отримання відомостей, коментарі оцінювача
	позначення дії з оцінювання	мета оцінювання дослідити чи..		
11	**Припинення сеансу**			
	11.ODP[01]	визначено умови або події, які вимагають відключення сеансу		
	11	завершується сеанс користувача автоматично після *<11.ODP[01]: умови або події>*		
	МЕТОДИ ТА ЕЛЕМЕНТИ ОЦІНЮВАННЯ: Дослідження: [ВИБІР: Політика та процедури контролю доступу; процедури завершення сеансу; документація з проєктування системи; налаштування конфігурації системи; перелік умов або подій, що вимагають відключення сеансу; записи системного аудиту; план безпеки системи; інші відповідні документи або записи]. Опитування: [ВИБІР: Персонал, відповідальний за інформаційну безпеку; розробники системи; адміністратори системи]. Випробування: [ВИБІР: Автоматизовані механізми для реалізації завершення сеансу користувача].			
	Загальна оцінка реалізації дії 11			

[1] – назва дії з безпеки;
[2] – мета оцінювання;
[3] – змінний параметр дії з безпеки;
[4] – потенційні методи та елементи оцінювання;
[5] – значення змінного параметра.

Рис. 1 – Приклад структури та змісту оцінювання дії з безпеки «Припинення сеансу»

10. На рис. 2 наведено приклад структури та змісту оцінювання заходу захисту АС-02(11) «Управління обліковими записами – умови використання» відповідно до НД ТЗІ 2.3-025-24:



№ дії/ заходу захисту	Оцінювання: позначення дії з оцінювання	Оцінювання: мета оцінювання дослідити чи..	Висновок з оцінювання	Докази, джерела отримання відомостей, коментарі оцінювача
85.	**АС-02(11) Управління обліковими записами - умови використання**			
	АС-02(11)_ODP[01]	визначено обставини та/або умови використання визначених облікових записів системи;		
	АС-02(11)_ODP[02]	визначені облікові записи системи, що підлягають виконанню обставин та/або умов використання;		
	АС-02(11)	*<АС-02(11)_ODP[01] обставини та/або умови використання> для <АС-02(11)_ODP[02] облікових записів системи>* застосовуються.		
	МЕТОДИ ТА ЕЛЕМЕНТИ ОЦІНЮВАННЯ: Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та супутня документація; сформований перелік облікових записів системи та пов'язані з ними призначення обставин використання та/або умов використання; записи аудиту системи; інші відповідні документи чи записи]. Опитування: [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. Випробування: [ВИБІР: Механізми, що реалізують функції управління обліковими записами]			
	Загальна оцінка реалізації заходу захисту АС-02(11)			

[1] – ідентифікатор заходу захисту;
[2] – назва заходу захисту;
[3] – змінний параметр заходу захисту;
[4] – значення змінного параметра заходу захисту;
[5] – мета оцінювання;
[6] – потенційні методи та елементи оцінювання.

Рис. 2 – Приклад структури та змісту оцінювання заходу захисту АС-02(11)

11. За результатами висновків з оцінювання досягнення кожної мети визначається загальна оцінка реалізації дії з безпеки та/або заходу захисту:

«реалізовано» або «не реалізовано». Для отримання оцінки «реалізовано» всі висновки з оцінювання повинні дорівнювати «позитивно».

12. Висновок щодо позитивного результату оцінювання реалізації заходів захисту ЦПБ системи робиться у випадку отримання результату «реалізовано» для кожної дії з безпеки та/або заходу захисту, що входить до цього ЦПБ.

IV. Оформлення звіту з оцінювання дотримання вимог ЦПБ

1. За результатами оцінювання дотримання вимог ЦПБ складається звіт з оцінювання.

2. У рамках оцінювання дотримання вимог ЦПБ з метою авторизації системи з безпеки такий звіт зберігається у власника або розпорядника системи протягом дії авторизації з безпеки системи та протягом року після скасування авторизації з безпеки системи.

3. Звіт з оцінювання дотримання вимог формується в довільній формі, включаючи таку інформацію:

назва системи;

умовне позначення системи;

ідентифікатор системи (за наявності);

відомості про власника або розпорядника системи;

відомості про оцінювача;

підстава для проведення оцінювання;

перелік засобів технічного та криптографічного захисту інформації, які використані для захисту інформації в системі та відомостей про документи з оцінки їх відповідності;

результати оцінювання реалізації кожної дії з безпеки ЦПБ та/або заходу захисту інформації ЦПБ та вимог ЦПБ у цілому з наведенням доказів і джерел отримання інформації;

коментарі оцінювачів (за наявності);

загальні висновки щодо реалізації вимог ЦПБ у системі.

4. Звіт може бути оформлено в паперовому або електронному вигляді з урахуванням вимог Законів України «Про електронні документи та електронний документообіг» та «Про електронну ідентифікацію та електронні довірчі послуги».

5. У таблиці 2 наведено приклад структури та змісту оцінювання дії з безпеки «Невдалі спроби входу в систему» ЦПБ системи.

Таблиця 2

№ дії/ заходу захисту	Оцінювання		Висновок з оцінювання	Докази, джерела отримання відомостей, коментарі оцінювача
	позначення дії з оцінювання	мета оцінювання: дослідити чи..		
8	Невдалі спроби входу в систему			
	8.ODP[01]	визначена кількість послідовних невдалих спроб входу користувача в систему, дозволених протягом певного періоду часу	П	*Дослідження:* «Політика інформаційної безпеки організації», п. 5.3.1: «Обліковий запис блокується після 5 невдалих спроб входу» (затверджено наказом директора організації від 10.02.2024 № 12)
	8.ODP[02]	визначено період часу, яким обмежено кількість послідовних невдалих спроб входу користувача	П	*Дослідження:* «Політика інформаційної безпеки організації», п. 5.3.2: «Тривалість блокування облікового запису після досягнення порогу невдалих спроб входу встановлюється на 15 хвилин» (затверджено наказом директора організації від 10.02.2024 № 12)
	8	визначено кількість послідовних невірних спроб входу користувача протягом *<8.ODP[02]: період часу>* обмежено до *<8.ODP[01]: кількість>*	П	*Дослідження:* Інструкція адміністратора системи, п. 4.2: Account Lockout Threshold = 5. Інструкція адміністратора системи, п. 4.3: Account Lockout Duration = 15 хв. Переглянуто налаштування OS Windows 11 у gpedit.msc (Account Lockout Policy) та підтвердили, що значення встановлені таким чином: Account lockout threshold = 5 invalid logon attempts Account lockout duration = 15 minutes Reset account lockout counter after = 15 minutes. *Опитування:* Адміністратор підтвердив налаштування OS Windows 11 у gpedit.msc (Account Lockout Policy) 5 невдалих спроб і блокування на 15 хв; користувачі підтвердили блокування облікових записів після 5 неправильних спроб та автоматичне розблокування через 15 хв. всі відповіді узгоджені з політикою та журналами подій. *Випробування:* Після 5 невдалих спроб входу в обліковий запис користувача OS Windows 11 автоматично його заблокувала; журнали подій довели блокування з інформацією про користувача та час; через 15 хв обліковий запис автоматично розблокувався; тестові докази та журнали підтверджують,

				що механізм контролю реалізований і працює відповідно до політики; висновок: контроль ефективний і функціонує належним чином
	Загальна оцінка реалізації дії 8		**Реалізовано**	

Висновок «позитивно» (П) вказує на те, що мета оцінювання була досягнута і отримано повністю прийнятний результат. Висновок «негативно» (Н) означає, що існують потенційні дії з реалізації, що не виконуються, на які організація повинна звернути увагу. Висновок «негативно» (Н) може також означати, що оцінювач не зміг отримати достатньої інформації для прийняття рішення, яке вимагається у звіті з оцінювання реалізації ЦПБ.

6. У таблицях 3 та 4 наведено приклад структури та змісту оцінювання заходів захисту ЦПБ системи АС-05 «Розмежування обов’язків», АС-12 «Припинення сеансу» відповідно.

Таблиця 3

№ дії/ заходу захисту	Оцінювання		Висновок з оцінювання	Докази, джерела отримання відомостей, коментарі оцінювача
	позначення дії з оцінювання	мета оцінювання: дослідити чи..		
85	**Розмежування обов’язків**			
	AC-05_ODP	визначено обов’язки осіб, які потребують розмежування	П	*Дослідження:* Політика інформаційної безпеки організації, п. 4.2.1–4.2.3 (затверджено наказом директора від 10.02.2024 № 12): в облікових записах враховані ролі користувачів та адміністраторів
	AC-05[a]	<AC-05_ODP обов’язки осіб> визначені та задокументовані	П	*Дослідження:* У п. 2.1 – 2.5 «Посадові інструкції» визначені обов’язки користувачів та адміністраторів; обов’язки задокументовані, облікові записи відповідають обов’язкам; Інструкція адміністратора системи, п. 3.1–3.5: встановлення прав доступу для користувачів і адміністраторів; контроль і журналювання доступу; *Опитування:* адміністратор підтвердив процедури призначення прав за обов’язками; користувачі підтвердили відсутність надлишкових прав. *Випробування:* користувач не зміг змінити права іншого користувача; адміністратор виконав лише адміністративні дії; Security Event Log та Audit Log Windows у системі підтвердили правильність виконання дій

	AC-05[b]	визначено права авторизації доступу до системи для підтримки розмежування обов’язків	Н	*Дослідження:* Переглянуто політику безпеки та матрицю ролей у Windows. Журнали змін прав (Security Event Log, події 4732, 4733, 4670) довели, що обліковий запис ivanov.01 після переведення на нову посаду не отримав оновлених прав доступу до корпоративних файлів, мережевих ресурсів та груп безпеки. *Опитування:* адміністратор підтвердив, що перегляд прав проводиться нерегулярно. Користувач ivanov.01 повідомив про обмеження доступу після зміни посади. *Випробування:* фактичний доступ облікового запису ivanov.01 обмежений неправильно і не відповідає новим посадовим обов’язкам. Недозволений доступ до нових ресурсів неможливий, але права для виконання нових завдань не надані
	Загальна оцінка реалізації заходу захисту AC-05			**Не реалізовано**

Таблиця 4

№ дії/ заходу захисту	Оцінювання		Висновок з оцінювання	Докази, джерела отримання відомостей, коментарі оцінювача
	позначення дії з оцінювання	мета оцінювання: дослідити чи..		
85	**Припинення сеансу**			
	AC-12_ODP	визначено обов’язки осіб, які потребують розмежування	П	*Дослідження:* У політиці доступу (розділ 4.3, наказ № 10/ІБ) визначено додаткові умови завершення сесій: неактивність облікового запису протягом 15 хв, завершення робочого дня
	AC-12	сеанс користувача автоматично завершується після виконання <AC12_ODP умов або подій>	П	*Дослідження:* Переглянуто налаштування групових політик (GPO) у Windows: machine inactivity limit = 15 хв; автоматичне завершення сесій налаштовано також на час завершення робочого дня (через планові завдання Windows). У журналах Windows Security Event Log виявлені події: 4634 (Logoff), 4647 (User initiated logoff), 4800 (Workstation locked). *Опитування:*

				Адміністратор підтвердив, що політики автоматичного завершення сесій налаштовувалися саме у Windows (через групові політики GPO) і застосовуються до всіх користувачів. Користувачі підтвердили, що після періоду неактивності сесія завершується або блокується. *Випробування:* Під час практичного тесту користувач залишив систему Windows бездіяльною. Через 15 хвилин система автоматично завершила сесію (подія 4634 – Logoff). Також перевірено завершення сесій після закінчення робочого дня – у встановлений час усі активні облікові записи Windows були автоматично відключені, у журналі зафіксовані події 4634
	Загальна оцінка реалізації заходу захисту AC-12			**Реалізовано**

7. У таблиці 5 наведено приклад структури та змісту оцінювання заходу захисту ЦПБ системи АС-18 «Бездротовий доступ для АС класу «1». Система є ізольованою та відповідно до Політики інформаційної безпеки має повну заборону використання будь-яких бездротових підключень. У технології обробки інформації бездротові інтерфейси не передбачені та технічно відсутні. Тому вимоги заходу АС-18 щодо визначення типів, обмежень, конфігурації, підключення та авторизації бездротового доступу не мають об’єкта для оцінювання. Реалізація заходу безпеки підтверджується через встановлену політикою заборону таких підключень та фактичну відсутність можливостей бездротового доступу в системі.

Таблиця 5

№ дії/ заходу захисту	Оцінювання		Висновок з оцінювання	Докази, джерела отримання відомостей, коментарі оцінювача
	позначення дії з оцінювання	мета оцінювання: дослідити чи..		
13.	**Бездротовий доступ**			
	13[01]	визначено типи бездротового доступу до системи	П	Реалізацію дії з безпеки підтверджено в рамках методів оцінювання 13[06]
	13[02]	визначено обмеження на використання для кожного типу бездротового доступу до системи	П	Реалізацію дії з безпеки підтверджено в рамках методів оцінювання 13[06]
	13[03]	визначено дії до конфігурації для кожного типу бездротового доступу до системи	П	Реалізацію дії з безпеки підтверджено в рамках методів оцінювання 13[06]

	13[04]	визначено дії до підключення для кожного типу бездротового доступу до системи	П	Реалізацію дії з безпеки підтверджено в рамках методів оцінювання 13[06]
	13[05]	авторизується кожен тип бездротового доступу до системи перед встановленням таких підключень	П	Реалізацію дії з безпеки підтверджено в рамках методів оцінювання 13[06]
	13[06]	вимкнуто можливості бездротового доступу, якщо вони не призначені для використання, перед їх запуском та розгортанням	П	*Дослідження:* Переглянуто Політику інформаційної безпеки, відповідно до якої (п. 4) встановлено заборону будь-яких бездротових підключень у системі. Інструкція адміністратора містить вимоги щодо налаштування системи з метою блокування функцій бездротового доступу. Інструкція користувача визначає пряму заборону підключення або використання будь-яких бездротових з'єднань. *Опитування:* Адміністратор системи підтвердив, що система не підтримує та не дозволяє використання жодних бездротових інтерфейсів (Wi-Fi, Bluetooth, NFC тощо), а встановлена заборона є обов'язковою вимогою політики. Також адміністратор повідомив, що ним проведено налаштування операційної системи для блокування можливості таких підключень. *Випробування:* Перевірка системного оточення довела відсутність інтерфейсів та служб, пов'язаних з ініціалізацією або роботою бездротового обладнання. Спроби виконати дії з керування бездротовими інтерфейсами під обліковим записом користувача не дали результату, що підтверджує відсутність такого функціоналу. Системні журнали подій не містять записів щодо ініціалізації, активації або підключення бездротових з'єднань
	13[07]	захищено бездротовий доступ до системи за допомогою автентифікації та шифрування	П	Реалізацію дії з безпеки підтверджено в рамках методів оцінювання 13[06]
	Загальна оцінка реалізації дії 1		**Реалізовано**	

Директор Департаменту захисту інформації
Адміністрації Держспецзв'язку
полковник Андрій ГОЛОВЕНКО