Ministry of Defense
of Ukraine

Досвід Міністерства оборони України в імплементацій міжнародних ризик-орієнтованих стандартів з кібербезпеки

полковник Олег ШЕМЕТОВ

Заступник директора директорату – керівник експертної групи політик інформаційної та кібербезпеки Директорату цифрової трансформації у сфері оборони Міністерства оборони України

Certified CISO, керівник СУІБ Міноборони, держексперт з ТЗІ

ОСНОВНІ НАПРЯМКИ ПОТОЧНОЇ ДІЯЛЬНОСТІ

Розробка проєктів та внесення змін до існуючих:

- ✓законів України
- ✓ ПКМУ,
- ✓наказів Міноборони

Розробка та впровадження **Стратегії кібербезпеки в системі Міноборони**

Розробка **політик інформаційної та кібербезпеки**

Формування **Галузевого профілю безпеки** в системі Міноборони

Формування **методології оцінки ризиків**

Впровадження **СУІБ в Міноборони**

Діяльність в рамках **дозволу ТЗІ для власних потреб МОУ**

Взаємодія з країнами-партерами, міжнародними організаціями та компаніями

Результати впровадження в Міноборони

Державна служба спеціального зв'язку та захисту інформації України

In English

Новини | CERT-UA | Про Держспецзв'язку | Діяльність | UNITED 24 MEDIA | Публікації

Перелік систем, що мають комплексні системи захисту інформації, створе використанням базових та цільових профілів безпеки інформації

№ з/п	Ідентифікатор/назва системи	Найменування власника системи	Дата подання декларації	Дата закінчення дії декларації	Стан декларації
1	Інформаційно-комунікаційна система "Інтеграційна платформа "Дельта" Збройних Сил України"	Міністерство оборони України	12.07.2024	12.07.2027	Дійсна
2	Інформаційно-комунікаційна система "Система виявлення вразливостей та реагування на кіберінциденти та кібератаки Міністерства оборони України", шифр "CSOC"	Міністерство оборони України	17.04.2025	17.04.2028	Дійсна
3	Інформаційно-комунікаційна система управління постачанням товарів та послу для потреб Збройних Сил України «DOT-Chain»	Державне підприємство Міністерства оборони України «Державний оператор тилу»	08.07.2025	08.07.2028	Дійсна

IMS

СЕРТИФІКАТ

На систему менеджменту згідно з

ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT)

Сертифікаційний орган ТОВ «ІМС ІНТЕРНЕШНЛ» цим на підставі аудиту, оцінки і сертифікаційного рішення згідно з ДСТУ EN ISO/IEC 17021-1:2017 підтверджує, що організація

Міністерство оборони України
проспект Повітряних Сил, 6
03168, Київ
Україна

Міністерство оборони України

з підрозділами згідно з додатком

провадить систему менеджменту згідно з вимогами ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) і протягом строку дії сертифіката, який складає 3 роки, буде перевірятися на відповідність.

Сфера діяльності

Забезпечення формування та реалізації державної політики з питань національної безпеки у воєнній сфері, сферах оборони і військового будівництва у мирний час та особливий період щодо визначення засад цифрової трансформації, інформаційних технологій, автоматизації, інформатизації, кібербезпеки та кіберзахисту.
Розробка, впровадження, оновлення та підтримка:
- базових та комунікаційних сервісів в інтересах Міністерства оборони України та Збройних Сил України;
- функціональних сервісів, що розгорнуті в інтересах Міністерства оборони України, Збройних Сил України та інших суб'єктів сектору безпеки і оборони.
Надання в інтересах Міністерства оборони України, Збройних Сил України та інших суб'єктів сектору безпеки і оборони послуг з:
- підтримки користувачів базових, комунікаційних та функціональних сервісів;
- керування подіями безпеки інформації та реагування на інциденти кібербезпеки.
З урахуванням заяви про застосовність версія 1.0 від 15.04.2025

Реєстраційний номер сертифіката 55 121 25 04 14
Звіт про аудит № 250014

Чинний від: 23.04.2025
Чинний до: 22.04.2028
Первинна сертифікація: 2025

A. Syniato

Керівник сертифікаційного органа
ТОВ «ІМС ІНТЕРНЕШНЛ»

м. Київ, 23.04.2025

ТОВ «ІМС ІНТЕРНЕШНЛ» вул. Софіївська 16/16, оф.5 01001, м. Київ, Україна www.ims.ua

8О166
Сертифікація систем менеджменту

Перевірити сертифікат

Перелік авторизованих систем з безпеки

16.09.2025 14:30

Порядковий номер системи у переліку	Ідентифікатор системи (за наявності)	Найменування системи	Найменування власника або розпорядника системи	Ідентифікатор власника або розпорядника системи *	Дата включення системи до переліку	Кінцевий термін проведення планової авторизації системи з безпеки.
1	0704038145200700	Інформаційно-комунікаційна система «Реєстр Прозорості»	Національне агенство з питань запобігання корупції	40381452	29.08.2025	29.08.2026
2	-	Інформаційно-комунікаційна система адміністративних процесів військової частини (“Імпульс”)	Міністерство оборони України	00034022	15.09.2025	15.09.2026

*Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України/реєстраційний номер облікової картки платника податків або серія (за наявності) та номер паспорта громадянина України (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомили про це відповідному контролюючому органу і мають відмітку у паспорті громадянина України).

ПЕРЕДУМОВИ В **2024** РОЦІ

- **ЗУ “Про захист інформації в ІКС”, Стаття 10**
  ЗУ “Про оборону”, Стаття 10
- **ЗУ “Про хмарні послуги”, Стаття 4**
- **ПКМУ № 627 “Порядок реалізації експериментального проекту з декларування КСЗІ, створених з використанням профілів безпеки”**
- **Накази Міноборони:**
  - ✓**Верхньорівнева політика кібербезпеки**
  - ✓**Власний порядок КСЗІ по профілям**
  - ✓**Внутрішні низькорівневі policy**

RECENT UPDATES AND PLANS

Стратегія кібербезпеки в системі Міністерства оборони України,
затверджена рішенням Міністра оборони України
№ 6203/уд від 22.10.2025

Наказ МОУ № 692/нм від 15.10.2025
“Про затвердження Галузевого профілю безпеки систем, де обробляється відкрита, конфіденційна або службова інформація”

“Порядок проведення авторизації з безпеки ІКС Міноборони, Збройних Сил України та Державної спеціальної служби транспорту”
Проєкт наказу

Методичні рекомендації щодо проведення авторизації з безпеки…

Порядок авторизації автоматизованих систем класу «1» та ЦПБ

Галузева оцінка ризиків та власна методологія оцінки ризиків

Масштабне навчання впроваджувачів/оцінювачів

УМОВИ ОБРОБКИ ІНФОРМАЦІЇ В ІКС

Закон України «Про захист інформації в інформаційно-комунікаційних системах»

Стаття 8. Умови обробки інформації в системі

Державні інформаційні ресурси або **інформація з обмеженим доступом**, вимога щодо захисту якої встановлена законом, у системах, об’єктах критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, **мають оброблятися в авторизованих системах з безпеки** або шляхом **отримання сертифіката відповідності стандарту інформаційної безпеки**, виданого органом з оцінки відповідності

Ключові зміни НПА України щодо профілів безпеки

ПКМУ від 18 червня 2025 р. № 712

Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем

- ✓ **Порядок авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем;**
- ✓ **Порядок розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем.**

Базові профілі безпеки

- ✓ **БПБ для відкритої та конфіденційної (Наказ Адміністрації Держспецзв'язку № 409 від 30.06.2025)**
- ✓ **БПБ для службової (Наказ Адміністрації Держспецзв'язку № 419 від 02.07.2025)**
- ✓ **БПБ що становить державну таємницю (за запитом)**

Ключові зміни НПА України щодо профілів безпеки

- ✓ **Рекомендації з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації (Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 10 липня 2024 року № 354)**

- ✓ **Методичні рекомендації з формування цільового профілю безпеки інформації схвалені рішенням ЕР з питань державної експертизи в сфері ТЗІ (протокол від 14.03.2025 №09-2025)**

- ✓ **Вимоги до юридичних осіб, фізичних осіб — підприємців, які здійснюють оцінювання реалізації цільового профілю безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем (Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України 11 липня 2025 року № 438, зареєстровано в Міністерстві юстиції України 31 липня 2025 року за № 1125/44531)**

ПРОФІЛІ БЕЗПЕКИ = АДАПТОВАНІ СТАНДАРТИ NIST

Каталог заходів безпеки
для інформаційних систем та організацій
Методика оцінювання

NIST SP 800-53 rev 5

НД ТЗІ 3.6-006-24

NIST SP 800-53A

НД ТЗІ 2.3-025-24

NIST
National Institute of Standards and Technology

Базові профілі безпеки
Методика оцінки достатності заходів захисту

NIST SP 800-171
NIST SP 800-172

Наказ АДССЗЗІ
від 30.06.2025 № 409
від 02.07.2025 № 419

NIST SP 800-171A
NIST SP 800-172A

Наказ АДССЗЗІ
від 10.07.2024 № 354

НЕ ПЛУТАЙТЕ NIST CSF ТА NIST RMF!!!

Критерій	NIST CSF	NIST RMF
Призначення	Управління кібербезпекою на стратегічному рівні	Управління ризиками для систем на тактичному рівні
Фокус	Захист бізнес-процесів та критичних функцій	Оцінка та контроль ризиків IT-систем
Структура	5 функцій: Identify, Protect, Detect, Respond, Recover	7 кроків: Categorize, Select, Implement, Assess, Authorize, Monitor
Рівень застосування	Організаційний (enterprise-wide)	Системний (system-level)
Гнучкість	Добровільний, адаптивний	Обов’язковий для федеральних систем США
Вихідні документи	Профілі, дорожні карти	План безпеки системи, оцінка ризиків, авторизація

ПРИБЛИЗНІ ЧАСОВІ РАМКИ ВПРОВАДЖЕННЯ

Етап 1

Оцінка ризиків

2-4 тижні

Етап 2

Формування цільового профіля безпеки

1-2 тижні

Етап 3

Впровадження заходів безпеки

3-4 місяці

Етап 4

Оцінка реалізації

3-4 тижні

Авторизаційний лист

1 день

АДССЗЗІ

ЕТАП 0 – інвентаризація активів

Реєстр активів (Asset Inventory Register)

- ✓ Інформаційні активи - ступінь обмеження доступу, формат представлення, місце зберігання;
- ✓ Апаратні активи - серверне та мережеве обладнання, робочі станції та мобільні пристрої;
- ✓ Програмні активи - операційні системи, системне та функціональне ПЗ;
- ✓ Фізичні активи - приміщення, СКУД, охоронно-пожежна сигналізація тощо);
- ✓ Персонал - ролі та доступ, в т.ч. постачальники;
- ✓ Документація - політики, інструкції, опис системи, схеми і т.д.

ЕТАП 1 – Оцінка ризиків

Оцінка ризиків — це процес виявлення та аналізу потенційних подій, що можуть негативно вплинути на людей, активи чи середовища. Вона визначає ймовірність та наслідки інцидентів

Мета: зменшення потенційних наслідків ризиків

Основні методології:

- **ДСТУ ISO/IEC 27005:2023 — управління ризиками інформаційної безпеки**
- **NIST SP 800-30 — керівництво з проведення оцінки ризиків**
- **FAIR — кількісний фреймворк**

Як зрозуміти терміни оцінки ризиків?

Фактор загрози

Створює

Загроза

Експлуатуючи

Вразливість

Породжує

Ризик

Впливає

Інформаційних активів

Захищається

Контрзаходи

Протидіє

Загальний приклад

Фактор загрози: зловмисник

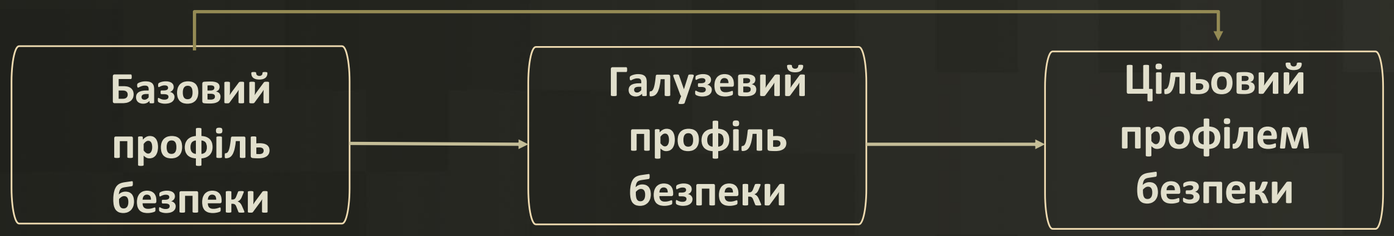
Загроза: отримання доступу до корпоративних ресурсів через WI-FI-мережу

Вразливість: відсутність розмежування доступу між гостьовою WI-FI-мережею і корпоративною

Ризик: ймовірність того, що злочинець отримає доступ до гостьової мережі і викраде конфіденційні дані (інформаційний актив) організації

Контрзаходи: розмежування доступу і контроль підключення пристроїв до гостьової WI-FI-мережі

ЕТАП 2 ФОРМУВАННЯ ЦПБ



Базовим профілем безпеки передбачено:

Для конфіденційної інформації: **129** заходів безпеки

Для ДСК: **158** заходу безпеки

ПРИКЛАДИ КОНТРОЛІВ БЕЗПЕКИ

Контроль: PE-3

Назва контролю: Керування фізичним доступом

1) 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;

2) вести журнали контролю фізичного доступу для точок входу та виходу;

3) супроводжувати відвідувачів і контролювати їхню діяльність [призначення: обставини, що вимагають супроводу відвідувачів та контролю за їхньою діяльністю, визначені організацією];

Контроль: CP-9(8)

Назва контролю: Резервне копіювання – криптографічний захист

Упровадити криптографічні механізми для запобігання несанкціонованому розкриттю службової інформації в місцях зберігання резервних копій.

КАТЕГОРІЇ КОНТРОЛІВ БЕЗПЕКИ (ЗАХОДІВ ЗАХИСТУ)

- ✓Управління доступом
- ✓Обізнаність і навчання
- ✓Аудит і підзвітність
- ✓Управління конфігурацією
- ✓Ідентифікація та автентифікація
- ✓Реагування на інциденти
- ✓Технічне обслуговування
- ✓Захист носіїв інформації
- ✓Кадрова безпека
- ✓Фізичний захист і захист робочого середовища
- ✓Оцінка ризику (управління вразливостями)
- ✓Оцінювання, акредитація та моніторинг безпеки
- ✓Захист інформаційної системи та комунікацій
- ✓Цілісність системи та інформації
- ✓Планування безпеки
- ✓Придбання систем та послуг
- ✓Управління ризиками ланцюга постачання

Чи є інструменти автоматизації?

CSF Tools

NIST Special Publication 800-53 > NIST SP 800-53, Revision 5 > AC: Access Control > AC-2: Account Management

AC-2(1): Automated System Account Management

Control Family: Access Control

Parent Control: AC-2: Account Management

CSF v1.1 References: PR.AC-4 DE.CM-3

PF v1.0 References: CT.DM-P1 CT.DM-P2 CT.DM-P3 CT.DM-P4 PR.AC-P4

Threats Addressed: Spoofing

Baselines: Moderate, High

Previous Version: NIST Special Publication 800-53 Revision 4:
AC-2(1): Automated System Account Management

Control Statement

Support the management of system accounts using [Assignment: *organization-defined automated mechanisms*].

Supplemental Guidance

Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

Нажаль знов…

Варіант формату представлення ЦПБ

1. Вимоги з безпеки інформації ІКС
1.1 Управління доступом
1.1.1 Управління обліковими записами
Номер вимоги базового профіля: 1.1
Вимога:
1) Визначити дозволені та заборонені типи облікових записів у системі;
…
6) деактивувати облікові записи в системі, коли:

термін дії облікових записів закінчився;
облікові записи були неактивні протягом [призначення: період часу, визначений організацією];

Параметр	Значення параметру
1.1(6)	90 днів

Заходи захисту відповідно до НД ТЗІ 3.6-006-24:

Управління обліковими записами.

Номер заходу: AC-2

Заходи захисту:

a. Визначити та задокументувати типи облікових записів системи, дозволених для використання в ІС для підтримки цілей, завдань, функцій і процесів організації.

…

e. Вимагати схвалення [Призначення: визначеною організацією відповідальною особою або роллю] запитів на створення облікових записів системи.

Параметр	Значення параметру
AC-2(e)	керівником проєктної групи

ЕТАП 3 РЕАЛІЗАЦІЯ КОНТРОЛІВ (організаційно/технічно)

✓ **Розробляємо план**	детальний опис того, як і чим кожен контроль буде реалізований (NIST SP 800-18 Rev. 1 Guide for Developing Security Plans for Federal Information Systems) SSP;
✓ **Визначаємо відповідальних**	призначаємо людей або команди, які відповідають за конкретні завдання та терміни;
✓ **Розробляємо або оновлюємо документацію**	реєструємо всі впроваджені контролі, їх налаштування та відповідальних осіб
✓ **Формуємо докази реалізації**	готуємо підтвердження, що заходи безпеки дійсно впроваджені та працюють

ЕТАП 4 ОЦІНЮВАННЯ (дії експерта/оцінювача)

✓ **Дослідження документації**	Оцінювач ознайомлюється та вивчає об'єкт та приймає вмотивоване рішення щодо коректності реалізації відповідної вимоги з безпеки.
✓ **Проведення технічних тестів**	Оцінювач проводить тестові випробування автоматизованих механізмів, розгорнутих для забезпечення реалізації вимоги з безпеки. Результати тестування вказуються у звіті оцінювача;
✓ **Проведення інтерв’ю**	Оцінювач може проводити співбесіди із залученими працівниками для кращого розуміння реалій впровадження вимоги з безпеки. Рішення за результатами співбесіди вказується у звіті оцінювача
✓ **Збір доказів**	Скріншоти, записи щодо інтерв’ю, скани документів з реквізитами
✓ **Формування звіту**	Детальний опис отриманих доказів по кожному котролю та формування висновку щодо успішності реалізації

ЕТАП 4 ОЦІНЮВАННЯ (можливий вигляд звіту)

2. Ідентифікація та автентифікація пристроїв

Номер вимоги базового профіля: 5.2

Вимога:

Унікально ідентифікувати та автентифікувати пристрої перед встановленням з'єднання з системою.

Заходи захисту відповідно до НД ТЗІ 3.6-006-24: ІА-3

2.1 Ідентифікація та автентифікація пристроїв

Номер заходу: ІА-3

Заходи захисту:	Докази, джерела отримання відомостей
Унікально ідентифікувати та автентифікувати ***[комп'ютери (ноутбуки)]*** перед установкою ***[дистанційного]*** підключення.	1. 14.03.2025 проведено інтерв'ю з Хххх Ххххх, співробітником підрозділу Хххх. 2. Визначено, що будь-які дії користувача фіксуються разом з Device ID. Це забезпечує унікальну ідентифікацію пристрою. 3. Кожна дія супроводжується перевіркою Conditional Access Policy (Політики умовного доступу), яка вимагає відповідності пристрою певним критеріям безпеки перед дозволом на підключення, що слугує механізмом автентифікації пристрою. 4. Надано скріншот: «0.0.1 Перевірка ідентифікації пристрою - унікальний Device ID та Conditional access.png», що підтверджує використання унікальних ідентифікаторів пристроїв та застосування політик умовного доступу.

ІКС реалізує вимоги ІА-3. Забезпечено унікальну ідентифікацію комп'ютерів (ноутбуків) та їх автентифікацію перед встановленням дистанційного підключення. Зазначене гарантує, що лише авторизовані та належним чином захищені пристрої можуть встановлювати з'єднання з системою.

Рекомендації з покращення (коментарі оцінювачів) – відсутні.

Висновок з оцінки - реалізовано (позитивно).

Можливий перелік документів (не обов’язковий!!!)

№	Назва документу та його вміст
1	Наказ на проведення заходів з авторизації з безпеки (із встановленням вимоги щодо проведення оцінки ризиків, формування цільового профілю безпеки, категоріювання, визначення комісій)
2	Перелік інформації, що підлягає автоматизованому обробленню та потребує захисту в ІКС
3	Акт категоріювання ОІД (для систем що обробляють держтаємницю)
4	Звіт за результатами оцінки ризиків
5	Положення про СЗІ (підрозділи кіберзахисту) та призначення складу (у разі відсутності штатного)
6	Цільовий профіль безпеки ІКС
7	Плану захисту інформації в ІКС (SSP)
8	Політики безпеки (порядки, правила тощо)
9	Експлуатаційна документація (інструкцій, настанов)
10	Акт проведення попереднього оцінювання впроваджених заходів захисту в ІКС (із зазначенням готовності до проведення зовнішнього оцінювання)
11	Звіту за результатами оцінки достатності впроваджених заходів захисту (з доказами реалізації кожного контролю)
12	Авторизаційний лист (направлення до Адміністрації Держспецзв’язку)

КОМПЛЕКСНИЙ ПІДХІД ІТ-СЕКТОРУ МІНОБОРОНИ

Побудова системи управління інформаційною безпекою (СУІБ)

Чим передбачено?

- Стаття 8 ЗУ «Про захист інформації в ІКС»

На чому базується?

- ДСТУ ISO/IEC 27001

Чому СУІБ?

- NIST деталізує вимоги та критерії для кожної системи, СУІБ – процеси безпеки в рамках організації
- Політики розроблені в рамках СУІБ повністю покривають політики NIST
- ІКС, що обробляють відкриту, конфіденційну та службову інформацію не потребують авторизації
- СУІБ покриває одразу всі підрозділи ІТ-сектору
- Сертифікація СУІБ є міжнародною і здійснюється виключно незалежним аудитором з відповідною акредитацією
- СУІБ імплементований в НБУ, МЦТ (ДП Дія), ДП ДОТ

Необхідні кроки

1. **Підтримка СУІБ на рівні керівництва**
2. **Фінансування незалежного аудиту СУІБ**
3. **Навчання фахівців (аудиторів)**

ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ СУІБ В ДЕРЖОРГАНАХ

Наявна нормативна база:

Багато контролів та вимог «тіла» Стандарту перекривається чинним законодавством

Відповідність ДСТУ, а не ISO/IEC при виборі органу сертифікації:

При побудові Системи Управління Інформаційною Безпекою необхідно враховувати його версію ДСТУ, яка фактично є ISO/IEC, але це висуває додаткові вимоги до вибору серт.органу

Персонал:

Нерозуміння керівниками та персоналом, навіщо це потрібно, якщо існує (існувало) КСЗІ. Також кваліфікація персоналу та відсутність відповідних курсів на державному рівні

ПІДГОТОВКА ПЕРСОНАЛУ

PECB

Professional Evaluation and Certification Board

hereby attests that

Ivan Punko

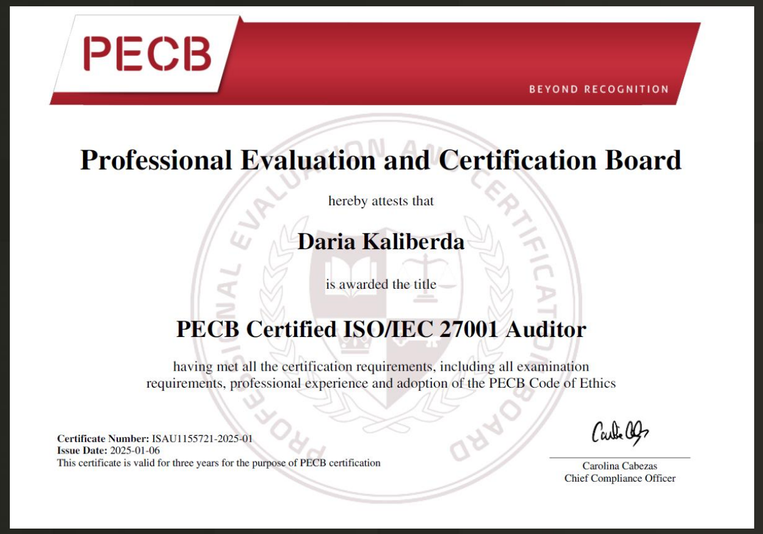
is awarded the title

PECB Certified ISO/IEC 27001 Lead Implementer

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: ISLI1151803-2024-07
Issue Date: 2024-07-18
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas
Chief Compliance Officer



PECB

BEYOND RECOGNITION

Professional Evaluation and Certification Board

hereby attests that

Daria Kaliberda

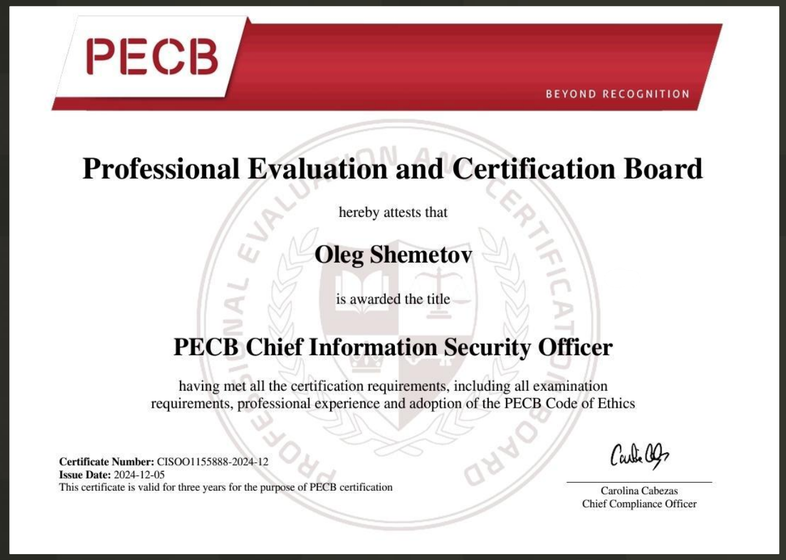
is awarded the title

PECB Certified ISO/IEC 27001 Auditor

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: ISAU1155721-2025-01
Issue Date: 2025-01-06
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas
Chief Compliance Officer



PECB

BEYOND RECOGNITION

Professional Evaluation and Certification Board

hereby attests that

Oleg Shemetov

is awarded the title

PECB Chief Information Security Officer

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: CISOO1155888-2024-12
Issue Date: 2024-12-05
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas
Chief Compliance Officer

ПОРАДИ

Ліцензіатам

1. Змінити парадигму «КСЗІшного» мислення
2. Організувати навчання та сертифікацію оцінювачів («minimum minimorum» - CCNA, NIST Consultant, ISO 27001 implementor/Auditor)
3. Визначитись з методологією оцінки ризиків та провести її апробацію на собі
4. Створити СУІБ у власній організації (РІВЕНЬ ДОВІРИ!)
5. Тверезо оцінювати скоуп проєктів замовника
6. Забудьте про СБІ

Власникам/розпорядникам ІКС

1. Мати власну стратегію розвитку кібербезпеки (прийняту на рівні організації)
2. Прийняти власну просту методологію оцінки ризиків
3. Розробити власний порядок авторизації в організації з деталізацією кроків (алгоритм)
4. Відмовитись від космічних термінів авторизації систем
5. Сертифікувати команду/підрозділ оцінювачів або хоча б впроваджувачів
6. Вимагати від зовнішніх оцінювачів додавати докази до реалізації кожного контролю
7. Звертати увагу на компетенції організацій підрядників (впровадження/оцінювання)
8. Забудьте про СБІ

ПОРАДИ

Держспецз’язку

1. Деталізувати ПКМУ 712 на рівні наказу АДССЗЗІ по аналогії з НД ТЗІ 2.6-001-11 (деталізований порядок проведення робіт)
2. Закріпити в нормативці чітке розмежування термінів і понять (де закінчується ТЗІ і починається кібер? Профілі це кібер чи ТЗІ?)
3. Надати зрозумілі всім рекомендації з оцінки ризиків
4. Уточнити та переписати базові профілі безпеки (переклад+зрозуміле тлумачення)
5. Запровадити механізми компенсаційних заходів для контролів
6. Сертифікувати власних спеціалістів та зобов’язати мати практичний досвід впровадження
7. Встановити жорсткий контроль за якістю проведення оцінювання та відповідальність організації-оцінювача
8. Відмінити недіючі НД ТЗІ (зокрема про СБІ)

ПРОХАННЯ ДО ВСІХ

НЕ ПЕРЕТВОРІТЬ ГАРНУ ІНІЦІАТИВУ в «КСЗІ»!!!®

Олег Шеметов
o.shemetov@mil.ua