МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА ТА АРХІТЕКТУРИ

Факультет автоматизації і інформаційних технологій
Кафедра кібербезпеки та комп’ютерної інженерії

Поєднання принципів побудови КСЗІ та імплементація норм європейських директив з кібербезпеки до національного законодавства

Виконав студент 2-ого курсу, група БІКСм-24:
Боднар Владислав Романович
Керівник:
к.т.н., доцент Шабала Є.Є.

ВСТУП

Мета роботи: *озроблення інтегрованої моделі побудови системи інформаційної безпеки державного органу та підприємства критичної інфраструктури в умовах агресії РФ на основі поєднання вимог КСЗІ, ISO/IEC 27001 та NIST CSF, а також формування профілів безпеки для системи електронного документообігу ТОВ «ПРОМІНЬ».*

Об'єкт дослідження: *процеси забезпечення інформаційної та кібернетичної безпеки в інформаційних системах державного сектору та критичної інфраструктури України в умовах війни.*

ЗАВДАННЯ

Створення інтегрованої моделі, яка б поєднувала:

- *вимоги КСЗІ як обов’язкової основи національного законодавства,*
- *стандарти ISO як міжнародну найкращу практику,*
- *фреймворк NIST CSF як гнучкий та дієвий інструмент управління кіберризиками.*

АКТУАЛЬНІСТЬ ТЕМИ

*Тема є надзвичайно **актуальною**, оскільки поєднання принципів побудови КСЗІ з директивами ЄС:*

- *забезпечує модернізацію української системи кіберзахисту;*
- *сприяє інтеграції України до європейського кіберпростору;*
- *підвищує рівень безпеки державних і корпоративних систем;*
- *відповідає сучасним загрозам та вимогам інформаційної безпеки.*

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Комплексна система захисту інформації (КСЗІ) — це сукупність організаційних, технічних та програмно-технічних заходів, спрямованих на забезпечення захисту інформації в автоматизованих системах (інформаційних, телекомунікаційних, інформаційно-телекомунікаційних), яка обробляє інформацію з обмеженим доступом.

ПРИНЦИПИ ПОБУДОВИ КСЗІ

1. *Принцип законності та нормативної регламентованості*
2. *Принцип комплексності*
3. *Принцип достатності заходів*
4. *Принцип безперервності*
5. *Принцип мінімізації привілеїв*
6. *Принцип документованості*
7. *Принцип контролю та аудиту*
8. *Принцип фізичного та інженерного захисту*
9. *Принцип інтегрованості з міжнародними стандартами*

ОБ’ЄКТИ ТА СУБ’ЄКТИ ЗАХИСТУ ІНФОРМАЦІЇ

Об’єктами захисту:

- інформація з обмеженим доступом (конфіденційна, службова, комерційна та ін.);
- засоби обробки інформації (сервери, ПК, мережеве обладнання);
- ·канали передавання інформації;
- програмне забезпечення, яке забезпечує обробку та збереження цієї інформації.

Суб’єктами захисту:

- Замовник та виконавець
- Контролюючий орган
- Організатор експертизи
- Підрядник

ISO 27001

ISO/IEC 27001 *— це міжнародний стандарт, який встановлює вимоги до створення, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення системи управління інформаційною безпекою (СУІБ, англ. ISMS — Information Security Management System).*

МЕТА ТА ПРИНЦИП ДІЇ ISO 27001

*Основна **мета ISO/IEC 27001** — забезпечити конфіденційність, цілісність та доступність інформації, що обробляється організацією. Стандарт допомагає ідентифікувати ризики безпеки інформації, впровадити відповідні заходи контролю, а також постійно вдосконалювати процеси безпеки.*

***ISO/IEC 27001** базується на циклі **PDCA (Plan–Do–Check–Act)**, що відображає підхід до постійного вдосконалення.*

УЗГОДЖЕНЯ ПРИНЦИПІВ ПОБУДОВИ КСЗІ З МІЖНАРОДНИМИ СТАНДАРТАМИ

Принцип КСЗІ	**ISO/IEC 27001**	**ISO/IEC 27002**	**NIST CSF**	**Ступінь узгодженості**
Комплексність	Annex A	Controls	PR.*	Повна
Ризики	6.1	-	ID.RA	Часткова
Мінімізація привілеїв	A.9	AC Controls	PR.AC	Повна
Аудит	9.2	12.7	DE.*	Повна
Фізична безпека	A.11	A.11.*	PR.PT	Повна

ПОГЛИБЛЕНЕ ПОРІВНЯННЯ МОЖЛИВОСТЕЙ КСЗІ ТА ISO/IEC 27001

Критерій	КСЗІ	ISO/IEC 27001
Відповідність законодавству України	Обов’язкова	Не регулюється законом
Міжнародне визнання	Обмежене	Високе
Підхід до ризиків	Частково (модель загроз)	Повноцінний (ISO 27005)
Гнучкість процесів	Низька	Висока
Можливість інтеграції з іншими стандартами	Обмежена	Висока (ISO 9001, 22301, 27701 тощо)
Затрати на впровадження	Високі у державному секторі	Гнучкі, залежать від масштабу
Атестація / аудит	Державна атестація	Незалежний міжнародний аудит
Циклічність процесів	Лінійний процес	PDCA (постійне вдосконалення)
Підтримка управління змінами	Обмежена	Системна (Change Management)
Орієнтація на бізнес-процеси	Низька	Висока

ПОРІВНЯННЯ ВИМОГ КСЗІ З ISO/IEC ТА NIST

Вимога	**КСЗІ (НД ТЗІ)**	**ISO 27001/27002**	**NIST CSF**
Модель загроз	Обов’язкова	Необов’язкова	Частково
Аналіз ризиків	Обмежено	Основна вимога	Основна вимога
Політики	Частина КСЗІ	Обов’язкові	Обов’язкові
Фізичний захист	Регламентований	Регламентований	Частково
Аудит	Експертиза	Сертифікація	Самооцінка

ПОРІВНЯННЯ АТЕСТАЦІЇ, ДЕКЛАРУВАННЯ ТА АВТОРИЗАЦІЇ

Параметр	**Атестат КСЗІ**	**Декларація**	**Авторизація**
Хто оцінює	Експерти	Власник	Власник + ДССЗЗІ
Орієнтація	НД ТЗІ	Профіль безпеки	Ризики + профілі
Гнучкість	Низька	Висока	Висока
Тривалість	6–12 міс.	5–30 днів	1–3 міс.
Інтеграція ISO	Низька	Середня	Висока
Інтеграція NIST	Мінімальна	Висока	Повна
Сфера	Усі ІКС	Більшість систем	Критичні системи

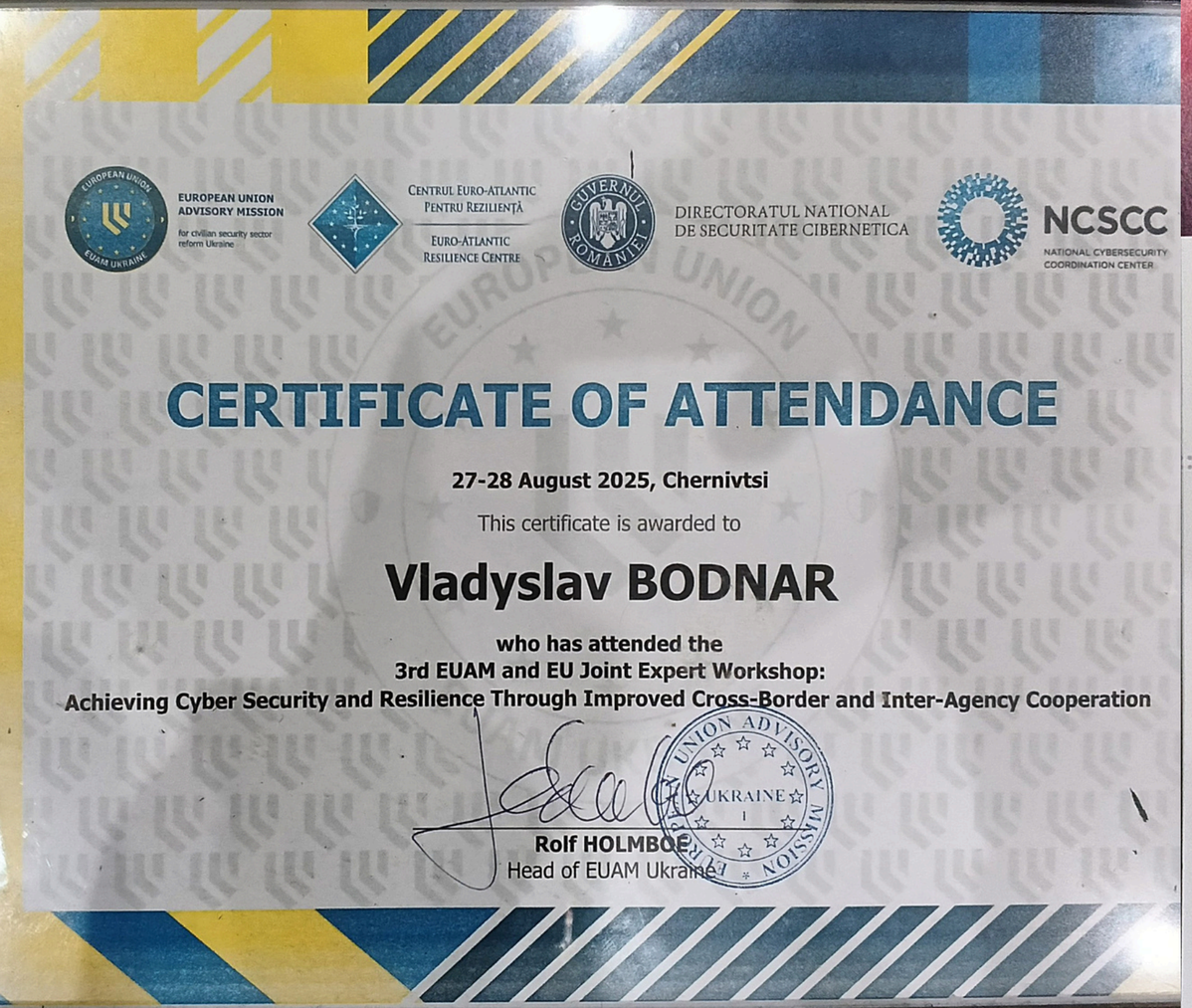
ПОРІВНЯННЯ ПРОФІЛІВ КСЗІ, NIST CSF, ISO 27001 ДЛЯ СЕД

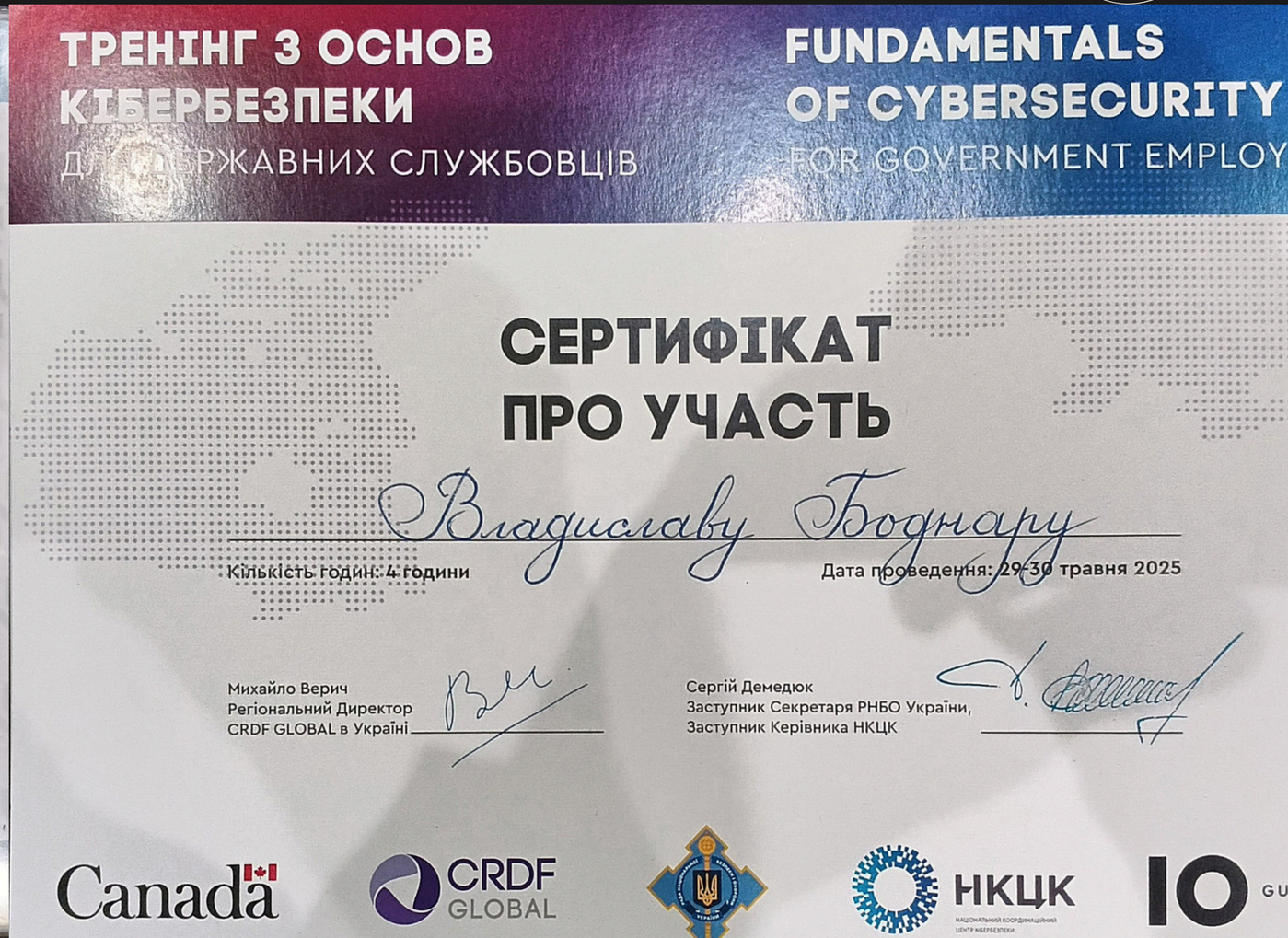
Критерій	**КСЗІ**	**NIST CSF**	**ISO 27001**
Гнучкість	Низька	Висока	Висока
Орієнтація	Нормативна	Практична	Процесна
Орієнтація на СЕД	Середня	Висока	Висока
Контроль доступу	Сильний	Дуже сильний	Сильний
Хмарні СЕД	Проблемні	Добре	Добре
Вартість	Висока	Середня	Середня
Документоорієнтованість	Висока	Середня	Висока
Актуальність	Середня	Висока	Висока
Ризик-орієнтованість	Низька	Висока	Висока

ВИСНОВКИ

Дипломна робота присвячена комплексному дослідженню теоретичних, методичних та практичних аспектів побудови сучасної системи інформаційної та кібернетичної безпеки в умовах повномасштабної агресії Російської Федерації проти України. У роботі виконано глибокий аналіз національної моделі технічного захисту інформації (КСЗІ), міжнародних стандартів ISO/IEC серії 27000 та фреймворку NIST CybersecurityFramework, а також розроблено інтегровану модель їх узгодження для державних органів і підприємств критичної інфраструктури.

ПУБЛІКАЦІЇ ТА ПУБЛІЧНА ДІЯЛЬНІСТЬ





ПУБЛІКАЦІЇ ТА ПУБЛІЧНА ДІЯЛЬНІСТЬ

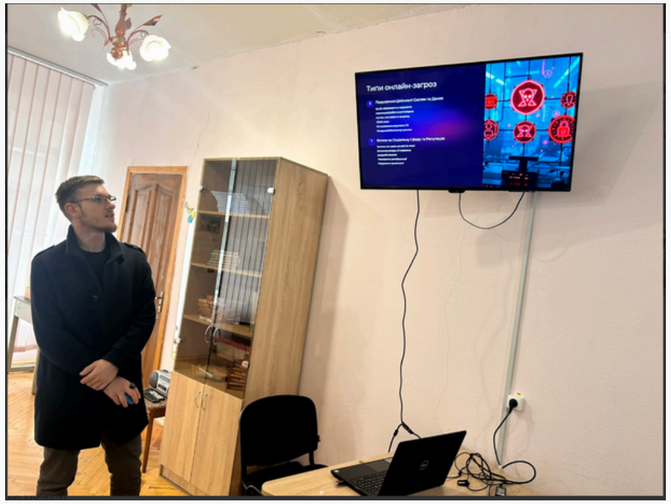
МІЖНАРОДНА НАУКОВА ІНТЕРНЕТ-КОНФЕРЕНЦІЯ
ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: ТЕХНОЛОГІЧНІ, ЕКОНОМІЧНІ ТА ТЕХНІЧНІ АСПЕКТИ СТАНОВЛЕННЯ (ВИПУСК 80) (19-20.09.2023)

“ВПЛИВ КІБЕРАТАК НА БІЗНЕС ТА ГРОМАДЯНСЬКЕ СУСПІЛЬСТВО”

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНИХ КОНФЕРЕНЦІЙ МОЛОДИХ ВЧЕНИХ «БУД-МАЙСТЕР-КЛАС-2025»

“Особливості застосування нормативних документів щодо побудови КСЗІ та ISO/IES 27001 ”

Проведення лекції за тематикою “Кібергігієна” для студентів КПКАТБМ в рамках Місяця Кібербезпеки



ДЯКУЮ ЗА УВАГУ!