

Від результатів аудиту до портфеля проєктів: як спланувати досягнення цільового рівня кібербезпеки.

Олександр Синекон

Виконавчий директор з інформаційної безпеки

11 вересня 2026

1. Кібербезпекова зрілість нижча за очікування акціонера

Поточна операційна модель не забезпечує реалістичне досягнення необхідного рівня зрілості відповідно CIS Controls у 2026 році.

2. Вимоги акціонера та регулятора потребують підсилення наявних спроможностей

Необхідне посилення контролю кібер-ризиків (CIS Controls, CIS RAM), регуляторної відповідності (постанова НБУ №№ 99, 143, 204 тощо) та безпечного використання ШІ (додаткові 20 контролів від акціонера).

3. Обмежена операційна стійкість ІТ-ландшафту

Висока людино-залежність, недостатня автоматизація та уніфікованість знижують швидкість відновлення після збоїв та гнучкість при змінах в ІТ.

OSFI + CIS Controls

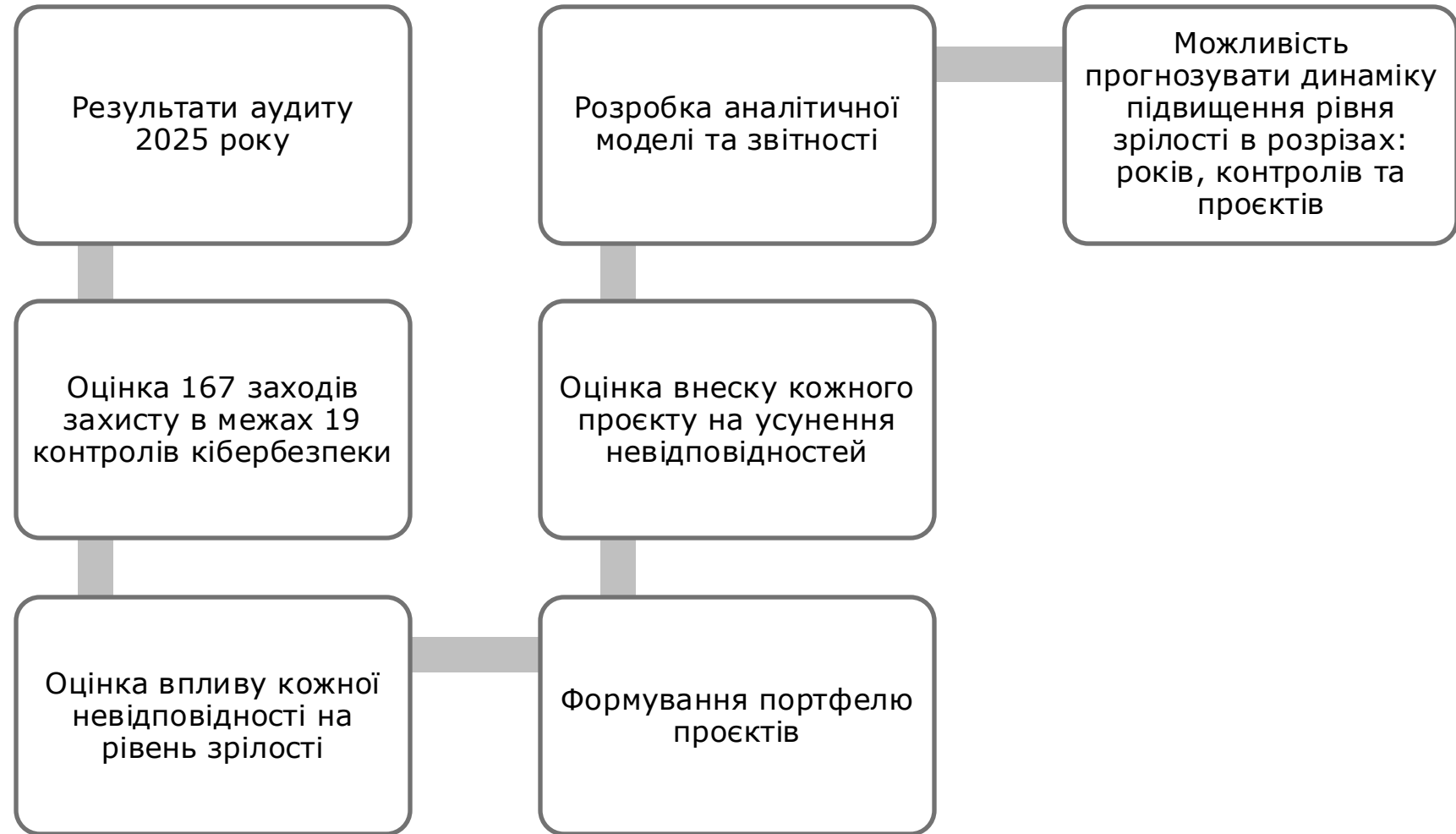
167 безпекових запобіжників

Перевірка	Опис
Політика	Відсутня → ... → Затверджена політика
Впровадження	Не впроваджено → ...→ Впроваджено на всіх системах
Автоматизація	Ручний процес → ... → Автоматизовано на всіх системах
Звітність	Відсутня → ... → Формується для всіх систем

Рівень зрілості

Початковий | Повторюваний | **Визначений** | Керований | Оптимізований

- 0 Governance / OSFI
- 1 Inventory and Control of Enterprise Assets
- 2 Inventory and Control of Software Assets
- 3 Data Protection
- 4 Secure Configuration of Enterprise Assets & Software
- 5 Account Management
- 6 Access Control Management
- 7 Continuous Vulnerability Management
- 8 Audit Log Management
- 9 Email and Web Browser Protections
- 10 Malware Defenses
- 11 Data Recovery
- 12 Network Infrastructure Management
- 13 Network Monitoring and Defense
- 14 Security Awareness and Skills Training
- 15 Service Provider Management
- 16 Application Software Security
- 17 Incident Response Management
- 18 Penetration Testing



Impact

Вплив проєкту на підвищення рівня зрілості, приведений до одного контролю

Budget

Орієнтовна оцінка вартості реалізації проєкту зовнішнім підрядником

Efforts

Орієнтовні трудовитрати внутрішньої команди для підтримки реалізації проєкту

EffortCost

Приведена до грошей вартість внутрішніх ресурсів, з розрахунку \$50 за одну людино-годину

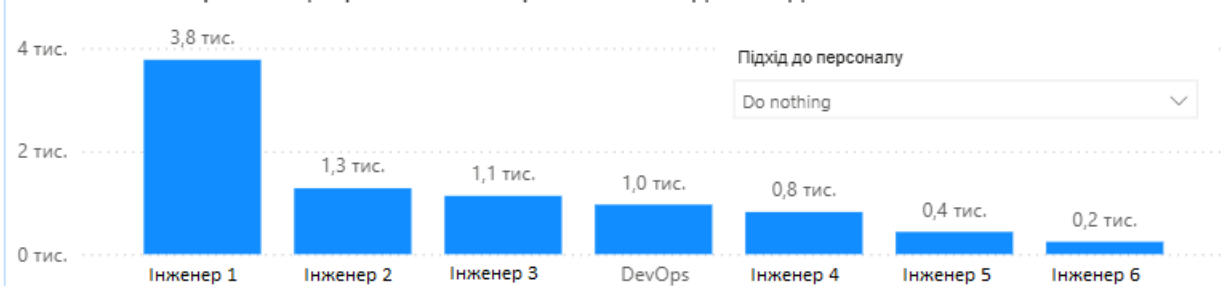
**ScorePoint
Cost**

Вартість підняття рівня зрілості одного контролю на 1 пункт, виходячи з бюджету проєкту

ДЕМО МОДЕРНІЗОВАНОГО ПОРТФЕЛЯ ПРОЄКТІВ 2026-2027

Project	Impact	Gaps	Efforts	ScorePointCost	
Automated network infrastructure management		0,83	70	379	\$24 090
Automated third-party risk management		1,24	26	271	\$4 033
Azure Landing Zones		0,82	59	650	\$0
Corporate web application protection		0,89	5	49	\$11 236
Data protection: Microsoft Pureview		1,24	56	2677	\$40 395
Data protection: System configurations		0,91	87	1342	\$54 803
Extending vulnerability scanning: Tenable		1,36	28	322	\$0
Integration DHCP logs into security systems		0,49	9	57	\$1 016
MDM Intune		0,54	53	202	\$33 080
Network Access Control: Cisco ISE		0,42	29	325	\$0
Network threat detection		0,15	14	137	\$33 875
Passive monitoring: Control of hidden IT assets		0,50	12	122	\$0
Secure remote work protection		0,45	70	98	\$0
Secure software development: DevSecOps		2,67	57	1604	\$14 994
Transparent operation of IT systems: Splunk		0,53	37	406	\$0
Усього		13,03	338	8641	\$217 522

Навантаження реалізації проєктів на співробітників (людино-годин)



Control	2025	2026	2027
00. Governance (OSFI)	3,2	3,2	3,2
01. Inventory and Control of Enterprise Assets	2,5	3,5	3,5
02. Inventory and Control of Software Assets	3,6	3,6	3,6
03. Data Protection	2,1	2,4	4,4
04. Secure Config of Ent. Assets and Software	3,2	4,1	4,8
05. Account Management	3,5	3,5	3,5
06. Access Control Management	3,5	3,5	3,5
07. Continuous Vulnerability Management	3,4	4,7	4,7
08. Audit Log Management	3,7	4,5	4,5
09. Email and Web Browser Protections	4,0	4,5	4,5
10. Malware Defenses	4,0	4,0	4,0
11. Data Recovery	3,7	3,7	3,7
12. Network Infrastructure Management	2,1	4,2	4,2
13. Network Monitoring and Defense	2,7	3,9	4,1
14. Security Awareness and Skills Training	4,7	4,7	4,7
15. Service Provider Management	2,9	4,1	4,1
16. Application Software Security	1,6	4,3	4,3
17. Incident Response Management	4,3	4,3	4,3
18. Penetration Testing	3,7	3,7	3,7
Усього	3,2	3,9	4,1



РЕСУРСНИЙ ПЛАН - ДОДАТКОВО 2 СПІВРОБІТНИКА

Role	2025-10	2025-11	2025-12	2026-01	2026-02	2026-03	2026-04	2026-05	2026-06	2026-07	2026-08	2026-09	2026-10	2026-11	2026-12	2027-01	2027-02	2027-03
+ 1-Вакансія										14%	46%	77%	80%	77%	72%	55%	44%	
+ 2-Вакансія											35%	35%	55%	82%	67%	60%	54%	
+ DevOps										55%	100%	97%	100%	97%	68%			
+ Контент										50%	42%	29%	25%	24%	25%	25%	23%	
+ Інформація											10%	73%	86%	87%	75%	75%	65%	
+ Операції	25%	24%	25%	25%	23%	75%	73%	82%	92%	97%	45%	73%	94%	90%	64%	50%	59%	29%
+ Ресурси	10%	10%	10%	10%	9%	10%	10%	45%	62%	65%	67%	36%	66%	75%	40%	25%	58%	29%
+ Ресурси										22%	40%	39%	40%	39%	27%			
+ Часовий	5%	5%	5%	5%	5%	5%	5%	5%	5%	50%	44%	34%	37%	44%	42%	35%	29%	

ActivityName	2025-10	2025-11	2025-12	2026-01	2026-02	2026-03	2026-04	2026-05	2026-06	2026-07	2026-08	2026-09	2026-10	2026-11	2026-12	2027-01	2027-02	2027-03	Total
+ Automated network infrastructure management													168	163	49				379
+ Automated third-party risk management										151	93								244
+ Azure Landing Zones	67	65	67	67	61	67	65	67	65	59									650
+ Corporate web application protection																	49		49
+ Data protection: Microsoft Pureview											85	211	218	211	218	218	176		1339
+ Data protection: System configurations													74	317	328	328	296		1342
+ Extending vulnerability scanning: Tenable												138	143	41					322
+ Integration DHCP logs into security systems									23	34									57
+ MDM Intune											39	98	65						202
+ Network Access Control: Cisco ISE							72	98	101	55									325
+ Network threat detection																39	98		137
+ Passive monitoring: Control of hidden IT											84	38							122
+ Secure remote work protection											55	42							98
+ Secure software development: DevSecOps										170	311	301	311	301	211				1604
+ Transparent operation of IT systems: Splunk						84	81	84	81	76									406
Total	67	65	67	67	61	151	146	223	267	591	722	828	979	1033	805	546	560	98	7276

ДОРОЖНЯ КАРТА ПРОЄКТІВ 2026-2027



! - Старт проєкту критично залежить від заповнення вакансій

1. Відслідковування прогресу в закритті невідповідностей.
2. Контроль відповідності не тільки в частині виконання вимог CIS Controls.
3. Зміна складу CIS Controls.
4. Балансування в ресурсному плануванні між операційними та проєктними задачами.
5. Ризик-менеджмент (CIS Risk Assessment).

01 ДЖЕРЕЛА ДАНИХ КІБЕРБЕЗПЕКИ

01 РЕЗУЛЬТАТИ АУДИТІВ

Спостереження, докази,
рекомендації

02 БЕЗПЕКОВІ КОНТРОЛІ

Вимоги та критерії
оцінювання

03 ВНУТРІШНІ
ДОКУМЕНТИ

Політики, стандарти,
процедури

СТРУКТУРОВАНИЙ КОНТЕКСТ

02 АНАЛІТИЧНЕ ЯДРО

MICROSOFT COPILOT STUDIO

COPILOT STUDIO ШІ АГЕНТ

Єдине аналітичне ядро для оцінювання, пріоритезації та планування
підвищення зрілості

Виявлення прогалин Автоматизоване зіставлення доказів із
безпековими контролями

Оцінка впливу Вплив змін і проєктів на контролі, ризики та
рівень зрілості

Дорожня карта Пріоритезований план заходів з очікуваним
ефектом

КОНТРОЛЬ І ДОВІРА

Entra ID

RBAC

DLP

Політики даних

03 УПРАВЛІНСЬКІ РЕЗУЛЬТАТИ

ПАНЕЛЬ КЕРУВАННЯ CISO

Рівень зрілості • Прогалини • Ключові ризики •
Динаміка

ІНІЦІАТИВИ З ПІДВИЩЕННЯ ЗРІЛОСТІ

План заходів • Пріоритезація • Контроль виконання

ОЦІНКА ВПЛИВУ ЗМІН

Вплив на контролі • Рівень зрілості • Залишковий
ризик

КОРИСТУВАЧІ: CISO • ПРОЄКТНИЙ ОФІС • МЕНЕДЖЕР З
КОМПЛАЄНСУ

БІЗНЕС-ЕФЕКТ

БЕЗПЕРЕРВНИЙ КОНТРОЛЬ
замість періодичних оцінок

ЗНИЖЕННЯ КІБЕРРИЗИКІВ
і регуляторна відповідність

ОПТИМІЗАЦІЯ РЕСУРСІВ
часу та витрат команди

ОБҐРУНТОВАНІ РІШЕННЯ
прозора пріоритезація

Дякую!

Олександр Синекон
+380674075057
osynekop@universalna.com
<https://www.linkedin.com/in/olexandrsynekop/>