**Курій Євгеній Олегович,** асистент кафедри захисту інформації Національного університету «Львівська політехніка», м. Львів

Email: yevhenii.o.kurii@lpnu.ua

ORCID: 0000-0002-3423-5655

**Опірський Іван Романович**, д.т.н., професор, професор кафедри захисту інформації Національного університету «Львівська політехніка», м. Львів

E-mail: ivan.r.opirskyi@lpnu.ua

Orcid ID: 0000-0002-8461-8996

# **ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ОСНОВНИХ ФРЕЙМВОРКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

Який з фреймворків інформаційної безпеки найкраще відповідає вашим вимогам? Перш за все, концепція «найкращого» фреймворку інформаційної безпеки є помилковою, оскільки вибір найбільш відповідного фреймворку значною мірою залежить від вашої бізнес-моделі [1]. Застосовні до вашої організації закони, нормативні акти та договірні зобов’язання найчастіше вкажуть вам на один з наступних фреймворків інформаційної безпеки [2]:

* ISO 27001/002
* NIST Special Publication 800-53
* NIST Cybersecurity Framework
* PCI DSS
* CIS Controls
* HITRUST Common Security Framework
* HIPAA
* AICPA Trust Services Criteria (SOC 2)
* COBIT

Коли ви графічно зображуєте різноманітні провідні фреймворки інформаційної безпеки від «простішого до складнішого» (Рисунок 1), ви, в першу чергу, повинні зосередити увагу на кількості унікальних елементів керування чи контролів безпеки. Обсяг цих контролів (вимог) безпосередньо впливає на кількість доменів, охоплених цим фреймворком [3]. Фреймворк із меншою кількістю контролів може здатися легшим для впровадження, але він також може не забезпечити необхідного покриття, якого потребує ваша організація з точки зору адміністративних, технічних та фізичних засобів забезпечення захисту інформації. Визначення «правильного» фреймворку для вашої організації – це перш за все бізнес-рішення, засноване на розумінні контексту організації та профілю ризику, яке повинно враховувати чинні закони, нормативні акти та договірні зобов’язання, необхідні для підтримки існуючих або запланованих бізнес-процесів [4].



Рисунок 1 – Класифікація основних фреймворків інформаційної безпеки за спеціалізацією і шириною покриття

Дуже важливим моментом при виборі фреймворка є необхідність його налаштування чи кастомізації. Малоймовірно, що окремий фреймворк ідеально відповідатиме вашим потребам, тому вам доведеться розраховувати на адаптацію фреймворку до ваших конкретних потреб (наприклад, додавання до нього необхідних контролів, видалення непотрібного вмісту або об’єднання кількох фреймворків).

Чим складніший і деталізованіший фреймворк ви виберете, тим більше охоплення доменів відповідними контролями безпеки ви можете очікувати в результаті його впровадження. Загалом це також означає, що ви матимете більш складні і комплексні політики та процедури для відповідності широкому охопленню [5]. Проте дилема, з якою стикаються багато компаній, полягає в тому, що вони прагнуть досягнути відповідності тому чи іншому фреймворку чи стандарту, і водночас звести до мінімуму кількість документів і контролів, які вони повинні підтримувати. Саме тут важливий аспект погодження стратегії інформаційної безпеки з керівництвом компанії і визначення профілю ризику організації на фундаментальному рівні.

Зрозуміло, що розглядати запропоновану вище класифікацію може бути дещо заплутаним, оскільки кожен фреймворк інформаційної безпеки має власну унікальну сферу застосування і ширину охоплення. Однак розуміння класифікації складності може допомогти організаціям прийняти обґрунтоване рішення про те, з чого почати роботу і який з фреймворків може стати найбільш відповідним до її потреб (проте часто організації використовують більше ніж один фреймворк). В процесі роботи, організації можуть виявити що їм потрібен метафреймворк (фреймворк фреймворків), щоб відповідати складнішим вимогам відповідності і безпеки.

**Література**

1. Hamed Taherdoost, Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview (2022). DOI: 10.3390/electronics11142181
2. Top 11 cybersecurity frameworks in 2023 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.connectwise.com/blog/cybersecurity/11-best-cybersecurity-frameworks>
3. Tom Conkle, Greg Witte, Improving cybersecurity through the use of the cybersecurity framework (2015) 9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT 2015, Volume 3, Pages 2479 – 2486
4. Kurii, Y. Opirskyy, I. (2021). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. Paper presented at the CEUR Workshop Proceedings, 3288, 21-32;
5. Cybersecurity Framework: Types, Components, Functions [Електронний ресурс] – Режим доступу до ресурсу: <https://www.knowledgehut.com/blog/security/cyber-security-frameworks>