Національний фонд досліджень України
Конкурс проєктів із виконання наукових досліджень і розробок
“Передова наука в Україні”.

Назва проєкту ФРЕЙМВОРК ОЦІНКИ КІБЕРЗАХИЩЕНОСТІ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
Науковий керівник проєкту Мілов Олександр Володимирович

Сучасний стан проблеми

Безпека особистості, суспільства і держави залежать від надійної роботи критичної інфраструктури. Загрози кібербезпеки використовують переваги підвищеної складності та зв’язності критично важливих інфраструктурних систем та ставлять під загрозу національну безпеку, економіку, громадську безпеку та здоров'я. Як і фінансові ризики, і ризики репутації, ризики кібербезпеки впливають також і на стан бізнесу. Вони можуть збільшити витрати і вплинути на результати діяльності. Ризики кібербезпеки можуть негативно впливати на стан організацій, їх здатність проводити повсякденну діяльність, впроваджувати інновації, залучати та утримувати клієнтів. Кібербезпека може бути важливим компонентом зростаючого значення для загального управління ризиками в організації.

У USA Patriot Act (https://www.congress. gov/bill/107th-congress/house-bill/3162) і Програмі критичної інфраструктури Департаменту внутрішньої безпеки (DHS) США (http://www.dhs.gov/critical-infrastructure-sectors) критична інфраструктура визначається як "системи та активи, фізичні чи віртуальні, настільки життєво важливі, що неадекватність чи знищення цих систем та активів матиме виснажливий вплив на безпеку, національну економіку, національне здоров'я та безпеку населення або будь-яка їх комбінація". Через зростаючий тиск зовнішніх та внутрішніх загроз організаціям, відповідальним за критичну інфраструктуру, необхідно мати цілісний та ітеративний підхід до виявлення, оцінювання та управління ризиками кібербезпеки. Такий підхід необхідний незалежно від форми власності, розміру організації, її схильності до загроз або рівня складності забезпечення кібербезпеки сьогодні. Тож спільнота критичної інфраструктури включає державних та приватних власників, операторів та інші організації, які впливають на сталість функціонування національної інфраструктури. Члени кожного сектора критичної інфраструктури виконують функції, що підтримуються широким спектром технологій, включаючи інформаційні технології (IT), промислові системи управління (ICS), кіберфізичні системи (CPS) та підключені пристрої в більш загальному сенсі, включаючи Інтернет речей (IoT). Ця залежність від

технології, комунікацій та взаємозв'язку змінила та розширила потенційні вразливості та збільшила потенційний ризик для операцій.

Для управління ризиками кібербезпеки потрібно чітке розуміння бізнес-процесів організації та міркувань безпеки, які є специфічними для способу використання технології. Оскільки ризики, пріоритети та системи кожної організації є унікальними, інструменти та методи, що використовуються для досягнення результатів, будуть різними. У багатьох організаціях вже є процеси управління інформаційною безпекою, наприклад згідно ISO серії 27000.

У лютому 2014 р. Національний інститут стандартів і технологій (NIST) випустив, а згодом у 2018 році оновив рекомендації (https://www.nist.gov/cyberframework), для поліпшення кібербезпеки критичної інфраструктури, які отримали загальну назву Cybersecurity Framework (далі - "фреймворк"). Фреймворк рекомендує певні процеси управління ризиками, які дозволяють організаціям інформувати та визначати пріоритети рішень щодо кіберзахисту на основі потреб бізнесу, без додаткових нормативних вимог. Це дає змогу організаціям - незалежно від сектору, розміру, ступеня ризику кібербезпеки чи складності кібербезпеки - застосовувати принципи та ефективні практики управління ризиками для підвищення захисту та стійкості критичної інфраструктури. Фреймворк покликаний доповнювати, а не замінювати або обмежувати процес організації управління ризиками та програму кіберзахисту. Кожен сектор та окрема організація можуть використовувати Фреймворк з урахуванням своїх цілей в галузі кібербезпеки. Тож метою існуючої методології формування і використання фреймворка кібербезпеки зазвичай вважається доповнення таких процесів та надання керівних принципів для полегшення управління ризиками інформаційної та кібернетичної безпеки відповідно до впроваджених організацією підходів щодо управління ризиками.

Новизна проєкту

Треба чітко розуміти, що поняття фреймворку, також існує в ІТ-середовищі, де воно розуміється достатньо вузько як програмна платформа (каркас). У нашому випадку йдеться про методологічну платформу (концепцію, принципи, методи, технології), яка на відміну від згаданих американських розробок базується на:

- розумінні КЗ критичної інфраструктури, як сутності, що об'єднує дві ключові складові безпеки: інформаційну (або кібербезпеку у вузькому сенсі) і

функціональну. Такий підхід, з огляду, зокрема, на понад 20 річний індустріальний досвід роботи виконавців проєкту, давно працює в ядерній енергетиці України і світу взагалі - при цьому функціональна безпека для АЕС є найважливішою характеристикою. Зрозуміло, що залежно від доменів таксономія і ієрархія складових може змінюватися;

- розумінні того, що фреймворк має бути міжсекторальним, тобто формуватися для КІ різних галузей, а ілюструвати його імплементування для енергоКІ;

- розумінні ієрархічності критичної інфраструктури (програмно-апаратні компоненти, інформаційні/інформаційно-керуючі системи, ІТ-інфраструктура) і таким чином слід досліджувати певний "безпековий куб": рівні ієрархії КІ - складові безпеки КІ - процеси (регулювання вимог, оцінювання, забезпечення їх виконання). Саме в такому, «гіперкубічному» сенсі» розглядається фреймворк кіберзахисту критичної інфраструктури в цьому проєкті.

Окремо слід наголосити, що Україна має унікальний досвід і отримала унікальні (позитивні і негативні) уроки масових кібератак на її критичну енергоінфраструктуру (інфраструктурних кібератак). Це визнається у світі, отже ми маємо всі підстави для узагальнення цього досвіду задля в дослідженні, спрямованому на підвищення надійності і динамічності захисту критичної інфраструктури.