ПОРТАЛ ENISA ЯК КОМПЛЕКСНИЙ РЕСУРС ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Чалий І.В., к.т.н., доц.
Міхальова К.М., здобувачка РВО бакалавр
Державний біотехнологічний університет
м. Харків, Україна, ivchaly@btu.kharkov.ua

Анотація: Робота присвячена дослідженню інструментів порталу ENISA, як комплексного ресурсу інформаційної безпеки Європейського Союзу, який може бути корисним для українських спеціалістів, організацій, урядових та приватних установ у покращенні захисту від кіберзагроз.
Ключові слова: інформаційна безпека, ЄС, ENISA, інструмент SIM3v2i, кібербезпека

Україна, подібно багатьом іншим країнам, розглядає кібербезпеку як важливий аспект свого благополуччя зараз та на майбутнє. Прагнення до співпраці з Європейським Союзом (ЄС) у сфері кібербезпеки є важливим елементом системи національної безпеки та впевненого сталого її розвитку.

Зважаючи на стрімке зростання та всеосяжність глобальних інформаційних викликів у царині кібербезпеки, стає очевидною неможливість їх вирішення зусиллями лише однієї чи кількох країн. Це робить розвиток міждержавного співробітництва в цій сфері не просто необхідним, а й екзистенціально важливим.

ЄС, визнаючи інформаційну безпеку одним із пріоритетних напрямів своєї діяльності, веде активну політику в цій сфері. Ця політика спрямована на захист критично важливих інфраструктур та особистих даних громадян, що є запорукою стійкого розвитку та добробуту суспільства в епоху ІТ. Співпраця на міжнародному рівні стає ключовим фактором успіху в боротьбі з кіберзагрозами. Важливим аспектом її є спільне дослідження та розробка нових технологій кібербезпеки, а також обмін інформацією та передовим досвідом. Це допоможе країнам світу підвищити свою стійкість до кібератак та мінімізувати ризики, пов'язані з кіберзлочинністю. Окрім того, важливим напрямком співпраці є координація зусиль з реагування на кіберінциденти. Створення спільних систем раннього попередження та реагування дозволить країнам світу ефективніше протистояти кіберзагрозам, що мають транскордонний характер. Таким чином, розвиток міжнародного співробітництва в сфері кібербезпеки є не просто доцільним, а й життєво необхідним кроком на шляху до забезпечення безпечного та сталого розвитку суспільства в епоху ІТ.

Для організації взаємодії країн ЄС у питаннях забезпечення безпеки було засноване 10 березня 2004 року Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA (англ. European Union Agency for Network and Information Security). Також було створено відповідний портал [1].

Законодавство ЄС про кібербезпеку на основі надає посилений мандат ENISA як наглядового органа ЄС у царині кібербезпеки подоланні загроз у цій сфері, а також сприяє створенню загальноєвропейської системи сертифікації кібербезпеки, в якій ENISA відіграватиме ключову роль.

Аналізуючи численні зустрічі та ухвалені в останній час документи можливо виділити такі основні напрямки співпраці ENISA та України [2]:

1. Підвищення обізнаності та навичок у сфері кібербезпеки.
2. Сприяння розвитку нормативної бази.
3. Зміцнення кібербезпеки критичної інфраструктури.
4. Участь у дослідницьких проєктах.
5. Сприяння міжнародному співробітництву.

Web-портал ENISA є офіційним ресурсом цієї організації і містить широкий спектр інформації з кібербезпеки, включаючи новини, публікації, звіти, інформаційні матеріали та рекомендації. Користувачі можуть знайти на ньому різні ресурси, призначені для підвищення кібербезпеки в Європі, такі як настанови, курси, інструкції та інші освітні матеріали. Ресурс також надає інформацію про проєкти ENISA, а також можливість зв'язку для отримання консультацій та експертної підтримки з питань кібербезпеки.

Інструменти, що доступні на порталі ENISA, стосуються різноманітних ресурсів, програмних додатків, інструкцій та інших матеріалів, спрямованих на допомогу окремим особам, організаціям і політикам у покращенні їхніх можливостей кібербезпеки. Ці інструменти розроблені для вирішення різних аспектів кібербезпеки, починаючи від оцінки ризиків і реагування на інциденти до механізмів відповідності та навчання з питань безпеки.

Структури оцінки ризиків: ці інструменти допомагають організаціям оцінювати ризики кібербезпеки та керувати ними, надаючи структуровані методології для виявлення, оцінки та пом’якшення загроз і вразливостей.

Інструкції з реагування на інциденти: ENISA пропонує практичні посібники та шаблони, які допоможуть організаціям розробити ефективні плани реагування на інциденти кібербезпеки, що дозволить ефективно виявляти і реагувати на них та відновлювати свою інфраструктуру після їх реалізації.

Навчальні матеріали з питань безпеки: ENISA може надавати освітні ресурси, такі як посібники з найкращих практик, інформаційні кампанії та модулі електронного навчання, щоб сприяти підвищенню обізнаності щодо кібербезпеки серед окремих осіб і компаній.

Інструменти та утиліти кібербезпеки: ENISA також співпрацює з галузевими партнерами, щоб надати доступ до інструментів кібербезпеки, програмних рішень і утиліт, які полегшують виявлення загроз, оцінку вразливості та моніторинг мережі.

Інструмент самооцінки SIM3v2i, відомий також як Модель зрілості CSIRT ENISA (рис. 1). ENISA виступає партнером CSIRTs (команда комп'ютерної безпеки з реагування на інциденти), надаючи їм експертні рекомендації для вдосконалення, підвищення зрілості та кращого захисту своїх клієнтів. Інструмент допомагає CSIRT самостійно оцінити зрілість своєї команди за 45 параметрами моделі SIM3v2i [3]. Це опитування поділене на чотири категорії: організація, людина, інструмент та процеси. Після кожної відповіді на діаграмі показують оцінку вашої організації та також надається таблиця з підсумком за кожним параметром. Усі параметри оцінюються, щоб визначити рівень зрілості (базовий, середній або просунутий).

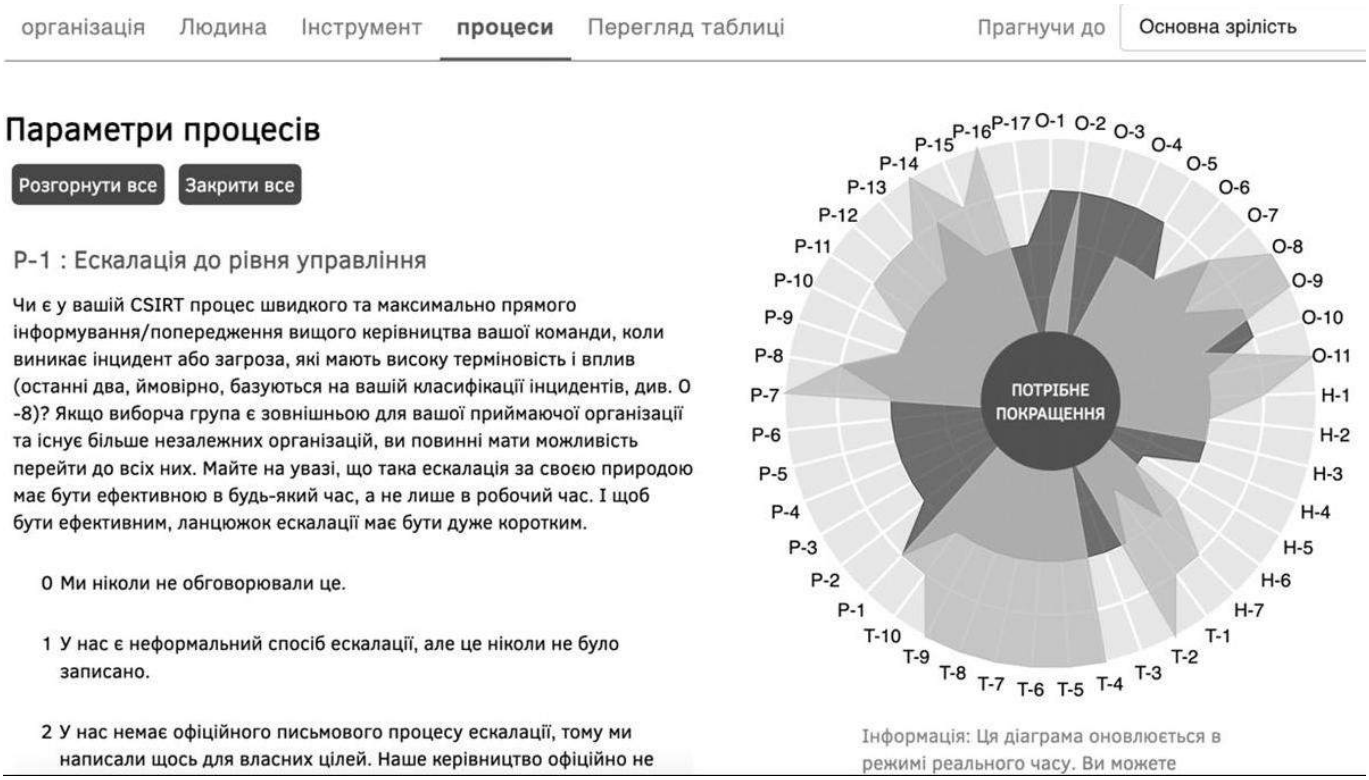

Рис. 1. Інструмент самооцінки SIM3v2i.

Модель зрілості CSIRT ENISA – це інструмент, що дає можливість CSIRT оцінити власний рівень зрілості. Самооцінка за її допомогою допомагає CSIRT встановити базовий рівень зрілості для внутрішнього аналізу, визначити відправну точку для подальшого розвитку та вдосконалення та розробити план дій з чіткими часовими рамками для досягнення вищого рівня зрілості. Модель також дає можливість порівняти результати самооцінки з іншими CSIRT, використовуючи її як орієнтир. Етапи зрілості, визначені в моделі, слугують прикладом належних практик для національних CSIRT. Таким чином вона:

- Сприяє самовдосконаленню CSIRT.
- Стимулює впровадження кращих практик.
- Підвищує загальний рівень кібербезпеки в Європі.

Інформаційні технології кібербезпеки для сталого розвитку України є одним із пріоритетних завдань. Можливості порталу ENISA, особливо практичні інструменти, що доступні на ньому, безумовно посприяють заходам для захисту інформаційного простору держави.

Список літератури

1. Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA). URL: https://www.enisa.europa.eu/.
2. Україна посилює співпрацю з ЄС у сфері кібербезпеки: НКЦК підписав Угоду про співпрацю з ENISA. URL: https://www.rnbo.gov.ua/ua/Diialnist/6706.html.
3. SIM3v2i self-assessment tool. ENISA. URL: https://www.enisa.europa.eu/ topics/incident–response/csirt–capabilities/csirt–maturity/sim3–v2i.