MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

KHARKIV NATIONAL
UNIVERSITY OF RADIO ELECTRONICS

RADIOTEKHNIKA

All-Ukrainian
interdepartmental scientific and technical collection

ISSN 0485-8972
eISSN 2786-5525

Founded in 1965

I S S U E 2 1 3

Kharkiv
Kharkiv National
University of Radio Electronics
2023

ЗМІСТ

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ, ОБРОБКА СИГНАЛІВ

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

УДК 004.056.5 **DOI:10.30837/rt.2023.2.213.04**

О.І. ПЕЛЮХ, М.В. ЄСІНА, канд. техн. наук, Д.Ю. ГОЛУБНИЧИЙ, канд. техн. наук

ОЦІНКА CERT-UA НА ОСНОВІ МОДЕЛІ ЗРІЛОСТІ CSIRT ENISA

Вступ

Відкритість та підключеність до глобальної мережі стали невід'ємною частиною сучасного світу, але разом з цим зростають і загрози, пов'язані з кібербезпекою. Кіберінциденти, такі як: хакерські атаки, витоки даних та викрадення конфіденційної інформації, стають все поширенішими й складнішими. У боротьбі з цими загрозами вирішальну роль відіграє ефективне реагування на кіберінциденти.

У цьому контексті оцінка команди з реагування на кіберінциденти набуває все більшої важливості. Команда з реагування складається з експертів з кібербезпеки, інженерів з мережі, аналітиків та інших фахівців, які працюють разом для виявлення, аналізу та врегулювання кіберінцидентів. Ефективна команда з реагування може швидко усунути загрозу, зменшуючи шкоду та відновлюючи нормальне функціонування систем.

Метою статті є розгляд важливості оцінки команди з реагування на кіберінциденти. Розглянемо ключові аспекти, які необхідно враховувати при оцінці команди, такі як навички, досвід, комунікація та співпраця за допомогою оновленої Моделі зрілості CSIRT ENISA [1]. Розглянуто інструменти та методики, що допомагають оцінити ефективність команди з реагування та виявити слабкі місця, які можна вдосконалити, що спрямовані на предмет статті – CERT-UA та урядова команда реагування на комп’ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв’язку та захисту інформації України [2].

Оцінка команди з реагування на кіберінциденти є необхідним етапом для будь-якої організації, яка прагне забезпечити свою безпеку та захистити свої цінності в кіберпросторі. Вона сприяє постійному вдосконаленню та зміцненню необхідних навичок та зусиль для готовності до реагування на небезпеки. Розуміння важливості оцінки команди з реагування допоможе організаціям стати більш впевненими в здатності захистити свою інформацію та протистояти кіберзагрозам у сучасному цифровому світі.

1. Модель зрілості CSIRT ENISA

1.1. Загальні відомості про Модель зрілості ENISA CSIRT

Модель зрілості ENISA CSIRT сприяє зміцненню глобальної спроможності управляти кіберінцидентами з фокусом на CSIRT (Команди реагування на кіберінциденти) [1]. Вона базується на стандарті OCF SIM [3] і пропонує трирівнений підхід до зрілості, разом з методологією оцінки ENISA. Ця модель не є нормативною або стандартизованою, але надає орієнтири для підвищення зрілості CSIRT та є цінним джерелом рекомендацій. Вона поєднує в собі попередні моделі, що мають широке визнання й вжиток.

Модель, що розглядається у цій роботі, містить у своїй основі три визначні складові:

- стандарт Моделі зрілості управління безпековими інцидентами SIM3 [3];
- трирівневий підхід до оцінки зрілості команди [4];
- унікальна методологія оцінювання [5].

Розглянемо суть кожного із наведених пунктів для повного розуміння Моделі й подальшого її використання для оцінки рівня зрілості CERT-UA.

1.2. Модель зрілості управління безпековими інцидентами SIM3

SIM3, або Модель зрілості управління інцидентами безпеки, є основою для оцінки зрілості можливостей організації щодо реагування на інциденти. Це широко прийнята модель, яку використовують організації всіх розмірів, від малого бізнесу до великих підприємств [1, 3]. SIM3 базується на чотирьох квадрантах (категоріях):

- Організаційний («O»).

Цей квадрант оцінює загальний підхід організації до управління інцидентами, включаючи її політики, процедури та ресурси.

- Людський фактор («Н»).

У цьому квадранті оцінюються навички та знання людей, залучених до реагування на інциденти, включаючи їхню підготовку, досвід і здатність до спільної роботи.

- Інструменти («Т»).

У цьому квадранті оцінюються інструменти та технології, які організація використовує для підтримки реагування на інциденти, включаючи їх можливості, зручність використання та інтеграцію з іншими системами.

- Процеси («Р»).

Цей квадрант оцінює процеси реагування на інциденти в організації, включаючи їх ефективність, результативність і масштабованість.

Слід зазначити, що оновлена Модель зрілості ENISA CSIRT використовує SIM3v2i – модернізовану версію SIM3, що має додатковий параметр (О–6). Загалом стандарт складається із 45 параметрів, що охоплюють усі чотири зазначені квадранти. Нижче наведений повний перелік параметрів SIMv2i [1] – табл.1.

Таблиця 1

Параметри SIMv2i

Номер параметра	Опис параметра	Номер параметра	Опис параметра
О–1	Повноваження	Т–6	Стійкість обміну повідомленнями
О–2	Виборчий округ	Т–7	Стійкість доступу в Інтернет
О–3	Управління	Т–8	Інструментарій для запобігання інцидентам
О–4	Обов’язки	Т–9	Інструментарій для виявлення інцидентів
О–5	Опис послуги	Т–10	Інструментарій для усунення інцидентів
О–6	Публічна медіаполітика	Р–1	Перехід на рівень управління
О–7	Опис рівня обслуговування	Р–2	Перехід до служби ЗМІ
О–8	Класифікація інциденту	Р–3	Перехід до юридичної служби
О–9	Участь в системах CSIRT	Р–4	Процес запобігання інцидентам
О–10	Організаційна модель	Р–5	Процес виявлення інцидентів
О–11	Політика безпеки	Р–6	Процес усунення інцидентів
Н–1	Кодекс поведінки/практики/етики	Р–7	Конкретні процеси обробки інцидентів
Н–2	Стійкість персоналу	Р–8	Процес аудиту та зворотного зв'язку
Н–3	Опис набору навичок	Р–9	Процес забезпечення доступності в надзвичайних ситуаціях
Н–4	Розвиток персоналу	Р–10	Найкращі методи забезпечення присутності в Інтернеті
Н–5	Технічна підготовка	Р–11	Безпечний процес обробки інформації
Н–6	Розвиток соціально-комунікативних навичок	Р–12	Процес пошуку джерел інформації
Н–7	Зовнішні зв’язки	Р–13	Процес інформаційно-просвітницької роботи
Т–1	ІТ-ресурси та конфігурація	Р–14	Процес звітування з питань управління
Т–2	Список джерел інформації	Р–15	Процес звітування виборчих округів
Т–3	Консолідована система (–и) обміну повідомленнями	Р–16	Процес проведення зустрічей
Т–4	Система відслідковування інцидентів	Р–17	Процес співпраці за принципом «рівний–рівному»
Т–5	Надійність голосових дзвінків		

Кожен параметр квадранту поділяється на рівні від 0 до 4, де 0 – найнижчий рівень зрілості, а 4 – найвищий [1, 3 – 5]. Загальний рівень зрілості організації визначається як середнє арифметичне балів за всіма чотирма квадрантами. Шкала вимірювання наведена у табл. 2.

Таблиця 2

Шкала вимірювання рівня параметрів SIMv2i

Рівень	Статус	Основні критерії
0	Недоступний / невизначений / невідомий	Відсутнє будь-яке розуміння параметра і його важливості в цілому.
1	Неявний	Наявне розуміння важливості, але жодним чином не задокументоване.
2	Явний, внутрішній	Наявність будь-якого документа, що не був формально погоджений із CSIRT.
3	Явний, формалізований на підставі повноважень керівника CSIRT	Наявність будь-якого документу, офіційно затвердженого керівництвом CSIRT. Якщо документ був офіційно затверджений на організаційному рівні, який є ієрархічно вищим, але в тій самій гілці організаційної структури організації, цей документ автоматично є дійсним і для CSIRT та її керівництва – проте, якщо він має безпосереднє відношення до справи, бажано, щоб керівництво CSIRT в будь-якому випадку схвалило цей документ і, наприклад, розмістило його на вікі-сторінці команди.
4	Чіткий, активно оцінюваний на регулярній основі авторитет рівнів управління над керівництвом CSIRT	Аналогічно рівню 3, але документ регулярно оцінюється на рівні керівництва вище за керівництво CSIRT.

SIM3 можна використовувати для оцінки спроможності організації реагувати на інциденти в будь-який час, але найчастіше її застосовують для порівняння прогресу з плином часу. Регулярно оцінюючи свій рівень зрілості, організації можуть визначити сфери, які потребують вдосконалення, і зробити цільові інвестиції, щоб поліпшити свої загальні можливості реагування на інциденти, зокрема у кіберпросторі.

1.3. Трирівневий підхід у визначенні етапів зрілості CSIRT

Стадії зрілості CSIRT – це спосіб вимірювання зрілості команди реагування на інциденти комп'ютерної безпеки. Трирівневий підхід до етапів зрілості CSIRT базується на моделі зрілості SIM3 [1, 3 – 5], яка є результатом зусиль спільноти з вимірювання зрілості CSIRT. Існує три стадії зрілості, кожна з яких має свою характеристику, що наведена у табл. 3.

Таблиця 3

Етапи зрілості у Моделі зрілості ENISA CSIRT

Рівень	Опис
Базовий	Команда має обмежене розуміння у реагуванні на інциденти та не здатна ефективно на них реагувати. На цьому рівні розпочато роботу над усіма параметрами з чітким фокусом на завдання та інших формальних аспектах ролі команди. Приблизно 80% організаційних параметрів уже опрацьовано до такої міри, що їх можна вважати "просунутими".
Проміжний	Команда має краще розуміння ніж на «Базовому» етапі й краще реагує на інциденти. На основі виконаної роботи було досягнуто прогресу за всіма параметрами, окрім тих, що вже знаходяться на "просунутому" рівні. Загалом, приблизно 50 % «H», «P» і «T» параметрів можна вважати "просунутими".
Просунутий	Команда має глибоке розуміння процедури реагування на інциденти та здатна максимально ефективно на них реагувати. Більшість з параметрів SIM3 має найвищий, 4-й рівень, однак деякі вкраплення 3-го рівня допускаються.

Кожна стадія зрілості визначається набором параметрів, яким повинна відповідати CSIRT. Ці параметри для кожної стадії зрілості ґрунтуються на моделі зрілості SIM3 і охоплюють цілий ряд, зазначений у п. 1.2. У [1] наведено таблицю, що показує необхідний рівень кожного із параметрів SIM3v2i, залежно від етапу зрілості команди реагування на інциденти. Детальні критерії для оцінки кожного з параметрів наведені у [4, 5].

Використання трирівневого підходу до етапів зрілості CSIRT у комбінації із параметрами SIM3 має наступні значні переваги:

- забезпечення структурованої основи для оцінки можливостей реагування на інциденти;
- допомога організаціям та командам з реагування визначити сфери для вдосконалення;

- потенційне використання у якості індикатора прогресу команди через певний проміжок часу.

1.4. Методологія оцінки Моделі зрілості ENISA CSIRT

Наведена система зрілості CSIRT у контексті оцінки використовує збалансований симбіоз самооцінки й експертної думки [1, 4]. Автори заявляють, що така методологія є доволі збалансованою та правильною, адже шляхом самооцінки команда рефлексує, у той час як експертний погляд допомагає більш критично оцінити загальну ситуацію в команді, що оцінюється. Пропоновані складові методології оцінки виглядають наступним чином:

- Система зрілості CSIRT надає можливість оцінити зрілість CSIRT шляхом самооцінки, що є першим кроком.

Самооцінка корисна для встановлення базової, але більш суб'єктивної оцінки для внутрішнього аналізу. Вона також може слугувати відправною точкою для підвищення рівня зрілості. Результати самооцінки використовуються для розробки плану дій з визначеними часовими рамками для досягнення вищого рівня зрілості. Також можна порівняти результати оцінки з іншими CSIRT, використовуючи Модель зрілості як орієнтир. Етапи зрілості, визначені в Моделі зрілості CSIRT, є прикладом належних практик, що слугують орієнтиром для національних CSIRT. Деякі параметри можуть мати меншу вагу для конкретної команди, в той час як інші є основою для стратегії.

- У якості другого кроку в оцінці, що передбачено Моделлю зрілості CSIRT, є експертна оцінка.

Національні CSIRT можуть звернутися до інших команд з проханням провести експертну оцінку їхньої самооцінки. Це можна зробити, запрошуючи групу колег, серед яких є досвідчені співробітники, які мають знання та досвід в оцінці зрілості CSIRT. Експертна оцінка проходить більш ефективно, якщо представники команди та експертів обох сторін ознайомлені з Моделлю зрілості CSIRT. Тому рекомендується активно брати участь у формальному та неформальному навчанні, що стосується використання цих оцінок.

По-перше, самооцінка часто буває упередженою. Люди схильні переоцінювати власні можливості, і це може призвести до неточної оцінки зрілості. З іншого боку, експертна оцінка забезпечує зовнішній і критичний погляд, який може допомогти пом'якшити цю упередженість.

По-друге, експертна оцінка може допомогти виявити "сліпі зони". Коли CSIRT проводить самооцінку, вона може не знати про всі свої слабкі сторони. Експертна оцінка може допомогти виявити ці слабкі сторони, які потім можуть бути усунені для підвищення зрілості CSIRT.

Додатково необхідно визначити наступне:

- Вагомість двох форм оцінки може змінюватися залежно від конкретних обставин.

Наприклад, якщо CSIRT є новою і має обмежений досвід, може бути важливіше покладатися на самооцінку, щоб отримати уявлення про власні можливості. Однак, у міру того, як CSIRT стає більш зрілою, може виявитися більш важливим покладатися на експертну оцінку для отримання об'єктивної оцінки рівня її зрілості.

- Вагомість цих двох форм оцінювання також може змінюватися залежно від конкретної мети оцінювання.

Наприклад, якщо оцінка проводиться для того, щоб визначити, чи відповідає CSIRT певним вимогам відповідності, слід більше покладатися на самооцінку. Якщо оцінка проводиться для визначення сфер, в яких CSIRT може покращити свою роботу, краще покластися на експертну оцінку.

Зрештою, рішення про те, як зважити ці дві форми оцінки, є складним і повинно прийматися в кожному конкретному випадку окремо.

Отже, Модель, наведена у [1], є динамічною структурою, що активно використовується не лише приватними компаніями, а й урядовими організаціями.

2. Оцінка CERT-UA

2.1. Загальні відомості про CERT-UA

CERT-UA, або Команда реагування на комп'ютерні надзвичайні події України, – це організація, що підтримується урядом і надає консультації з реагування на інциденти та безпеки організаціям в Україні. CERT-UA була заснована у 2007 р. і з 2009 р. є членом Форуму команд реагування на інциденти та безпеки (FIRST) [2, 7]. Послуги CERT–UA включають:

- реагування на інциденти: CERT-UA може допомогти організаціям розслідувати та реагувати на кіберінциденти;
- консультування з питань безпеки: CERT-UA може надати організаціям поради щодо покращення їхньої системи безпеки;
- навчання: CERT-UA пропонує навчальні курси з різних тем безпеки;
- публікації: CERT-UA публікує різноманітні матеріали, пов'язані з безпекою, включаючи інформаційні бюлетені, звіти та технічні документи;
- CERT-UA є цінним ресурсом для організацій в Україні, які шукають допомоги з реагування на інциденти та забезпечення безпеки. Послуги організації доступні як державним, так і приватним організаціям.

Отже, можна стверджувати, що CERT-UA є певним аналогом національної CSIRT, а значить, не лише можливо, а й важливо оцінити рівень зрілості CERT-UA за допомогою запропонованої моделі від ENISA. Однак, через певний ступінь конфіденційності внутрішніх документів організації, неможливо надати вичерпну й точну оцінку. Тому нижче наводиться приблизна оцінка етапу зрілості команди CERT-UA, заснована на інформації, що доступна на офіційному сайті організації [2].

2.2. Оцінка CERT-UA за допомогою SIM3v2i

Для спрощеної процедури оцінки команда SIM3 розробила сайт [6], що допомагає швидко та якісно пройти оцінювання й отримати діаграму.

Таблиця 4

Оцінка CERT-UA за допомогою параметрів SIM3v2i

Параметр	Рівень	Обґрунтування
O-1	4	Організація підпорядковується Державній службі спеціального зв’язку та захисту інформації України та має чітко визначені завдання.
O-2	4	Згідно з нормативно-правовою базою організації чітко визначено цільову групу розповсюдження послуг CERT-UA.
O-3	3	Наявне письмове затвердження повноважень на сайті, але у жодному із документів чітко не зазначено про дозволені дії.
O-4	4	Існують чітко сформовані й задокументовані визначення від органу, вищого за рангом (Державна служба спеціального зв’язку та захисту України).
O-5	4	Наявний офіційний сайт із зазначенням послуг, контактів для зв’язку, тощо.
O-6	3	Простежується наявність медіа-політики, але існує значна відмінність у висвітленні різних інцидентів/новин.
O-7	4	Наявні контакти, графіки роботи й можливість отримання цілодобової допомоги.
O-8	4	Класифікація зазначена серед нормативно-правових документів, в межах яких організація здійснює свою діяльність.
O-9	4	CERT-UA є акредитованим членом FIRST протягом останніх 14 років.
O-10	–	Відсутній загальний доступ до документу, що визначає внутрішню організаційну структуру.
O-11	4	Політика безпеки зазначена у нормативно-правових документах.
H-1	3	Кодекс поведінки базується на засадах FIRST.
H-2	–	Відсутній загальний доступ до документу, що визначає внутрішню організаційну структуру.

Продовження табл. 4

Параметр	Рівень	Обґрунтування
Н-3	3	Опис навичок можливо сформувати на основі деяких організаційних параметрів.
Н-4	4	Розвиток забезпечений основними положеннями членства у FIRST й нормативно-правовою базою діяльності організації.
Н-5	4	Розвиток забезпечений основними положеннями членства у FIRST й нормативно-правовою базою діяльності організації.
Н-6	2	Розвиток забезпечений основними положеннями членства у FIRST, але чітко не є визначеним
Н-7	4	CERT-UA є акредитованим членом FIRST протягом останніх 14 років й активно співпрацює із Форумом.
Т-1	4	Визначено нормативно-правовою базою діяльності організації.
Т-2	4	Джерела інформації окреслені нормативно-правовими документами.
Т-3	–	Відсутня загальнодоступна інформація з цього приводу.
Т-4	4	Послужний список реагування на інциденти в кіберпросторі дає впевненість у наявності чіткої, постійно обновлюваної системи.
Т-5	–	Відсутня загальнодоступна інформація з цього приводу.
Т-6	–	Відсутня загальнодоступна інформація з цього приводу.
Т-7	–	Відсутня загальнодоступна інформація з цього приводу.
Т-8	3	Послужний список реагування на інциденти в кіберпросторі дає впевненість у наявності певного набору інструментів для запобігання інцидентам.
Т-9	3	Послужний список реагування на інциденти в кіберпросторі дає впевненість у наявності певного набору інструментів для виявлення інцидентів.
Т-10	3	Послужний список реагування на інциденти в кіберпросторі дає впевненість у наявності певного набору інструментів для вирішення інцидентів.
Р-1	4	Визначено нормативно-правовою базою діяльності організації.
Р-2	3	Наявна велика кількість прикладів взаємодії зі ЗМІ, що вказує на існування письмового процесу.
Р-3	4	Визначено нормативно-правовою базою діяльності організації.
Р-4	3	Наявні інструкції із запобігання деяким інцидентам.
Р-5	3	Реальні приклади дозволяють засвідчити наявність певного письмового процесу з виявлення інцидентів.
Р-6	4	Визначено нормативно-правовою базою діяльності організації.
Р-7	3	Доступні офіційні процеси реагування на інциденти.
Р-8	4	Наявний регулярний і прогресуючий процес зворотного зв’язку через контактні джерела й ЗМІ.
Р-9	3	Існує джерело для надання цілодобової консультації та підтримки.
Р-10	3	Аналіз соціальних мереж CERT-UA надає розуміння наявності певного формального процесу для формування процесу присутності в Інтернеті.
Р-11	4	Наявні оновлюванні бібліотеки процесів шифрування та підпису повідомлень.
Р-12	3	Аналіз прикладів реагування на інциденти показує існування таких процесів.
Р-13	2	Складно стверджувати про ефективність чи наявність процесу масового охоплення.
Р-14	--	Відсутня загальнодоступна інформація з цього приводу.
Р-15	3	Наявне часткове інформування громадян про інциденти та шляхи їх усунення.
Р-16	--	Відсутня загальнодоступна інформація з цього приводу.
Р-17	4	CERT-UA є акредитованим членом FIRST протягом останніх 14 років.

Отже, через деякі обмеження в доступі та наявності, частина параметрів, а саме: О-10, Н-2, Т-3-5-6-7, Р-14-16 не можуть бути оцінені належним чином. Слід зауважити, що загальний відсоток параметрів, що були оцінені на основі сайту організації, нормативно-правових документів, тощо, складає 82 %.

2.3. Узагальнення отриманих результатів

Наведена нижче кругова діаграма показує визначені рівні параметрів CERT-UA. Діаграма була створена на основі даних, отриманих у табл. 4.

Слід зазначити, що діаграма не містить параметрів, оцінка яких відсутня. Наступним кроком для узагальнення є визначення рівнів кожного із квадрантів за допомогою середнього арифметичного значення та медіани. Ця інформація систематизована у табл. 5.

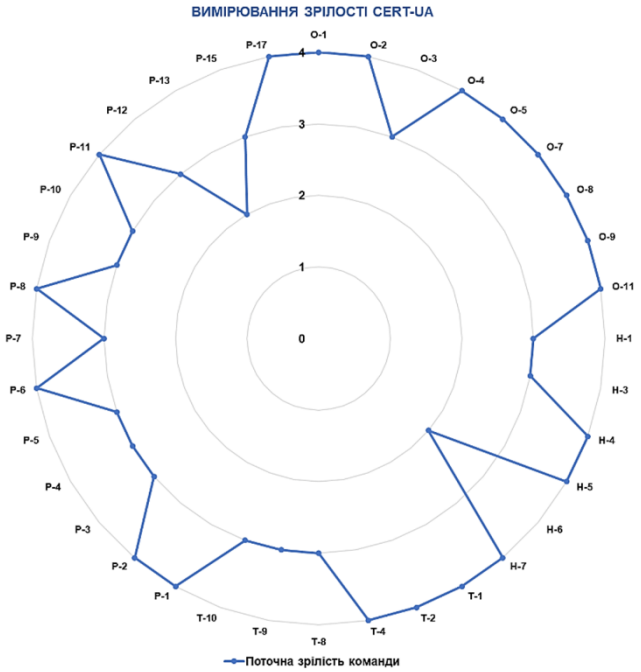

Рис. 1. Отримана діаграма рівнів параметрів CERT–UA

Таблиця 5

Рівні квадрантів параметрів CERT-UA

Квадрант параметрів	Середнє арифметичне	Медіана вибірки	Рівень-відповідник
Організаційний («О»)	3,9	4	«Просунутий»
Людський фактор («Н»)	3,3	3	«Просунутий»
Інструменти («Т»)	3,5	3	«Просунутий»
Процеси («Р»)	3,3	3	«Проміжний»

Отже, згідно з отриманими результатами оцінки й критеріями, висунутими у [1, 3 – 5], спостерігається «Просунутий» рівень 3 з 4 категорій CERT-UA. Квадрант, що відповідає за процеси, відповідає рівню «Проміжний» й потребує покращень процедур або їх часткового висвітлення для ознайомлення широкого загалу. Загалом, зрілість CERT-UA знаходиться на межі «Просунутого» рівня, однак потребує деяких покращень параметрів у категорії «Р».

Висновки

1. Модель зрілості CSIRT ENISA є цінним інструментом для покращення зрілості CSIRT. Це комплексна та гнучка модель, яка може бути використана CSIRT будь-якого розміру. Модель також підкріплена методологією оцінки, яка допомагає оцінити поточний рівень команди.

2. SIM3 є цінним інструментом для організацій, які прагнуть поліпшити свої можливості реагування на інциденти. Модель є комплексною, гнучкою та простою у використанні. Використовуючи SIM3, організації можуть визначити області для вдосконалення і зробити відповідні кроки для поліпшення своїх загальних можливостей реагування на інциденти.

3. Трирівневий підхід до етапів зрілості CSIRT в поєднанні з параметрами SIM3 є цінним інструментом для вимірювання зрілості команди реагування на інциденти комп'ютерної безпеки. Модель є структурованою, комплексною та простою у використанні.

4. Вага самооцінки та експертної оцінки у методології має бути різною, із наданням переваги експертній оцінці. Однак вагомість цих двох форм оцінювання може змінюватися залежно від конкретних обставин і мети оцінювання.

5. CERT-UA є цінним ресурсом в Україні, націленим на допомогу в реагуванні на інциденти та забезпеченні безпеки. Послуги організації доступні як державним, так і приватним організаціям, вона має широкий спектр можливостей, включаючи реагування на інциденти, консультування з питань безпеки, навчання та сповіщення про актуальні новини.

6. Через обмежений доступ до певної документації вдалося оцінити лише 82 % параметрів для CERT-UA. Параметри, які не вдалося оцінити, були такими: O-10, H-2, T-3, T-5, T-6, T-7, P-14, P-16.

7. Попри обмеженість оцінювання можна зробити деякі висновки щодо рівня зрілості CERT-UA. Організація має чітке розуміння своєї ролі та обов'язків, а також чітко визначений процес реагування на інциденти. Однак є деякі сфери, в яких CERT-UA може покращити свій рівень зрілості. Наприклад, організація могла б покращити свою документацію та зробити її більш доступною.

8. Систематизовані результати показують, що рівень зрілості CERT-UA знаходиться на рівні "Просунутий" у трьох з чотирьох квадрантів: «O», «H» та «T». Рівень зрілості у квадранті «P» знаходиться на "Проміжному" рівні. Це свідчить про те, що CERT-UA має міцну основу з точки зору організаційної структури, людських ресурсів та інструментів. Однак слід покращити свій рівень зрілості шляхом подальшого розвитку ефективності деяких процесів.

Список літератури:

1. ENISA CSIRT Maturity Framework – Updated and improved, ENISA, Feb. 23, 2022. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/publications/enisa–csirt–maturity–framework.
2. CERT–UA, cert.gov.ua. [Електронний ресурс]. Режим доступу: https://cert.gov.ua/.
3. SIM3 : Security Incident Management Maturity Model – Open CSIRT Foundation. Mar. 30, 2015. [Електронний ресурс]. Режим доступу: https://opencsirt.org/csirt–maturity/sim3–and–references/.
4. ENISA CSIRT maturity assessment model. ENISA, Apr. 30, 2019. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/publications/study–on–csirt–maturity.
5. ENISA Maturity Evaluation Methodology for CSIRTs. ENISA, Apr. 09, 2019. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/study–on–csirt–maturity–evaluation–process.
6. SIM3v2i self–assessment tool. ENISA. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/topics/incident–response/csirt–capabilities/csirt–maturity/sim3–v2i.
7. FIRST – Improving Security Together. FIRST – Forum of Incident Response and Security Teams. [Електронний ресурс]. Режим доступу: https://www.first.org/.

Надійшла до редколегії 25.05.2023

Відомості про авторів:

Пелюх Олександр Іванович – Харківський національний університет імені В. Н. Каразіна, студент факультету комп'ютерних наук; Україна; e-mail: oleksandrpelyukh@gmail.com; ORCID: https://orcid.org/0000-0003-0507-0262.

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «Інститут Інформаційних технологій»; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

Голубничий Дмитро Юрійович – канд. техн. наук, доцент, начальник наукового відділу АТ "Інститут Інформаційних Технологій"; Україна; e-mail: goldim1971@gmail.com; ORCID: https://orcid.org/0000-0002-6873-7004

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 213
In English and Ukrainian

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 213
Англійською та українською мовами

Коректор Л.І. Сащенко

Підп. до друку 30.06.2023. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 10,9. Обл.-вид. арк. 8,0. Тираж 300 прим. Зам. № 547. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”, тел. (057) 703-53-74.
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.