EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ЯК НАЛАШТУВАТИ РОБОТУ CSIRT (команда реагування на інциденти комп'ютерної безпеки) ТА SOC (центр операційної безпеки)

КЕРІВНИЦТВО З НАЛЕЖНОЇ ПРАКТИКИ

ГРУДЕНЬ 2020

ПРО ЄВРОПЕЙСЬКЕ АГЕНТСТВО З ПИТАНЬ МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ENISA)

Європейське Агентство з питань мережевої та інформаційної безпеки, ENISA, є агентством Європейського Союзу, метою діяльності якого є досягнення високого загального рівня кібербезпеки в Європі. Засноване в 2004 році та посилене Законом ЄС про кібербезпеку, Європейське Агентство з питань мережевої та інформаційної безпеки здійснює свій внесок у кіберполітику ЄС, підвищує надійність продуктів, послуг та процесів інформаційно-комунікаційних технологій (ІКТ) за допомогою схем сертифікації кібербезпеки, співпрацює з державами-членами та органами ЄС і допомагає Європі підготуватися для кібервикликів майбутнього. Шляхом обміну знаннями, розбудови спроможності та підвищення обізнаності Агентство працює разом зі своїми ключовими заінтересованими особами заради зміцнення довіри до пов'язаної економіки, підвищення стійкості інфраструктури Європейського Союзу та, врешті-решт, для забезпечення цифрового захисту європейського суспільства і громадян. Більше інформації про ENISA (Європейське Агентство з питань мережевої та інформаційної безпеки) та його роботу можна знайти за посиланням: www.enisa.europa.eu.

КОНТАКТНА ІНФОРМАЦІЯ

Із запитаннями стосовно цього дослідження звертайтеся, будь ласка, за посиланням: csirt-relations@enisa.europa.eu. Для запитів ЗМІ щодо цього документа, будь ласка, пишіть: press@enisa.europa.eu.

АВТОРИ

Едгарс Таурінс, ENISA.
Заходи, що підтримують це дослідження, проводилися за контрактом з NRD Cyber Security.

СЛОВА ВДЯЧНОСТІ

Дослідження було проведено за участю неофіційної експертної групи держав — членів ЄС з питань реагування на інциденти.

ПРАВОВЕ ПОПЕРЕДЖЕННЯ

Слід звернути увагу, що в цій публікації наведені погляди та інтерпретації ENISA, якщо не зазначено інше. Ця публікація не повинна трактуватись як правова дія ENISA або органів ENISA, якщо її не прийнято відповідно до Регламенту (ЄС) № 2019/881.
Ця публікація не обов'язково включає в себе найактуальнішу інформацію, і ENISA може час від часу оновлювати її.

Сторонні джерела цитуються належним чином. ENISA не несе відповідальності за зміст зовнішніх джерел, включно із зовнішніми вебсайтами, які згадуються в цій публікації.

Ця публікація призначена лише для інформаційних цілей. Вона повинна бути у безоплатному доступі. Ані ENISA, ані будь-яка особа, яка діє від її імені, не несе відповідальності за використання інформації, що міститься в цій публікації.

Повідомлення про авторські права

ISBN 978-92-9204-410-7 - DOI 10.2824/056764

ЗМІСТ

КОРОТКИЙ ОГЛЯД

У цій публікації надаються орієнтовні на результат рекомендації для тих, хто зацікавлений у створенні команди реагування на інциденти комп'ютерної безпеки (CSIRT) або центру операційної безпеки (SOC), а також рекомендації щодо можливого вдосконалення різних типів CSIRT та SOC, які наразі існують.

Зміст цього звіту базується на аналізі поточних публікацій щодо створення CSIRT (аналіз наведено в Додатку B); опитувальника на місцях (додаток A), який заповнили 40 команд CSIRT та SOC; досвіду автора у створенні та вдосконаленні діяльності CSIRT у рамках численних проєктів, які реалізуються в Європі, Азії, Африці та Південній Америці.

Публікація при наданні рекомендацій щодо різних етапів створення CSIRT або організації SOC використовує підхід, орієнтований на результат:

- Оцінка готовності
- Проєктування
- Впровадження
- Операції
- Вдосконалення.

Читач отримає практичний посібник щодо того, на чому слід зосередитися на окремих етапах створення та вдосконалення.

До липня 2020 року ENISA опублікувало на своєму вебсайті 61 доповідь та 21 перекладену версію доповідей, що підтримують CSIRT ([1]). Навчальний пакет ([2]) ENISA забезпечує навчальні онлайн-матеріали, навчальні курси та практичні матеріали для фахівців з кібербезпеки, засновані на концепції «Навчи тренера». Цей документ було розроблено з метою підсилення наявного обсягу знань ENISA щодо створення CSIRT.

[1] https://www.enisa.europa.eu/publications#c8=CSIRTs
[2] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/

1. ВСТУП

1.1 КОНТЕКСТ РОБОТИ

Загрози кібербезпеці зростають і стають більш складними. Одним з найефективніших способів протидії цим загрозам є створення глобальної екосистеми команд реагування на інциденти комп'ютерної безпеки (CSIRT) та центрів операційної безпеки (SOC), які можуть ефективно спілкуватися, обмінюватися інформацією та реагувати на кіберзагрози. Цьому можна сприяти шляхом забезпечення відповідних загальних механізмів, збільшуючи кількість CSIRT і SOC у всьому світі та вдосконалюючи діяльність існуючих CSIRT і SOC.

Більш зріла екосистема CSIRT та SOC забезпечує кращу взаємодію та колективні дії у відповідь на загрози кібербезпеки

В Європі ENISA допомагає державам-членам в їх спроможності реагування на інциденти, надаючи їм різні ресурси, такі як документи, інструменти, матеріали та настанови. Наприклад, ENISA розміщує перелік європейських CSIRT — інтерактивну мапу на вебсайті ENISA, в якій наведено загальні відомості про офіційно зареєстрованих CSIRT в Європі. Крім того, *дослідження з огляду на CSIRT і спроможності реагування на інциденти в Європі 2025 ([3])* враховує загальний статус спроможності CSIRT керування та реагування на інциденти, тоді як *звіт про стан реагування на інциденти у державах — членах ЄС ([4])* надає уявлення про Директиву NIS ([5]) (Директива (ЄС) 2016/1148 про безпеку мереж та інформаційних систем) щодо галузевої спроможності реагування на інциденти. ENISA також проводило роботу в сфері спроможності національних та урядових CSIRT та спроможності реагування на інциденти, включно з наданням навчальних матеріалів, що висвітлюють деякі аспекти розвитку CSIRT.

Для надання додаткових ресурсів було прийнято рішення про публікацію керівних принципів та створення інтерактивного інтернет-сховища інформації для використання в процесі створення різних типів CSIRT та SOC з огляду на роботу ENISA, особливо у сферах вдосконалення та навчання.

1.2 ЦІЛІ РОБОТИ

Ця публікація являє собою посібник, орієнтований на досягнення результатів, для тих, хто зацікавлений у створенні CSIRT або SOC або в структурованій модернізації CSIRT або SOC.

Публікація при наданні рекомендацій щодо різних етапів створення CSIRT або організації SOC використовує підхід, орієнтований на результат: оцінка готовності, проєктування, впровадження, функціонування та вдосконалення.

Очікується, що читач використовуватиме цю публікацію як практичний посібник на окремих етапах створення CSIRT. Читачі можуть виступати заінтересованими особами CSIRT, які будуть створені.

Цей звіт має на меті заохотити створення CSIRT та SOC та ознайомити з практичними техніками для забезпечення ефективності процесу створення та вдосконалення.

[3] https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025
[4] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

1.3 ОГЛЯД МЕТОДОЛОГІЇ

Наявні документи про створення CSIRT зосереджуються на заходах, які потрібно здійснити, без детального опису кінцевих результатів. Ця публікація має на меті побудувати постійний процес вдосконалення діяльності та пов'язаних з ним кінцевих результатів під час зростання та розвитку CSIRT. Її було розроблено таким чином, щоб забезпечити керівництво для всіх CSIRT незалежно від стадії, на якій вони перебувають, або їх теперішньої готовності.

Для досягнення цього результату використовуються такі методи збору даних, як аналіз поточних публікацій щодо створення CSIRT (аналіз узагальнений у Додатку B); опитувальник на місцях, спрямований на створення CSIRT та SOC (додаток A); та практичний досвід авторів та рецензентів у створенні та вдосконаленні CSIRT. За мету ставилося максимально наблизити цю публікацію до реального життя. З цієї причини були включені цитати від різних CSIRT, а також реалістична собівартість та терміни.

Концепція сервісів CSIRT FIRST.org, а також модель оцінки SIM3 згадуються як супутники процесу, оскільки вони приймаються до уваги при визначенні початкового каталогу послуг для нових CSIRT та для оцінки та зрілості CSIRT.

1.4 ВИЗНАЧЕННЯ CSIRT І SOC

Найпоширенішими термінами, що використовуються для опису команд, відповідальних за реагування на інциденти, є CSIRT, CERT ([6]) та SOC.

1.4.1 Команди реагування на інциденти комп’ютерної безпеки

Термін CSIRT, або команда реагування на інциденти комп’ютерної безпеки, був створений у 1990-х. CSIRTs також відомі як CIRTs (команди реагування на комп'ютерні інциденти), CERTs (команди реагування на комп'ютерні надзвичайні події), SIRT (команди реагування на інциденти безпеки). Національні команди також можна назвати національними центрами кібербезпеки (NCSC), яким, відповідно до закону, відводиться роль CSIRT, а також ними надаються додаткові послуги для країни (наприклад, обслуговування схем класифікації інформації в країні). Кожна команда обирає собі назву з огляду на те, чому організація віддає перевагу.

Назва CSIRT стала загальною назвою для команди, яка надає такі сервіси: управління інформацією та інцидентами в кібербезпеці (основна служба), моніторинг безпеки, управління вразливістю, ситуаційна обізнаність та управління знаннями у сфері кібербезпеки.

Якщо пояснити просто, то CSIRT7 — це команда, завданням якої є обробка інцидентів комп'ютерної безпеки (отже, мається на увазі кібербезпека). Часто це включає додаткові обов'язки, від виявлення до аналізу і навіть практичного виправлення, а також діяльність стосовно різно-ситуаційної обізнаності, передачі знань та управління вразливістю. Протягом років роль CSIRT еволюціонувала від надання послуг з моніторингу та обробки інцидентів до координації та спілкування з різними заінтересованими особами, країнами та конкретними секторами.

Наразі FIRST.org розміщує та постійно вдосконалює рамковий документ щодо послуг CSIRT (8), який є документом високого рівня, що описує діяльність, яку виконують CSIRT. Ця діяльність організована за п’ятьма основними сервісними сферами, які далі поділяються на сервіси, функції та підфункції. CSIRT може обирати, які сервіси та функції відповідають її повноваженням, та включити ці сервіси у її власну структуру сервісів. Незважаючи на те, що ця структура не визначає структуру SOC, сервіси з деяких зон відповідальності також можуть бути застосовані до SOC.

[6] CERT, або команда реагування на комп'ютерні надзвичайні події, є найстарішим терміном, який був зареєстрований як товарний знак Інституту програмної інженерії (SEI) при Університеті Карнегі — Меллона (CMU).
[7] Дивись визначення CSIRT, наприклад, у розділі “Базові можливості для національних/урядових CERT” https://www.enisa.europa.eu/publications/baseline-capabilities-or-national-governmental-certs
[8] https://www.first.org/standards/frameworks/csirts/csirt_services_framework

всіх команд. Рамковий документ щодо сервісів CSIRT підтримується ENISA, Міжнародним союзом електрозв'язку (МСЕ) та багатьма іншими організаціями.

Мінімальний набір сервісів для CSIRT зазвичай включає ті, що виділені напівжирним шрифтом нижче, відповідно до ПЕРШОГО рамкового документу щодо сервісів.

Рисунок 1. Перший рамковий документ щодо сервісів — типові сервіси CSIRT

1.4.2 Центри операційної безпеки

SOC, або центр операційної безпеки, надає сервіс виявлення інцидентів шляхом спостереження за технічними подіями в мережах та системах, а також може нести відповідальність за реагування на інциденти та їх обробку. На великих підприємствах SOC іноді зосереджуються лише на сервісах моніторингу та виявлення, а потім передають обробку інцидентів до окремої CSIRT. В організаціях менших за розміром CSIRT та SOC часто вважаються синонімами.

Здебільшого команди SOC працюють із кімнат SOC, де аналітики сидять біля своїх робочих станцій перед стіновою відеопанеллю, на якій проєктується зведення даних поточної ситуації (Рисунок 2). Команди SOC зазвичай виростають з команд безпеки інформаційних технологій (IT), що автоматизують свою роботу з використанням управління інформаціною безпекою та подіями безпеки (SIEM) та інших технологій автоматизації безпеки та системи автоматизованого адміністрування для моніторингу безпеки. Команди SOC переважно фокусують свої ключові показники ефективності (KPI) відповідно до показників якості — швидкості виявлення, діапазону виявлення, охоплення, хибно-позитивних показників, а також оброблених інцидентів, співвідношення попереджень/подій/інцидентів, кількості ескалацій та робочого навантаження на один інцидент.

SOC — це центри першої лінії, вони отримують усі сповіщення, тоді як IRT будуть отримувати лише попередження або братимуть участь у координації. Центр SOC перебуває в зоні відповідальності наших членів, оскільки ми є секторною CERT *(секторальною CSIRT)*

Рисунок 2. Міждержавний центр обміну та аналізу інформації (MS-ISAC) SOC
Джерело: MS-ISAC вебсайт (https://www.cisecurity.org/ms-isac/)

Крім персональної діяльності, SOC можуть звикористовувати віртуальний підхід та залучати субпідрядників, або застосовувати гібридну модель з залученням своїх спеціалістів та субпідрядників. Поширеною практикою є те, що з часом SOC обирають між виконанням операцій врнутрішніми силами або силами залучених субпідрядників.

Оскільки організації CSIRT та SOC дотримуються одного рамкового документа щодо послуг, то як CSIRT, так і SOC у цьому звіті зазначені як CSIRT.

Мінімальний набір сервісів для SOC зазвичай включає ті, що виділені напівжирним шрифтом нижче, відповідно до концепції сервісів FIRST.

Рисунок 3. Перший рамковий документ щодо сервісів – типові сервіси SOC

1.5 ПОПЕРЕДНЯ РОБОТА ENISA ЩОДО CSIRT

До липня 2020 року ENISA опублікувало на своєму вебсайті 61 доповідь та 21 перекладену версію доповідей щодо CSIRT ([9]).

Основоположним документом стосовно створення *CSIRT* є *Посібник із створення CSITRT* ([10]), опублікований в 2006 році. Він був перекладений більш ніж на 20 мов, включаючи китайську та хінді. Ця публікація на 86 сторінок висвітлює покроковий процес створення CSIRT і є чинною на сьогодні.

«ENISA пропонує відмінні публікації, які добре організовані, легкі для читання та сприйняття»
(Unicom CSIRT)

Керівництво ENISA з *належної практики щодо управління інцидентами* ([11]), опубліковане 2010 року, містить вказівки щодо створення структур та спроможності стосовно управління інцидентами; його можна використовувати як довідник напрямків встановлення, включно з процесами обробки інцидентів та робочими процесами.

Навчальний пакет ENISA ([12]) включає навчальні матеріали онлайн, навчальні курси та практичні матеріали для фахівців з кібербезпеки, засновані на концепції «Навчи тренера».

ENISA також опублікувало збірник для національних та урядових CSIRT щодо, наприклад, базових можливостей ([13]) та профілів зрілості ([14]), а також інструменту самооцінки.

«Більшість публікацій та рекомандацій ENISA стосуються нашої ефективної роботи. Характер загроз ENISA використовується для встановлення основних даних відносно щорічних загроз
(BGD e-GOV CIRT)

За останні кілька років ENISA опублікувало керівництво щодо партнерства CSIRT та правоохоронних органів ([15]), включно з аналізом моделей партнерства, технічним співробітництвом, електронним аналізом доказів ([16]) та навчальними модулями. Крім того, додаткову інформацію про те, як вибрати модель співпраці CSIRT, та про порядок технічного впровадження моделей співпраці, можна знайти на вебсайті ENISA.

Цей звіт має на меті покращити наявний обсяг знань ENISA щодо створення CSIRT. Зміст цього звіту базується на аналізі попередніх публікацій про створення CSIRT (аналіз узагальнений в Додатку B); опитувальника на місцях (додаток A), який склали 40 команд CSIRT та центрів SOC; та досвіді авторів у створенні та вдосконаленні діяльності CSIRT у рамках численних проєктів, що здійснюються в Європі, Азії, Африці та Південній Америці.

[9] https://www.enisa.europa.eu/publications#c8=CSIRTs
[10] https://www.enisa.europa.eu/publications/csirt-setting-up-guide
[11] https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[12] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/
[13] https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities
[14] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity
[15] https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation
[16] https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders

2. РЕКОМЕНДАЦІЇ ЩОДО СТВОРЕННЯ CSIRT

2.1 ОРГАНІЗАЦІЯ НАСТАНОВ

Настанови щодо створення CSIRT сформульовані відповідно до різних фаз процесу створення CSIRT ([17]):

- Оцінка готовності
- Проєктування
- Впровадження
- Операції
- Вдосконалення.

Рисунок 4. Життєвий цикл CSIRT

Створення нового CSIRT розпочинається з фази "оцінки готовності", яка починається з обговорення причин та необхідності створення CSIRT і закінчується затвердженням початкового бюджету та формуванням вимог на етапі проєктування.

На етапі "проєктування" розробляються детальні плани етапу впровадження.

Етап "впровадження" включає такі організаційні питання: управління, персонал, процеси, сервіси та технології.

Під час фази "операції" CSIRT надає сервіси CSIRT.

Наявні CSIRT можуть слідувати керівним принципам на етапі "вдосконалення", а не на етапі "оцінки готовності".

На етапі "вдосконалення" команда CSIRT формує запити на вдосконалення, визначає пріоритети ініціатив та отримує затверджений бюджет для виконання циклу "проєктування — впровадження — діяльність — вдосконалення".

[17] У цьому звіті "створення" відповідає шляху CSIRT від концептуальної ідеї до сильної та зрілої CSIRT через кілька років або до просування наявної CSIRT на подальші етапи розвитку.

Ці настанови сформульовані на підставі результатів кожної фази.

1. Оцінка готовності

- Попередній мандат
- Структура управління
- Ідентифікація організації, в структурі якої створена CSIRT
- Дорожня карта високого рівня та бюджет
- Детальні вимоги до етапу проєктування

2. Проєктування

- Затверджений детальний мандат
- План сервісів CSIRT
- Процеси CSIRT та план робочих процесів
- План організації, навичок та навчальної структури CSIRT
- План об`єктів CSIRT
- План автоматизації технологій та процесів CSIRT
- План співпраці CSIRT
- План управління IT та інформаційною безпекою CSIRT
- Детальні вимоги до етапу впровадження

3. Впровадження

- Затверджена та впроваджена організаційна структура
- Найнятий та призначений персонал
- Виконаний план навчання щодо виконання посадових обов'язків персоналу
- Підготовлені об'єкти
- Розроблено та впроваджено детальні процеси та процедури
- Впроваджена технологія автоматизації процесів
- Впроваджено процедури управління IT та інформаційною безпекою
- Проведено навчання персоналу для ведення операційної діяльності CSIRT
- Підписані відповідні угоди із клієнтами, заінтересованими особами та партнерами
- Тестовий запуск сервісів CSIRT та налаштування результатів
- Запуск комунікації CSIRT і відзначення

4. Операція

- Вимірювані KPI
- Щорічний огляд ефективності операцій
- Щорічний огляд потреб заінтересованих осіб
- Погоджений річний бюджет
- Зібрані вимоги до вдосконалення

5. Вдосконалення

- Список обраних ініціатив для вдосконалення
- Детальні вимоги до вдосконалення на етапі проєктування
- Попередній бюджет на вдосконалення

Рисунок 5. Підсумок результатів створення CSIRT

Оцінка готовності
- Попередній мандат
- Структура управління
- Організація, в структурі якої створена CSIRT
- Бюджет на 1–3 роки
- Детальні вимоги до етапу проєктування

Проєктування
- Затверджений детальний мандат
- План сервісів CSIRT
- Процеси CSIRT та план робочих процесів
- Організація CSIRT
- Структурний план навичок та навчання
- План об`єктів CSIRT
- План автоматизації технологій та процесів CSIRT
- План співпраці CSIRT
- IT та інформаційна безпека CSIRT
- План управління
- Детальні вимоги до етапу впровадження

Впровадження
- Затверджена та впроваджена організаційна структура
- Найнятий та призначений персонал
- Виконаний план навчання щодо виконання посадових обов'язків персоналу
- Підготовлені об'єкти
- Розроблено та впроваджено детальні процеси та процедури
- Впроваджена технологія автоматизації процесів
- Впроваджено процедури управління IT та інформаційною безпекою
- Проведено навчання персоналу для ведення операційної діяльності CSIRT
- Підписані відповідні угоди із клієнтами, заінтересованими особами та партнерами
- Результати тестового запуску сервісів та налаштування CSIRT
- Запуск комунікації CSIRT і відзначення

Операція
- Вимірювані KPI
- Щорічний огляд ефективності операцій
- Щорічний огляд потреб заінтересованих осіб
- Затверджено щорічний бюджет
- Зібрані вимоги до вдосконалення

Вдосконалення
- Список обраних ініціатив для вдосконалення
- Детальні вимоги до вдосконалення на етапі проєктування
- Попередній бюджет на вдосконалення

Рисунок 6. Зразок етапів створення команди CSIRT та необхідні зусилля

На рисунку 6 показано графік створення CSIRT, очікувані необхідні внутрішні та зовнішні ресурси та інтенсивність роботи, необхідної для виконання різними спеціалістами, на кожному етапі.

Відсотки на схемі 6 представляють навантаження та час, необхідний для виконання різними спеціалістами. Наприклад, "1 х менеджер проєкту 50 %" означає, що потрібен один менеджер проєкту і що для виконання необхідних завдань потрібно витратити до 50 % їх максимального навантаження/часу.

2.2 ОЦІНКА ГОТОВНОСТІ

На етапі оцінки готовності очікуються такі результати.

- Попередній мандат
- Структура управління
- Ідентифікація організації, в структурі якої створена CSIRT
- Дорожня карта високого рівня та бюджет
- Детальні вимоги до етапу проєктування

Рисунок 7. Фази втілення

2.2.1 Попередній мандат

Діяльність CSIRT починається з мети — початкової ідеї та причин, чому CSIRT потрібна. Створення CSIRT має бути виправданим.

Перед прийняттям рішення про створення CSIRT слід ретельно врахувати очікування заінтересованих осіб та клієнтів. На практиці це означає врахування таких аспектів.

1. Визначення всіх основних заінтересованих осіб та розуміння їх потреб та очікувань від CSIRT. Залежно від заінтересованої особи, їх потреби можуть включати виявлення інцидентів, безпекову обізнаність, вирішення інцидентів та дотримання певних стандартів.
2. Визначення клієнтів. Це може бути невелика група компаній для галузевої CSIRT, мешканці міста чи навіть населення цілої країни. Оцінка та задоволення потреб та очікувань конкретного клієнта надзвичайно важливі для успіху CSIRT.

Слід запланувати низку семінарів-практикумів з основними заінтересованими особами та представниками клієнтів, щоб отримати їхню підтримку для створення CSIRT та розпочати розмову про реальну цінність, яку могла б принести CSIRT. Потім це може бути використано як матеріали для обґрунтування створення CSIRT, а також для визначення її мандату та бюджетування.

Загальні обґрунтування створення CSIRT наступні:

1. Необхідність організації професійного вирішення інцидентів в галузі кібербезпеки для мінімізації впливу інцидентів.
2. Необхідність мати професійну команду, яка б реагувала на інциденти кібербезпеки за допомогою міжнародно визнаних методів обробки інцидентів.
3. Необхідність довіри від інших CSIRT у всьому світі під час розслідування інцидентів.
4. Необхідність мати координаційну команду з питань обробки інцидентів у сфері кібербезпеки, обробки вразливостей, підвищення рівня ситуаційної та безпекової обізнаності та аналізу загроз.

Мета команди визначається в мандаті CSIRT, який повинен містити повноваження та обов'язки, що надаються команді.

Зазвичай мандат включає:

1. повноваження, надане CSIRT для здійснення сервісів та діяльності для клієнтів;
2. обов'язки CSIRT;
3. вимоги, цілі та завдання.

Для CSIRT, яка має лише внутрішню клієнтуру в організації або структуру постачальника послуг з управління інформаційною безпекою (MSSP), мандата зазвичай виражається в одному з таких документів:

1. наказ по офісу (в державному відомстві);
2. рішення або резолюція ради чи органу виконавчого управління (на приватному підприємстві).

Для галузевих або національних CSIRT мандат зазвичай виражається щонайменше у двох документах, а саме:

1. стратегія кібербезпеки, закон, підзаконний акт або урядовий наказ про надання повноважень та загальної відповідальності (єдиний спосіб встановити повноваження через різні організації країни);
2. наказ по офісу організації, в структурі якої створюється CSIRT, який окреслює детальні вимоги, цілі та завдання, а також перелік сервісів.

Також слід дотримуватися додаткових вказівок щодо мандата.

1. Повинні бути зазначені обов'язки CSIRT . Простої заяви про те, що створюється CSIRT, недостатньо; мандат також повинен визначати, які обов'язки встановлюються і навіщо це потрібно.
2. Обов'язки повинні зазначати, для якої клієнтів буде працювати CSIRT: наприклад, CSIRT для фінансового сектору для управління кіберзагрозами, обміну інформацією про загрози та координації критичних інцидентів або CSIRT для внутрішніх бізнес-підрозділів для моніторингу кібербезпеки та обробки інцидентів.
3. Повноваження CSIRT надає уповноважений орган. Для галузевих або національних CSIRT це може бути національний уряд, парламент або міністерство.
4. Організація або бізнес-підрозділ повинні бути призначені для створення CSIRT. Іноді це може бути нова організація.

Для національних урядів або галузевих регуляторних органів розробка мандату зазвичай починається з підготовки проєкту закону, програми, стратегії кібербезпеки або плану кібербезпеки.

Для CSIRT організації розробка мандату здебільшого починається після отримання дозволу на створення CSIRT від правління або керівників рівня C, із зазначенням мети її створення.

Затверджений мандат повноважень та обов'язків зазвичай вказує на особу, підрозділ чи організацію, яка керуватиме створенням CSIRT.

Приклади фраз, які зазвичай використовуються в мандатних документах, включають таке.

1. Питання кібербезпеки дуже важливі; таким чином, CSIRT створюється для підвищення стійкості інформаційних систем до кібератак; управління кіберзагрозами; роботи над зниженням витрат від наслідків інцидентів шляхом встановлення суворого контролю за управлінням інцидентами; вдосконалення ноу-хау; сприяння співпраці між заінтересованими особами; та забезпечення обізнаності щодо кіберситуацій та їх помітності.
2. Галузева (національна, в організації) CSIRT створюється шляхом модернізації поточного підрозділу IT-безпеки для забезпечення ефективної кіберстійкості, організації реагування на інциденти, забезпечення кіберситуаційної обізнаності, та створення каналів обміну кіберінформацією з партнерськими організаціями.

Для держав — членів ЄС Додатки I та II Директиви NIS містять вимоги, завдання та обов’язкову клієнтуру національних CSIRT; відповідальність CSIRT на високому рівні описується таким чином: «Відповідає за ризик та обробку інцидентів відповідно до чітко визначеного процесу».

Приклади мандатів для створення CSIRT включають:

- btCIRT ([18]) — національний CIRT Бутану, заснований за розпорядженням уряду;
- BGD e-GOV CIRT ([19]) — Бангладеш, урядова, галузева CSIRT, заснована офісним наказом.

Додаткові вказівки щодо мандатів та відповідальності можна знайти в Посібнику з *належної практики* ENISA *з управління інцидентами* (2010), розділ 5.4.

2.2.2 Структура управління

Структура управління визначає відповідальність заінтересованих осіб CSIRT. Він може бути представлений як плановий документ або навіть як частина мандата.

Документ про структуру управління повинен містити відповіді на низку питань.

1. Хто надаватиме фінансування для створення та діяльності CSIRT і на яких підставах?
2. Хто забезпечить керівництво, моніторинг та нагляд за діяльністю CSIRT?
3. Які типи угод має укладати CSIRT та з якими заінтересованими особами (наприклад, правоохоронними органами, спецслужбами, міжнародними організаціями, технологічними партнерами, науковими колами)?
4. Кому, як часто та в якій формі буде звітувати CSIRT?

Власником структури управління CSIRT здебільшого є організація, в структурі якої створена CSIRT.

Структура управління зазвичай уточнюється під час семінарів, які проводяться для обговорення мандата з різними заінтересованими особами.

2.2.3 Ідентифікація організації, в структурі якої створена CSIRT

Організація, в структурі якої створюється CSIRT, зазвичай зазначається в попередньому мандаті. Можливо, організація, в структурі якої створюється CSIRT, вже існує або, можливо, її потрібно створити.

Якщо засновується нова організація, в структурі якої створюється CSIRT, бюджет CSIRT може бути затверджений лише після того, як організація почне функціонувати з точки зору управління та юридичних процесів, а це означає, що на цьому етапі буде потрібен додатковий час.

Вибираючи організацію, в структурі якої створюється CSIRT, потрібно враховувати повноваження організації щодо надання сервісів відповідно до мандата CSIRT.

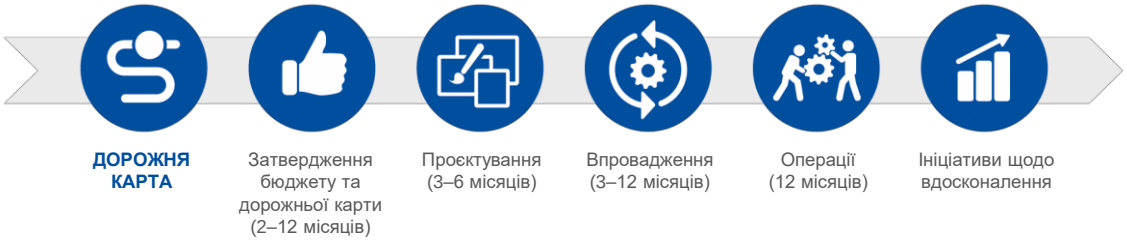
2.2.4 Дорожня карта високого рівня та бюджет

Після визначення мандата необхідно затвердити дорожню карту високого рівня та бюджет.

Дорожня карта повинна включати очікуваний поетапний графік створення CSIRT — проєктування, впровадження та діяльність — та подальших ініціативи щодо вдосконалення.

[18] https://www.btcirt.bt/wp-content/uploads/2016/01/BtCIRT-Mandatep2.pdf
[19] https://www.cirt.gov.bd/wp-content/uploads/2016/08/Government-Mandate-of-BGD-e-GOV-CIRT.pdf

Рисунок 8. Приклад дорожньої карти



Зазвичай необхідно 2–3 роки від розробки попереднього мандата до затвердження початкового мандата, коли CSIRT стає повністю функціональною. Це включає декілька кроків.

1. Затвердження бюджету, встановлення об'єктів, створення організації та початкове наймання на роботу може зайняти до 1 року.
2. Проєктування та впровадження зазвичай займає 1–2 роки, особливо якщо допомога зовнішніх консультантів та технології отримуються шляхом проведення державних тендерів.

Бюджет на початковий рік, який витрачається на створення CSIRT та початкові сервіси, повинен покривати щонайменше:

1. початкову заробітну плату персоналу — принаймні для мінімально необхідної кількості персоналу (менеджер CSIRT, керівник проєкту створення CSIRT, адміністративний асистент);
2. вартість встановлення об'єкту;
3. заробітну плату або винагороду за консультаційні послуги щодо створення результатів етапу проєктування (юридичні процеси, навички, пов'язані з CSIRT, впровадження технологій);
4. отримання навичок CSIRT та тренування.
5. попередню технологію та ліцензування.

"Ми працюємо 24/7"
(національна CSIRT)

Бюджет повинен бути скоригований відповідно до дорожньої карти, мандата, зобов'язань заінтересованої особи та вимог щодо того, як швидкого повинна бути створена CSIRT.

Бюджет слід повторно скорегувати як тільки завершиться фаза проєктування, а також коли підготовлені детальні плани для етапів впровадження та експлуатації. Наприклад, якщо бюджету недостатньо, деякі аспекти можна перенести на наступну фазу вдосконалення в дорожній карті.

Далі у примітках наведено орієнтовні витрати на 2020 рік. Оцінка витрат проводиться лише як ілюстрація і не відображає жодної конкретної країни.

1. У країнах ЄС працівник команди CSIRT (включно з менеджерами) коштує у середньому 40 000–60 000 євро на рік.
2. Вартість утримання невеликих операційних команд CSIRT із трьома співробітниками (керівник, двоє осіб, що працюють безпосередньо з інцидентами) повинна щорічно складати близько 120 000–180 000 євро.
3. Якщо необхідно, щоб CSIRT здійснювала операції 24/7 протягом 365 днів на рік, то потрібно щонайменше 12 додаткових співробітників (шість команд із двох співробітників для забезпечення цілодобової роботи, без вихідних, з тривалістю кожної зміни у 8 годин). Це щороку додаватиме до бюджету 480 000 євро.
4. Зазвичай у CSIRT така кількість працівників: у малій — 3–7, у середній — 10–15, у великій — 30–60, залежно від кількості клієнтів та мандата.
5. Зазвичай вартість оренди офісів становить близько 3000–4000 євро на одного працівника на рік.

6. Зазвичай витрачається 3 000–10 000 євро на рік на професійну підготовку одного працівника. Наполегливо рекомендується відвідувати конференції (одна подія на людину на рік).
7. Залежно від сфери застосування, консультаційні послуги щодо створення CSIRT (проєктування та впровадження) можуть коштувати від 75 000 до 1 000 000 євро протягом 1–3-річного періоду.
8. Зазвичай витрачається 100 000–300 000 євро на технології: обладнання (принаймні два сервери з віртуалізацією, рішення для резервного копіювання, брандмауери, комп'ютери, принтери), мережеве та спеціалізоване обладнання для виконання специфічних операцій CSIRT (комп'ютерна криміналістика, зворотна інженерія, оцінка вразливості тощо). Використання хмарних сервісів може бути ефективним способом обмежити початкові інвестиції в обладнання, дозволяючи витрачати лише на те, що фактично використовується.
9. Що стосується компонентів програмного забезпечення, то CSIRT можуть почати переважно з програм з відкритим кодом[20], використовуючи комерційні інструменти, лише якщо не існує порівнювальних альтернатив або для їх кращої ефективності. У цьому випадку бюджет на програмне забезпечення та програмні послуги повинен починатися з 50 000 євро. Якщо CSIRT зосереджуються на комерційних технологіях, бюджет слід збільшити; однак, зосередження уваги на комерційних технологіях може призвести до вищої продуктивності, тобто необхідна буде менша кількість співробітників.

Початкові суми в бюджеті та період часу, протягом якого бюджет буде витрачений, можуть змінюватися з часом. Діяльність на етапі проєктування буде обумовлена затвердженим наявним бюджетом.

Затверджений бюджет вплине на остаточний детальний мандат, оскільки організація може досягти очікуваних результатів лише за умови доступності достатнього бюджету. Невідповідність між детальним мандатом та бюджетом є типовою причиною того, чому CSIRT не виконують свій мандат.

Для того, щоб CSIRT запрацювала, може знадобитися 3 роки, тому бюджет повинен відображати очікувану інтенсивність процесу створення CSIRT.

2.2.5 Детальні вимоги до етапу проєктування

Діяльність на етапі проєктування базуватиметься на вимогах та обмеженнях стосовно CSIRT, таких як:

1. погоджений мандат;
2. дорожня карта та бюджет;
3. люди, навички та ресурси, визначені для етапу проєктування.

Вони повинні бути перевірені та затверджені.

Коли залучається зовнішня консультаційна робота, деталізовані вимоги часто виражаються як технічне завдання стосовно консультаційного проєкту (ТЗ) для конкурсного тендеру (запит на отримання інформації (RFI) / запит на отримання пропозиції (RFP)).

Під час підготовки ТЗ на таку роботу доцільно включити:

1. визначення мандату CSIRT;
2. чітке формулювання очікуваних результатів;
3. очікуваний план продуктивності;
4. досвід, який вимагається від консультантів для проведення подібної діяльності

Ми купуємо деякі конкретні послуги у постачальників від імені цілої галузі, наприклад TI для конкретних географічних регіонів / суб'єктів; ізольованих програмних середовищ, видалення доменів тощо *(секторальні CSIRT).*

[20] При використанні рішень з відкритим кодом CSIRT повиннна враховувати, хто керує та оновлює певне рішення.

2.3 ПРОЄКТУВАННЯ

Передумовами фази проєктування є всі результати фази оцінки готовності.

Рекомендації на етапі проєктування узгоджуються з SIM3 (модель рівня зрілості управління інцидентами в системі безпеки, яка оцінює, наскільки добре команда керує, документує, виконує та вимірює свою функціональність), охоплюючи всі чотири сфери — організацію, особовий склад, інструменти та процеси — послідовно, як представлено нижче. Цей посібник не містить конкретних порад щодо того, як досягти рівнів зрілості, оскільки цю інформацію можна знайти в інструментах оцінки SIM3 від ENISA ([21]) або Відкритому фонді CSIRT ([22]).

На етапі проєктування очікуються наступні результати у вигляді або окремо затверджених документів або одного затвердженого документа.

1. Затверджений детальний мандат
2. План сервісів CSIRT
3. Процеси CSIRT та план робочих процесів
4. План організації, навичок та навчальної структури CSIRT
5. План об`єктів CSIRT
6. План автоматизації технологій та процесів CSIRT
7. План співпраці CSIRT
8. План управління IT та інформаційною безпекою CSIRT
9. Детальні вимоги до етапу впровадження

Крім того, отримана структура дизайну часто публікується у форматі RFC 2350 ([23]) — це фактичний формат офіційної презентації CSIRT, що охоплює назву команди, контактну інформацію, часовий пояс, PGP (алгоритм шифрування "надійна приватність") ключі, мандат (статут), правила та сервіси тощо. Для CSIRT є належною практикою опублікування документу RFC 2350 на власному вебсайті.

2.3.1 Затверджений детальний мандат

Етап проєктування базується на вимогах мандата CSIRT, який все ще може перебувати на етапі заключного обговорення, або може включати деякі широкі комплексні заяви. На цій фазі повинно бути забезпечено надання остаточного схвалення (наприклад, мандат був підписаний міністром, або радою директорів або виконавчим органом), та що мандат чіткий та легкий для сприйняття і визначає:

1. повноваження, якими наділена CSIRT для обслуговування та діяльності для клієнтів;
2. обов'язки CSIRT;
3. вимоги, цілі та завдання.

Успішно підготувати проєкт можливо в разі затвердження мандата разом із бюджетними обмеженнями та початковою дорожньою картою для створення CSIRT.

Детальний мандат може визначати, як назвати CSIRT, у спосіб, описаний нижче.

1. Назва організації повинна відображати мандат з чітким формулюванням та зазначенням функції CSIRT.
2. Тип клієнтів, що охоплюється, часто відображається в назві; наприклад, національні CSIRT часто називаються за допомогою двобуквеного коду країни та CSIRT/CIRT/CERT.

[21] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey
[22] https://sim3-check.opencsirt.org/
[23] https://tools.ietf.org/html/rfc2350

скорочення з рискою, крапкою, або будь-яким іншим символом, наприклад: CERT-LV, CERT-MU, SK-CERT. Сектор часто додається також у скороченому вигляді; наприклад, фінансовим сектором буде FinCIRT або FS-CSIRT, додатково з назвою країни за допомогою двобуквеного коду країни, наприклад EG (EG-FinCIRT).

3. Часто ім'я обирають на основі короткого імені компанії чи організації та додають CSIRT, наприклад Adidas CSIRT, CSIRT BNP Paribas.
4. CSIRT часто називають CIRT, CERT або SIRT. Такі організації повинні надавати сервіси з обробки (реагування) на інциденти.
5. Назва SOC зазвичай використовується для організацій, які контролюють операції для безпеки мереж та центрів обробки даних, наприклад NestleSOC, TDC SOC. Останнім часом такі назви, як iSOC ([24]) та gSOC ([25]), також використовуються.
6. Коли основною функцією команди реагування на інциденти є усунення вразливості продуктів певної компанії, її зазвичай називають PSIRT ([26]), наприклад Adobe PSIRT, NVIDIA PSIRT, Fujitsu PSIRT. Окремий посібник щодо PSIRT був створений на сайті FIRST.org ([27]).
7. Приклади наявних назв команд доступні на FIRST.org ([28]), Trusted Introducer ([29]) та мапі ENISA CSIRTs[30].
8. Якщо обрана назва містить абревіатуру CERT, запит на затвердження повинен бути поданий власнику торгової марки CERT SEI ([31]) (політика SEI може бути змінена в майбутньому).

2.3.2 План сервісів CSIRT

План сервісів CSIRT пояснює, які послуги організація CSIRT надаватиме клієнтам для виконання обов'язків та задач, визначених в мандаті, та дотримання дорожньої карти та бюджетних обмежень.

Рисунок 9. Концепція сервісів FIRST

[24] iSOC — це інтегрований SOC, наприклад, в енергетичному секторі, що поєднує SOC операційної технології (OT) та IT SOC.
[25] Центр gSOC — це глобальний або урядовий SOC.
[26] PSIRT — це команда реагування на інциденти безпеки продукту.
[27] https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1
[28] https://www.first.org/members/teams/
[29] https://www.trusted-introducer.org/directory/teams.html
[30] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map
[31] https://www.sei.cmu.edu/education-outreach/license-sei-materials/authorization-to-use-cert-mark/

Наступні рекомендації надаються для підготовки плану сервісів CSIRT.

1. CSIRT має враховувати останню версію Концепції сервісів CSIRT FIRST.org ([32]). Цей документ тепер доступний кількома мовами. У цьому документі представлена концептуальна карта сервісів CSIRT, яка наведена нижче.
2. Виберіть, які сервісні сфери (із п'яти) та які саме сервіси повинна надавати CSIRT для виконання конкретних положень мандата.
3. Виберіть та відрегулюйте назви сервісних сфер, оскільки назви, зазначені у Концепції сервісів CSIRT, можуть бути дуже деталізованою на початку. Наприклад, коли йдеться про сервісну сферу управління подіями інформаційної безпеки для SOC, може бути вирішено об'єднати обидва сервіси (моніторинг і виявлення та аналіз подій) в один та перейменувати таку сервісну сферу в моніторинг безпеки. Подібним чином до сервісної сфери управління інцидентами інформаційної безпеки можна залучити два сервіси: сервіс обробки інцидентів та сервіс аналізу артефактів.
4. Перевірте перелік створюваних сервісів, щоб переконатися, що всі вимоги мандата виконані та не зазначено більше сервісів, ніж вимагає мандат. Ресурси CSIRT обмежені; отже, доцільно зосередитися на тому, що є обов'язковим для забезпечення надання якісних сервісів, на які надаються відповідні повноваження.

Список обраних сервісів CSIRT повинен бути зазначений у переліку каталога сервісів CSIRT. ITIL (бібліотека інфраструктури інформаційних технологій) може бути корисною для організації надання сервісів. Важливо чітко розуміти різницю між різними значеннями слова "інцидент": у CSIRT "обробка інцидентів" — це назва сервісу, тоді як у методології ITIL "інцидент" означає порушення в наданні сервісу, тобто те, що сервіс не може бути наданий, при цьому "інцидент" закривається в разі відновлення сервісу.

Про заходи: "реагування на інциденти, мережа датчиків контролю, розсилка повідомлень, побудова клієнтської бази, підвищення обізнаності та освіта, тренінги та кібернавчання" (національний CSIRT)

Реалістично, CSIRT повинні забезпечувати надання сервісів належної якості, і якщо ці сервіси порушуються, вони мають бути швидко відновлені. Наприклад, якщо виходить з ладу IT-система CSIRT, її можна відновити за допомогою внутрішнього процесу IT-підтримки відповідно до принципів ITIL [33].

2.3.3 Процеси та план робочих процесів CSIRT

Процеси CSIRT необхідні для впровадження та підтримки узгоджених сервісів CSIRT.

Зазвичай, надання кожного виду сервісів впроваджується за допомогою принаймні одного процесу. Для надання сервісу може знадобитися більше одного процесу, якщо, наприклад, надання сервісу вимагає залучення декількох робочих груп або повинні бути досягнуті конкретні проміжні цілі.

Деякі процеси можуть бути встановлені як допоміжні, наприклад, процес IT-підтримки для управління та оновлення IT-інфраструктури CSIRT. Цей процес можна здійснити, використовуючи методологію ITIL, окремий каталог IT-сервісів (не плутати з каталогом сервісів CSIRT).

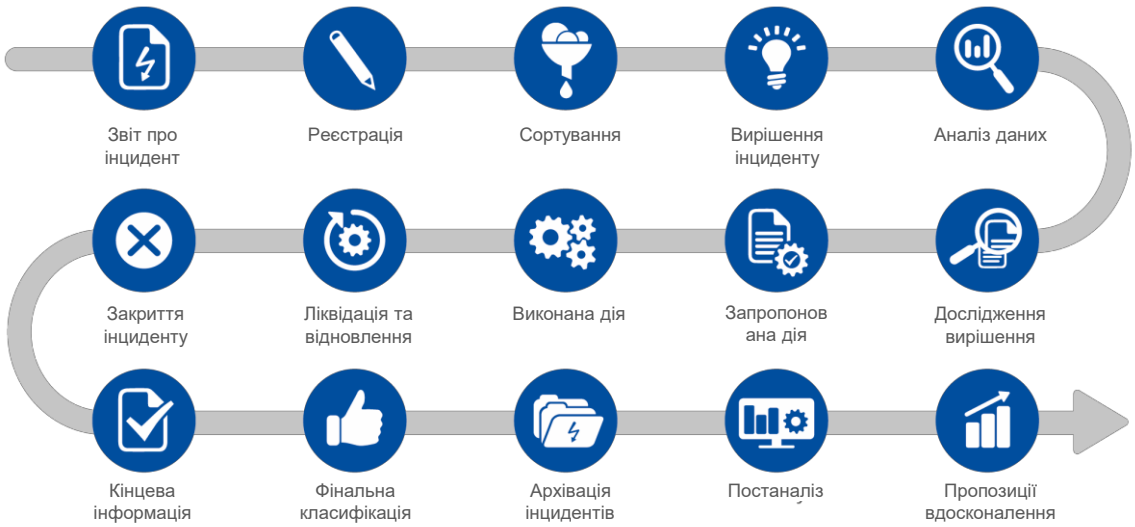
Співвідношення між ідентифікованими процесами слід аналізувати та документувати. Наприклад, результатом процесу моніторингу безпеки є виявлений інцидент, який передається в процес обробки інцидентів як вхід; у разі потреби процес аналізу артефактів може бути розпочатий з процесу обробки інцидентів.

[32] https://www.first.org/standards/frameworks/
[33] https://www.axelos.com/best-practice-solutions/itil

Кожен процес складається з одного або декількох робочих процесів, представлених діаграмами робочих процесів, що зображують кожен крок від початку до кінцевої фази діяльності. Крім того, загальноприйнятим є надання опису кожного кроку в таблиці.

Приклад діаграми робочого процесу обробки інцидентів безпеки, взятий з Посібника з *належної практики* ENISA щодо *управління інцидентами* (2010), наведено нижче.

Рисунок 10. Зразок робочого процесу обробки інцидентів

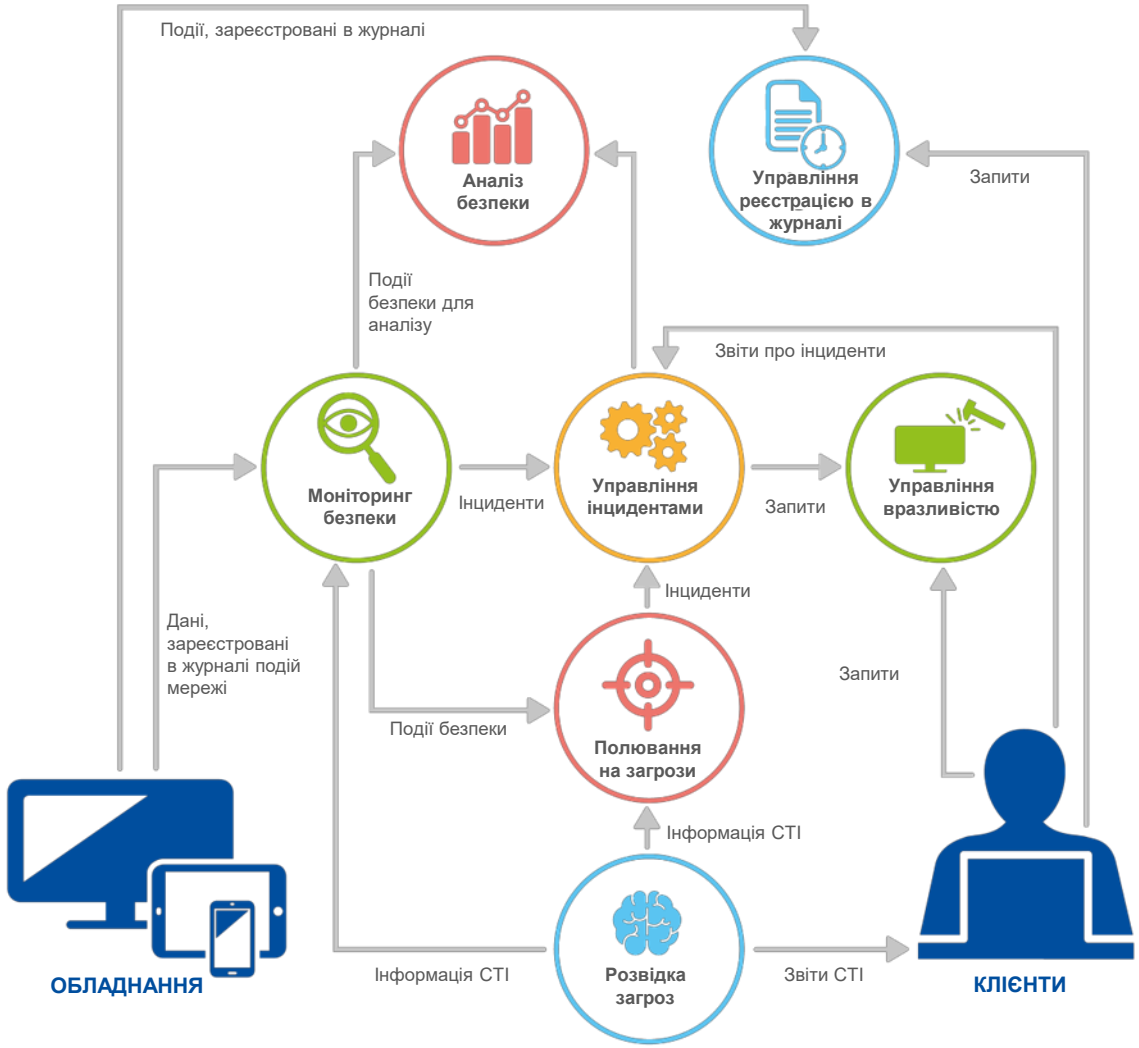


Приклад діаграми взаємовідносин для різних сервісів і процесів представлений на рисунку 11.

При проєктуванні процесів та робочих процесів, людських параметрів SIM3, модель оцінки зрілості CSIRT за ENISA ([34]) та модель можливостей та зрілості SOC (SOC-CMM) ([35]) можуть бути відповідними інструментами для перевірки їх повноти та покриття.

[34] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity
[35] https://www.soc-cmm.com/

Рисунок 11. Діаграма взаємовідносин між сервісами та процесами для внутрішньої CSIRT



Приклади обробки інцидентів безпеки та процесів моніторингу безпеки, які використовуються для впровадження сервісів управління інцидентами безпеки та моніторингу безпеки, наведені у таблицях 1 та 2 відповідно. Визначення процесів, адаптованих до потреб CSIRT.

Таблиця 1. Приклади процесів опбробки інцидентів безпеки

Назва процесу	Управління інцидентами безпеки
Опис	Управління інцидентами безпеки охоплює реєстрацію звітів про інциденти, сортування, вирішення інцидентів та закриття інцидентів
Власник процесу	Менеджер з питань інцидентів безпеки
Мета	Забезпечити обробку кожного виявленого інциденту відповідно до визначених вимог до якості та проведення заходів реагування з метою пом'якшення будь-яких інцидентів з подальшими діями щодо вдосконалення заходів безпеки; і підвищення рівня зрілості процесів безпеки клієнта, щоб він був більш стійким до кіберзагроз у майбутньому
Вхід сервісу / тригери	1. Події, виявлені функціонуванням сервісу моніторингу безпеки 2. Звіти про інциденти зареєстровані:

Назва процесу	Управління інцидентами безпеки
	1. Телефон 2. Електронна адреса 3. Онлайн-форма 4. Інтерфейс дошки сервісного самообслуговування
Вихід сервісу / похідні	1. Допомога клієнтам щодо пом'якшення інцидентів безпеки 2. Надання рекомендацій щодо поліпшення безпеки інфраструктури клієнтів
Діяльність сервісів	1. Сортування інцидентів безпеки 2. Аналіз інцидентів безпеки 3. Керівництво що стримування інциденту безпеки 4. Керівництво щодо ліквідації та відновлення після інциденту 5. Закриття інциденту 6. Висновки

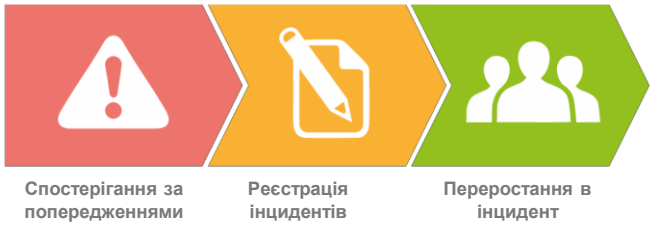
Потім процес зазвичай відображається як діаграма робочого процесу.

Рисунок 12. Діаграма простого робочого процесу щодо процесу управління інцидентами безпеки

Таблиця 2. Приклади процесів моніторингу інцидентів безпеки

Назва процесу	Моніторинг безпеки
Опис	Дані про події з інфраструктури моніторингу безпеки обробляються та аналізуються для виявлення інцидентів
Власник процесу	Менеджер моніторингу безпеки
Мета	Своєчасно виявляти зловмисні та підозрілі дії
Вхід сервісу / тригери	1. Події, виявлені інфраструктурою моніторингу безпеки 2. Повідомлення від платформи розвідки загроз
Вихід сервісу / похідні	1. Забезпечувати сповіщення клієнтів про інциденти безпеки 2. Зареєструвати інциденти в процесі управління інцидентами безпеки 3. Дані про здійснення процесу полювання на загрози
Діяльність сервісів	1. Спостерігати за повідомленнями 2. Реєструвати інциденти 3. Передати дані про інциденти до команди з обробки інцидентів

Рисунок 13. Діаграма простого робочого процесу щодо процесу моніторингу безпеки



Приклади рекомендацій щодо поводження в разі обробки інциденту наведені в таблиці 3.

Таблиця 3. Приклади рекомендацій щодо поводження у разі обробки інциденту

Секція	Опис
Керівництво щодо стримування	**Мета:** консультування клієнтів, координація їхніх зусиль та участь у розслідуванні критичних інцидентів 1. Консультувати клієнтів щодо залучення до розслідування правоохоронних органів 2. Що стосується інцидентів з високим рівнем критичності, розгляньте можливість направити CSIRT для проведення розслідування на місці або запросіть дозволу на спільне використання журналу реєстрації та проведіть розслідування у приміщеннях CSIRT. Надайте виявлену інформацію клієнту. 3. Порадьте клієнту: 1. Проаналізувати журнал реєстрації 2. З'ясувати причину інциденту 3. Оцінити шкоду 4. Заблокувати зловмисні адреси IP та DNS 5. Впровадити швидкі обхідні варіанти 4. Оцініть ризик для іншої інфраструктури та поділіться анонімними деталями інциденту із клієнтом 5. Перевірте нещодавні подібні інциденти, оцініть ситуацію та, в разі потреби, підвищіть рівень критичності. Повідомте керівництво про підозрілі повторні вторгнення
Рекомендації щодо пом'якшення негативних наслідків	**Мета**: допомогти клієнту знайти та усунути причину інциденту зі збереженням будь-яких доказів криміналістики 1. Порадьте клієнту: 1. Застосувати патчі 2. Замінити застарілі системи та системи без підтримки 3. Впровадити постійні обхідні варіанти 4. Впровадити найкращі практики безпеки 2. Для високо критичних інцидентів запитайте детальні звіти про розслідування або запропонуйте ресурси для забезпечення належного аналізу інцидентів
Рекомендації щодо відновлення	**Мета:** підтримка клієнтів у відновленні нормальної роботи після інциденту та скасування тимчасових запобіжних заходів 1. У випадку високо критичного інциденту проведіть оцінку безпеки, щоб оцінити ефективність заходів з усунення негативних наслідків 2. Організуйте семінари для персоналу системи безпеки та поясніть загальні методи вторгнення та стратегії усунення негативних наслідків 3. Раз на рік проводьте технічне навчання з кібербезпеки або тренінги у просторі реального життя

2.3.4 План організації, навичок та навчальної структури CSIRT

Процесами CSIRT керують її співробітники, які організовані в певні організаційні структури.

Рисунок 14. Приклад організаційно-штатної структури малої CSIRT

Менші CSIRT з кількістю до п'яти-семи людей переважно організовані як один підрозділ, яким керує менеджер підрозділу (рис. 15). У цьому випадку обов'язки персоналу можуть бути сформульовані на підставі концепції NIST NICE стосовно розподілу робочих обов'язків команди реагування на інциденти кіберзахисту (PR-CIR-001) ([36]).

Навчання песоналу: "ТРАНЗИТИ I та II для всіх, а також внутрішні політики/процедури для використання інструментів та спілкування з рештою команди" *(ISP CSIRT)*

Рисунок 15. Приклад організаційного підрозділу більшої CSIRT

Для більших організацій CSIRT, які налічують понад 10 осіб, структурні підрозділи повинні бути розроблені відповідно до структури сервісів або виконуваної діяльності чи інших організаційних практик (рис. 16). Знов-таки, обов'язки за NIST NICE[37] можуть слугувати відправною точкою для розподілу обов'язків персоналу.

[36] https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Cyber+Defense+Incident+Responder
[37] Національний інститут стандартів і Національної ініціативи технологій з освіти в галузі кібербезпеки https://www.nist.gov/itl/applied-cybersecurity/nice

Слід зазначити, що цілодобова змінна робота може бути дуже дорогою, оскільки необхідно шість команд, щоб забезпечити 8-годинні зміни, включно зі святковими днями. Таким чином, CSIRT часто використовують одну з таких операційних процедур:

1. Працюють лише у звичайний робочий час.
2. Призначають чергового для контролю дзвінків чи ескалації надзвичайних ситуацій.
3. Передають моніторинг реєстрації вночі та у вихідні дні стороннім спеціалістам для початкового сортування.
4. Покладаються на оперативні центри мережі, що працюють цілодобово та без вихідних, та обробляють вхідні дзвінки відповідно до типових базових стандартних операційних процедур (SOP) та телефонують експертам у разі потреби, якщо працює черговий телефон.

ENISA розробило близько 50 навчальних курсів на теми, пов'язані з роботою CSIRT, ці курси є в безкоштовному доступі на її вебсайті ([38]). Ці навчальні матеріали охоплюють технічні та експлуатаційні аспекти, налаштування роботи CSIRT, правові аспекти та аспекти співпраці, а також рекомендації щодо, наприклад, активного навчання для CSIRT та навчальних методологій. Усі навчальні матеріали ліцензовані відповідно до Creative Commons BY-NC-SA 4.0, тобто вони відкриті для використання будь-ким, хто належить до ENISA. Однак навчальні матеріали є некомерційними та, таким чином, найбільш корисними для внутрішнього навчання співробітників CSIRT старшого щабля.

ENISA розробило близько 50 безкоштовних навчальних курсів для CSIRT, які доступні на 'Тренінгах ENISA для фахівців з кібербезпеки', див.:

ENISA — навчальні матеріали онлайн

Подібним чином FIRST.org пропонує зростаючу кількість навчальних курсів на своїх навчальних веб-сторінках ([39]) на тих самих ліцензійних умовах. Також GEANT проводить тренінги для CSIRT TRANSITS I та TRANSITS II[40]

Запропоновані курси технічного навчання та лабораторії для осіб, що займаються обробкою інцидентів, наведені в таблицях 4 і 5.

Таблиця 4. Тренінгові курси для CSIRT, які займаються обробкою інцидентів

Обов'язки/ навички	Навчальний курс	Провайдер
Черговий офіцер, який займається обробкою інцидентів		
Основи нетворкінгу	Internet History, Technology, and Security (https://www.coursera.org/learn/internet-history)	Курс університету Мічіган
Networks, ICT концепції, кібербезпека основи	Основи CSX та додаткова практика (https://www.isaca.org/credentialing/cybersecurity/csx-fundamentals-certificate)	ISACA
	Безпека + (https://certification.comptia.org/certifications/security)	Comp TIA
	Сертифікований спеціаліст із системної безпеки (SSCP) (https://www.isc2.org/Certifications/SSCP)	(ISC)²
	Information Security Foundation (https://www.seco-institute.org/certifications/information-security-certification-track/information-security-foundation-online-course/) IT Security Foundation (https://www.seco-institute.org/certifications/it-security-certification-track/it-security-foundation-online-course/)	SECO інститут

[38] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
[39] https://www.first.org/education/trainings
[40] https://www.geant.org/Services/Trust_identity_and_security/Pages/TRANSITS_Training.aspx

Обов'язки/ навички	Навчальний курс	Провайдер
	Спеціаліст з IT-безпеки (https: //www.seco-institute.org/certifications/it-security-certification-track/it-security-Practitioner-Online-course /)	
	SEC301: Вступ до кібер безпеки (http://www.sans.org/course/intro-information-security)	SANS
Основи обробки інцидентів	TRANSITS I (https://tf-csirt.org/transits/transits-events/transits-i/)	GEANT
	Основи управління інцидентами (https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P139)	Інститут програмного забезпечення
Основи нетворкінгу	Cisco Certified Networking Associate (CCNA) (https://learningnetwork.cisco.com/s/ccna)	Cisco
Технічна практика кібербезпеки	ISACA CSX Спеціаліст з кібербезпеки (CSX-P) (https://nexus.isaca.org/products/145)	ISACA
Старший спеціаліст з обробки інцидентів		
Обробкая інцидентів	Сертифікований спеціаліст з обробки інцидентів (ECIH) (https://www.eccouncil.org/Certification/ec-council-certified-incident-handler; http://iclass.eccouncil.org/?p=728)	Рада ЄС
	SOC Аналітик (https://www.seco-institute.org/certifications/it-security-certification-track/soc-analyst-online-course/)	SECO інститут
	TRANSITS II (https://tf-csirt.org/transits/transits-events/transits-ii/)	GEANT
	SEC504: Хакерські знаряддя, Техніки, Експлуатація та Обробка інцидентів (https://www.sans.org/course/hacker-techniques- exploits-incident-handling)	SANS
Тестування на проникнення	Сертифікований етичний хакер (CEH) (https://www.eccouncil.org/Certification/certified-ethical-hacker; http://iclass.eccouncil.org/?p=719)	Рада ЄС
	SEC560: Тестування на проникнення в мережу та етичний злом (http://www.sans.org/course/network-penetration-testing- ethical-hacking)	SANS
	Основи етичного злому(https://www.seco-institute.org/certifications/ethical-hacking-certification-track/ethical-hacking-foundation-online-course/)	SECO інститут
	Спеціаліст з питань етичного злому(https://www.seco-institute.org/certifications/ethical-hacking-certification-track/ethical-hacking-practitioner-online-course/)	
Архітектура безпеки	Сертифікований спеціаліст із захисту інформаційних систем (https://www.isc2.org/cissp/default.aspx)	(ISC)²
Менеджер з обробки інцидентів		
Удосконалена обробка інцидентів	FOR508: удосконалена відповідь на інциденти, полювання на загрози та комп'ютерна криміналістика (https://www.sans.org/course/advanced-incident-response-digital-forensics)	SANS
Удосконалене реагування на інциденти	FOR572: удосконалена мережева криміналістика: полювання на загрози, аналіз та реагування на інциденти (https://www.sans.org/course/advanced-network-forensics- analysis)	SANS

Обов'язки/ навички	Навчальний курс	Провайдер
	FOR578: Розвідка кіберзагроз (https://www.sans.org/course/cyber-threat-intelligence)	SANS
	Сертифікований аналітик з розвідки загроз (https://www.eccouncil.org/programs/certified-threat-intelligence-analyst-ctia/)	Рада ЄС
	Діамантова модель аналізу вторгнень (https://school.threatintel.academy/collections)	Академія розвідки загроз

Таблиця 5. Запропоновані навчальні лабораторії для спеціалістів CSIRTs обробки інцидентів

Титул	Опис	Цільова група
iLabs CEH	iLabs CEH забезпечує віртуальні машини, попередньо налаштовані на вразливості, використання, інструменти та тестові драйвери. Це сервіс, заснований на хмарній підписці від Ради ЄС, призначений для надання практичної допомоги професіоналам з інформаційної безпеки. Портал iLabs CEH дозволяє учаснику курсу запустити цілий ряд цільових машин і отримати до них віддалений доступ. Цей продукт надає 6-місячний доступ до віртуального лабораторного середовища Ради ЄС для сертифікованих етичних хакерів. Див. https://store.eccouncil.org/product/ilabs-ceh та https://www.youtube.com/watch?v=iU_7zKypJZI для додаткової інформації	Старший аналітик
iLabs CTIA	Див. https://store.eccouncil.org/product/ilabs-ctia/ для додаткової інформації	Старший аналітик
ISACA CSX лабораторії	Лабораторні лекції ISACA на різні технічні теми. Див. https://nexus.isaca.org/products для додаткової інформації	Аналітик
Вразлива вебпрограма (DVWA)	DVWA — це PHP/MySQL вразлива вебпрограма. Її,її основні цілі полягають у тому, щоб допомогти професіоналам безпеки перевірити свої навички та інструменти в юридичному середовищі, допомогти розробникам вебсайтів краще зрозуміти процеси захисту вебдодатків та допомогти викладачам/студентам викладати/вивчати питання безпеки вебдодатків у класі. Див. http://www.dvwa.co.uk/ для додаткової інформації	Аналітик
Теорія розслідування	Див. https://www.networkdefense.io/library/the-analyst-mindset/110302/about/ для додаткової інформації	Аналітик
ELK для аналізу безпеки	Див. https://www.networkdefense.co/courses/elk/ для додаткової інформації	Аналітик

Запропонованого тренінгу для розвитку технічних навичок недостатньо, щоб забезпечити успішне функціонування CSIRT. Крім того, кожна CSIRT повинна розвивати всебічні професійні, лідерські та оперативні навички на етапі впровадження, використовуючи такі засоби.

1. Передача знань експертами з впровадження у формі семінарів, тренінгів, наставництва та підтримки після впровадження.
2. Відвідайте інші CSIRT, для того щоб дізнатися про їх діяльність. Принаймні два чи три візити до CSIRT потрібно запланувати в інших країнах. Візити зазвичай тривають кілька годин і спрямовані на обмін досвідом роботи. Деякі CSIRT проводять обмін персоналом для здобування знань.

Усі співробітники CSIRT повинні розвивати професійні навички, як описано в концепції NIST NICE (де KSA означає знання, вміння та навички) (таблиця 6).

При прийманні на роботу: "Зазвичай ми просимо про CISSP" (Certified Information Systems Security Professional — сертифікований спеціаліст із захисту інформаційних систем *(CSIRT)*

Таблиця 6. Важливі професійні навички співробітників CSIRT

Навички	Опис
Управління конфліктами	KSA (знання, навички, уміння), які стосуються управління та вирішення конфліктів, скарг, конфронтацій або розбіжностей у конструктивному руслі, щоб мінімізувати негативні персональні впливи; співпрацює з іншими для заохочення співпраці та роботи в команді
Критичне мислення	KSA, які стосуються об'єктивного аналізу фактів для формування судження
Навички міжособистісного спілкування	KSA, які стосуються розвитку та підтримання ефективних стосунків з іншими, а також гарних стосунків з людьми різного походження та різних ситуацій; врахування та відповідне реагування на потреби, почуття та можливості підлеглих, співробітників однакового рівня та людей похилого віку
Усна комунікація	KSA, які стосуються процесу надання інформації чи висловлювання ідей з вуст в уста
Ефективна презентація	KSA, які стосуються діяльності, в якій хтось щось показує, описує або пояснює аудиторії
Письмова комунікація	KSA, які стосуються процесу надання інформації чи висловлювання ідей з вуст в уста

Керівний та адміністративний персонал CSIRT повинен розвивати свої лідерські та оперативні навички, наприклад, як зазначено в концепції NICE NICE (таблиці 7 та 8).

Таблиця 7. Важливі навички лідерства для керівного та адміністративного персоналу CSIRT

Навички	Опис
Менеджмент проєкту	KSA, які стосуються принципів, методів чи інструментів для розробки, планування, координації та управління проєктами та ресурсами, включно з моніторингом та перевіркою витрат, роботи та результатів роботи підрядника
Стратегічне планування	KSA, які стосуються формулювання ефективних стратегій, що відповідають цілі, баченню та конкурентній стратегії організації та/або бізнес-підрозділу
Навчання інших	KSA, які стосуються передачі знань або надання інформації або викладання (предмета чи навички)
Управління персоналом	KSA, які стосуються діяльності, необхідної для підтримки продуктивності персоналу

Таблиця 8. Важливі оперативні навички керівного та адміністративного персоналу CSIRT

Навички	Опис
Безперервність бізнесу	KSA, які стосуються планування та підготовки, що здійснюється компанією для забезпечення подолання серйозних інцидентів або катастроф та відновлення своєї нормальної роботи протягом досить короткого періоду часу
Управління відносинами з клієнтами	KSA, які стосуються концепцій, практик та методів, що використовуються для ідентифікації, залучення, впливу на, та відслідковування стосунків з людьми та групами, пов'язаними з роботою, включно з тими, хто бере активну участь, впливає на процес та його результати та має зацікавленість у результаті (позитивному чи негативному)
Договірна робота / закупівля	KSA, які стосуються різних типів контрактів, методів укладання контрактів або здійснення закупівель, а також ведення переговорів та адміністрування контрактів

Навички	Опис
Конфіденційність та захист даних	KSA, які стосуються взаємозв'язку між збиранням, зберіганням та розповсюдженням даних з одночасним захистом конфіденційності приватних осіб
Зовнішня обізнаність	KSA, які стосуються виявлення та розуміння того, як внутрішні та зовнішні проблеми (наприклад, економічні, політичні та соціальні тенденції) впливають на роботу організації
Юридичні, урядові та правові	KSA, які стосуються законів, нормативних актів, положень та етики, які можуть впливати на організаційну діяльність
Організаційна обізнаність	KSA, які стосуються розуміння місії та функцій організації, її соціальної та політичної структури, а також того, як програми, внутрішні положення, процедури, правила та норми керують та впливають на роботу та цілі організації
Управління внутрішніми правилами	KSA, які стосуються процесу створення, передачі та підтримки правил та процедур в організації
Контроль за опрацюванням	KSA, які стосуються активної зміни процесу на основі результатів моніторингу процесу
Управління ризиками	KSA, які стосуються методів та інструментів, що використовуються для оцінки ризику та зменшення ризику
Сторонній нагляд / управління збором даних	KSA, які стосуються процесу аналізу та контролю ризиків, представлених вашій компанії, даних, операцій та фінансів третіми сторонами, не вашою власною компанією

Усі ці навички можна набути шляхом участі в академічних або онлайн-курсах, що надаються на місцях, або в інтегрованих програмах. Наприклад, Coursera.org пропонує понад 1000 курсів з лідерства.

2.3.5 План об`єктів CSIRT

Безпечні об'єкти з окремими робочими площами та чіткі фізичні правила і норми мають суттєве значення для ефективного функціонування CSIRT.

Як мінімум об'єкти CSIRT повинні включати кімнату даних для розміщення будь-якої технології, офісну кімнату для персоналу, що займається обробкою інцидентів, та гостьову кімнату або кімнату для переговорів.

Для забезпечення безперервності бізнесу слід забезпечити безперервність інфраструктури CSIRT. Із цією метою повинні бути доступними резервні системи та резервний робочий простір.

Під час планування об'єктів необхідно враховувати таке.

1. Потрібно звернути увагу на фізичну безпеку та встановити належний контроль та моніторинг доступу. Крім того, оцінку ризику слід проводити на основі сусідніх об'єктів.
2. Кімната даних повинна забезпечувати рівень фізичної та екологічної безпеки, який відповідає даним, якими CSIRT буде володіти та керувати.
3. Офісна кімната для персоналу, що займається обробкою інцидентів, повинна забезпечити відповідне, зручне та безпечне робоче середовище з доступом персоналу до "мінімально необхідних привілеїв".

Команди CSIRT повинні застосовувати відповідні заходи фізичної безпеки, такі як забезпечення контролю по периметру приміщень та забезпечення контролю доступу для входу в різні кімнати з міркувань конфіденційності.

Додатковими джерелами інформації про вимоги фізичної безпеки є стандарт ISO 27001[41] Міжнародної організації із стандартизації, Галузевий посібник FM 3-19.30[42] та національні нормативні акти. Організації повинні звертатися до своїх команд внутрішньої безпеки або фізичної безпеки для отримання подальших порад щодо впровадження заходів безпеки.

Більші за розміром CSIRT можуть мати окремі зони для комп'ютерної криміналістики та лабораторії реагування на інциденти (DFIR), моніторингу безпеки (кімната SOC), кризову кімнату та кімнату для відвідувачів.

Рисунок 16. Приклад планування внутрішніх кімнат для CSIRT

Щодо інструментів: „MISP для обміну інформацією про загрози. Гнучкість для аналізу даних, matrix.org як внутрішня комунікаційна платформа. Gitlab для управління внутрішніми проєктами. BBB для відеоконференцій. Комерційні канали та інструменти для конкретних завдань, якщо не існує життєздатної альтернативи з відкритим кодом".
(національна CSIRT)

2.3.6 План автоматизації технологій та процесів CSIRT

Успіх CSIRT передусім залежить від автоматизації її процесів. Загальні процеси автоматизації IT використовуються для робочих місць та роботи в офісі. Існують також специфічні процеси CSIRT, які стосуються автоматизації.

Типова CSIRT повинна дотримуватися таких практик щодо своєї технічної інфраструктури.

1. Як рішення локального центру обробки даних, CSIRT повинна мати принаймні два сервери віртуалізації для забезпечення високої доступності та відновлення. У разі виходу одного з ладу резервне копіювання виконується на третьому сервері за допомогою стрічок або альтернативного рішення, розташованого в іншій кімнаті.
2. Сегментація мережі повинна гарантувати, що виробничі системи, LAN (локальна мережа), гостьова мережа, лабораторія та DMZ (демілітаризована зона) відповідно розділяються за допомогою правил брандмауера.
3. Як показують опитування, CSIRT та SOC часто обережно ставляться до широкого використання хмарних систем. Хмарні сервіси є обов'язковими, принаймні, для сервісів SaaS (програмне забезпечення як сервіс), наприклад, канали даних від зовнішніх постачальників наборів даних або вебсайтів, що використовуються для взаємодії. Використання хмарних сервісів часто призводить до доступності, цінності та операційної ефективності з меншим управлінням даними. Залежно від потреб у безпеці даних CSIRT та схильності до ризику можуть використовуватися різні хмарні сервіси.

[41] https://www.iso.org/isoiec-27001-information-security.html
[42] https://www.wbdg.org/FFC/ARMYCOE/FIELDMAN/fm31930.pdf

Часто потреби в автоматизації стосуються таких сфер:

1. системи позначок для реєстрації та звітів про обробку інцидентів — зазвичай, CSIRT використовують RTIR, OTRS, ServiceNow та Jira серед інших технологій позначок;
2. обробки та маршрутизації стрічок даних — використовуються маршрутизатори каналів, платформи розвідки загроз або сховища наборів даних;
3. видавничих платформ для попередження та інформування — це портали вебсайтів, платформи видавництва та канали соціальних мереж.

"Автоматизація робить аналіз великих подій простішим та ефективнішим. Автоматизація допомагає виконувати щоденні завдання, дозволяючи співробітникам зосередитися на аналізі шкідливих програм, аналізі даних криміналістики та додатковому навчанні".
(CSIRT-CY)

2.3.7 План взаємодії CSIRT

Успіх CSIRT багато в чому залежить від налагодження ефективних робочих партнерських відносин з різними заінтересованими особами та міжнародною спільнотою CSIRT.

Після створення CSIRT може бути невідомою всім заінтересованим особам та клієнтам; отже, вона повинна активно підходити до заінтересованих осіб та клієнтів та будувати механізми співпраці. Деякі з цих ініціатив співпраці призведуть до підписання офіційних меморандумів про взаєморозуміння (МпВ) чи угод про партнерство або до офіційного та неформального членства в асоціаціях і спільнотах, що обмінюються інформацією.

Довірчі та довготривалі партнерські стосунки вимагають планування, включно з чіткими цілями кожного партнерства та стратегії, як підтримувати відносини.

Викладені нижче рекомендації потребують виконання.

1. Активний підхід до побудови партнерських стосунків з місцевими та міжнародними правоохоронними та розвідувальними органами може допомогти ефективніше боротися з інцидентами кіберзлочинності або передовими стійкими загрозами (APT) у кризових ситуаціях.
2. Слід розглянути регіональні та національні (якщо такі є) ініціативи CSIRT щодо вдосконалення співпраці. Статус (43) (44), який входить до списку довірених представників, відносно легко досягти для CSIRT, яка вже працює, має підтримку інших CSIRT та бере участь у заходах та конференціях, пов'язаних зі CSIRT. Згодом CSIRT повинні зосередитися на досягненні акредитованого статусу (45) або навіть сертифікованого статусу (46). Схема Trusted Introducer є єдиною схемою сертифікації, доступною наразі для CSIRT, а послуги довіреного представника більше орієнтовані на CSIRT, що працюють в Європі.
3. Настійно рекомендується CSIRT приєднатися до асоціації FIRST.org, оскільки це головна глобальна асоціація для CSIRT.
4. Активний підхід до різних ISAC (47) для партнерства та вивчення цінності таких партнерств часто є належним способом визначити, які партнерські стосунки будуть цінними.
5. Структуру МпВ та угоди про партнерство зазвичай можна розділити на три частини:
   a. цілі партнерства — можуть відображати мандати обох сторін;
   b. що саме кожна зі сторін буде робити стосовно одна одної, наприклад запрошувати одна одну для проведення навчальних сесій, обміну знаннями, участі у семінарах та навчаннях, обміну показниками, реагування на запити про співпрацю щодо інцидентів;
   c. початковий план дій та графік, які будуть виконані після підписання МпВ, або угода, яка включає спільну оцінку угоди та планування діяльності на наступний рік.

"Anyrun для ізольованого програмного середовища, записане майбутнє для потоку загроз"
(MSSP SOC)

[43] https://tf-csirt.org/membership/why-listed/
[44] https://www.trusted-introducer.org/processes/registration.html
[45] https://www.trusted-introducer.org/processes/accreditation.html
[46] https://www.trusted-introducer.org/processes/certification.html
[47] Стосовно обміну інформацією та Аналітичного центру див. https://www.enisa.europa.eu/topics/national-cyber-security- strategies/information-sharing

6. Задля забезпечення співпраці та пов'язаних з цим заходів, наприклад, організація, поїздки, проведення хостингів, семінарів та неформальних спілкувань, має виділятися спеціальний бюджет як частина річного бюджету.

2.3.8 План управління IT та інформаційною безпекою CSIRT

Команда CSIRT повинна впровадити план управління IT та інформаційною безпекою або прийняти та адаптувати основи IT-безпеки від організації, в якій створена CSIRT.

Рекомендується, щоб CSIRT дотримувалися галузевих належних практик, наприклад системи управління інформаційною безпекою (ISMS) на основі ISO 27001.

План управління IT може відповідати принципам і методам COBIT ([48]) (цілі контролю за інформацією та суміжними технологіями) та принципам і методам ITIL.

2.3.9 Детальні вимоги до етапу впровадження

Результати проєктних планів повинні бути включені до вимог до впровадження з детальним поясненням:

1. які вимоги є та як їх слід виконувати;
2. яких точних результатів слід досягти.

Детальні вимоги можуть бути включені як Tor (браузер, створений для забезпечення анонімності в мережі Інтернет.).

2.4 ВПРОВАДЖЕННЯ

Фаза впровадження зосереджена на розподілі всіх сервісів, забезпеченні процесів, підготовці детальних процедур та навчанні співробітників.

Наприкінці етапу впровадження CSIRT готова надати сервіси своїм клієнтам та розпочати фазу операцій.

На етапі впровадження очікуються такі результати.

1. Затвердження та впровадження організаційної структури.
2. Наймання та призначення персоналу.
3. Виконання плану навчання для персоналу за різними посадами.
4. Підготовка об'єктів.
5. Розробка і впровадження детальних процесів та процедур.
6. Впровадження технології автоматизації процесів.
7. Впровадження процедур управління IT та інформаційною безпекою.
8. Навчання персоналу для ведення операційної діяльності CSIRT.
9. Підписання відповідних угод з клієнтами, заінтересованими особами та партнерами.
10. Тестовий запуск сервісів CSIRT та налаштування результатів.
11. Запуск комунікацій CSIRT та відзначення.

2.4.1 Затвердження та впровадження організаційної структури

Для того щоб CSIRT стала операційною, має бути затверджена розроблена організаційна структура та визначені різні посади.

[48] https://www.isaca.org/resources/cobit

Іноді цей процес може зайняти місяці; таким чином, організація може розпочати роботу з використання проміжної структури, щоб забезпечити прогрес роботи незалежно від процесу створення CSIRT.

Наприклад, наймання персоналу може розпочатися з використання наявної структури, з чітким планом переміщення ресурсів пізніше, або шляхом коригування початкового плану сервісів, якщо доступна менша кількість персоналу.

2.4.2 Наймання та призначення персоналу

Нова структура повинна бути укомплектована компетентним та кваліфікованим персоналом. Імовірно, що лише декілька посад будуть заміщені поточним персоналом; таким чином, потрібно найняти додаткових співробітників.

Зазвичай, є великий інтерес у тих, хто хоче працювати в новоствореній CSIRT та здобути професійний досвід; однак, потенційним претендентам часто бракує необхідних компетенцій.

Що стосується інших посад, то важливо наймати персонал, який виявляє рішучість і готовність надавати сервіси професійно.

"SEI (Інститут з розробки програмного забезпечення) має ряд інструментів з відкритим кодом на своєму вебсайті github. До них належать SiLK, Cyberticket Studio, Cyobstract та інші. У нас є набір інструментів щодо мережевої ситуаційної обізнаності: https://tools.netsa.cert.org/ Ми також використовуємо MISP" *(CERT/CC)*

2.4.3 Виконання плану навчання для різних посад

Увесь персонал CSIRT повинен мати початкові навички, необхідні для виконання своїх функціональних обов'язків. Для підвищення кваліфікації персоналу розроблений план навчання повинен підтримувати впровадження та участь співробітників у стандартних навчальних сесіях, конференціях та семінарах.

Також має бути проведено додаткове навчання для ведення операційної діяльності CSIRT — щодо процесів та стандартних операційних процедур.

2.4.4 Підготовка об'єктів

Об'єкти CSIRT повинні бути підготовлені відповідно до затвердженого плану з урахуванням фізичної безпеки та відповідних прав доступу.

Деякі команди приймають рішення маркувати свої об'єкти логотипами та впізнаваними знаками, тоді як інші команди, особливо якщо вони розміщуються в зоні об'єктів національної безпеки, не наносять ніяких позначень на своїх будівлях; CSIRT видно лише всередині приміщення.

2.4.5 Розробка та впровадження детальних процесів та процедур

Заплановані процеси CSIRT реалізуються у формі встановлених процедур.

Деякі типові дії, які повторюються, визначені в SOP та автоматизовані за допомогою технологій.

2.4.6 Втілення технології для автоматизації процесів

Впровадження технологій здійснюється шляхом встановлення, налаштування, документування та тестування технологій.

CSIRT широко використовують програмне забезпечення з відкритим кодом, часто написане або внесене іншими членами CSIRT.

2.4.7 Впровадження процедур управління IT та інформаційною безпекою

CSIRT повинні визначити та впровадити детальні процедури щодо управління IT та інформаційною безпекою.

Загальним викликом є те, що основні сервіси та процеси CSIRT є пріоритетними на етапі впровадження, тоді як IT-підтримка та внутрішні процеси управління безпекою зазвичай отримують менше уваги на початку. Отже, очікується, що ці процеси та процедури потребуватимуть подальшого вдосконалення.

Коли CSIRT є частиною більшої за розміром організації, IT-процеси організації, в структурі якої створена CSIRT, та система управління інформаційною безпекою можуть бути застосовані на практиці.

2.4.8 Навчання персоналу для ведення операційної діяльності CSIRT.

Широка практична та теоретична передача знань членам CSIRT щодо впроваджених технологій та процедур є вирішальною для успіху.

Заходи з передачі знань зазвичай проводяться у формі практичних семінарів, де всі процеси та процедури пояснюються та відпрацьовуються на практиці.

У процесі подальшого навчання можна проводити та виявляти прогалини в навичках, що досягається шляхом кризових тренувань та синьо-червоно-фіолетових навчань.

2.4.9 Підписання відповідних угод з клієнтами, заінтересованими особами та партнерами

Під час виконання плану партнерства CSIRT може виникнути потреба в реалізації додаткових правил та процедур.

Заявки на членство в FIRST.org та Trusted Introducer слід подавати, як тільки вони будуть готові та вимоги щодо функціональної та експлуатаційної готовності будуть виконані. На затвердження заявок на членство може знадобитися кілька місяців.

Побудова та підтримка партнерських відносин вимагає активної участі та спілкування, і це повинно контролюватися менеджером CSIRT або у випадку більших за розміром CSIRT, - менеджером партнерства.

2.4.10 Функціональне тестування сервісів CSIRT та корегування результатів

Після впровадження процесів та технологій важливо запустити тести принаймні на день і надавати повідомлення про будь-які недоліки в процесах і технологіях у звіті про тестовий запуск. Потім слід виконати налаштування, тобто налаштувати процеси, робочий порядок та впровадити необхідні технології.

Незалежно від початкової підготовки та планування результати часто виявляють, що деякі припущення на стадії проєктування були неправильними, тому деякі заходи щодо впровадження повинні бути змінені.

2.4.11 Запуск комунікацій CSIRT і відзначення

Після завершення впровадження, CSIRT може виконувати операції. Важливо належним чином повідомляти про нові сервіси, спосіб роботи CSIRT, практичну цінність, яку вона надаватиме, та відповідальність клієнтів і CSIRT.

Зазвичай таке повідомлення збігається із відзначенням запуску та прес-релізом CSIRT.

Відзначення запуску передбачає невелику презентацію, відвідування об'єктів клієнтами, заінтересованими особами та журналістами та надання друкованих матеріалів.

Успішний запуск може надихнути та дати позитивний імпульс всій CSIRT.

Подібним чином варто відзначити інші вдосконалення, щоб привернути позитивну увагу заінтересованих осіб до CSIRT, наприклад, це може бути відкриття лабораторії CSIRT або об'єктів кібертренажерного залу, випуск річного звіту або будь-яка інша важлива подія в житті CSIRT.

2.5 ОПЕРАЦІЇ

Фаза операцій зосереджена на ефективному та продуктивному наданні сервісів, тобто щоденному виконанні мандату CSIRT.

На етапі операцій очікуються такі результати.

1. Обчислення KPI.
2. Щорічний огляд результатів діяльності.
3. Щорічний огляд потреб заінтересованих осіб.
4. Затвердження річного бюджету.
5. Збирання ініціатив щодо вдосконалення.

2.5.1 Обчислення ключових індикаторів діяльності.

KPI використовуються з метою реалізації менеджменту, управління та моніторингу якості. Не всі CSIRT керуються KPI. Відмічалось, що багато CSIRT перевантажені та здійснюють свої загальні операції без гострого зосередження уваги на управлінні якістю сервісів CSIRT.

Щодо KPI: Статистика інцидентів, статистика управління вразливістю (щомісяця та щокварталу), включно з кількістю виявлених та усунених вразливостей (лише критична та висока на сьогодні) *(університет CSIRT)*

Нижче наведено рекомендації щодо використання KPI.

1. KPI потрібно вимірювати щомісяця. Для зрілих організацій щотижневі показники також можуть бути актуальними. Річний KPI — це сума місячних KPI.
2. Ключові показники ефективності повинні бути пов'язані з наданням сервісів, тобто з кожним сервісом, і повинні полегшувати розуміння того, який сервіс є якісним, а який, - ні та чи відповідає він цілям сервісу.
3. Деякі KPI використовуються лише для статистичного аналізу, тоді як інші — для здійснення заходів щодо вдосконалення. Наприклад, кількість проаналізованих інцидентів щомісяця є важливим показником для статистичного аналізу — в разі їх більшої чи меншої кількості рідко приймаються заходи щодо вдосконалення, тоді як кількість відвідувачів вебсайту CSIRT, де здійснюється обмін попередженнями та інформацією про обізнаність, вказує на тенденції актуальності, які можуть призвести до дій вдосконалення.

Приклади KPI:

1. Кількість зустрічей з клієнтами щомісяця з метою підвищення обізнаності (мета: принаймні одна).
2. Порушення угоди щодо рівня сервісів з обробки інцидентів (SLA) щодо критичних інцидентів (ціль: менше ніж 5 %).
3. Кількість відвідувачів вебсайту щомісяця (ціль: збільшення порівняно з попереднім місяцем).
4. Кількість проведених кампаній з підвищення обізнаності (мета: принаймні одна кожного другого місяця).
5. Тенденції в статистиці інцидентів (мета: пріоритетні інциденти повинні оброблятися відповідно до SLA).

Щодо KPI: "Час відповісти та пом'якшити поточні інциденти DDoS електронною поштою (1,5 години), зреагувати на та пом'якшити поточні інциденти DDoS (45 хвилин)" *(ISP CSIRT)*

2.5.2 Щорічний огляд ефективності операцій

Команда керівництва оперативної CSIRT повинна проводити щорічний огляд результатів діяльності CSIRT, щоб визначити успіхи, які слід відзначити, та напрями для вдосконалення.

На внутрішньому етапі огляду оцінюються навички персоналу та індивідуальні результати, перевіряються процеси CSIRT, оцінюється автоматизація та аналізуються ключові показники ефективності.

Огляд операцій зазвичай представлений у щорічному звіті CSIRT.

2.5.3 Щорічний огляд потреб заінтересованих осіб

Належною практикою є організація щорічного семінару або зустрічей із заінтересованими особами CSIRT, де буде представлено результати діяльності CSIRT, визначені для неї пріоритети та очікування заінтересованих осіб від CSIRT.

Ці пріоритети сприяють плануванню подальших удосконалень для CSIRT.

2.5.4 Затвердження річного бюджету

Як і будь-яка організація, CSIRT повинні щороку розробляти та отримувати погодження свого річного бюджету. У бюджеті визначено, які ініціативи отримають додаткове фінансування.

Бюджет повинен бути підготовлений відповідно до місцевих законів, норм і положень.

2.5.5 Збирання ініціатив щодо вдосконалення

Внутрішній щорічний огляд, аналіз потреб заінтересованих осіб та щоденні операції дозволяють визначити вимоги CSIRT, які, можливо, доведеться вдосконалити. Вони аналізуються в рамках фази вдосконалення.

Ідеї для вдосконалення можуть також випливати з огляду на операції. Усі ініціативи щодо вдосконалення повинні бути представлені в таблиці, включно з обґрунтуванням і поясненням потреби.

6. ВДОСКОНАЛЕННЯ

Етап вдосконалення фокусується на відборі та затвердженні ініціатив щодо вдосконалення діяльності CSIRT. Після затвердження ці ініціативи переходять до фази проєктування, впровадження та операцій. Процес вдосконалення повинен бути постійним протягом існування CSIRT.

На фазі вдосконалення очікуються такі результати.

1. Список ініціатив вдосконалення.
2. Детальні плани ініціатив щодо вдосконалення на стадії проєктування.
3. Попередній бюджет для ініціатив щодо вдосконалення.

2.6.1 Список ініціатив щодо вдосконалення

Спочатку часто важко виконати мандат CSIRT на відмінному рівні якості через відсутність навичок, автоматизації, процесів та ресурсів; таким чином, збалансування пріоритетів вдосконалення є спільною діяльністю для CSIRT.

Ініціативи щодо вдосконалення виходять з фази операцій як сфери, що потребує вдосконалення; з дорожньої карти високого рівня; з додаткових настанов заінтересованих осіб; або з вимог керівництва CSIRT щодо підвищення зрілості та можливостей CSIRT.

Рекомендації щодо вдосконалення зрілості доступні в таких структурах, як SIM3 та SOC-CMM, а також в ENISA, Глобальному форумі з питань кібернетики (GFCE), Координаційному центрі CERT (CERT/CC) та FIRST.org тощо.

Знаючи наявні ресурси, доступні для ініціатив щодо вдосконалення, керівна команда CSIRT вирішує, яким ініціативам надати пріоритет і затвердити та які ресурси виділити, наприклад бюджет і кількість людей. Приклади ініціатив щодо вдосконалення стосовно встановлення пріоритетів наведені в таблиці 9.

Таблиця 9. Приклади ініціатив щодо вдосконалення стосовно встановлення пріоритетів

Ініціатива	Необхідний бюджет[49] (євро)	Тривалість *(місяців)*	Обґрунтування	Затверджено
Автоматизація виявлення інцидентів	150 000	4	CSIRT вимагає автоматизації реєстрації та маршрутизації інцидентів із загальнодоступних джерел та внутрішніх мереж	Так
Система виявлення вторгнень Honeypot	80 000	6	Система виявлення вторгнень Honeypot забезпечує видимість того, хто і як атакує мережі	Так
Проєктування, впровадження та 1-річна діяльність служби інформування	75 000	3	Клієнт не має своєчасної та цілеспрямованої обізнаності з контекстною інформацією; таким чином, він має обмежену стійкість до соціальних та технічних атак	Так
ISO 27001 сертифікація	50 000	8	CSIRT обробляє конфіденційні дані і, отже, повинна забезпечувати належну роботу внутрішніх процесів захисту інформації	Так
Лабораторія DFIR	250 000	12	Потрібно для кількох випадків	Відкладено на наступний рік, оскільки кількість кейсів, що вимагають аналізу даних комп'ютерної криміналістики, є низькою
SOP розвиток	60 000	4	Чіткі та детальні інструкції стосовно процедур призводять до зменшення кількості помилок у роботі та швидшого навчання нового персоналу	Відкладено на наступний рік через брак ресурсів
Автоматизація інформації про розвідку загроз та комерційний постачальник інформації	60 000	3	Покращити якість щодо виявлення та аналізу інцидентів	Відкладено на наступний рік; наразі неможливо належним чином використовувати дані через брак персоналу
Досягнення SIM3 ENISA / Глобальна концепція CSIRT щодо зрілості (GCMF) середнього рівня	40 000	5	Підвищений рівень зрілості дозволяє надавати якісніші послуги більш упорядкованим та рівномірним способом та зменшувати кількість дефектів, а також підвищує довіру та репутацію CSIRT	Відкладено на наступний рік, оскільки для здійснення удосконалень потрібно виділити ключові внутрішні експертні ресурси

[49] Цифри лише для наглядності.

2.6.2 Детальні плани ініціатив щодо вдосконалення на стадії проєктування

Після затвердження ініціатив щодо вдосконалення наступним кроком є підготовка детальних планів на стадії проєктування.

У разі залучення зовнішніх консультантів детальні вимоги часто виражаються як ТЗ проєкту вдосконалення в конкурсних тендерах (RFI / RFP).
Вимоги до результатів стадії проєктування повинні бути конкретно зазначені. На цьому етапі доречно врахувати:

1. цілі ініціатив щодо вдосконалення;
2. чітко сформульовані очікування будь-яких вдосконалень;
3. очікуваний план втілення;
4. досвід, необхідний експертам, що виконують подібні роботи.

2.6.3 Попередній бюджет для ініціатив щодо вдосконалення

Щорічний бюджет повинен містити будь-який затверджений попередній бюджет для ініціатив щодо
вдосконалення. Це може знадобитися для покриття витрат на внутрішній персонал, додаткові об'єкти, технології, зовнішні консультації, адміністрування, співпрацю, маркетинг та додаткове навчання.

Попередній бюджет визначатиме обмеження ресурсів та проєктування на стадії проєктування під час планування.

Нормально очікувати, що щонайменше 15 % річного бюджету CSIRT буде витрачено на ініціативи щодо вдосконалення зрілості CSIRT. Для CSIRT з нижчим рівнем зрілості ініціативи щодо вдосконалення зазвичай складають щонайменше 30 % бюджету CSIRT.

3. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

У цій доповіді представлені рекомендації щодо створення CSIRT та SOC з використанням поетапного підходу з огляду на результати, включно з прикладами від існуючих CSIRT на різних етапах впровадження.

Створення — це тривалий процес. Можна визначити початок процесу; проте кінцева стадія передбачає постійний цикл вдосконалення — для кращого обслуговування клієнтів, ефективнішої діяльності та кращого реагування на потреби заінтересованих осіб.

Автори сподіваються, що ця публікація надихне на кращий менеджмент проєктів стосовно CSIRT та SOC та надасть чіткіші описи проміжних кроків, пов’язаних із створенням CSIRT та SOC.

Деякі виклики, пов'язані зі створенням CSIRT та SOC, не висвітлені у цій доповіді та вимагають додаткової роботи.

1. Ця публікація зосереджена на створенні єдиної CSIRT. Однак єдина CSIRT зазвичай є частиною екосистеми багатьох CSIRT. Майбутні дослідження можуть зосередитися на побудові екосистем та створенні цінності за допомогою партнерства та спеціалізації.
2. У багатьох країнах у різних секторах виникають галузеві CSIRT; однак, наразі є замало даних і настанов щодо належної практики, які можна було б надати для різних галузевих CSIRT.
3. Занадто мало актуальних і практичних рекомендацій щодо технологій та автоматизації CSIRT та SOC.
4. Підхід «зроби це самостійно» до процесу створення CSIRT все ще є складним завданням, оскільки необхідні відповідні експертні знання, які є недоступними в багатьох країнах. Важливо визначити в майбутньому, як це можна подолати.

ENISA продовжує підтримувати команди реагування на інциденти, створюючи відповідний контент для CSIRT.

4. Глосарій та скорочення

Будь ласка, зверніться до глосаріїв ENISA та списків скорочень:

- https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-_risk/bcm-resilience/glossary
- https://www.enisa.europa.eu/topics/csirts-in-europe/glossary
- https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary

5. Бібліографія

Університет Карнегі — Меллона, 2016 р., *Створення CSIRT*, Інститут програмного забезпечення, Пітсбург, Пенсільванія.

Cowley, C. та Pescatore, J., 2019, *Загальні та найкращі практики діяльності центрів безпеки: результати опитування SOC, 2019 р.*, Інститут SANS.

ENISA, 2006 р. *Покроковий підхід до створення CSIRT* (https://www.enisa.europa.eu/publications/csirt-setting-up-guide)

FIRST, 2019 р. Концепція сервісу реагування на інциденти комп'ютерної безпеки (CSIRT) (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1).

Робоча група інтернет-інженерії IETF, 1998, RFC 2350 для створення CSIRT (https://tools.ietf.org/html/rfc2350)

Форум врядування Internet, 2014 р., Форум найкращих практик щодо створення та підтримки команд реагування на інциденти комп'ютерної безпеки (CSIRT) з питань інтернет-безпеки (https://www.intgovforum.org/multilingual/content/establishing-and-supporting-computer-incident-security-response-teams-csirts-for-Internet).

MITRE, 2014, *Десять стратегій операційного центру кібербезпеки світового класу*, MITRE, Bedford, MA.

Morgus, R., Skierka, I., Hohmann, M. and Maurer, T., 2015, *Національні CSIRT та їх роль у реагуванні на інциденти комп'ютерної безпеки*, New America та GPPi. (https://www.researchgate.net/publication/323358191_National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response)

Національний центр кібербезпеки, 2015, *Рівні розвитку CSIRT*, Національний центр кібербезпеки, Гаага.

Національний центр кібербезпеки, 2017, *Створення SOC: почніть з малого*, Національний центр кібербезпеки, Гаага.

Організація американських штатів, 2016 р. *Найкращі практики створення національної CSIRT*, OAS, Вашингтон, округ Колумбія.

Open CSIRT Foundation, 2008—2019, SIM3: Модель підвищення зрілості управління інцидентами безпеки ((https://opencsirt.org/csirt-maturity/sim3-and-references/)

Skierka, I., Morgus, R., Hohmann, M. та Maurer, T., 2015. *Основи CSIRT для управлінця*, Нова Америка та GPPi. (https://www.researchgate.net/publication/323358187_CSIRT_Basics_for_Policy-Makers)

Сектор розвитку телекомунікацій (ITU-D), 2020, Концепція MCE CIRT, Міжнародний союз електрозв'зку, Женева.

ThaiCERT, 2017 р. *Створення CSIRT*, Таїландська команда реагування на комп'ютерні надзвичайні події, Бангкок.

TNO, 2017. *Глобальна належна практика GFCE: національні команди реагування на інциденти комп'ютерної безпеки (CSIRT).* (https://thegfce.org/wp-content/uploads/2020/06/NationalComputerSecurityIncidentResponseTeamsCSIRTs-1.pdf)

ДОДАТОК А: ОПИТУВАЛЬНИК

Збір даних за допомогою опитувальника

Зміст звіту "Керівні принципи створення CSIRT та SOC" базується на аналізі поточних публікацій про створення CSIRT, відповідях у цьому опитувальнику, та досвіді авторів у створенні та вдосконаленні CSIRT серед численних проєктів в Європі, Азії, Африці та Південній Америці.

Цей опитувальник на місцях (представлений нижче) був опублікований із використанням опитувальної платформи Європейської комісії (пряме посилання на опитувальник https://ec.europa.eu/eusurvey/runner/HowtosetupCSIRTandSOC) та розповсюджене між різними CSIRT та SOC у різних частинах світу через мережі обміну, а також через індивідуальне заохочування до участі. CSIRT та SOC було запропоновано заповнити їх за допомогою особистих запрошень, а також через довіреного представника та спілкування в мережі CIRTs.

Протягом встановленого часу були отримані докладні відповіді від понад 40 CSIRT та SOC з різних географічних локацій, у тому числі від різних типів CSIRT та SOC (національні, галузеві, внутрішні для організації тощо).

Опитувальник використовувався для таких цілей.

Завдання опитувальника — послужити дослідженню ENISA щодо керівних принципів для створення CSIRT та SOC. Відповіді очікуються щонайменше від 40 організацій, а отримані дані будуть оброблені та інтегровані з іншими методами дослідження. Деякі зібрані дані будуть використані в публікації ENISA стосовно рекомендацій щодо створення CSIRT та SOC як тематичне дослідження, приклад або статистично оброблені дані.

Дані збираються на платформі опитувальника Європейської комісії і не будуть використовуватися, продаватися чи оброблятися будь-яким іншим способом, крім прямого аналізу ENISA, для досягнення її мети:

"Починаючи з 2009 року, ENISA провело значний обсяг робіт у галузі дослідження можливостей та зрілості CSIRT, і ця робота сприяє формуванню ролі ENISA у допомозі CSIRT на шляху до вищих стандартів зрілості та вдосконалених можливостей".

Заповнюється керівником CSIRT або SOC або призначеною особою.

Ви можете відповісти лише на запитання, які вам здаються актуальними/цікавими, щодо яких ви готові поділитися своїм досвідом.

A.1 Про вашу команду CSIRT/SOC:

1. Назва команди/організації: (текстове поле)

2. Країна (текстове поле)

3. Тип CSIRT або SOC: національний / галузевий / MSSP / внутрішній для організації (багато варіантів на вибір)

4. Розмір команди: (текстове поле)

5. Клієнти CSIRT або SOC: (текстове поле)

6. Рік заснування: (текстове поле)

7. Контакти через електронну пошту та/або телефон для отримання роз'яснень у разі потреби: (текстове поле)

8. Дозвіл на використання даних: анонімний (тобто без будь-якого приписування команді) / може бути віднесений до вашої команди, але потрібно отримати попереднє підтвердження для точних даних, які слід віднести / усі дані можна використовувати в дослідженнях ENISA і, можливо, віднести до діяльності вашої команди)

A.2 Термінологічні питання:

1. Чи є у вашій організації CSIRT, SOC або обидва? (один вибір)

2. Якщо обидва, то як розподіляються ролі між CSIRT та SOC? (текстове поле)

3. Як ви сприймаєте різницю між CSIRT та SOC як організаціями? (текстове поле)

A.3 Питання знань, які стосуються CSIRT/SOC:

1. Які публікації ви використовуєте або вважаєте доречними для впровадження вдосконалення можливостей та зрілості вашої організації? (текстове поле)

2. Які публікації та рекомендації з контенту ENISA, на вашу думку, відсутні стосовно тематик CSIRT та SOC для вашої ефективної роботи? (текстове поле)

3. Якщо ви виконуєте роль координатора CSIRT (тобто ваша команда координує інциденти, які відбуваються за межами вашої установи/підприємства), яку діяльність ви регулярно здійснюєте відповідно до цієї ролі? (текстове поле)

4. Якщо ви виконуєте роль внутрішнього або MSSP (постачальник послуг з управління інформаційною безпекою) CSIRT/SOC (тобто ви займаєтеся власною організацією / інцидентами на підприємстві або працюєте як контрактний MSSP), яку діяльність ви регулярно здійснюєте відповідно до цієї ролі? (текстове поле)

5. Якщо ви передаєте деякі функції стороннім CSIRT/SOC, які саме? Яка мотивація використання зовнішніх джерел? (текстове поле)

6. Яку регулярну звітність ви подаєте (будь ласка, вкажіть кому (не потрібні імена, крім загальної цільової групи, наприклад — енергетичний сектор), який зміст і як часто? Наприклад, щорічний звіт для громадськості зі статистикою інцидентів, щокварталу до ENISA щодо загроз CII, щотижнева статистика вразливості до CISO тощо) (текстове поле)

7. Опишіть методи обміну інформацією, які ви застосували у своїх операціях (наприклад: інформаційні бюлетені та попередження вебсайтів; надання індивідуального каналу на основі MISP/IntelMQ передплатникам CII; надання щорічної/квартальної статистики з внутрішніх/зовнішніх джерел щодо інцидентів/вразливостей та повідомлення про них клієнтів; використання датчиків PassiveDNS і надання отриманого каналу спільноті passiveDNS; внесення даних MISP за допомогою OSIN до FIRST.org і данних ваших розслідувань; використання T-POT та надання доступу до даних платформі sicherheitstacho тощо) (текстове поле)

8. Ви використовуєте свої інструменти в приміщеннях, у хмарі (державній чи приватній) або застосовуєте змішану модель? Які ваші подальші плани щодо цієї теми? Яка ваша думка щодо галузевої тенденції на цю тему? (текстове вікно)

9. Чи є оркестрація та автоматизація важливими завданнями для вашого CSIRT/SOC? Чи використовуєте ви зараз чи будете використовувати в майбутньому подібні SOAR інструменти?

10. Чи працюєте ви 24/7? Чи використовуєте ви follow-the-sun — підгалузь глобально розподіленої програмної інженерії як рішення (команда розподілена в різних часових поясах), принаймні розглядали на майбутнє? (текстове вікно)

11. Які інструменти з відкритим кодом і для якої мети ви використовуєте? Які і з якої причини ви б пропонували іншим CSIRT/SOC як особливо цінні? (текстове вікно)

12. Які комерційні інструменти та з якою метою ви використовуєте? Які з них і з якої причини ви б пропонували іншим CSIRT/SOC як цінні? (текстове вікно)

13. Які основні показники ефективності та їх цільові рівні ви застосовували для своїх операцій CSIRT/SOC? (текстове вікно)

14. Назвіть основні проблеми, з якими ви стикалися під час налаштування роботи CSIRT або SOC? (текстове вікно)

15. Які дії ви б вжили (або рекомендували б), щоб уникнути згаданих проблем під час створення нового CSIRT або SOC? (текстове вікно)

16. Якби вам необхідно було створити нову команду CSIRT або SOC в тій самій чи іншій організації, на яких пріоритетах діяльності ви б зосередилися? Будь ласка, виберіть до 5. (текстове поле)

A.4 Посадові обов'язки:

1. Скільки посадових обов'язків ви б визначили у своїй організації CSIRT/SOC? Яких саме? Надайте стислий опис. (текстове вікно)

2. Яке навчання для різних посадових ролей (визначених вами раніше) ви рекомендуєте або плануєте, перш ніж вважати працівника повністю підготовленим фахівцем на певну посаду у вашій організації? (текстове вікно)

3. Які шляхи постійного навчання для поточного персоналу (наприклад, ad-hoc, організовані в певному порядку тощо)? (текстове поле)

4. З якими проблемами ви стикаєтеся під час розробки та визначення ролей співробітників у вашій організації? (текстове вікно)

A.5 SIM3 та інші запитання, пов'язані з моделями CSIRT:

1. Про використання моделі SIM3 у вашій організації CSIRT або SOC: ми не знаємо і не використовуємо модель / вона використовується як довідкова / це наша модель розвитку та вдосконалення зрілості / ми використовуємо альтернативну модель;

2. Якщо ви використовуєте або плануєте використовувати модель SIM3 у своїй організації: як SIM3 створив цінність для вашої організації? (текстове вікно)

3. Будь ласка, вкажіть, які сервіси CSIRT/SOC ви визначили, впровадили, надаєте та обчислюєте для вашого клієнта? (текстове вікно)

4. Які найбільші виклики для організації та персоналу ви бачите для покращення діяльності вашої CSIRT/SOC? (текстове вікно)

5. Які операційні процеси CSIRT/SOC ви офіційно задокументували та впровадили (наприклад, процес запобігання інцидентам, процес виявлення інцидентів, процес вирішення інцидентів, процес аудиту / зворотного зв'язку тощо)? (текстове вікно)

6. ДОДАТОК B: МЕТОДОЛОГІЯ КАРТУВАННЯ

1. Що охоплює методологія CSIRT :					
Аспект/ джерело	1. Національна CSIRT	2. CSIRT/SOC критичної галузі	3. MSSP CSIRT/SOC	4. Організація CSIRT/ SOC	5. 3. Термінологія, яка застосовується (CSIRT/CERT/SOC)
FRST	x	x	x	x	CSIRT
ENIS1	x	x	x	x	CSIRT
THAI	x	x	x	x	CSIRT
OAS	x				CSIRT
GPP2	x				CSIRT
GPP1	x	x		x	CSIRT
GFCE	x				CSIRT
CMU1				x	CSIRT
MITRE	x	x	x	x	SOC
SIM3	x	x	x	x	CSIRT
NL1	x	x	x	x	CSIRT
NL2				x	SOC
RFC				x	CSIRT
SANS1		x	x	x	SOC
IGF1		x	x	x	CSIRT
MCE	x				CIRT
Облік	12	9	8	12	16

2. Етапи створення CSIRT/SOC охопили:					
Аспект/ джерело	**1. Оцінка готовності**	**2. Проектування**	**3. Впровадження**	**4. Експлуатація**	**5. Вдосконалення**
FRST				x	
ENIS1		x	x	x	x
THAI	x	x	x	x	x
OAS		x	x		
GPP2		x			
GPP1		x		x	x
GFCE		x	x	x	x
CMU1	x	x	x	x	x
MITRE	x	x	x	x	x
SIM3	x	x		x	x
NL1		x	x	x	
NL2	x	x	x		x
RFC		x	x	x	
SANS1				x	
IGF1		x		x	
MCE	x	x	x		
Облік	6	14	10	12	8

3. Покриття параметрів SIM3: 1.0 "Організація" параметрів										
Аспект/ джерело	O-1: Мандат	O-2: Клієнти	O-3: Орган	O-4: Відповідальність	O-5: Опис сервісу	O-7: Опис рівня сервісу	O-8: Класифікація інциденту	O-9: Інтеграція наявних систем CSIRT	O-10: Організаційний концепція	O-11: Політика безпеки
FRST					x					
ENIS1	x	x		x	x	x	x	x	x	x
THAI	x	x	x	x	x		x	x	x	x
OAS	x	x	x	x	x					x
GPP2	x		x	x	x				x	
GPP1	x				x			x		
GFCE	x	x	x	x	x			x		
CMU1	x	x	x	x	x				x	
MITRE	x	x	x	x	x			x		
SIM3	x	x	x	x	x	x	x	x	x	x
NL1					x		x	x	x	x
NL2	x		x		x				x	x
RFC	x	x	x	x	x	x	x	x	x	x
SANS1	x	x		x	x				x	
IGF1					x				x	x
MCE	x	x	x	x	x				x	x
Облік	13	10	10	11	16	3	5	8	11	9

3. Покриті параметри SIM3: 2.H "Людські" параметри							
Аспект/ джерело	H-1: Правила поведінки / Практика / Етика	H-2: Особиста стійкість	H-3: Опис набору навичок	H-4: Внутрішнє навчання	H-5: Зовнішнє технічне навчання	H-6: Зовнішнє комунікаційне навчання	H-7: Зовнішні зв'язки
FRST				x	x	x	
ENIS1	x	x	x	x	x		x
THAI	x	x	x	x	x		x
OAS		x	x		x		
GPPI 2							x
GPPI 1							
GFCE							
CMU 1							
MITRE	x	x	x	x	x		x
SIM 3	x	x	x	x	x	x	x
NL 1	x	x	x	x	x	x	x
NL 2			x				
RFC							
SANS 1	x	x					
IGF 1							
MCE				x			
Облік	6	7	7	7	7	3	6

3. Покриті параметри SIM3: 3.Т Параметри «Інструменти»										
Аспект/ джерело	Т-1: Список ресурсів IT	Т-2: Список інформаційних ресурсів	Т-3: Консолідована система e-mail	Т-4: Система відстеження інциденту	Т-5: Безперервний телефонний зв'язок	Т-6: Безперервна робота електронної пошти	Т-7: Безперервний інтернет-доступ	Т-8: Набір інструментів запобігання інцидентам	Т-9: Набір інструментів виявлення інцидентів	Т-10: Набір інструментів вирішення інцидентів
FRST										
ENIS1	x	x		x	x			x	x	
THAI	x	x	x	x	x	x	x			
OAS										
GPPI2										
GPPI1										
GFCE					x	x	x			
CMU1										
MITRE	x	x		x				x	x	x
SIM3	x	x	x	x	x	x	x	x	x	x
NL1	x		x	x						
NL2	x			x						
RFC						x				
SANS1									x	x
IGF1										
ITU			x	x		x	x		x	x
Облік	6	4	4	7	4	5	4	3	5	4

3. Покриті параметри SIM3: 4.P Параметри "Процеси"																	
Аспект/ джерело	P-1: Ескалація до управлінського рівня	P-2: Ескалація до прес-функції	P-3: Ескалація до юридичної функції	P-4: Процес запобігання інцидентам	P-5: Процес виявлення інцидентів	P-6: Процес вирішення інцидентів	P-7: Процеси специфічних інцидентів	P-8: Процес аудиту/відгуку	P-9: Забезпечення доступності при надзвичайних подіях	P-10: Найкраща практика e-mail та web-присутності	P-11: Безпечний процес обробки інформації	P-12: Процес забезпечення інформаційних джерел	P-13: Процес діапазону дії	P-14: Процес доповіді	P-15: Процес статистики	P-16: Процес зустрічі	P-17: Процес однорангової взаємодії
FRST	x	x			x	x	x						x	x			
ENIS1		x		x	x	x		x	x	x	x	x	x	x			x
THAI						x		x	x		x			x			
OAS																	
GPPI2																	
GPPI1																	
GFCE											x		x				
CMU1																	
MITRE	x			x	x	x					x			x			
SIM3	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
NL1					x	x			x	x	x		x				
NL2								x			x						
RFC						x											
SANS1					x	x	x							x	x		
IGF1																	
ITU				x	x	x	x	x									
Облік	3	3	1	4	7	9	4	5	4	3	7	2	5	6	2	1	2

4. Сервіси FIRST.org охоплюють:																										
Аспект/ джерело	Сервісна сфера: управління подіями інформаційної безпеки	Послуга: моніторинг та виявлення	Сервіс: аналіз подій	Сервісна сфера: управління інцидентами інформаційної безпеки	Сервіс: прийняття звіту про інцидент інформаційної безпеки	Сервіс: аналіз інцидентів інформаційної безпеки	Сервіс: аналіз артефактів та даних криміналістики	Сервіс: пом'якшення наслідків та відновлення	Сервіс: координація інцидентів інформаційної безпеки	Сервіс: підтримка антикризового управління	Сервісна сфера: управління вразливостями	Сервіс: виявлення вразливості / дослідження	Сервіс: прийняття звіту про вразливість	Сервіс: аналіз вразливості	Сервіс: координація вразливості	Сервіс: розкриття вразливості	Сервіс: реагування на вразливість	Сервісна сфера: ситуаційна обізнаність	Сервіс: збір даних	Сервіс: аналіз та синтез	Сервіс: зв'язок	Сервісна сфера: передача знань	Сервіс: побудова обізнаності	Сервіс: навчання та тренування	Сервіс: навчання	Сервіс: технічне консультування та консультування стосовно правил
FRST	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ENIS1	x	x	x	x	x	x	x	x	x		x	x		x	x	x	x		x		x		x	x	x	x
THAI					x	x	x	x	x																	
OAS		x			x	x	x	x				x					x									x
GPPI2				x							x										x					x
GPPI1		x		x		x	x	x	x		x			x	x		x			x	x		x	x		x
GFCE				x														x			x	x	x	x	x	
CMU1																										
MITRE		x				x	x	x				x							x	x	x			x	x	x
SIM3																										
NL1		x				x		x													x		x	x	x	
NL2	x	x		x		x									x		x		x							x
RFC					x	x			x																	
SANS1	x	x	x																							
IGF1																										
ITU	x	x	x	x	x	x	x	x	x	x								x	x	x	x					
Облік	5	9	4	7	6	10	7	8	6	2	4	4	1	3	4	2	5	3	5	4	8	2	5	6	5	7

Абревіатури, використані на діаграмі відображення методології, пояснюються в наступній таблиці.

Місцева абревіатура	Назва публікації
FRST	Концепція сервісів реагування на інциденти комп'ютерної безпеки (CSIRT), FIRST, 2019.
ENIS1	Покроковий підхід до створення CSIRT, Агентство Європейського Союзу з питань мережевої та інформаційної безпеки, 2006 р.
THAI	Створення CSIRT, ThaiCERT, 2017.
OAS	Найкращі практики створення національної CSIRT, Організація американських штатів, 2016.
GPP2	Національні CSIRT та їх роль у реагуванні на інциденти комп'ютерної безпеки, Нова Америка та GPPi, 2015.
GPP1	Основи CSIRT для політиків, Нова Америка та GPPi, 2015.
GFCE	Глобальна належна практика GFCE: національні команди реагування на інциденти комп'ютерної безпеки (CSIRT), TNO, 2017.
CMU1	Створити CSIRT, Університет Карнегі — Меллона, 2016.
MITRE	Десять стратегій операційного центру кібербезпеки світового класу, MITER, 2014.
SIM3	SIM3: Модель підвищення зрілості управління інцидентами безпеки, S-CURE bv та PRESECURE GmbH, 2015.
NL1	Рівні зрілості CSIRT, Національний центр кібербезпеки, Нідерланди, 2015.
NL2	Створення SOC: почніть з малого, Національний центр кібербезпеки, Нідерланди, 2017.
RFC	RFC 2350 для організацій CSIRT, IETF, 1998.
SANS1	Загальна та найкраща практика роботи центрів безпеки: результати опитування SOC 2019 року, SANS, 2019.
IGF1	Форум найкращих практик щодо створення та підтримки команд реагування на інциденти в галузі комп'ютерної безпеки (CSIRT) для інтернет-безпеки, Форум з управління Інтернетом, 2014.
MCE	Концепція ITU щодо CIRT, ITU-D, 2020.

TP02-20-935-EN-N

ПРО ЄВРОПЕЙСЬКЕ АГЕНТСТВО З ПИТАНЬ МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ENISA)

Європейське Агентство з питань мережевої та інформаційної безпеки, ENISA, є агентством Європейського Союзу, метою діяльності якого є досягнення високого загального рівня кібербезпеки в Європі. Засноване в 2004 році та посилене Законом ЄС про кібербезпеку, Європейське Агентство з питань мережевої та інформаційної безпеки здійснює свій внесок у кіберполітику ЄС, підвищує надійність продуктів, послуг та процесів інформаційно-комунікаційних технологій (ІКТ) за допомогою схем сертифікації кібербезпеки, співпрацює з державами-членами та органами ЄС і допомагає Європі підготуватися для кібервикликів майбутнього. Шляхом обміну знаннями, розбудови спроможності та підвищення обізнаності Агентство працює разом зі своїми ключовими заінтересованими особами для зміцнення довіри до пов'язаної економіки, підвищення стійкості інфраструктури Європейського Союзу та, врешті-решт, для забезпечення цифрового захисту європейського суспільства і громадян. Більше інформації про ENISA та його роботу можна знайти на www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-410-7
DOI 10.2824/056764