неофіційний переклад

Інтероперабельний інструментарій управління ризиками ЄС

ЛЮТИЙ 2023

Про ENISA

Агентство Європейського Союзу з кібербезпеки (ENISA) – це агентство ЄС, яке займається досягненням високого загального рівня кібербезпеки в Європі. Заснована в 2004 році та посилена Законом ЄС про кібербезпеку, ENISA робить внесок у кіберполітику ЄС, підвищує надійність продуктів, послуг і процесів ІКТ за допомогою схем сертифікації кібербезпеки, співпрацює з державами-членами ЄС та органами ЄС і допомагає Європі підготуватися до кібервикликів завтра. Завдяки обміну знаннями, нарощуванню потенціалу та підвищенню обізнаності агентство співпрацює зі своїми ключовими зацікавленими сторонами, щоб зміцнити довіру до пов'язаної економіки, підвищити стійкість інфраструктури ЄС і, зрештою, зберегти європейське суспільство та громадян у цифровій безпеці. Більше інформації про ENISA та її роботу можна знайти тут: www.enisa.europa.eu.

Автори
Kostas Papadatos, Cyber Noesis Konstantinos Rantos, Cyber Noesis Argyris Makrygeorgou, Cyber Noesis Konstantinos Koulouris, Cyber NoesisStefania Klontza, Cyber Noesis

Costas Lambrinoudakis, University of PiraeusStefanos Gritzalis, University of Piraeus Christos Xenakis, University of Piraeus Sokratis Katsikas, University of Piraeus Maria Karyda, University of Piraeus

Aggeliki Tsochou, University of PiraeusAlexandros Zacharis, ENISA

Print ISBN 978-92-9204-609-5 doi:10.2824/713364 TP-04-22-275-EN-CPDF ISBN 978-92-9204-608-8 doi:10.2824/68948 TP-04-22-275-EN-N

Зміст

1. ВСТУП 6

1.1. Призначення та сфера застосування 6

1.2. Структура звіту 6

1.3. Визначення абревіатур 7

2. ВЗАЄМОСУМІСНИЙ ІНСТРУМЕНТАРИЙ EU RM 8

2.1. Метод роботи 8

2.2. Опис інструментарію EU RM 8

2.3. Компоненти панелі інструментів 10

2.3.1. База знань 10
2.3.2. Функціональні компоненти 15

3. СПОСІБ ЗАСТОСУВАННЯ 16

3.1. Основні поняття і терміни 16

3.2. Оцінка ризику щодо конкретної загрози 17

3.3. Процес розробки варіантів використання 19

4. РОЗВИТОК ІНСТРУМЕНТІВ 20

5. ВИСНОВКИ 22

A Додаток I – Термінологія панелі інструментів 23

B Додаток II – Класифікація активів на панелі інструментів 32

C Додаток III – Класифікація загроз інструментарію 33

D Додаток IV – Інструментальна шкала впливу 41

E Додаток V – Шкала ризику інструментарію 43

F Додаток VI – Приклади сумісності розрахунку ризику 45

G Додаток VII – Бібліотеки панелі інструментів 46

H Додаток VIII – Приклад застосування 47

Опис сценарію 47

Індикативні активи у сфері 47

Шлях атаки 48

Сценарії атаки 49

Результати 51

6. БІБЛІОГРАФІЯ/ПОСИЛАННЯ 52

Короткий зміст

Переваги європейської цифрової економіки та суспільства можна повністю отримати лише за умови кібербезпеки. Усі верстви суспільства можуть постраждати, і ЄС має бути готовим реагувати на масові (широкомасштабні та транскордонні) кібератаки та кіберкризи. Транскордонні взаємозалежності підкреслили необхідність ефективної співпраці між державами-членами ЄС та установами ЄС для швидшого реагування та належної координації зусиль на всіх рівнях (стратегічному, оперативному, технічному та комунікаційному). З огляду на цю перспективу, важливо не лише визначити взаємосумісні терміни в управлінні ризиками (RM) ЄС та нормативно-правовій базі, але також розробити загальні/порівняльні шкали ризику, які дозволять інтерпретувати результати аналізу ризиків, які є результатом різних RM. методи, щоб рівні ризику були порівнянними.

У цьому документі представлено інструментарій EU RM, рішення, запропоноване ENISA для вирішення проблем сумісності, пов'язаних із використанням методів RM інформаційної безпеки. Набір інструментів спрямований на сприяння плавній інтеграції різних методів управління менеджментом у середовищі організації або між організаціями та усунення прогалин, пов'язаних із різними відповідними підходами методів. За допомогою набору інструментів акціонери зможуть мати загальне розуміння ризиків і звітувати про сумісні результати оцінки ризиків спільноті та компетентним органам.

1. Вступ

1.1. Призначення та сфера застосування

Цей звіт є частиною проекту ENISA «Створення взаємосумісних структур ЄС з управління ризиками, том. 02', який розширює та ґрунтується на попередній роботі, виконаній у 2021 році, і підготував такі звіти:

1. *Інтероперабельна структура управління ризиками ЄС* (https://www.enisa.europa.eu/publications/interoperable-eu-risk-management- framework);
2. *Компендіум структур управління ризиками з потенційною сумісністю* (https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks).

Інтероперабельний інструментарій EU RM (також згадуваний у цьому документі як «набір інструментів») має на меті забезпечити еталонну структуру, яка підтримує інтерпретацію, порівняння та агрегацію результатів, отриманих різними методами оцінки ризику. Набір інструментів EU RM дозволить різним зацікавленим сторонам працювати над загальними загрозами та сценаріями ризиків і порівнювати їхні рівні ризиків, навіть якщо вони оцінюються за допомогою різних або власних інструментів і методів. Такі порівняльні результати щодо стану безпеки організацій дозволять різним організаціям разом із політиками та регуляторами розробити інтегрований погляд на стан кібербезпеки організацій проти конкретних та/або нових загроз у конкретних секторах, а також у різних секторах і країнах.

З цією метою інструментарій EU RM надаватиме вказівки та полегшуватиме порівняння та інтерпретацію готовності різних інфраструктур інформаційних систем до кібербезпеки проти конкретного сценарію загрози або набору сценаріїв загроз (наприклад, фізичних загроз).

Метою цього документу є визначення схеми та необхідного набору компонентів (загальна термінологія, класифікація активів, таксономія загроз і масштаби впливу/ризику), які дозволять інтерпретувати результати аналізу ризиків, отримані в результаті використання різних систем управління ризиками.

1.2. Структура звіту

Цей звіт містить чотири розділи: Розділ 1 (Вступ) визначає призначення та сферу застосування інструментарію; Розділ 2 (Інтероперабельний інструментарій EU RM) представляє концепцію, схему та компоненти інструментарію; Розділ 3 (Спосіб використання) описує спосіб, у який зацікавлені сторони використовуватимуть інструментарій EU RM; і Розділ 4 (Розвиток інструментарію) пропонує шляхи подальшого збагачення інструментарію додатковою інформацією для досягнення довгострокових цілей. Розділ 5 (Висновки) підсумовує наші висновки.

Цей звіт також містить такі додатки:

- Додаток I – Термінологія
- Додаток II – Класифікація активів
- Додаток III – Класифікація загроз
- Додаток IV – Шкала впливу
- Додаток V – Шкала ризику
- Додаток VI – Приклади сумісності розрахунку ризику
- Додаток VII – Бібліотеки панелі інструментів
- Додаток VIII – Приклад застосування.

1.3. Визначення абревіатур

Нижче наведено скорочення, які використовуються в цьому документі, і їх визначення.

Абревіатура	Визначення
API	інтерфейс прикладного програмування
CIS	комунікаційно-інформаційна система
DSO	оператор системи розподілу
ICT	інформаційні та комунікаційні технології
IoT	Інтернет предметів
IT	інформаційні технології
ITSRM²	Методологія управління ризиками безпеки IT
NIS	мережеві та інформаційні системи
OT	оперативна техніка
RM	управління ризиками

2. Інтероперабельний інструментарій EU RM

2.1. Метод роботи

Інструментарій EU RM було розроблено та розроблено на основі вказівок, наданих у звіті ENISA 2022 року Interoperable EU Risk Management Framework, щоб полегшити впровадження скоординованої та сумісної структури RM, яка забезпечить узгоджену методологію та практику оцінки ризиків між держав-членів.

Щоб розробити набір інструментів управління менеджментом ЄС, було враховано результати оцінки потенційної сумісності кількох відомих структур і методологій менеджменту менеджменту, які включені в попередній звіт. Набір інструментів складається з основних елементів, які були ідентифіковані та оцінені як важливі для сумісності методів управління ризиками, включаючи ідентифікацію та категоризацію активів, ідентифікацію загроз, опис сценаріїв атак, оцінку та порівняння рівнів ризику, а також із загальним словником, який полегшує розуміння результатів різних методів RM.

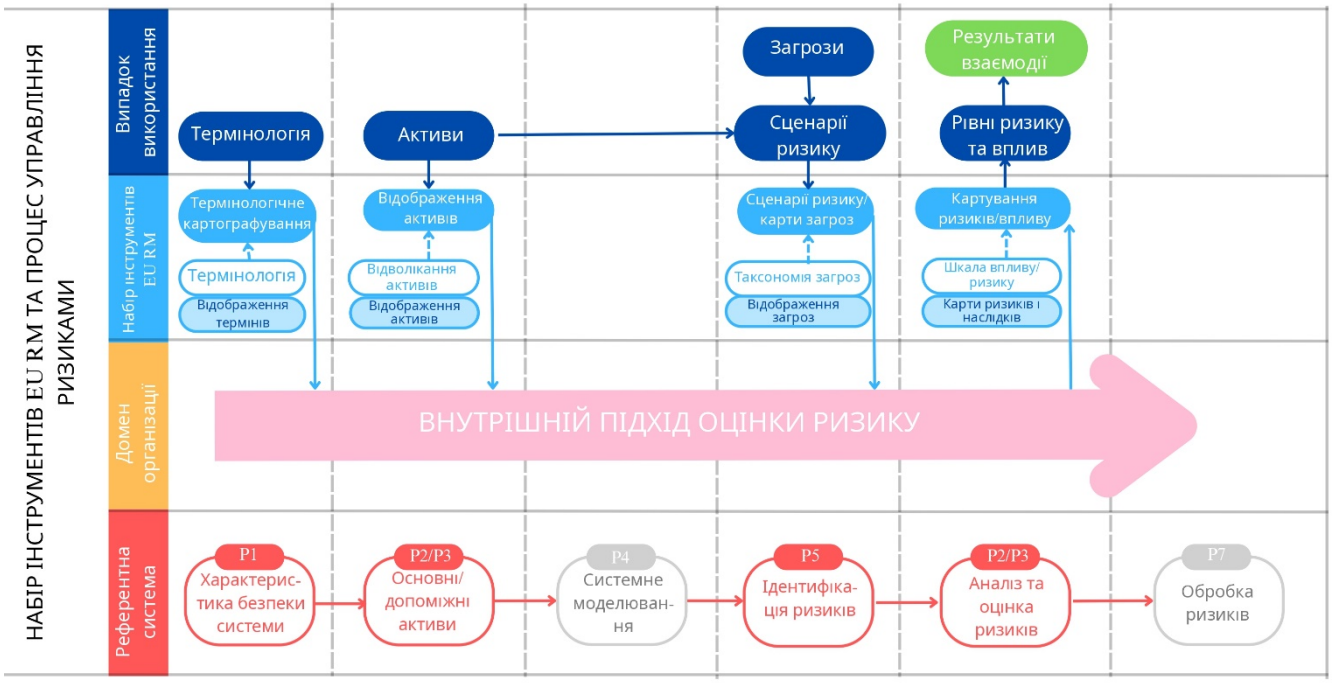
Нарешті, також спираючись на результати звіту ENISA 2022 року Interoperable EU Risk Management Framework, метод, який використовується для застосування набору інструментів, відповідає основним процесам управління ризиками, включеним у ISO/IEC 27005:2018, і методології управління ризиками безпеки інформаційних технологій (ITSRM2), як було показано у звіті, вони надали розширені можливості для підтримки сумісності..

2.2. Опис інструментарію EU RM

Інструментарій EU RM має на меті надати зацікавленим сторонам довідкову структуру для узгодження їхніх зусиль з RM таким чином, щоб вони мали спільне розуміння ризиків і пов’язаних із ними рівнів ризику, незалежно від підходу до RM, який вони застосовують, та інструмента(ів), які вони використовують. Зважаючи на це, набір інструментів EU RM поважає особливості відповідних методів RM і не змінює те, як організації працювали над управлінням ризиками інформаційної безпеки. З набором інструментів EU RM зацікавлені сторони зможуть використовувати сумісні компоненти для порівняння результатів з іншими організаціями для конкретних сценаріїв ризику, навіть якщо використовуються різні методи та інструменти RM.

За допомогою інструментарію EU RM регуляторні та наглядові органи можуть мати горизонтальне уявлення про рівні ризику та стан безпеки організацій у певному секторі або в їхній сфері повноважень чи юрисдикції з огляду на конкретні загрози та сценарії ризику. (можливі несприятливі події, які можуть вплинути на стратегію та цілі організації), і тому може належним чином керувати ними. Узгодження відповідних зусиль зацікавлених сторін з управління ризиками та нормалізація відповідних результатів, використовуючи еталонну структуру та загальні показники для рівнів ризику, допоможе цим організаціям краще порівнювати результати та отримувати відчутні результати, які легко керуватимуть ними у подальших діях. діяльності.

Малюнок 1: Роль інструментарію EU RM і його позиціонування в процесі RM



Малюнок 1 демонструє позиціонування інструментарію EU RM щодо сценаріїв використання та відповідних інструментів, які організації використовують у своєму середовищі. Набір інструментів EU RM діє як проміжний і абстрактний рівень між сценаріями використання (тобто набором сценаріїв ризику, за якими організація або компетентний орган хоче оцінити рівні ризику) і прийнятою організацією методологією RM, яка використовується для цієї оцінки. . З цією метою інструментарій не має на меті змінити спосіб внутрішнього управління ризиками організацій. Замість цього він надає зацікавленим сторонам засоби для загального розуміння сценаріїв ризику та однозначного тлумачення відповідних активів і загроз перед використанням обраних ними інструментів управління ризиками для оцінки ризиків, а також засоби для інтерпретації їхніх розрахованих рівнів ризику для сумісних результатів.

Зважаючи на це, набір інструментів інтерпретує сценарії ризиків, розроблені з використанням термінології набору інструментів, класифікації активів і таксономії загроз, відповідно до методологій оцінки ризиків і нормалізує результати оцінки ризиків на загальну матрицю ризиків, яка забезпечує порівняльні результати.

Використовуючи ITSRM2 як еталонну структуру для діяльності з менеджменту менеджменту, набір інструментів ЄС з менеджменту менеджменту полегшує узгодження діяльності з менеджменту менеджменту в чотирьох функціях менеджменту менеджменту (мал. 1).

- **Встановіть спільне розуміння щодо заходів, які будуть здійснюватися під час процесу управління ризиками.** нструментарій ЄС RM надає набір сумісних термінів на основі RM і нормативних рамок, а також міжнародних стандартів, які використовуються для встановлення контексту RM. Це дозволяє однозначно описувати та розуміти діяльність RM, незалежно від використовуваної методології RM. Якщо необхідно, відповідність між інструментами EU RM і відповідною термінологією методологій RM доповнюватимуть інструментарій у майбутньому, щоб не виникало неоднозначних дій.
- **Визначте сферу дії середовища, в якому буде застосовуватися процес оцінки ризику.** Набір інструментів EU RM сприяє цій функції, забезпечуючи класифікацію активів для класифікації тих, хто бере участь у сценарії ризику, і додаткових активів організації, знайдених у досліджуваному середовищі. Ця класифікація полегшує розробку однозначних сценаріїв ризику та правильну інтерпретацію для відповідних активів, які будуть розглянуті в процесі оцінки ризику. Визначивши та класифікувавши свої активи за допомогою наданих категорій, організації зможуть

визначити, чи і як сценарій ризику або атаки застосовується до їхнього середовища (тобто перевірити, чи активи, знайдені в середовищі організації, використовуються та чи підпадають під вплив певного сценарію ризику).

- **Визначення сценаріїв ризику, пов'язаних із конкретною загрозою або групою загроз.** Сценарії високого рівня ризику, пов'язані з конкретною загрозою або групою загроз, які досліджуються за допомогою інструментарію EU RM, повинні бути зіставлені з середовищем організації, щоб отримати належну оцінку. Після того, як сценарій ризику обрано для оцінки, він може використовувати таксономію загроз, надану набором інструментів, і активи, пов'язані зі сценарієм ризику, щоб зіставити його з відповідним внутрішнім методом управління ризиками. Це дозволяє організаціям легко оцінити свої рівні ризику та стан безпеки своєї організації для сценаріїв ризику та перейти до нормалізації обчислених результатів.
- **Зіставте розраховані значення ризику на загальну шкалу ризиків.** Розрахувавши значення ризику за допомогою вибраного внутрішнього методу управління ризиками, організація повинна нормалізувати результати на основі процесу відображення рівня ризику, спеціально розробленого для кожного методу управління ризиками, і набору попередньо визначених рівнів ризику, прийнятих набором інструментів. У процесі відображення використовується шкала ризиків вибраного внутрішнього методу та зіставляється зі шкалою ризиків інструментарію, таким чином надаючи зацікавленим сторонам засоби для використання загальної еталонної шкали для оцінки своїх ризиків. Очікується, що в майбутніх оновлених версіях інструментарій надасть розширений набір зіставлень для різних методів.

Зауважте, що термінологія, класифікація активів, таксономія загроз, масштаб ризику та, що більш важливо, відповідні відображення різних методів управління менеджментом на них, які матимуть форму бібліотек інструментів, передбачені як компоненти, які динамічно збагачуватимуться для задоволення потреб, які випливають з різних застосовних доменів, а також із методів та інструментів RM, як детально описано в розділі 4.

Крім того, наступні версії набору інструментів також можуть прагнути до розробки спільного набору заходів, які також будуть зіставлені з різними методами, щоб сприяти належному та єдиному розгляду ризиків.

2.3. Компоненти панелі інструментів

Інструментарій EU RM складається з кількох компонентів, які сприяють або як функціональні компоненти узгодженню діяльності з RM, або як база знань для процесів оцінки ризиків. Функціональні компоненти заповнюють прогалини між різними методами оцінки ризику шляхом узгодження відповідних функцій управління ризиками з набором інструментів управління ризиками ЄС. База знань надає всю необхідну інформацію для функціональних компонентів для виконання зіставлення сценаріїв ризику з методами управління ризиками та звітування про рівні ризику.

2.3.1. База знань

База знань EU RM toolbox, яку також називають визначеннями, містить усю інформацію, необхідну для узгодження зусиль RM з основними функціями, які складають такий процес. База знань містить:

- термінологія
- класифікація активів
- систематика загроз
- шкала вливу/ризику.

Незважаючи на те, що ця початкова версія набору інструментів EU RM надає базову інформацію для сумісної діяльності з оцінки ризиків, очікується, що ця база знань буде збагачена додатковою інформацією, яка сприятиме взаємодії. Така інформація включає нові категорії активів, які виходять за межі цієї початкової категоризації, нові загрози або загрози, пов'язані з конкретними середовищами (наприклад, у промислових середовищах), і списки заходів безпеки, як також пояснюється в Розділі 4.

Додатково до визначень, прийнятих набором інструментів, є зіставлення цих визначень із відповідними компонентами різних методів RM. Для даної методології RM X очікується, що такі відповідності будуть існувати

між термінологією набору інструментів і термінами X, а також між класифікацією активів набору інструментів і категоріями активів X. Подібні відображення очікуються для таксономії загроз і рівнів ризику. Ці відображення матеріалізуються у формі бібліотек і, як і база знань, будуть збагачені за допомогою функціональних компонентів і використовуватимуться зацікавленими сторонами для забезпечення сумісних результатів управління менеджментом. Більше інформації про функціональні компоненти панелі інструментів наведено в розділі 2.3.2

2.3.1.1. Термінологія

Основна мета термінологічного компонента інструментарію полягає в тому, щоб досягти спільного розуміння термінів, пов'язаних з RM, і сприяти взаємодії методологій, які використовують різні терміни для подібних проблем.

У Додатку I наведено базовий набір термінів, які зазвичай використовуються різними системами/методологіями аналізу ризиків. Значення кожного терміна також задокументовано у формі глосарію. Набір термінів разом із їхніми значеннями формує термінологію інструментарію або, іншими словами, спосіб інтерпретації кожного терміна набором інструментів.

Щоб вирішити, які терміни будуть прийняті набором інструментів, терміни та визначення ISO/IEC 27005:2018 та ITSRM2 були ретельно вивчені з метою охоплення, консолідації та зв'язку всіх термінів, згаданих у цих стандартах.

2.3.1.2. Класифікація активів

Ідентифікація активів, які потребують захисту в інформаційній системі, та оцінка їхньої вартості (з точки зору впливу, який зазнає організація у разі інциденту), мають вирішальне значення під час аналізу ризиків. З цього приводу інструментарій пропонує конкретні категорії активів (Додаток II), пояснюючи водночас активи, включені до кожної категорії, як показано нижче.

Основні активи

- Усі основні бізнес-процеси та функції разом із послугами, що надаються зовнішнім сторонам.
- Інформація/дані, що обслуговують конкретний бізнес-процес або діяльність організації.

Допоміжні активи

- Апаратне забезпечення, пристрої та обладнання, включаючи обчислювальні пристрої, мережеві пристрої, засоби масової інформації, пристрої Інтернету речей (IoT), пристрої операційної технології (OT), телекомунікаційні пристрої, периферійні пристрої та пристрої зберігання.
- Програмне забезпечення та програми, такі як системне програмне забезпечення та операційні системи, мікропрограмне забезпечення, проміжне програмне забезпечення, пакетне програмне забезпечення та програми для бізнесу/кінцевих користувачів. Персонал, що стосується ролей, пов'язаних із бізнес-процесами та функціями, підтримкою користувачів, розробкою та підтримкою програмного забезпечення, підтримкою апаратного забезпечення, наданням послуг та управлінням інформацією/даними.
- Розташування та комунальні послуги, включаючи всі відповідні приміщення, такі як будівлі, кімнати, офіси та контейнери, а також основні послуги та комунальні послуги, що надаються зовнішніми операторами/постачальниками, електро- та водопостачання.
- Організаційна інфраструктура, включаючи політику, процедури та допоміжні послуги інформаційно-комунікаційних технологій (ІКТ) (наприклад, телекомунікації, мережа, хмара, хостинг).

Досягнення консенсусу щодо такої класифікації активів сприяє легшій ідентифікації загроз для кожної категорії активів і, таким чином, для кожного члена цієї категорії активів. Крім того, з точки зору сумісності, це дозволяє зацікавленим сторонам легко зіставляти активи своєї організації з категоріями активів, запропонованими набором інструментів.

Подібно до термінології набору інструментів, вибір кожної категорії активів та його членів ґрунтувався на

категоріях, прийнятих ISO/IEC 27005:2018 та ITSRM2, хоча й адаптовано до потреб набору інструментів. Наприклад, у термінології панелі інструментів немає окремої категорії для мережевих компонентів, оскільки вони включені до категорії «Апаратне забезпечення». Крім того, пристрої IoT і OT були класифіковані як апаратні компоненти.

Варто зазначити, що категорія «Організаційна інфраструктура (включаючи ІКТ-послуги)» містить організаційні ролі, політики та процедури, а також ІКТ-послуги, такі як телекомунікації, мережа, хмара та хостинг.

Інша важлива диференціація активів – це основні та допоміжні активи. Основними активами є бізнес-процеси, функції та служби, а також будь-які форми даних. Усе інше вважається допоміжним майном. Таким чином, вони розглядаються як актив, який можна використовувати для обробки та управління основними активами, і, отже, є засобом, за допомогою якого можна отримати доступ до основного активу.

2.3.1.3. Таксономія загроз

Набір інструментів також пропонує таксономію загроз (Додаток III), яка також спирається на вказівки, надані в ISO/IEC 27005:2018 та ITSRM[2].
Подібно до підходу, використаного для побудови класифікації активів, були визначені основні категорії загроз

- природні загрози;
- промислові загрози;
- помилки та ненавмисні збої;
- навмисні напади;
- загрози, пов'язані з обслуговуванням (хмарні сервіси, сервіси, що надаються сторонніми особами).

Після визначення категорій загроз кожну окрему загрозу було включено до певної категорії. Крім того, кожна загроза пов’язана з категоріями активів, на які вона може вплинути (наприклад, загроза може вплинути на апаратне забезпечення, але не на програмне забезпечення), і з наслідками, які вона може спричинити щодо конфіденційності, цілісності та доступності. Нарешті, враховується походження загрози (навмисна, випадкова, екологічна).

2.3.1.4. Шкали впливу/ризику

Рівень ризику інформаційної безпеки є показником ступеня впливу на організацію потенційної події кібербезпеки, і він визначається ймовірністю виникнення загрози та її впливу на активи організації. Зазвичай існує три типи методологій оцінки ризиків інформаційної безпеки: кількісна, якісна та напівкількісна. Якісна оцінка ризику використовує знання та досвід для встановлення ймовірності ризику, тоді як кількісна оцінка ризику використовує об’єктивні факти, які піддаються кількісній оцінці, щоб зрозуміти процес управління ризиками. Напівкількісний метод оцінки ризику зазвичай використовує описові або числові рейтинги.

Метод розрахунку ризику інструментарію EU RM використовує загальноприйняті підходи та враховує вплив і рівні ймовірності для розрахунку ризику інформаційної безпеки відповідно до наступного рівняння.

$$RRRsk = (probabIIIty\ ooo\ occurence\ ooo\ a\ threat) \times (IIIpact\ ooo\ a\ threat)$$

Імовірність виникнення загрози являє собою оцінку ймовірності того, що певна загроза може використовувати конкретну вразливість або сукупність вразливостей. Імовірність настання використовується як один з основних факторів розрахунку ризику більшістю існуючих методів. Однак це не стандартне значення; це залежить від використовуваного методу. Наприклад, ITSRM2 приймає такі рівні ймовірності виникнення ненавмисних загроз: (i) щодня; (ii) кожного місяця; (iii) один раз на рік; (iv) один раз на 10 років; та (v) один раз на століття. З іншого боку, метод управління ризиками Magerit1 використовує чотирирівневу шкалу для оцінки ймовірності виникнення загрози: (i) щоденна; (ii) щомісяця; (iii) Щорічно; та (iv) кожні кілька років.

Набір інструментів EU RM визначає п’ять окремих рівнів ймовірності виникнення загрози. Рівні ймовірності наступні.

- Дуже висока: ймовірність виникнення загрозливої події є майже високою.

o Висока ймовірність виникнення загрозливої події, оскільки існують пов'язані з нею вразливості, якими можна скористатися, а адекватних заходів безпеки для їх захисту немає.

- Високий: ймовірність виникнення загрозливої події.

o Подія загрози, ймовірно, матеріалізується, оскільки існують пов'язані з нею вразливості, якими можна скористатися, і застосовуються неефективні або застарілі заходи безпеки для їх захисту.

- Помірний: потенційно може виникнути загроза.

o Подія загрози потенційно може матеріалізуватися, оскільки існують уразливості, якими можна скористатися, і, незважаючи на заходи безпеки, можна було б застосувати кращі заходи безпеки.

- Низький: загрозлива подія малоймовірна.

o Подія загрози навряд чи реалізується, оскільки всі пов'язані з нею вразливості були покриті відповідними заходами безпеки.

- Дуже низький: загрозлива подія малоймовірна.

o Дуже малоймовірно, що загроза реалізується, оскільки всі пов'язані з нею вразливості були покриті ефективними заходами безпеки.

Рівень впливу є другим параметром, який впливає на результат ризику інформаційної безпеки. Загалом вплив – це рівень збитку, який можна оцінити в результаті різних дій, включаючи, але не обмежуючись, наслідки незаконного розкриття інформації, незаконної модифікації інформації, несанкціонованого знищення інформації або втрати інформації чи доступності інформаційної системи. Вплив використовується більшістю існуючих методів, спрямованих на розрахунок ризику інформаційної безпеки. Однак, як і у випадку з ймовірністю виникнення, вплив також не є стандартним значенням; це залежить від використовуваного методу. Наприклад, шкала впливу в ITSRM2 має 10 різних рівнів. Крім того, вартість залежить від 10 окремих параметрів, таких як фінансові втрати внаслідок події. З іншого боку, метод управління ризиками Monarc2 оцінює вплив від 0 до 4, і його значення залежить від впливу різних параметрів (таких як конфіденційність, цілісність, доступність, репутація, операційні, юридичні, фінансові та особистісні параметри), які можуть бути постраждали після інциденту кібербезпеки.

[1] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en
[2] https://www.monarc.lu/

Інструментарій EU RM визначає наступні п’ять рівнів впливу, які детально описані з точки зору операційних, правових, фінансових та інших наслідків у Додатку IV.

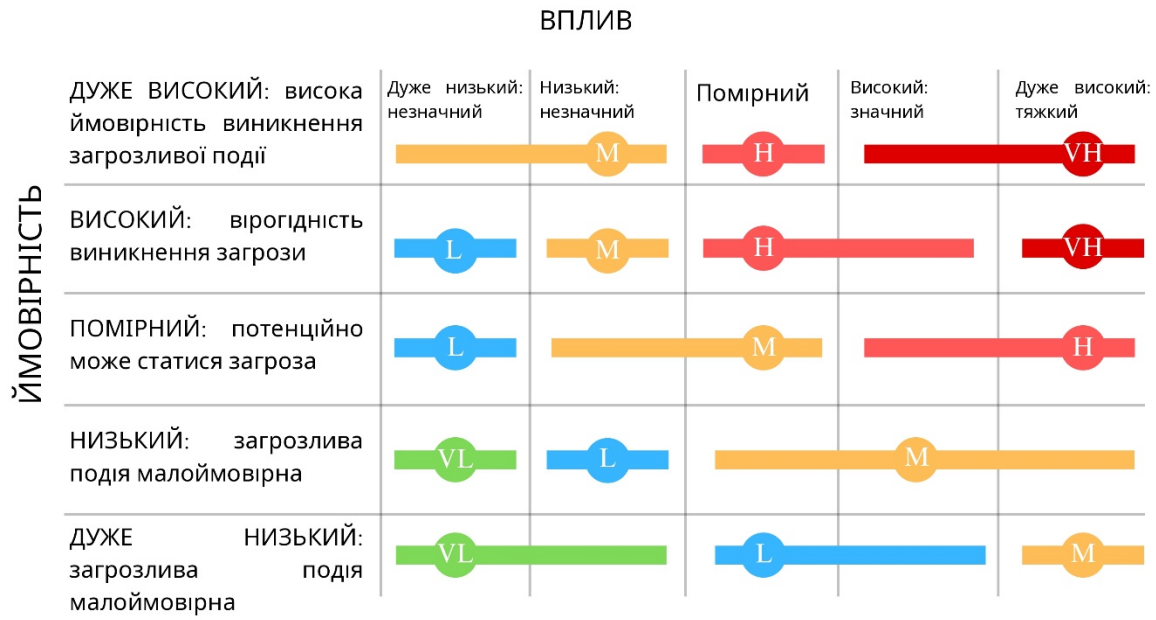
- Дуже високий: серйозний – вплив на організацію вважається серйозним, оскільки очікується, що він матиме екстремальні наслідки та наслідки.
- Високий: значний – вплив на організацію вважається критичним, оскільки очікується, що він матиме серйозні наслідки та наслідки.
- Помірний: помірний – вплив на організацію вважається помірним, оскільки очікується, що він матиме помірні наслідки та наслідки.
- Низький: незначний – вплив на організацію вважається незначним, оскільки очікується, що він матиме незначні наслідки та наслідки.
- Дуже низький: незначний – вплив на організацію вважається незначним, оскільки очікується, що він матиме незначні наслідки та наслідки.

Зауважте, що, залежно від методології управління ризиками, рівні впливу можуть розглядатися на ранніх етапах методу оцінки ризику, де розраховується оцінка активів для організації.

Розглянувши рівень впливу на активи організації та ймовірність виникнення загрозливої події, слід розрахувати рівні ризику нестандартизованим способом. Різні методи RM використовують різні підходи. Наприклад, ITSRM2 обчислює ризик, який коливається від 1 до 50, розділяючи його на п’ять окремих діапазонів. З іншого боку, Monarc оцінює ризик від 0 до 16 у трьох діапазонах.

Незважаючи на те, що багато методів не класифікують і не відображають значення ризику за рівнями, для загального розуміння відповідних значень ризику та рівнів ризиків, яким зазнає організація щодо конкретних загроз, інструментарій визначає шкалу, яка включає п’ять таких рівнів ризику, які сприятимуть сумісності оцінка значень ризику, про які повідомляють організації. Ці рівні сильно залежать від різних рівнів впливу та ймовірності, як показано на матриці ризиків, показаній на рисунку 2. Деталі рівнів ризику – дуже низький (VL), низький (L), помірний (M), високий (H) і дуже високий (VH) – аналізуються в Додатку V. Ми можемо помітити, що п’ять дискретних рівнів ризику кібербезпеки походять від конкретних сценаріїв, які поєднують різні рівні впливу та ймовірності.

Малюнок 2: Матриця ризиків інструментарію EU RM



2.3.2. Functional components

Функціональні компоненти інструментарію EU RM забезпечують відображення між базою знань інструментарію (термінологія, активи, загрози, шкала ризиків) і відповідними компонентами, прийнятими різними методологіями RM. Більш конкретно, очікуваний внесок функціональних компонентів інструментарію EU RM – це підтримка порівняння результатів, отриманих різними методологіями RM, і сприяння загальному розумінню різних термінів, прийнятих ними.

Функціональні компоненти інструментарію EU RM наведені нижче:

- термінологічне картографування
- картографування активів
- відображення загроз
- картування рівнів ризику.

Як уже було зазначено, через базу знань набір інструментів пропонує конкретні терміни управління менеджментом, категорії активів, категорії загроз і рівні ризику. Функціональність, яку забезпечують вищезазначені компоненти, дозволяє зіставляти терміни/значення/категорії інструментарію з відповідними, що використовуються в інших методологіях RM. Це відображення вже виконано між пропозиціями інструментарію та ISO/IEC 27005:2018 та ITSRM2.
Проте очікується, що база знань інструментарію буде постійно розширюватися. Очікується, що це буде досягнуто спільнотою під час оцінки сценаріїв ризику, використовуючи, наприклад, методики, які досі не розглядалися, а отже, не включені в базу знань інструментарію. У цьому випадку залучені сторони повинні докласти зусиль, щоб провести це відображення сумісності між відповідними компонентами, і результат може поповнити бібліотеки інструментів і базу знань, які будуть використані в подальших діях.

3. Спосіб застосування

У цьому розділі описано, як інструментарій EU RM буде використовуватися зацікавленими сторонами, які включають, але не обмежуються, наступні групи.

- Групи реагування на інциденти комп'ютерної безпеки та національні чи інші компетентні органи, такі як компетентні органи держав-членів з мережевих та інформаційних систем (NIS), на рівні держав-членів, ЄС або на міжнародному рівні, які мають (законний) інтерес оцінювати організації. рівні ризику або готовність проти конкретних загроз. Ці організації можуть працювати в певному домені чи географічному регіоні.
- Співпрацюючі організації в певній області чи географічній зоні, зі схожими проблемами та інтересами.
- Окремі організації, які з часом можуть використовувати різні інструменти оцінки ризиків.

Інструментарій EU RM може допомогти вищезазначеним суб'єктам встановити спільні основи щодо того, як вони оцінюють ризики у своєму середовищі, і мати спільне розуміння відповідних рівнів ризику та порівнянних результатів.

Після того, як компетентний орган або організація прийме рішення про розгортання інструментарію EU RM для вирішення проблем сумісності RM, вона повинна включити методологію EU RM інструментарію в свою стратегію RM. Очікується, що ця інтеграція не вплине на існуючу практику оцінки ризиків, оскільки інструментарій і його відповідні компоненти лише інкапсулюють існуючі процеси управління менеджментом для надання сумісних результатів.

На роль кожного з компонентів панелі інструментів у цьому процесі впливає сценарій використання. Передбачено два основні сценарії використання інструментарію..

1. Оцінка готовності організації проти конкретної загрози. У цьому випадку для певного набору сценаріїв ризику буде використано інструментарій EU RM.
2. Оцінка стану безпеки організації в цілому або для конкретної послуги. У цьому випадку організації запустять процес оцінки ризиків, розроблять різні сценарії ризиків і оцінять ризики для кожного з них, і зосередяться лише на компоненті рівнів ризику в набір інструментів, щоб звітувати про результати.

У наступному розділі ми надаємо детальну інформацію про перший сценарій, який передбачає використання всіх компонентів панелі інструментів.

3.1. Основні поняття і терміни

Набір інструментів EU RM (також згадуваний у цьому документі як «набір інструментів») надає засоби для оцінки рівнів ризику, пов'язаного з несприятливими подіями, адаптованими до середовища організації та відмінними рисами відповідних підходів RM, прийнятих організаціями. Перш ніж надавати деталі про інструментарій EU RM, корисно надати опис основних понять і термінів, які використовуються в цьому документі.

Терміни сценарій ризику та сценарій атаки використовуються як синоніми для позначення опису можливої несприятливої події, яка може вплинути на стратегію та цілі організації. Сценарій атаки описує активи, які знаходяться під загрозою або залучені до сценарію ризику, фактичну загрозу та аспект безпеки активів, на який ця загроза може вплинути.

Набір інструментів EU RM розроблено для розгляду сценаріїв ризику або їх набору, які пов'язані з конкретним кроком атаки та є частиною сценарію використання. Цей підхід здебільшого підходить, коли зацікавлені сторони мають розглянути зловмисну діяльність, пов'язану з кампанією, яка обов'язково включає набір сценаріїв атак. Однак це не виключає використання інструментарію для оцінки сценаріїв одиничних атак, пов'язаних із методами гранульованих атак і конкретними активами.

Кожен сценарій атаки зазвичай є частиною етапу атаки, як показано на малюнку 3. Так само сценарій використання може включати кілька кроків атаки, які організації повинні оцінити.

Малюнок 3: Сценарії використання, етапи атаки та сценарії атаки

3.2. Оцінка ризику щодо конкретної загрози

Припустімо, що компетентний орган NIS, Група співробітництва NIS або інший компетентний орган хоче визначити рівні ризику в ЄС щодо виниклої загрози. Деталі цієї загрози та типи систем, на які вона спрямована, утворюють так званий сценарій інциденту, який компетентний орган хоче оцінити. Компетентний орган прагне визначити рівні ризику для конкретної групи організацій, які належать до цільової групи суб'єктів загрози.

Щоб мати можливість порівнювати звітні результати, організації повинні надавати порівнювані результати компетентному органу, використовуючи загальну еталонну систему, на відміну від відповідних результатів, наданих їх відповідними інструментами управління менеджментом. У той же час, щоб мати загальне розуміння сценаріїв, які вони повинні розглянути, організації повинні мати можливість однозначно адаптувати сценарій, описаний компетентним органом, до своїх власних інструментів і середовища, щоб усі пов'язані атаки/ розглядаються сценарії ризику, які є частиною загального сценарію інциденту.

Враховуючи, що сценарій інциденту передбачає багато сценаріїв атаки/ризику (див. Розділ 3.1), які відображаються на шляху атаки, компетентний орган хоче знати рівні ризику, пов'язані з кожним кроком цього шляху. Зазвичай це означає, що кожен сценарій атаки має бути представлений як набір триплетів, кожен з яких містить <актив(и), загроза(и), вплив>, які використовуватимуться як основа для розрахунку відповідних рівнів ризику. У той час як вплив відображає добре встановлені параметри безпеки (конфіденційність (C), цілісність (I) і доступність (A)), активи та загрози не мають загальноприйнятих класифікацій і списків. Відповідні компоненти набору інструментів використовуватимуться для визначення сценаріїв ризику, які потім необхідно адаптувати до кожного методу управління ризиками за допомогою відображень набору інструментів. Зважаючи на це, використання інструментарію EU RM вимагає наступних кроків.

1. Компетентний орган установлює набір сценаріїв атаки/ризику, які або відповідають шляху атаки виниклої загрози, або компетентний орган вважає важливими для оцінки. Сценарії атак повинні використовувати терміни інструментарію, список активів і список загроз.

2. Організації-учасники мають відобразити визначені сценарії атаки/ризику у своєму середовищі, щоб дозволити їм оцінити відповідні ризики за допомогою їх власної методології. Цей процес вимагає використання бібліотек панелі інструментів, які вже можуть мати відображення щодо обраної організацією методології RM. Якщо такі відображення недоступні, вони повинні бути відповідним чином збагачені. На кожному з цих кроків організація повинна ознайомитися з термінами інструментарію, щоб однозначно інтерпретувати кожен сценарій атаки/ризику.

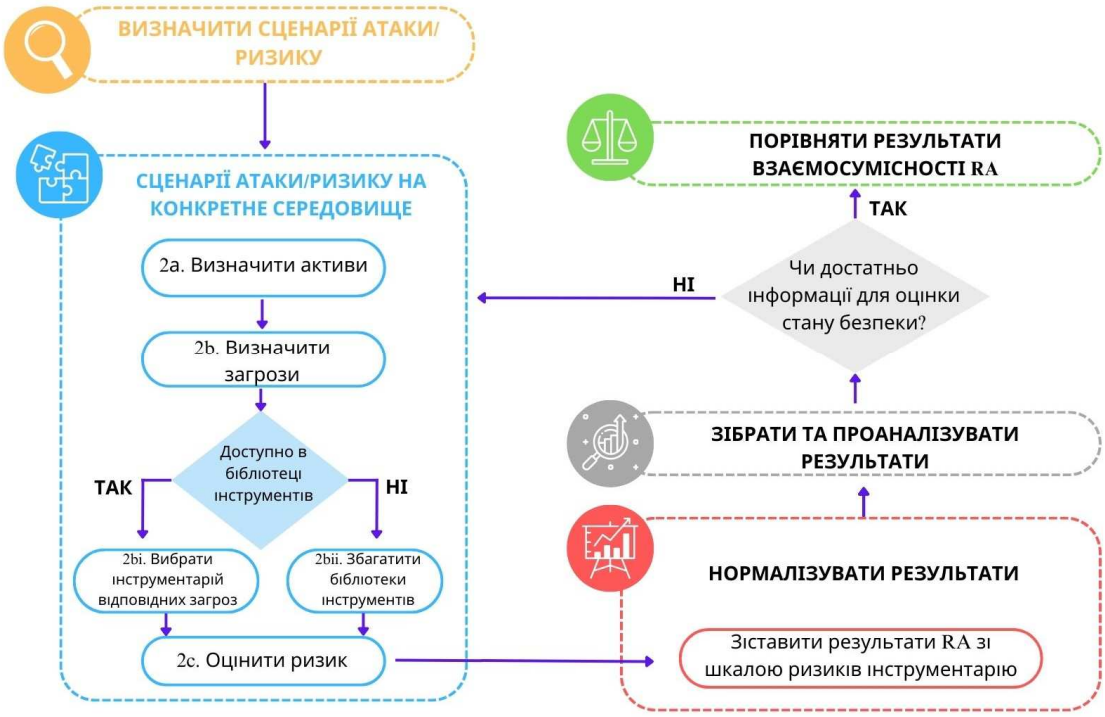
a. Точніше, організація встановлює контекст для досліджуваного сценарію інциденту. Тобто він має визначити активи, які беруть участь у сценаріях атаки/ризику, і зіставити їх із середовищем і типами активів, які визначає їхня методологія. Як зазначалося вище, бібліотеки панелі інструментів можуть уже забезпечувати відображення активів панелі інструментів на типи активів методології організації. Якщо ні, експерти-учасники мають запропонувати своє відображення та збагатити бібліотеки інструментів.
b. Після встановлення контексту та визначених активів організація має однозначно визначити загрози, на які спрямовані сценарії атаки/ризику сценарію інциденту. Список загроз, на які спрямований сценарій інциденту, взято з таксономії загроз інструментарію, яка не обов'язково безпосередньо відповідає таксономії загроз методології організації. Щоб подолати цю прогалину, необхідно розробити бібліотеку відображення загроз для відповідної методології ризиків, якщо такої ще немає. Ця бібліотека відображення загроз буде поступово збагачуватися. Зверніть увагу, що під час цього процесу нові загрози або категорії загроз також можуть бути введені в таксономію загроз інструментарію. Отже, як і зі списком активів, є два випадки.
    i. Зіставлення між прийнятим набором інструментів списком загроз і списком загроз, обраних організацією, вже доступне в бібліотеці інструментарію. У цьому випадку організація повинна вибрати відповідні загрози для сценаріїв атаки/ризику.
    ii. Немає доступного відображення, тому організація має виконувати це завдання всередині себе та, як наслідок, збагачувати бібліотеки інструментів.
c. Визначивши та відобразивши список активів і загроз, організація повинна оцінити ризики для кожного із запитуваних сценаріїв атаки/ризику. Якщо метод враховує вразливі місця в процесі оцінки ризиків, вони повинні бути належним чином визначені для задіяних активів і використані в процесі розрахунку ризиків.

3. Розраховані значення ризику для відповідних сценаріїв ризику надають цінну інформацію організації, яка використовує певні методології. Однак ця інформація не має значення для компетентного органу, який не хоче або не повинен знати особливості кожного методу контролю ризиків. Останнім кроком у процесі використання інструментарію є нормалізація результатів оцінки ризику до шкал ризику інструментарію. Це можна зробити за допомогою бібліотек набору інструментів, якщо існує таке відображення між шкалами ризику набору інструментів і шкалами методології управління менеджментом організації. Якщо ні, організація повинна розпочати процес картографування та збагатити бібліотеки інструментів.

4. Компетентний орган збирає результати вищезазначеного процесу, який виконується в середовищі організації, і на основі повідомлених результатів він або має інформацію, необхідну для оцінки стану безпеки організації, або повинен сам виконати останній крок.

Зауважте, що в цьому процесі не всі початково визначені сценарії атаки/ризику обов'язково застосовуються до всіх середовищ. Залежно від системного моделювання організації та залежностей між загрозою та основними активами та того, як загроза може вплинути на основний актив через інші додаткові допоміжні активи, організація вирішить застосовність кожного зі сценаріїв атаки/ризику.

Малюнок 1: Діаграма процесів EU RM toolbox



3.3. Процес розробки варіантів використання

Набір інструментів може використовуватися компетентним органом для оцінки рівнів ризику організації щодо сценарію інциденту. Сценарій інциденту, як визначено раніше, використовується компетентним органом для опису набору загроз, щодо яких організації-учасники оцінюватимуть свою позицію. Він спрямований на те, щоб допомогти організаціям розглянути конкретні загрози та звузити діапазон шляху атаки та кількість сценаріїв атаки/ризику, які мають розглянути організації-учасники. Таким чином, передбачається, що сценарій інциденту включатиме наступну інформацію.

1. **Опис сценарію.** This outlines the incident scenario that the competentauthority addresses in the scenario.
2. **Показові активи за обсягом.** Сценарій має надати перелік активів, основних або допоміжних, на які впливають або використовуються суб'єктами загрози під час їх кампанії.
3. **Шлях атаки.** У ньому описано кроки, які зазвичай виконують суб'єкти загрози, щоб дати учасникам краще зрозуміти сценарій інциденту та набір загроз, які досліджуються.
4. **Сценарії атаки.** Вони утворюють список триплетів про задіяні або зачеплені активи, розглянуту загрозу та відповідний вплив (тобто вимір безпеки, на який впливає ця загроза) для відповідних кроків, описаних у шляху атаки.

Приклад використання можна знайти в Додатку VIII.

4. Розвиток інструментарію

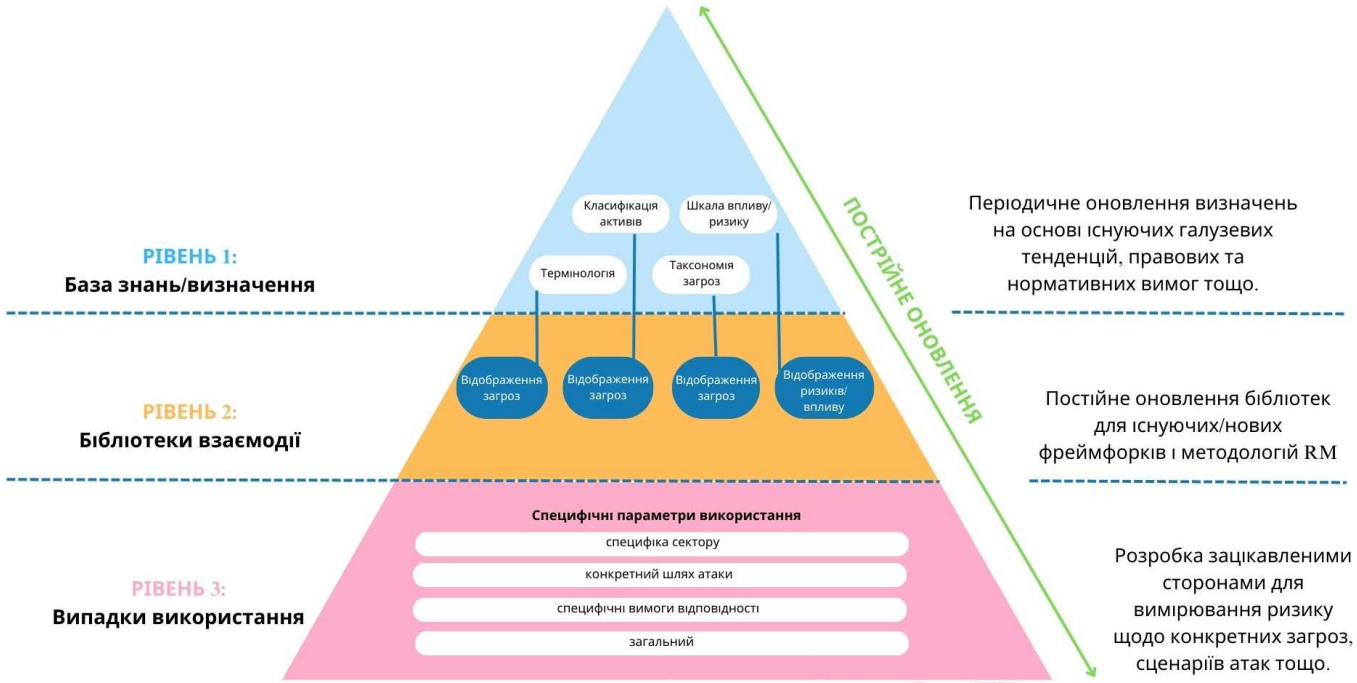
Набір інструментів EU RM передбачається як довідковий інструмент, який буде збагачений додатковою інформацією для досягнення поставлених цілей. Очікується, що це станеться на різних рівнях, які відповідають базі знань інструментарію, яка містить набір визначень інструментарію (тобто термінологія, класифікація активів, таксономія загроз і масштаб впливу/ризику), а також відображення інших компонентів методології, як показано на малюнку 5.

Очікується, що визначення набору інструментів будуть переглянуті та збагачені спільнотою, щоб задовольнити потреби всіх доменів, які приймуть набір інструментів EU RM. Приклади цих удосконалень включають обґрунтування впливу для різних рівнів, які адаптовані до конкретних областей, таких як енергетична сфера, або набір загроз, які є більш значущими для конкретної області.

Іншим важливим компонентом інструментарію EU RM є набір бібліотек сумісності, які забезпечать відображення визначень інструментарію інших методологій RM. Ці бібліотеки можуть бути результатом використання набору інструментів спільнотою, де залучені сторони пройдуть процес проведення цього відображення між набором інструментів і власними компонентами методології RM, якщо вони ще не доступні, і нададуть свої відгуки збагачувати бібліотеки панелі інструментів. Це допоможе подальшим зусиллям або користувачам і призведе до інтегрованого інструменту, який допоможе організаціям порівнювати свої рівні ризику.

Подібно до визначень і бібліотек сумісності, третій набір цінної інформації, яка доповнює набір інструментів, — це описи варіантів використання, які можуть виступати або як шаблони для подальших процесів оцінки ризиків, або як конкретні сценарії, які можна застосовувати в доменах або організаціях.

Малюнок 2: Розвиток інструментарію EU RM



5. Висновки

У цьому документі представлено основні компоненти інструментарію ЄС щодо управління ризиками, який служить еталонною основою для узгодження різних зусиль з управління ризиками та, таким чином, досягнення загального розуміння ризиків і пов’язаних з ними рівнів ризику, незалежно від прийнятого підходу до управління ризиками та використовуваного інструменту(ів). організаціями.

За допомогою запропонованого ЄС інструментарію управління ризиками різні зацікавлені сторони зможуть порівнювати свої результати управління ризиками для конкретних сценаріїв ризику з іншими організаціями, які можуть використовувати різні методи/інструменти управління ризиками. Крім того, регулюючі та наглядові органи отримають підтримку щодо загального уявлення про рівні ризику та стан безпеки організацій у певному секторі або в різних секторах.

Основні функції RM, які підтримуються набором інструментів EU RM:

- встановлення спільного розуміння щодо діяльності, яка виконується під час процесу RM;
- визначення обсягу середовища, в якому буде застосовуватися процес оцінки ризику;
- визначення сценаріїв ризику, пов'язаних із конкретною загрозою або загрозами, які розслідуються;
- зіставлення розрахованих рівнів ризику з рівнями, визначеними спільною шкалою ризиків.

Важливо підкреслити, що база знань, надана набором інструментів (набори термінів, класифікація активів і загроз), буде динамічно збагачуватися, щоб охоплювати додаткові методи та інструменти разом з іншими областями.

Крім того, наступні версії набору інструментів можуть прагнути до розробки загального набору заходів, які також будуть зіставлені з різними методами, щоб сприяти належному та єдиному обробленню ризиків.

A Додаток I – Термінологія панелі інструментів

Цей додаток містить перелік термінів, які формують термінологію нструментарію.

Таблиця 1: Термінологія сумісного інструментарію EU RM

Основи та методології / термінологія	Глосарій інструментарію	Пов'язані терміни
Управління доступом	Засоби для забезпечення авторизації та обмеження доступу до активів відповідно до вимог бізнесу та безпеки..	-
Актив	Актив — це все, що має цінність для організації і тому потребує захисту. Для ідентифікації активів слід мати на увазі, що інформаційна система складається не лише з апаратного та програмного забезпечення.	-
Власник активу	Власник активу має бути визначений для кожного активу, щоб забезпечити відповідальність і звітність за актив. Власник активу, можливо, не має прав власності на актив, але несе відповідальність за його виробництво, розвиток, технічне обслуговування, використання та безпеку відповідно. Власник активу часто є найбільш підходящою особою для визначення цінності активу для організації.	Системний власник
Вартість активів	Вартість активу, оцінена з точки зору максимального впливу (захист бізнесу або даних) у разі втрати параметрів безпеки (конфіденційність, цілісність, доступність); це також відомо як потреба безпеки.	Необхідність безпеки інформаційних технологій (IT).
Шлях атаки	Набір навмисних дій для реалізації сценарію загрози.	-
Сценарій атаки	«Сценарій ризику».	Сценарій ризику
Крок атаки	Набір сценаріїв атак, пов’язаних зі зловмисною діяльністю.	-
Атака	Спроба знищити, викрити, змінити, вивести з ладу, викрасти або отримати несанкціонований доступ або несанкціоноване використання активу.	-
Аудит	Систематичний, незалежний та задокументований процес отримання аудиторських доказів та їх об’єктивної оцінки для визначення ступеня дотримання критеріїв аудиту.	-
Події аудиту	Переконайтеся, що дії в системі залишають записи, які забезпечують надійне розслідування інцидентів безпеки.	-
Обсяг аудиту	Обсяг і межі аудиту.	-
Аутентифікація	Надання впевненості в тому, що заявлена характеристика суб’єкта є правильною.	-
Автентичність	Власність, якою суб’єкт є те, за що себе видає.	-

Власність, якою суб'єкт є те, за що себе видає	Глосарій інструментарію	Пов'язані терміни
Наявність	Властивість бути доступною та використовуватися за запитом уповноваженої особи.	-
Базовий захід	Міра, визначена в термінах атрибута та методу його кількісного визначення.	-
Керуючий справами	Роль, відповідальна за те, щоб функція організації відповідала потребам бізнесу та користувачів.	-
Компетентність	Здатність застосовувати знання та навички для досягнення бажаних результатів.	-
Комунікаційно-інформаційна система (CIS)	Будь-яка система, що дозволяє обробляти інформацію в електронній формі, включаючи всі активи, необхідні для її роботи, разом з інфраструктурою, організацією, персоналом та інформаційними ресурсами. Це визначення включає бізнес-додатки, спільні IT-послуги, аутсорсингові системи та пристрої кінцевих користувачів.	Інформаційна система
Конфіденційність	Власність, інформація про яку не надається або не розкривається неавторизованим особам, організаціям або процесам.	-
Відповідність	Виконання вимог.	-
Наслідки	Результат події, що впливає на цілі.	-
Постійне вдосконалення	Повторювана діяльність для підвищення продуктивності.	Безперервність інформаційної безпеки
Контроль	Захід, що змінює ризик – контроль також використовується як синонім захисту або протидії.	Міра-запобіжний захід
Контрольна мета	Заява, що описує, що має бути досягнуто в результаті впровадження заходів контролю.	-
Корекція	Дії щодо усунення виявленої невідповідності.	-
Коригувальні дії	Дії для усунення причини невідповідності та запобігання повторенню.	-
Контролер даних	Фізична чи юридична особа, державний орган, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних.	-
Власник даних	Особа, відповідальна за забезпечення захисту та використання певного набору даних, який обробляє CIS.	-
Набір даних	Набір інформації, яка обслуговує певний бізнес-процес або діяльність.	-
Суб'єкт даних	Будь-яка особа, чиї персональні дані збираються, зберігаються або обробляються.	-
Похідний захід	Міра, яка визначається як функція двох або більше значень базових мір.	-

Основи та методології / термінологія	Глосарій інструментарію	Пов'язані терміни
Документально підтверджена інформація	Інформація, яку організація повинна контролювати та підтримувати, а також носій, на якому вона міститься.	-
Легкість	Оцінка зусиль, необхідних для реалізації даної навмисної загрози.	-
Ефективність	Ступінь реалізації запланованих заходів і досягнення запланованих результатів.	-
Подія	Виникнення або зміна певного збігу обставин. Іноді подію можна назвати інцидентом або нещасним випадком.	Інцидент
Зовнішній контекст	Зовнішнє середовище, в якому організація прагне досягти своїх цілей.	-
Частота	Опис кількісних або якісних значень, що використовуються для вираження періодичності випадкових загроз від матеріалізації.	-
Функціонал	Обробка інформації включає всі функції CIS щодо наборів даних, включаючи створення, модифікацію, відображення, зберігання, передачу, видалення та архівування інформації. Обробка інформації може надаватися KIC як набір функціональних можливостей для користувачів і як IT-сервіси для інших CIS.	-
Управління інформаційною безпекою	Система, за допомогою якої діяльність організації з інформаційної безпеки спрямовується та контролюється.	-
Керуючий орган	Особа або група людей, які відповідають за продуктивність і відповідність організації.	-
Вплив	Несприятлива зміна рівня досягнутих бізнес-цілей.	-
Сценарій впливу	Комбінація основного активу, параметра безпеки (конфіденційність, цілісність або доступність), типу впливу, наслідків і рівня, пов’язаного з найгіршими сценаріями, описаними організацією для визначення вартості основних активів.	-
Інцидент	Подія, яка була оцінена як така, що має фактичний або потенційно несприятливий вплив на безпеку або продуктивність системи. Іноді подію можна назвати інцидентом або нещасним випадком.	Подія
Сценарій інциденту	Сценарій інциденту — це опис загрози, яка використовує певну вразливість або набір уразливостей в інциденті інформаційної безпеки. Вплив сценаріїв інцидентів необхідно визначити з урахуванням критеріїв впливу, визначених під час діяльності зі встановлення контексту. Це може вплинути на один або кілька активів або частину активу. Таким чином, активам можуть бути присвоєні значення як через їхню фінансову вартість, так і через бізнес-наслідки, якщо вони пошкоджені або скомпрометовані. Наслідки можуть бути тимчасовими або постійними, як у випадку знищення активу.	-

Основи та методології / термінологія	Глосарій інструментарію	Пов'язані терміни
Індикатор	Міра, яка забезпечує оцінку або оцінку.	-
Внутрішній ризик	Ризик без урахування заходів безпеки. Внутрішній ризик представляє обсяг ризику, який існує за відсутності засобів контролю (Інститут FAIR). Внутрішній ризик – це поточний рівень ризику з огляду на існуючий набір засобів контролю, а не гіпотетичне уявлення про відсутність будь-яких засобів контролю (Інститут FAIR). ISO не визначає поняття невід'ємного ризику, але його можна визначити за допомогою протиставлення поняттю залишкового ризику як: ризик, що існує до обробки ризику.	-
Інформаційна потреба	Розуміння, необхідне для управління цілями, цілями, ризиками та проблемами.	-
Засоби обробки інформації	Будь-яка система обробки інформації, послуга чи інфраструктура або фізичне розташування, у якому вони розміщені.	-
Інформаційна безпека	Збереження конфіденційності, цілісності та доступності інформації.	-
Безперервність інформаційної безпеки	Процеси та процедури для забезпечення безперервних операцій із забезпечення інформаційної безпеки.	Постійне вдосконалення
Захід інформаційної безпеки	Виявлений стан системи, служби чи мережі, що вказує на можливе порушення політики інформаційної безпеки чи збій засобів керування, або раніше невідому ситуацію, яка може мати значення для безпеки.	-
Інцидент інформаційної безпеки	Подія, яка може негативно вплинути на конфіденційність, цілісність або доступність CIS.	-
Управління інцидентами інформаційної безпеки	Набір процесів для виявлення, звітування, оцінки, реагування на інциденти інформаційної безпеки, роботи з ними та навчання на них.	-
Професійна система управління інформаційною безпекою	Особа, яка встановлює, впроваджує, підтримує та постійно покращує один або більше процесів системи управління інформаційною безпекою.	Менеджер ризиків у сфері безпеки
Спільнота обміну інформацією	Група організацій, які погоджуються обмінюватися інформацією.	-
Інформаційна система	Набір програм, служб, IT-активів або інших компонентів обробки інформації..	CIS
Цілісність	Властивість точності та повноти.	-
Інтерес	Рівень зацікавленості супротивника вчинити загрозу щодо даного основного активу.	-
Зацікавлена сторона (бажаний термін) – зацікавлена сторона (допущений термін)	Особа чи організація, яка може вплинути на рішення чи діяльність, зазнати впливу або вважати себе такими, що на них впливає рішення чи діяльність..	Організація зацікавлених сторін

Основи та методології/ термінологія	Глосарій інструментарію	Пов'язані терміни
Внутрішній контекст	Внутрішнє середовище, в якому організація прагне досягти своїх цілей.	-
Потреба в IT-безпеці	Див. «Вартість активів».	Вартість активів
Ризик безпеки IT	Див. «Ризик»	Ризик
Рівень ризику	Величина ризику, виражена в термінах поєднання наслідків та їхньої ймовірності.	-
Ймовірність	Ймовірність того, що щось станеться.	-
Офіцер місцевої інформаційної безпеки	Офіцер, який відповідає за зв'язок із IT-безпекою для комісійного відділу.	-
Система управління	Набір взаємопов'язаних або взаємодіючих елементів організації для встановлення політики та цілей і процесів для досягнення цих цілей.	-
Виміряти	Див. «Заходи безпеки»	Захід безпеки – контроль
Вимірювання	Процес визначення значення.	-
Функція вимірювання	Алгоритм або обчислення, які виконуються для поєднання двох або більше базових показників.	-
Метод вимірювання	Логічна послідовність операцій, описана у загальному вигляді, яка використовується для кількісного визначення атрибута щодо заданої шкали.	-
Фактор пом'якшення	Відсоток ризику (ймовірності та/або наслідків), який зменшується заходом безпеки.	-
Моніторинг	Визначення статусу системи, процесу або діяльності..	-
Невідповідність	Невиконання вимоги.	-
Незаперечування	Переконайтеся, що суб'єкти, які виконували певні типи дій, не можуть пізніше фальшиво заперечити, що вони їх виконали.	-
Мета	Результат, якого потрібно досягти.	-
Організація	Див. «Зацікавлена сторона».	Зацікавлена сторона – стейкхолдер
Аутсорсінг	Укладіть угоду, згідно з якою зовнішня організація виконує частину функцій або процесу організації.	-
Продуктивність	Вимірний результат.	-
Особисті дані	Будь-яка інформація, що стосується ідентифікованої або ідентифікованої фізичної особи (суб'єкта даних).	-

Основи та методології / термінологія	Глосарій інструментарію	Пов'язані терміни
Поліція	Наміри та напрямок організації, офіційно виражені її вищим керівництвом.	-
Потенційний супротивник	Особа або група, зацікавлена у провокуванні втрати конфіденційності, цілісності та/або доступності активів організації.	-
Потужність	Поєднання знань про потенційного супротивника, його можливостей і ресурсів для успішного виконання атаки.	-
Основний актив	Дані та бізнес-процеси/функції.	-
Процес	Набір взаємопов'язаних або взаємодіючих дій, які перетворюють входи на результати.	-
Реабілітація	Властивість послідовної запланованої поведінки та результатів.	-
Вимога	Потреба чи очікування, які виражені, зазвичай маються на увазі або є обов'язковими.	-
Залишковий ризик	Ризик, що залишився після обробки ризику.	-
Огляд	Діяльність, здійснювана для визначення придатності, адекватності та ефективності предмета дослідження для досягнення встановлених цілей.	-
Об'єкт огляду	Перевіряється конкретна позиція.	-
Мета огляду	Заява, що описує, що має бути досягнуто в результаті перевірки.	-
Ризик	Вплив невизначеності на цілі.	Ризик безпеки IT
Прийняття ризику	Технічне завдання, згідно з яким приймається ризик.	-
Критерії прийнятності ризику	Критерії, які використовуються для прийняття ризику.	-
Аналіз ризиків	Процес розуміння природи ризику та визначення рівня ризику.	-
Оцінка ризику	Загальний процес ідентифікації, аналізу та оцінки ризиків.	-
Уникнення ризику	Діяльність або стан, що створює певний ризик, якого слід уникати.	-
Повідомлення про ризики та консультації	Набір безперервних і повторюваних процесів, які організація проводить для надання, обміну або отримання інформації та для вступу в діалог із зацікавленими сторонами щодо управління ризиками.	-
Критерії ризику	Технічне завдання, за яким оцінюється значущість ризику.	-

Основи та методології / термінологія	Глосарій інструментарію	Пов'язані терміни
Оцінка ризику	Процес порівняння результатів аналізу ризику з критеріями ризику для визначення того, чи є ризик та/або його величина прийнятними або допустимими.	-
Ідентифікація ризиків	Процес пошуку, розпізнавання та опису ризиків.	-
Управління ризиками	Скоординована діяльність з управління та контролю над організацією щодо ризику.	-
Процес управління ризиками	Систематичне застосування управлінської політики, процедур і практики до діяльності з комунікації, консультування, встановлення контексту та ідентифікації, аналізу, оцінки, обробки, моніторингу та перегляду ризику.	-
Зменшення ризику	Лікування ризику, яке бореться з негативними наслідками.	-
Модифікація ризику	A process where the level of risk is managed by introducing,removing or altering controls so that the residual risk can bereassessed as being acceptable.	-
Власник ризику	Особа або організація, яка має відповідальність і повноваження керувати ризиком.	-
Зниження ризику	Дії, вжиті для зменшення ймовірності, негативних наслідків або обох, пов’язаних із ризиком.	-
Утримання ризику	Варіант лікування ризику, коли ризик зберігається без подальших дій.	-
Сценарій ризику	Поєднання залучених активів, загрози та порушеного аспекту безпеки.	Сценарій нападу
Розподіл ризиків	Sharing the risk with another party that can most effectivelymanage the particular risk depending on risk evaluation.	-
Дослідження ризиків	Набір зібраної інформації та результатів, отриманих під час виконання заходів RM. В основному він складається з: — характеристика СНД та її середовища; — ризики з властивим і залишковим рівнями; — заходи безпеки.	-
Передача ризику	Розподіл з іншою стороною тягаря збитків або прибутку на ризик. Замінено на «Розподіл ризиків».	-
Лікування ризику	Процес зміни ризику. Це може включати: — уникнення ризику шляхом прийняття рішення не починати або продовжувати діяльність, яка породжує ризик; — прийняття або збільшення ризику з метою використання можливості; — усунення джерела ризику; — зміна ймовірності;	-

Основи та методології / термінологія	Глосарій інструментарію	Пов'язані терміни
	— зміна наслідків; — розподіл ризику з іншою стороною або сторонами (включаючи контракти та фінансування ризику); — збереження ризику шляхом усвідомленого вибору.	
Захід безпеки	Дійсний контроль, який можна запровадити відповідно до рівня пріоритету для зменшення ризику.	Міра – контроль
Менеджер ризиків безпеки	Особа, відповідальна за діяльність RM.	Система управління інформаційною безпекою професійна
Масштаб	Упорядкований набір значень, безперервний чи дискретний, або набір категорій, на які зіставляється атрибут.	-
Обслуговування	Послуга — це засіб обробки даних (наборів даних і функцій) клієнтам, внутрішнім або зовнішнім. IT-послуга складається з поєднання IT-продуктів (апаратного та програмного забезпечення), людей і місць розташування.	-
Спільне обслуговування	Послуга надається спільно, коли її дослідження ризиків публікується, повністю або частково, її постачальником послуг для повторного використання в дослідженнях ризиків CIS, які використовують послугу.	-
Зацікавлені сторони	Внутрішні та зовнішні організації або люди, зацікавлені в даних і функціях цільової системи.	Зацікавлена сторона – організація
Рівень вишуканості	Шкала, що використовується для вимірювання технічного рівня впровадження (ефективності) заходів безпеки.	-
Допоміжний актив	Активи, які використовуються або залучаються до обробки даних і функцій/послуг, що надаються цільовою системою.	-
Системна модель	Представлення архітектури системи щодо допоміжних активів, які використовуються для керування даними та функціями (основними активами), якими керує цільова система.	-
Власник системи	Особа, відповідальна за загальну закупівлю, розробку, інтеграцію, модифікацію, експлуатацію, обслуговування та виведення з експлуатації CIS.	Власник активу
Офіцер системної безпеки	Консультує власника системи, системного менеджера та менеджера проекту щодо підходу до IT-безпеки та бере активну роль як експерт з IT-безпеки, щоб визначити вимоги до IT-безпеки та допомагає в архітектурі, проектуванні, реалізації та верифікації IT-безпеки.	-
Стандарт реалізації безпеки	Документ, що визначає дозволені способи здійснення безпеки.	-
Об'єкт заходу безпеки	Місце, де захід може бути фактично реалізований. Такою метою може бути організація (наприклад, загальна політика безпеки), система (наприклад, RM, перегляд коду, сканування вразливостей) або певний допоміжний актив (наприклад, шифрування на каналі передачі даних або жорсткому диску, контроль доступу до операційної системи).	-

Основи та методології / термінологія	Глосарій інструментарію	Пов'язані терміни
Цільова система	Конкретний CIS підлягає виконанню процесу RM.	-
Загроза	Потенційна причина небажаного інциденту, який може завдати шкоди системі чи організації.	-
Сценарій загрози	Набір окремих подій загрози, пов’язаних із певним джерелом загрози або кількома джерелами загрози, частково впорядкованих у часі.	-
Вище керівництво	Особа або група людей, які керують і контролюють організацію на найвищому рівні.	-
Довірений інформаційний комунікаційний суб’єкт	Автономна організація, що підтримує обмін інформацією в межах спільноти обміну інформацією.	-
Користувач	Будь-яка особа, яка використовує функціональні можливості, надані CIS, як всередині, так і за межами організації.	-
Сценарій застосування	Опис випадку використання послідовності подій з точки зору користувача для виконання завдання в заданому контексті.	-
Вразливість	Слабкість активу або контролю, яка може бути використана однією або кількома загрозами.	-

B Додаток II – Класифікація активів на панелі інструментів

У цьому додатку наведено класифікацію активів, прийняту набір інструментів EU RM.

Таблиця 2: Інтероперабельні активи набору інструментів ЄС RM

Активи	Панель інструментів RM	
Основні активи: загальний опис	**Визначення**	**Підкатегорії/приклади**
Бізнес процеси, функції, сервіси	Бізнес-процеси, функції та сервіси.	Включіть усі основні бізнес-процеси та функції, а також послуги, що надаються стороннім сторонам.
Інформація/дані	Інформація та дані в усіх формах (зберігання, передача тощо), які мають цінність.	Набір інформації/даних, які обслуговують певний бізнес-процес або діяльність організації.
Допоміжні активи: загальний опис		
Техніка, прилади та обладнання	Усі фізичні елементи/пристрої та обладнання, що підтримують бізнес-процеси, функції та послуги.	Обчислювальні пристрої (наприклад, пристрої кінцевої точки, сервери), мережеві пристрої та засоби масової інформації, пристрої IoT, пристрої OT, телекомунікаційні пристрої, периферійні пристрої та пристрої зберігання.
Програмне забезпечення та програми	Програмне забезпечення та програми.	Системне програмне забезпечення (наприклад, операційні системи), мікропрограмне забезпечення, проміжне програмне забезпечення, пакетне програмне забезпечення, програми для бізнесу/кінцевих користувачів.
Персонал	Персонал, який виконує функції, пов'язані з бізнес-процесами та функціями, підтримкою користувачів, розробкою та підтримкою програмного забезпечення, підтримкою обладнання, наданням послуг та управлінням інформацією/даними.	Особи, які приймають рішення, користувачі, розробники, адміністратори, оператори, обслуговуючий персонал, підрядники.
Розташування та комунікації	Приміщення, що містять/пов'язані з основними та допоміжними активами.	Розташування та приміщення, такі як будівлі, кімнати, офіси та контейнери. Мобільні платформи, такі як вантажівки, легкові автомобілі, кораблі. Основні послуги та комунальні послуги, що надаються зовнішніми операторами/постачальниками, електро- та водопостачання тощо.
Організаційна інфраструктура (включаючи послуги ICT)	Ролі, управління та допоміжні заходи та послуги ICT	Організаційна інфраструктура, включаючи ролі, політики, процедури та послуги ІКТ (телекомунікації, мережа, хмара, хостинг тощо).

C Додаток III – Класифікація загроз інструментарію

У цьому додатку наведено таксономію загроз, прийняту набір інструментів EU RM.
NB: короткий опис кожної загрози можна знайти в таблиці 4 цього додатку..

Таблиця 3: Інтероперабельний каталог загроз інструментарію EU RM

Категорія загрози	Загроза	Виміри безпеки (конфіденційність, цілісність і доступність)			Походження (навмисне, випадкове, екологічне)			Допоміжні категорії активів				
		C	I	A	D	A	E	Техніка, прилади, обладнання	Програмне забезпечення /додатки	Персонал	Розташування та комунальні послуги	Організаційна інфраструктура (включаючи послуги ICT services)
Природні	Пожежа			X			X	X			X	
Природні	Повінь			X			X	X			X	
Природні	Велика аварія			X			X	X			X	
Природні	Інші стихійні лиха			X			X	X			X	
Промислові	Пожежа			X	X	X		X			X	
Промислові	Пошкодження від води			X	X	X		X			X	
Промислові	Інші промислові аварії			X	X	X		X			X	
Промислові	Забруднення навколишнього середовища			X	X	X	X	X			X	
Промислові	Електромагнітне / теплове випромінювання			X	X	X	X	X			X	
Промислові	Збій апаратного або програмного забезпечення			X	X	X		X	X			
Промислові	Перебої в живленні			X	X	X	X	X				
Промислові	Невідповідна температура або умови вологості			X	X	X	X	X				
Промислові	Збій служб зв'язку			X	X	X						X
Промислові	Переривання інших послуг або основних поставок			X	X	X					X	X
Промислові	Погіршення носія/обладнання			X	X	X		X				
Промислові	Електромагнітні випромінювання	X			X			X			X	

Категорія загрози	Загроза	Виміри безпеки (конфіденційність, цілісність і доступність)			Походження (навмисне, випадкове, екологічне)			Допоміжні категорії активів				
		C	I	A	D	A	E	Техніка, прилади, обладнання	Програмне забезпечення/ додатки	Персонал	Розташування та комунальні послуги	Організаційна інфраструктура (включаючи послуги ICT)
Помилки та ненавмисні збої	Помилки користувача	X	X	X		X		X	X			X
Помилки та ненавмисні збої	Помилки адміністратора системи/безпеки	X	X	X		X		X	X			X
Помилки та ненавмисні збої	Моніторинг помилок (журнали)		X			X		X	X			X
Помилки та ненавмисні збої	Помилки конфігурації	X	X	X		X		X	X			X
Errors and unintentional failures	Організаційні недоліки			X		X				X		
Помилки та ненавмисні збої	Розповсюдження шкідливих програм	X	X	X		X			X			
Помилки та ненавмисні збої	Помилки (пере)маршрутизації	X				X			X			X
Помилки та ненавмисні збої	Помилки послідовності		X			X			X			X
Помилки та ненавмисні збої	Випадкова зміна інформації		X			X		X	X	X	X	X
Помилки та ненавмисні збої	Знищення інформації			X		X		X	X	X	X	X
Помилки та ненавмисні збої	Витік інформації	X				X		X	X	X	X	X
Помилки та ненавмисні збої	Уразливості програмного забезпечення	X	X	X		X			X			
Помилки та ненавмисні збої	Дефекти в обслуговуванні / оновленні програмного забезпечення		X	X		X			X			
Помилки та ненавмисні збої	Дефекти в обслуговуванні / оновленні обладнання			X		X		X				
Помилки та ненавмисні збої	Збій системи через виснаження ресурсів			X		X		X				X
Помилки та ненавмисні збої	Відновлення перероблених або викинутих носіїв	X		X		X		X				
Помилки та ненавмисні збої	Порушення готовності персоналу			X		X				X		
Навмисні напади	Маніпулювання записами про діяльність (журнал)		X		X			X	X			X
Навмисні напади	Маніпуляції з конфігураційними файлами	X	X	X	X			X	X			X
Навмисні напади	Маскування ідентичності	X	X		X				X			X
Навмисні напади	Зловживання правами доступу	X	X	X	X				X		X	X
Навмисні напади	Неправильне використання	X	X	X	X				X		X	X

Категорія загрози	Загрози	Security dimensions (confidentiality, integrity and availability)			Origin (deliberate, accidental, environmental)			Supporting asset categories				
		C	I	A	D	A	E	Hardware, devices, equipment	Software/applications	Personnel	Locations and utilities	Organisational infrastructure (including ICT services)
Навмисні напади	Розповсюдження шкідливих програм	X	X	X	X				X			
Навмисні напади	(Пере)маршрутизація повідомлень	X			X				X			X
Навмисні напади	Зміна послідовності		X		X				X			X
Навмисні напади	Несанкціонований доступ	X	X		X			X	X		X	X
Навмисні напади	Аналіз трафіку	X			X							X
Навмисні напади	Відмова (відмова від дій)		X		X							X
Навмисні напади	Підслуховування	X			X							X
Навмисні напади	Свідома зміна інформації		X		X			X	X	X	X	X
Навмисні напади	Знищення інформації			X	X			X	X	X	X	X
Навмисні напади	Розкриття інформації	X			X				X	X	X	X
Навмисні напади	Втручання в програмне забезпечення	X	X	X	X	X			X			
Навмисні напади	Втручання в обладнання	X			X			X				
Навмисні напади	Відмова від послуг			X	X			X				X
Навмисні напади	Theft of media or documents	X		X	X			X				
Навмисні напади	Theft of equipment	X		X	X			X				
Навмисні напади	Destructive attack			X	X			X			X	
Навмисні напади	Enemy overrun	X		X	X						X	
Навмисні напади	Staff shortage			X	X					X		
Навмисні напади	Extortion	X	X	X	X					X		
Навмисні напади	Social engineering	X	X	X	X					X		
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Loss of governance			X	X	X						X
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Lock-in			X		X						X
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Isolation failure	X	X	X	X	X						X

Категорія загрози	Загрози	Виміри безпеки (конфіденційність, цілісність і доступність)			Походження (навмисне, випадкове, екологічне)			Допоміжні категорії активів				
		C	I	A	D	A	E	Техніка, прилади, обладнання	Програмне забезпечення/додатки	Персонал	Розташування та комунальні послуги	Організаційна інфраструктура (включаючи послуги ICT)
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Порушення інтерфейсу керування			X	X	X						X
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Небезпечне або неефективне видалення даних	X			X	X						X
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Компрометація сервісного двигуна	X	X	X	X	X						X
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Повістка та електронне відкриття	X		X	X	X						X
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Ризик зміни юрисдикції	X		X	X	X						X
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Ризики захисту даних	X				X						X
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Конфіденційність користувача та вторинне використання даних	X										X
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Аналіз подій та судово-медична підтримка	X	X	X								X
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	Незахищені інтерфейси та інтерфейси прикладного програмування (APIs)	X	X	X		X						X

Таблиця 4: Опис загроз сумісного інструментарію EU RM

Категорія загрози	Загрози	Опис загрози
Природні	Пожежа	Ймовірність того, що пожежа знищить системні ресурси.
Природні	Повінь	Ймовірність того, що вода знищить системні ресурси.
Природні	Масштабна аварія	Події, що відбуваються без участі людини (блискавка, гроза, землетрус, циклон тощо).
Природні	Інші природні катастрофи	Зовнішня подія або пошкодження, пов'язані з природним середовищем поблизу активів і здатні завдати їм дуже серйозної фізичної шкоди.
Промислові	Пожежа	Можливість того, що вогонь знищить ресурси системи (тероризм, вандалізм тощо).
Промислові	Пошкодження від води	Можливість того, що вода руйнує ресурси системи (витоки, повені, тероризм, вандалізм тощо).
Промислові	Інші промислові катастрофи	Випадкові катастрофи внаслідок діяльності людини (вибухи, обвали, хімічне забруднення, електричні перевантаження, електричні коливання тощо).
Промислові	Забруднення навколишнього середовища	Наявність пилу, парів, корозійних або токсичних газів у навколишньому повітрі.
Промислові	Електромагнітне/теплове випромінювання	Радіоперешкоди, магнітні поля, ультрафіолетове світло тощо. Термічний ефект, викликаний пошкодженням або винятковими погодними умовами. Пошкодження, що викликають винятковий електромагнітний ефект.
Промислові	Збій апаратного або програмного забезпечення	Збої в обладнанні та/або програмах.
Промислові	Перебої в живленні	Збій, відключення або неправильне визначення розміру джерела живлення для активів, що виникає або через службу постачальника, або від внутрішньої системи розподілу. Саботаж або порушення роботи електроустановки.
Промислові	Невідповідна температура або умови вологості	Недоліки в кондиціонуванні приміщень, що перевищують робочі норми для обладнання (надлишок тепла, надлишок холоду, надлишок вологості тощо).
Промислові	Збій служб зв'язку	Скорочення можливості передачі даних з одного місця в інше.
Промислові	Переривання інших послуг або основних поставок	Перерва в роботі послуг або ресурсів, від яких залежить робота обладнання.
Промислові	Погіршення якості носія/обладнання	Логічна або фізична подія, яка спричиняє несправність елемента обладнання або є результатом плину часу.
Промислові	Електромагнітні випромінювання	Майже всі електричні пристрої випромінюють назовні випромінювання, яке може бути перехоплено іншим обладнанням (радіоприймачами), викликаючи витік інформації.
Помилки та випадкові збої	Помилки користувача	Помилки, допущені людьми під час використання служб, даних тощо. Людина допускає помилку в роботі, помилку введення або помилку використання апаратного чи програмного забезпечення.
Помилки та випадкові збої	Помилки системного адміністратора/адміністратора безпеки	Помилки, допущені людьми, відповідальними за встановлення та експлуатацію системи/систем безпеки. Системний адміністратор/адміністратор безпеки допускає операційну помилку, помилку введення або помилку використання апаратного чи програмного забезпечення.
Помилки та випадкові збої	Моніторинг помилок (журнали)	Відсутність записів, неповні записи, неправильно датовані записи, неправильно атрибутовані записи тощо.
Помилки та випадкові збої	Помилки конфігурації	Введення помилкових конфігураційних даних. Майже всі активи залежать від їх конфігурації, а це залежить від старанності адміністратора (права доступу, потоки активності, записи активності, маршрутизація тощо).

Категорія загрози	Загрози	Опис загрози
Помилки та випадкові збої	**Організаційні недоліки**	Коли незрозуміло, хто саме і коли повинен робити, зокрема вживати заходів щодо активів або звітувати перед управлінською ієрархією.
Помилки та випадкові збої	**Розповсюдження шкідливих програм**	Ненавмисне розповсюдження вірусів, шпигунського програмного забезпечення, хробаків, троянів, логічних бомб тощо.
Помилки та випадкові збої	**Помилки (пере)маршрутизації**	Надсилання інформації через систему чи мережу з використанням випадкового неправильного маршруту, який надсилає інформацію неправильному пункту призначення. Це можуть бути повідомлення, надіслані людям, процесам або тим і іншим.
Помилки та випадкові збої	**Помилки послідовності**	Випадкова зміна порядку надсилання повідомлень.
Помилки та випадкові збої	**Випадкова зміна інформації**	Випадкова зміна інформації.
Помилки та випадкові збої	**Знищення інформації**	Випадкова втрата інформації.
Помилки та випадкові збої	**Витік інформації**	Розголошення через необережність (словесна необережність, електронні носії, друковані копії тощо).
Помилки та випадкові збої	**Уразливості програмного забезпечення**	Дефекти в коді, які спричиняють неправильну роботу без наміру з боку користувача, але з наслідками для конфіденційності, цілісності, доступності даних або їх здатності працювати.
Помилки та випадкові збої	**Дефекти в обслуговуванні / оновленні програмного забезпечення**	Дефекти в процедурах або елементах керування для оновлення коду, які дозволяють продовжувати використовувати програми з відомими дефектами, які були виправлені виробником.
Помилки та випадкові збої	**Дефекти в обслуговуванні / оновленні обладнання**	Дефекти в процедурах або елементах керування для оновлення обладнання, які дозволяють йому працювати за нормальних умов. Відсутність досвіду в системі робить неможливим модернізацію та модернізацію.
Помилки та випадкові збої	**Збій системи через виснаження ресурсів**	Відсутність достатніх ресурсів призводить до збою системи, коли робоче навантаження є надмірним. Перевантаження простору для зберігання (наприклад, місця резервного копіювання, зберігання поштової скриньки, робочої зони тощо).
Помилки та випадкові збої	**Відновлення перероблених або викинутих носіїв**	Втрата обладнання безпосередньо спричиняє відсутність засобів для надання послуг, тобто їх обслуговування недоступність.
Помилки та випадкові збої	**Порушення готовності персоналу**	Випадкова відсутність на роботі (хвороба, порушення громадського порядку, бактеріологічне ураження тощо). Відсутність кваліфікованого або уповноваженого персоналу затримується з причин, які не залежать від нього.
Навмисні напади	**Маніпулювання записами про діяльність (журнал)**	Маніпуляція записами діяльності для видалення будь-яких доказів або слідів.
Навмисні напади	**Маніпуляції з конфігураційними файлами**	Введення помилкових конфігураційних даних.
Навмисні напади	**Маскування ідентичності**	Коли зловмисникам вдається видати себе авторизованими користувачами, вони користуються привілеями користувачів для власних цілей.
Навмисні напади	**Зловживання правами доступу**	Коли користувачі зловживають своїм рівнем привілеїв для виконання завдань, за які вони не відповідають, виникають проблеми.
Навмисні напади	**Неправильне використання**	Використання системних ресурсів для незапланованих цілей, як правило, в особистих інтересах (ігри, особистий пошук в Інтернеті, персональні бази даних, персональні програми, зберігання персональних даних тощо).
Навмисні напади	**Розповсюдження шкідливих програм**	Навмисне розповсюдження вірусів, шпигунського програмного забезпечення, хробаків, троянів, логічних бомб тощо.
Навмисні напади	**(Пере)маршрутизація повідомлень**	Надсилання інформації через систему чи мережу з використанням, навмисне, неправильного маршруту, який пересилає інформацію не тому адресату.
Навмисні напади	**Зміна послідовності**	Надсилання інформації через систему чи мережу з використанням, навмисного, неправильного маршруту, який пересилає інформацію не ту адресу.
Навмисні напади	**Несанкціонований доступ**	Зловмиснику вдається отримати доступ до ресурсів системи без авторизації для цього, як правило, користуючись збоєм у системі ідентифікації та авторизації.

Категорія загрози	Загрози	Опис загрози
Навмисні напади	**Аналіз трафіку**	Не потребуючи аналізу вмісту повідомлень, зловмисник може зробити висновки на основі аналізу походження, призначення, обсягу та частоти обміну.
Навмисні напади	**Відмова (заперечення дій)**	Суб'єкт заперечує участь в обміні з третьою стороною або проведення операції. Пізніше відмова від дій або починань, придбаних у минулому.
Навмисні напади	**Підслуховування**	Зловмисники мають доступ до інформації, яка їм не належить, при цьому сама інформація не змінюється.
Навмисні напади	**Свідома зміна інформації**	Навмисна зміна інформації з метою отримання вигоди або заподіяння шкоди.
Навмисні напади	**Знищення інформації**	Навмисне видалення інформації з метою отримання вигоди або заподіяння шкоди.
Навмисні напади	**Розкриття інформації**	Навмисне розголошення інформації.
Навмисні напади	**Втручання в програмне забезпечення**	Навмисна зміна роботи програми з метою отримання непрямої вигоди, коли її використовує уповноважена особа.
Навмисні напади	**Втручання в обладнання**	Навмисна зміна роботи обладнання для отримання непрямої вигоди, коли його використовує уповноважена особа.
Навмисні напади	**Відмова від послуг**	Відсутність достатніх ресурсів призводить до збою системи, коли робоче навантаження занадто велике.
Навмисні напади	**Крадіжка носіїв інформації або документів**	Крадіжка медіа безпосередньо спричиняє брак ресурсів для надання послуг, тобто недоступність.
Навмисні напади	**Крадіжка техніки**	Крадіжка обладнання безпосередньо спричиняє відсутність ресурсів для надання послуг, тобто недоступність.
Навмисні напади	**Руйнівна атака**	Вандалізм, тероризм, військові дії тощо.
Навмисні напади	**Нагін ворога**	При вторгненні в приміщення і втраченому контролі над засобами роботи.
Навмисні напади	**Нестача кадрів**	Умисна відсутність на робочому місці (страйки, прогули, невиправдані неявки, блокування доступу тощо).
Навмисні напади	**Вимагання**	Тиск погрозами, на людей, щоб змусити їх діяти певним чином.
Навмисні напади	**Соціальна інженерія**	Використання доброї волі деяких людей, щоб змусити їх здійснювати діяльність, яка представляє інтерес для третьої сторони.
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Втрата правління**	Втрата управління та контролю може потенційно серйозно вплинути на стратегію організації, а отже, на здатність виконувати її місію та цілі.
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Зафіксувати**	Сильне покладання на послуги одного постачальника може призвести до серйозних труднощів при зміні постачальника.
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Порушення ізоляції**	Збій механізмів, що розділяють сховище, пам'ять, маршрутизацію та навіть репутацію між різними орендарями спільної інфраструктури. Збій механізмів, що розділяють сховище, пам'ять, маршрутизацію та навіть репутацію між різними орендарями спільної інфраструктури.
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Компроміс інтерфейсу керування**	Інтерфейс керування скомпрометовано.
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Небезпечне або неефективне видалення даних**	Видалення даних зі сховища насправді не означає, що дані остаточно видаляються зі сховища. Пізніше до даних може отримати доступ інший клієнт аутсорсингового партнера/постачальника.

Категорія загрози	Загрози	Опис загрози
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Компрометація сервісного двигуна**	Компрометація механізму обслуговування надасть зловмиснику доступ до даних усіх клієнтів, що призведе до потенційної повної втрати даних або відмови в обслуговуванні.
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Повістка та електронне відкриття**	Компрометація механізму обслуговування надасть зловмиснику доступ до даних усіх клієнтів, що призведе до потенційної повної втрати даних або відмови в обслуговуванні.
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Ризик зміни юрисдикції**	When data is stored or processed in a data centre located in a country other than the customer country, there are numerous ways in which the change in jurisdiction could affect the security of the information.
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Ризики захисту даних**	Закон про захист даних базується на передумові, що завжди зрозуміло, де знаходяться персональні дані, хто їх обробляє та хто відповідає за обробку даних. Розподілені середовища, здається, суперечать цим доказам.
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Конфіденційність користувача та вторинне використання даних**	Клієнти повинні бути проінформовані про те, які дані можуть використовуватися постачальниками для вторинних цілей. Це включає дані, які можуть бути отримані постачальниками безпосередньо з даних користувача або опосередковано на основі поведінки користувача (кліки тощо).
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Аналіз подій та судово-медична підтримка**	У разі інциденту безпеки програми та служби, розміщені у постачальника, важко дослідити, оскільки журналювання може бути розподілено між кількома хостами та центрами обробки даних у різних країнах.
Загрози, пов'язані з послугами (хмарні служби, послуги, що надаються сторонніми особами)	**Незахищені інтерфейси та APIs**	Ініціалізація, керування, оркестровка та моніторинг виконуються через API. Безпека та доступність загальних служб залежить від безпеки цих інтерфейсів.

D Додаток IV – Інструментальна шкала впливу

Шкала впливу інструментарію EU RM складається з п'яти рівнів, які є: (i) дуже високими; (ii) високий; (iii) помірний; (iv) низький; і (v) дуже низький. Вплив, який відповідає кожному з цих рівнів, детально описано нижче, щоб допомогти зацікавленим сторонам визначити відповідні рівні, які найкраще відповідають їхньому середовищу.

- Дуже високий: катастрофічний.
  - Загрозлива подія призводить до катастрофічних наслідків для бізнесу.
  - Загрозлива подія призводить до фінансових втрат, які перевищують 5% річного обороту/бюджету організації.
  - Витік інформації може загрожувати виживанню організації.
  - Загрозлива подія призводить до пошкодження, яке неможливо відновити, або спричиняє постійний простой.
  - Недоступність, для відновлення якої потрібні надзвичайні зусилля, або яка є постійною.
  - Негативний вплив на репутацію організації або її співробітників із висвітленням у світових ЗМІ.
  - Загрозлива подія призводить до припинення надання всіх організаційних послуг.
  - Організація може отримати суворе покарання, яке може зробити деякі смертельні витрати майже нездоланними.
  - Значні наслідки, які є майже незворотними та не можуть бути перевершені (смерть, неможливість працювати).

- Високий: критичний.
  - Загрозлива подія призводить до критичних впливів на бізнес.
  - Загрозлива подія призводить до фінансових втрат, які коливаються від 2% до 5% річного обороту/бюджету організації.
  - Витік інформації серйозно підриває інтереси організації.
  - Загрозлива подія призводить до корупції, яка накладає значний тягар на зацікавлені сторони.
  - Інтенсивна недоступність, що спричиняє значні незручності для зацікавлених сторін.
  - Значне зниження репутації організації через повторну критику в ЗМІ.
  - Загрозлива подія призводить до повного зриву відділу. Обвинувальний акт проти бізнесу.
  - Загрозлива подія коштує організації значних грошових зборів.
  - Значні результати, які можна перевершити, але зі значними проблемами (наприклад, заборона банку).

- Помірний: середній.
  - Загрозлива подія призводить до середнього впливу на бізнес.
  - Загрозлива подія призводить до фінансових втрат, які коливаються від 0,05 % до 2 % річного обороту/бюджету організації.
  - Витік інформації підриває інтереси організації.
  - Загрозлива подія призводить до корупції, що створює труднощі для постраждалих сторін, однак відновлення є простим.
  - Обмежена доступність створює труднощі для відповідних зацікавлених сторін.
  - Загрозлива подія призводить до тимчасової шкоди репутації організації з періодичною критикою ЗМІ.
  - Загрозлива подія призводить до окремих подій з мінімальним впливом на споживача/громадян.
  - Загрозлива подія призводить до можливих штрафів для організації та може запровадити неграничні витрати.
  - Значні труднощі, які можуть бути ускладнені декількома ускладненнями (відмова в доступі до комерційної доставки).

- Низький: граничний.
  - Загрозлива подія призводить до незначного впливу на бізнес.
  - Загрозлива подія призводить до фінансових втрат, які коливаються від 0,01 % до 0,05 % річного обороту/бюджету організації.
  - Витік інформації завдає шкоди загальним інтересам організації.
  - Викорінення корупції не матиме жодних негативних наслідків.

- Відсутність доступності, що спричиняє незручності, але серйозно не загрожує інтересам зацікавлених сторін.
- Загрозлива подія призводить до нечастої критики ЗМІ.
- Подія загрози призводить до незначних подій, які не впливають на користувачів послуг.
- Подія загрози вводить деякі додаткові витрати. Дуже низька ймовірність будь-яких речень або, можливо, дуже незначна ймовірність одного.
- Невелика невдача, яку можна легко подолати (наприклад, втрата часу).

- Дуже низький: незначний.
  - Загрозлива подія призводить до незначного впливу на бізнес.
  - Загрозлива подія призводить до фінансових втрат, які менше або дорівнюють 0,01% річного обороту/бюджету організації.

E Додаток V – Шкала ризику інструментарію

Шкала ризику інструментарію EU RM складається з п'яти рівнів, які є: (i) дуже високими; (ii) високий; (iii) помірний; (iv) низький; і (v) дуже низький. На ці рівні впливають рівні впливу та ймовірності, як показано на матриці ризиків, наведеній на рисунку 2 і детально описаному нижче.

- Дуже високий.
  - Загрозлива подія, що призведе до катастрофічних (дуже значних наслідків) наслідків для бізнесу, передбачається як майже напевне (дуже висока ймовірність) матеріалізації.
  - Загрозлива подія, що призведе до катастрофічних (дуже значних наслідків) наслідків для бізнесу, прогнозується як дуже ймовірна (висока ймовірність) матеріалізації.
  - Загрозлива подія, що призведе до критичного (значного впливу) впливу на бізнес, прогнозується як майже напевне (дуже висока ймовірність) матеріалізації.

- Високий.
  - Загрозлива подія, що призведе до катастрофічних (дуже значних наслідків) впливу на бізнес, прогнозується як малоймовірна (з низькою ймовірністю) для реалізації.
  - Загрозлива подія, що призведе до катастрофічного (дуже сильного впливу) впливу на бізнес, за прогнозами, потенційно (помірна ймовірність) матеріалізується.
  - Загрозлива подія, яка призведе до критичного (значного впливу) впливу на бізнес, прогнозується як майже вірогідна (дуже висока ймовірність) матеріалізація.
  - Загрозлива подія, що призведе до критичного (значного впливу) впливу на бізнес, прогнозується як дуже ймовірна (дуже висока ймовірність) матеріалізації.
  - Загрозлива подія, що призведе до середнього (помірного впливу) впливу на бізнес, прогнозується як дуже ймовірна (висока ймовірність) матеріалізації.
  - Загрозлива подія, яка призведе до середнього (помірного впливу) впливу на бізнес, прогнозується як майже вірогідна (дуже висока ймовірність) матеріалізація.
  - Загрозлива подія, яка призведе до незначного (з низьким впливом) впливу на бізнес, передбачається як майже вірогідна (дуже висока ймовірність) матеріалізації.

- Помірний.
  - Загрозлива подія, що призведе до катастрофічних (дуже сильних) впливів на бізнес, прогнозується як дуже малоймовірна (дуже низька ймовірність) для матеріалізації.
  - Загрозлива подія, що призведе до критичного (значного впливу) впливу на бізнес, прогнозується як малоймовірна (низька ймовірність) для матеріалізації.
  - Загрозлива подія, що призведе до середнього (помірного впливу) впливу на бізнес, прогнозується як малоймовірна (низька ймовірність) для матеріалізації.
  - Загрозлива подія, яка призведе до середнього (помірного впливу) впливу на бізнес, прогнозується, що потенційно (помірна ймовірність) матеріалізується.
  - Передбачається, що загрозлива подія, що призведе до незначного (з низьким рівнем впливу) впливу на бізнес, потенційно (помірна ймовірність) матеріалізується.
  - Загрозлива подія, що призведе до незначного (низького впливу) впливу на бізнес, прогнозується як дуже ймовірна (висока ймовірність) матеріалізації.
  - Загроза, що призведе до незначного (дуже низького впливу) впливу на бізнес, прогнозується як майже вірогідна (дуже висока ймовірність) матеріалізації.

- Низький.
  - Загрозлива подія, що призведе до критичного (значного впливу) впливу на бізнес, прогнозується як дуже малоймовірна (дуже низька ймовірність) для матеріалізації.
  - Загрозлива подія, що призведе до середнього (помірного впливу) впливу на бізнес, прогнозується як дуже

малоймовірна (дуже низька ймовірність) для матеріалізації.

- Загрозлива подія, що призведе до незначного (низького впливу) впливу на бізнес, прогнозується як малоймовірна (низька ймовірність) реалізації.
- Передбачається, що загрозлива подія, що призведе до незначного (дуже слабкого впливу) впливу на бізнес, потенційно (помірна ймовірність) матеріалізується.
- Загрозлива подія, що призведе до незначного (дуже слабкого впливу) впливу на бізнес, прогнозується як дуже ймовірна (висока ймовірність) матеріалізації.

- Дуже низький.
- Загрозлива подія, що призведе до незначного (низького впливу) впливу на бізнес, прогнозується як дуже малоймовірна (дуже низька ймовірність) для матеріалізації.
- Загроза, що призведе до незначного (дуже низького впливу) впливу на бізнес, прогнозується як дуже малоймовірна (дуже низька ймовірність) для матеріалізації.
- Загрозлива подія, що призводить до незначного (дуже слабкого впливу) впливу на бізнес, прогнозується як малоймовірна (низька ймовірність) для матеріалізації.

F Додаток VI – Зразки сумісності розрахунку ризику

У цьому додатку представлено два експерименти, які доводять сумісність між різними методологіями та запропонованим набором інструментів. Слід зазначити, що інструментарій бездоганно працює з ITSRM^2, Monarc, EBIOS (вираження потреб і визначення цілей безпеки) і Magerit. Панель інструментів оснащена розкривними списками, які містять, у числовому підході, вплив і рівень ймовірності вищезазначених методологій. ITSRM^2 гармонізовано на 5 рівнях замість 10 на основі підходу, запропонованого у відповідній настанові. EBIOS і Magerit — це методології, які підтримують п’ять шкал ризиків кібербезпеки. Хоча Monarc підтримує три шкали ризиків кібербезпеки (високий, середній і низький). Щоб підтвердити вищезазначену функцію сумісності, ми провели два експерименти з Monarc і Magerit.

Експеримент 1.

Ми припускаємо, що кінцевим користувачем є організація, яка працює в енергетичному секторі та виконує ризик за загрозу за методом Monarc. На цьому етапі ми розрахуємо ризик цієї організації проти загрози відмови в обслуговуванні. З одного боку, вплив Monarc залежить від параметрів, включаючи вплив загрози на конфіденційність, цілісність, доступність, репутацію, операційні, юридичні, фінансові та особисті. Загальний вплив оцінюється 4 з 4. З іншого боку, ймовірність загрози, залежно від наявних уразливостей системи та ймовірність появи відповідної загрози, оцінюється 4 з 4. Загальний ризик через підхід Monarc вважається високим . Однак, виходячи з підходу інструментарію, ризик відповідної організації вважається дуже високим.

Експеримент 2.

Ми припускаємо, що кінцевим користувачем є організація, яка працює в секторі охорони здоров’я та виконує ризик за загрозу за методом Magerit. На цьому етапі ми розрахуємо ризик цієї організації проти загрози відмови в обслуговуванні. З одного боку, ефект від Magerit залежить від параметрів, які безпосередньо пов'язані з економічними втратами. Загальний вплив оцінюється 4 з 5 (менше 1 000 000 000,00 грошових одиниць). З іншого боку, частота появи загрози набирає 3 бали з 5 (менше року). Загальний ризик через підхід Monarc вважається високим. Після цього експерименту набір інструментів узгоджується з початковим результатом, який дає право на високий ризик.

G Додаток VII – Бібліотеки панелі інструментів

У цьому додатку наведено список бібліотек панелі інструментів.

- EU RM Toolbox Library 01 – Відображення термінів v1.0
- EU RM Toolbox Library 02 – Відображення активів v1.0
- EU RM Toolbox Library 03 – Відображення загроз v1.0
- EU RM Toolbox Library 04 – Відображення рівнів ризику та впливу v1.0

H Додаток VIII – Приклад використання

У цьому додатку наведено приклад варіанту використання, розробленого в контексті компетентного органу, який бажає отримати огляд рівнів ризику, з якими стикається організація в певному секторі..

Опис сценарію

Компетентний орган NIS хоче визначити ризики на національному рівні щодо виниклої загрози, яка пов'язана з поширенням програм-вимагачів, націлених переважно на операторів систем розподілу (DSO) в енергетичному секторі. Зокрема, мета атаки – зашифрувати бази даних розподілених систем управління енергетичними ресурсами, таким чином вимикаючи прогнозування навантаження та виробництва, а також роботу мережі на рівні розподілу (див. Малюнок 6). Зловмисники спочатку заражають мережу DSO шкідливими завантажувачами через оновлення кількох пакетів резервних серверів, розгорнутих у мережах DSO.

Малюнок 3: Логічна архітектура цільової мережі DSO

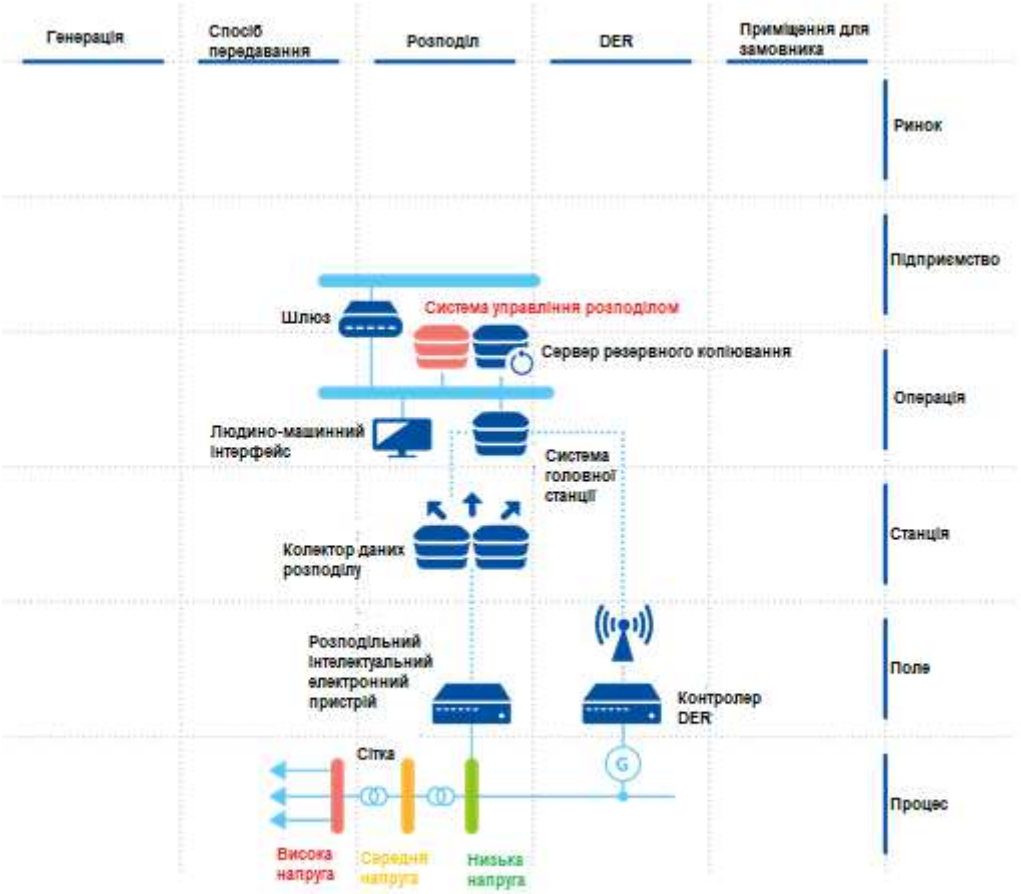
Орієнтовні активи в масштабі

У цьому розділі наведено орієнтовні активи, залучені до сценарію інциденту. Типовий взаємозв'язок залучених матеріальних активів зображено на малюнку 7, хоча очікується, що архітектура DSO буде різною. У дужках наведено тип активів відповідно до класифікації активів інструментарію: дані, функції, програмне забезпечення, обладнання, IT-послуги, персонал, місцезнаходження.

Орієнтовні залучені активи сценарію використання:

Дані системи управління розподілом (DMS) / дані резервного копіювання DMS (дані) / прогноз навантаження (функція) / прогноз виробництва (функція) / резервний сервер (програмне забезпечення) / резервний сервер (апаратне забезпечення) / мережеві пристрої (IT-послуги) / DMS сервер (програмне/апаратне).

Малюнок 4: Активи, залучені до сценарію інциденту, зіставлені з моделлю архітектури інтелектуальної мережі



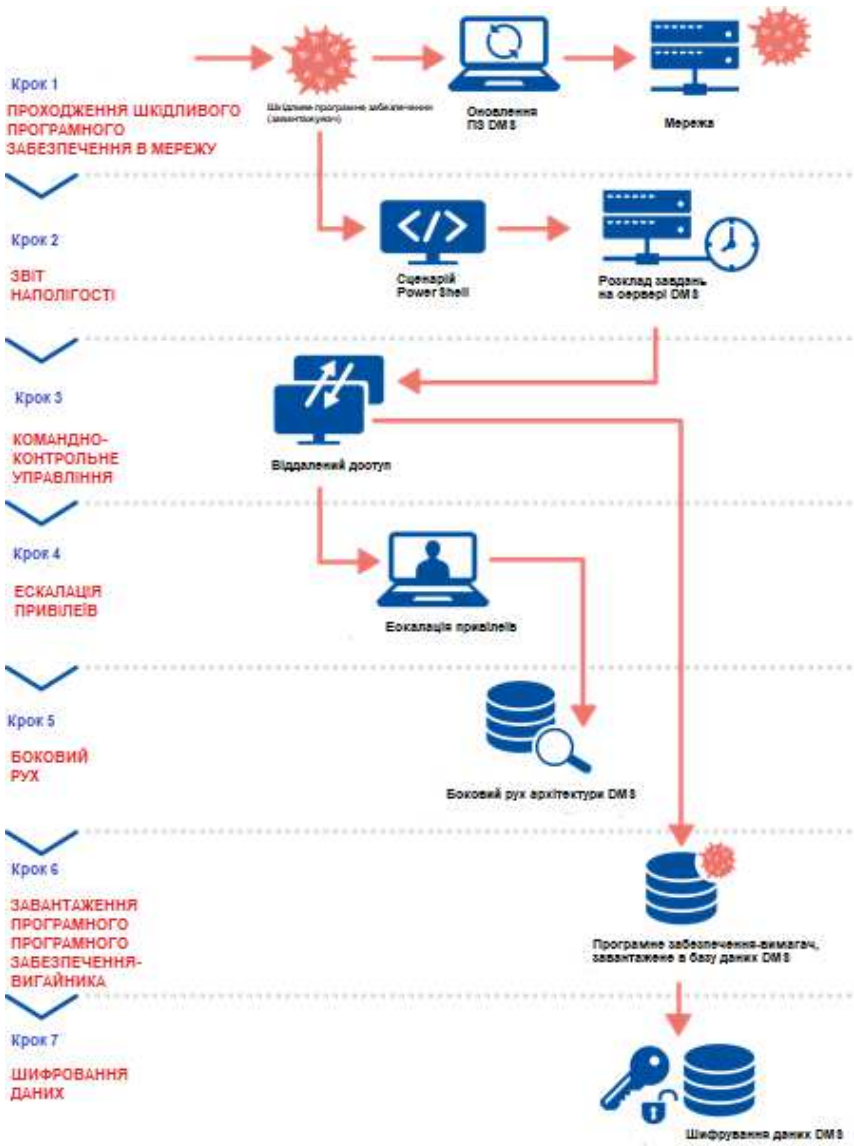
Шлях атаки

Шлях атаки для сценарію інциденту програм-вимагачів складається з наступних кроків.

1. **Крок шляху атаки 1.** Початкове шкідливе програмне забезпечення (завантажувач) потрапляє в мережу через канал оновлення програмного забезпечення резервного програмного забезпечення (розташоване в операційній мережі організації).
2. **Крок шляху атаки 2.** Завантажувач виконує сценарій PowerShell, щоб створити заплановане завдання на сервері резервного копіювання та отримати постійність у цільовій мережі.
3. **Крок шляху атаки 3.** Заплановане завдання виконується щодня та створює канал керування між віддаленим сервером, яким керує зловмисник, і системою жертви.
4. **Крок шляху атаки 4.** Зловмисне програмне забезпечення отримує доступ до дійсних локальних облікових записів адміністратора, щоб використовувати привілеї адміністратора в бічному русі.
5. **Крок шляху атаки 5.** Зловмисне програмне забезпечення проводить дистанційне виявлення системи для бокового руху.
6. **Крок шляху атаки 6.** Програмне забезпечення-вимагач завантажується в DMS через канал керування.
7. **Крок шляху атаки 7.** Зловмисник отримує доступ до резервного сервера / знищує резервні копії.
8. **Крок шляху атаки 8.** Програма-вимагач шифрує базу даних системи розповсюдження.

Наведені вище кроки зображено на малюнку 8.

Малюнок 5: Кроки шляху атаки



Сценарії нападу

У цьому розділі ми описуємо сценарії атак для кожного кроку атаки, кожен з яких складається з <активів, загроз, впливу>. Список задіяних активів включає цільові активи, такі як дані DMS, і активи, які є частиною поверхні атаки або вектора атаки. Крім того, список загроз є орієнтовним, і додаткові загрози також можуть бути розглянуті.

Таблиця 5: Орієнтовні сценарії атак

Кроки атаки	Сценарій атаки (опис ID)	Орієнтовні залучені активи (тип)	Орієнтовні сценарії загроз	MITRE ATT&CK® структура	Вплив/порушений аспект безпеки (конфіденційність, цілісність, доступність)
1. Початкова шкідлива програма (завантажувач) потрапляє в мережу	1.1. Зловмисне програмне забезпечення поширюється через оновлення програмного забезпечення (атака на ланцюг поставок)	Дані резервного копіювання DMS (дані) / прогноз навантаження (послуга) / прогноз виробництва (послуга) / резервний сервер (програмне забезпечення) / резервний сервер (апаратне забезпечення)	Ненавмисне поширення шкідливих програм	Початковий доступ (компрометація ланцюга поставок T1195)	C-I-A
2. Зловмисник набуває стійкості	2.1. Виконується сценарій PowerShell і створюється заплановане завдання	Дані резервного копіювання DMS (дані) / прогноз навантаження (послуга) / прогноз виробництва (послуга) / резервна операційна система сервера (програмне забезпечення)	Маніпуляції з конфігураційними файлами	Виконання (виконання користувачем T1204, інтерпретатор команд і сценаріїв T1059)	C-I-A
3. Налагоджено канал управління	3.1. Канал C2 забезпечує зв'язок із серверами, контрольованими противником	DMS резервне копіювання даних (дані) / резервне копіювання операційної системи сервера (програмне забезпечення) / мережеві пристрої (IT-послуги)	Маніпуляції з конфігураційними файлами	Командування та контроль (протокол прикладного рівня T1071, програмне забезпечення віддаленого доступу T1219)	C-I-A
4. Підвищення привілеїв	4.1. Супротивники використовують вкрадені дійсні облікові записи під час бокового руху	Дані DMS (дані) / операційна система сервера резервного копіювання (програмне забезпечення)	Маскування ідентичності	Підвищення привілеїв (дійсні облікові записи T1078)	C-I
5. Відкриття	5.1. Зловмисники намагаються дізнатися деталі архітектури DMS	Дані DMS (дані) / прогноз навантаження (послуги) / прогноз виробництва (послуги) / мережеві пристрої (IT-послуги)	Несанкціонований доступ (мережа)	Виявлення (виявлення файлів і каталогів T1083)	C
6. Боковий рух	6.1. Програмне забезпечення-вимагач, завантажене в базу даних DMS	Дані DMS (дані) / прогноз навантаження (сервіс) / прогноз виробництва (сервіс) / сервер DMS (програмне/апаратне забезпечення)	Навмисне поширення шкідливих програм	Боковий рух (експлуатація віддалених служб T1210), командування та управління (передача інструменту входу T1105)	C-I-A
7. Резервні копії видаляються	7.1. Зловмисник видаляє всі резервні копії на сервері резервного копіювання	DMS резервне копіювання даних (даних) / сервер резервного копіювання	Знищення інформації	Вплив (знищення даних T1485)	A

Кроки атаки	Сценарій атаки (опис ID)	Орієнтовні залучені активи (тип)	Орієнтовні сценарії загроз	MITRE ATT&CK® структура	Вплив/порушений аспект безпеки (конфіденційність, цілісність, доступність)
8. Дані зашифровані	8.1. Дані DMS шифруються за допомогою завантаженої програми-вимагача	Дані DMS (дані) / прогноз навантаження (сервіс) / прогноз виробництва (сервіс) / сервер DMS (програмне забезпечення)	Несанкціонований доступ	Вплив (маніпулювання даними T565)	C-I-A

Результати

Очікується, що учасники нададуть результати оцінки ризику для всіх сценаріїв ризику, які вони запускатимуть, у формі списку. Крім того, вони повинні назвати метод та/або інструмент, який вони використовували для оцінки ризику. Надана інформація дозволить використовувати інструментарій для нормалізації значень ризику та порівняння результатів.

Важлива NB: Щоб уникнути ненавмисного розголошення конфіденційної інформації щодо середовища учасників, ми просимо учасників надавати упереджену інформацію, яка не обов'язково відображає фактичний стан, оскільки це не є метою цього завдання.

6. Бібліографія/посилання

ENISA (2021) Interoperable EU Risk Management Framework [онлайн]. Доступний на: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

Міжнародна організація стандартизації, 2018. ISO/IEC 27005:2018 Інформаційні технології. Методи безпеки. Управління ризиками інформаційної безпеки.

Генеральний директорат Європейської комісії з комунікацій, стандарти безпеки, що застосовуються до всіх інформаційних систем Європейської комісії. EU ITSRM, МЕТОДОЛОГІЯ УПРАВЛІННЯ РИЗИКАМИ IT-БЕЗПЕКИ V1.2. [Онлайн]. Доступний на: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission- information-systems_en

Міжнародна організація стандартизації, 2018. ISO/IEC 27000:2018, Інформаційні технології – Методи безпеки – Системи управління інформаційною безпекою – Огляд і словник, s.l.: Міжнародна організація стандартизації.

ISO/IEC 2382-1:1993 Інформаційні технології – Словник – Частина 1: Основні терміни. Міжнародна організація стандартизації (ISO). [Онлайн]. в наявності: http://www.iso.org/iso/catalogue_detail.htm?csnumber=7229

Joint Task Force Transformation Initiative, 2012. Керівництво з проведення оцінки ризиків. [Онлайн]. Доступний на: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Joint Task Force, 2018. Структура управління ризиками для інформаційних систем і організацій: підхід життєвого циклу системи для безпеки та конфіденційності. [Онлайн]. Доступний на: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Стандартний комп'ютерний словник IEEE, компіляція стандартних комп'ютерних глосаріїв IEEE. IEEE, Нью-Йорк, Нью-Йорк, 1990 https://www.standardsuniversity.org/article/standards-glossary/#I

Ларс Фішер, Матіас Услар (OFFIS), Даг Моррілл (Navigant), Майкл Дьорінг, Едвін Хасен (Ecofys), 2018. Дослідження щодо оцінки ризиків кіберінцидентів і витрат на запобігання кіберінцидентів в енергетичному секторі. [Онлайн]. Доступний на: https://energy.ec.europa.eu/study-evaluation-risks-cyber-incidents-and-costs-preventing-cyber-incidents-energy-sector_en

Lockheed Martin, 2021. Кіберланцюг вбивств. [Онлайн]. Доступний на: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

МИТР, 2015-2021. MITP ATT&CK. [Онлайн]. Доступний на: https://attack.mitre.org/

TP-04-22-275-EN-C

Про ENISA

Агентство Європейського Союзу з кібербезпеки (ENISA) – це агентство ЄС, яке займається досягненням високого загального рівня кібербезпеки в Європі. Заснована в 2004 році та посилена Законом ЄС про кібербезпеку, ENISA робить внесок у кіберполітику ЄС, підвищує надійність продуктів, послуг і процесів ІКТ за допомогою схем сертифікації кібербезпеки, співпрацює з державами-членами та органами ЄС і допомагає Європі підготуватися до кібервикликів завтрашнього дня. . Завдяки обміну знаннями, нарощуванню потенціалу та підвищенню обізнаності агентство співпрацює зі своїми ключовими зацікавленими сторонами, щоб зміцнити довіру до пов'язаної економіки, підвищити стійкість інфраструктури ЄС і, зрештою, зберегти європейське суспільство та громадян у цифровій безпеці. Більше інформації про ENISA та її роботу можна знайти тут: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-609-4