Додаток 8
до Методики оцінювання
ризиків кібербезпеки
(пункт 6 розділу VII)

Приклад
оцінки ризиків кібербезпеки об'єктового рівня

1. Якісна оцінка ризиків кібербезпеки об'єктового рівня

1.1. Ідентифікація активів та контексту

Формування переліку активів: сервер баз даних (СБД) порталу «Державні послуги Онлайн», що містить конфіденційні персональні дані громадян.

Класифікація активів: рівень критичності – **критичний**, оскільки компрометація може призвести до розголошення інформації, що становить значну цінність для держави, та до масового порушення прав громадян щодо захисту персональних даних.

Визначення власників активів: відповідальна особа за СБД (наприклад, керівник ІТ-відділу або начальник відділу інформаційної безпеки).

Визначення сфери застосування: інформаційна система вебпорталу надання електронних адміністративних послуг «Державні послуги Онлайн».

1.2. Ідентифікація загроз та вразливостей

Ідентифікація загроз: **несанкціонована компрометація сервера баз даних (СБД) порталу**, що може призвести до витоку персональних даних громадян. Джерелами інформації для ідентифікації загроз є загальні каталоги загроз (IT-Grundschutz, NIST, ENISA), дані від НКЦК при РНБО України та CERT-UA, результати попередніх аудитів та проведення сканувань з метою виявлення вразливостей, аналіз журналів подій та інцидентів, документація виробників, публікації про вразливості, досвід організації та мозковий штурм із залученням співробітників.

Ідентифікація вразливостей: Критична вразливість у програмному забезпеченні СУБД (наприклад, CVE-YYYY-XXXX у PostgreSQL), яка використовується на СБД порталу, а також можливі слабкі політики паролів, відсутність належного розмежування доступу або недостатня обізнаність персоналу.

1.3. Оцінювання ймовірності та впливу (якісний метод)

Шкала оцінки впливу (наслідків):

Опис впливу: «Порушення функціонування об'єкта критичної інфраструктури, розголошення інформації, що становить значну цінність для держави, значна шкода національній безпеці, тривале (понад 24 год) припинення

надання послуг суб’єктом кіберзахисту.». Цей опис вказує на національний рівень, але для об'єктового рівня наслідки витоку персональних даних громадян можуть бути прирівняні до «Катастрофічний» через масове порушення прав громадян та репутаційні/фінансові втрати для держави. **Рівень (бали): 5 (катастрофічний)**.

Оцінка ймовірності (частоти виникнення):

Опис стану кібербезпеки: «Нерегулярне оновлення ПЗ та систем безпеки. Високий відсоток успішних фішингових атак (наприклад, понад 10% співробітників клікають на шкідливі посилання). Відсутність багатофакторної автентифікації для привілейованих облікових записів. Існують невиправлені критичні вразливості, виявлені під час сканувань. Висока активність зловмисників, націлених на компанії в цьому секторі.». **Категорія ймовірності: висока (бали: 4)**.

1.4. Визначення рівня ризику (якісний метод)

Використовуючи Матрицю ризиків кібербезпеки (відповідно до додатка 3 Методики оцінювання ризиків кібербезпеки), вплив: 5 (катастрофічний), ймовірність 4 (висока) − поєднання, ймовірно, дає **критичний** рівень ризику (від 20 до 25 балів, де 5 × 4 = 20).

Обґрунтування початкового рівня: високий ризик через критичність даних (персональні дані громадян), значний потенційний вплив (масове порушення прав, репутаційні та фінансові втрати) та наявність відомої критичної вразливості, яка активно експлуатується.

2. Кількісна оцінка ризиків кібербезпеки об'єктового рівня

Застосуємо методологію розрахунку річних очікуваних втрат (РОВ).

2.1. Визначення фінансових показників

Ризик: «Несанкціонована компрометація сервера баз даних (СБД) порталу «Державні послуги Онлайн»».

Розрахунок вартості активу (ВА): вартість активу для ДІР включає балансову вартість обладнання та ПЗ, вартість відновлення даних та працездатності системи, вартість простою, компенсацію збитків третім особам (штрафи за порушення законодавства про захист персональних даних), репутаційні втрати (оцінюються експертно), вартість розслідування інциденту та інші витрати. *Припустимо експертну оцінку загальної вартості активу для СБД порталу, який містить конфіденційні персональні дані:* ВА **= 10 000 000 грн.** (включає вартість обладнання, ПЗ, розробки, потенційні штрафи за витік даних, вартість відновлення, репутаційні збитки).

2.2. Розрахунок коефіцієнта вразливості (КВ**)**

У випадку повної компрометації СБД з витоком даних коефіцієнт вразливості буде дуже високим. *Припускаємо:* КВ **= 0.9 (або 90%)**, оскільки втрата конфіденційних даних є майже повною втратою вартості активу в контексті його призначення та довіри.

2.3. Розрахунок очікуваних разових втрат (ОРВ**)**

ОРВ = ВА х КВ = 10 000 000 грн. × 0.9 = **9 000 000 грн.** Це означає, що кожна успішна компрометація СБД коштуватиме суб'єкту кіберзахисту 9 000 000 грн.

2.4. Визначення очікуваної частоти реалізації (ОЧР**)**

На основі внутрішньої статистики інцидентів за попередні 3 роки та галузевих звітів НКЦК при РНБО України аналітики кібербезпеки суб'єкта кіберзахисту визначили, що апріорна ймовірність компрометації СБД_Портал становить 0.01 (тобто 1% ймовірності реалізації ризику на рік).

Таким чином, ОЧР **= 0.01** (одна така атака очікується один раз на 100 років або 1% ймовірність за рік).

2.5. Розрахунок річних очікуваних втрат (ОЧР**):**

$$РОВ = ОРВ \times ОЧР = 9\,000\,000 \text{ грн} \times 0.01 = 90\,000 \text{ грн/рік.} \quad (1)$$

Висновок кількісної оцінки: бездіяльність щодо цього ризику в середньому обходитиметься суб'єкта кіберзахисту у 90 000 грн на рік.

3. Оцінка ризиків кібербезпеки об'єктового рівня за допомогою Баєсівського методу

Використаємо приклад з додатка 7 до Методики ідентифікації та оцінювання ризиків кібербезпеки для застосування Баєсівського методу.

3.1. Ідентифікація та формалізація ризику − цільова подія (ризик А)

Ризик А: несанкціонована компрометація сервера баз даних «СБД_Портал».

3.2. Встановлення апріорної ймовірності (P(A))

На основі внутрішньої статистики інцидентів за попередні 3 роки та галузевих звітів НКЦК при РНБО України аналітики кібербезпеки суб'єкта кіберзахисту визначили, що апріорна ймовірність компрометації СБД_Портал становить

$$P(A) = 0.01\ (1\%). \quad (2)$$

Ймовірність того, що ризик не реалізується (¬A):

$$P(\neg A) = 1 - P(A) = 1 - 0.01 = 0.99. \quad (3)$$

3.3. Збір нової інформації щодо ймовірності реалізації ризику кіберзагрози (B) та її підтвердження

Оновлена інформація B: «Надходження офіційного повідомлення від CERT-UA про активну експлуатацію критичної вразливості CVE-YYYY-XXXX у програмному забезпеченні СУБД (наприклад, PostgreSQL), яка використовується на нашому СБД_Портал, та про рекомендацію негайно застосувати патч».

3.4. Оцінка релевантності оновленої інформації

P(B | A) (ймовірність отримання оновленої інформації за умови реалізації ризику): якщо наш СБД_Портал вже був скомпрометований (що є нашою гіпотезою A), наскільки ймовірно, що ми отримаємо таке повідомлення від CERT-UA? Експерти з безпеки припускають цю ймовірність як високу, оскільки CERT-UA активно відстежує такі загрози.

$$P(B \mid A) = 0.8\ (80\%). \quad (4)$$

$P(B \mid \neg A)$ (ймовірність отримання оновленої інформації за умови нереалізації ризику): якщо наш СБД_Портал не скомпрометовано (тобто ¬A), наскільки ймовірно, що ми все одно отримаємо таке повідомлення від CERT-UA? Навіть якщо СБД не скомпрометовано, CERT-UA все одно розсилає попередження про критичні вразливості, щоб суб'єкти кіберзахисту могли превентивно захиститися. Однак ймовірність того, що таке повідомлення буде отримано саме в той момент, коли система не скомпрометована, але загроза настільки ж висока, як у випадку її реалізації, є меншою. Експерти оцінюють цю ймовірність як нижчу.

$$P(B \mid \neg A) = 0.1\ (10\%). \quad (5)$$

3.5. Обчислення апостеріорної ймовірності ($P(A \mid B)$)

Обчислення граничної ймовірності отримання оновленої інформації (P(B)):

$$P(B) = P(B \mid A) \times P(A) + P(B \mid \neg A) \times P(\neg A), \quad (6)$$

$$P(B) = (0.8 \times 0.01) + (0.1 \times 0.99) = 0.008 + 0.099 = \mathbf{0.107} \quad (7)$$

Застосування Баєсівської формули:

$$P(A \mid B) = \frac{P(B|A) \times P(A)}{P(B)}, \quad (8)$$

$$P(A \mid B) = (0.8 \times 0.01) \div 0.107 = 0.008 \div 0.107 \approx \mathbf{0.07476\ (7.48\%)} \quad (9)$$

3.6. Інтерпретація та ітерація

Аналіз оновленої оцінки: початкова (апріорна) ймовірність компрометації СБД_Портал становила 0.01 (1%). Після отримання оновленої інформації (повідомлення CERT-UA про критичну вразливість) оновлена (апостеріорна) ймовірність зросла до ≈ 0.0748 (7.48%).

Висновки щодо впливу оновленої інформації: надходження повідомлення про критичну вразливість від CERT-UA суттєво збільшило оцінку ймовірності компрометації СБД. Це зростання з 1% (**90 000 грн/рік**.) до майже 7.5% (**673 200 грн/рік)** є значним і вимагає негайних дій.

Прийняття управлінських рішень: на підставі цієї оновленої кількісної оцінки, керівництво суб'єкта кіберзахисту «Державні послуги Онлайн» має прийняти рішення про термінове впровадження заходів зменшення ризику, наприклад: негайне застосування патча для усунення вразливості CVE-YYYY-XXXX на СБД_Портал; проведення додаткового сканування вразливостей та аналізу логів СБД для виявлення ознак компрометації; посилення моніторингу трафіка, що йде до/від СБД.

Динамічне оновлення оцінок (ітерація): якщо через тиждень після патчування СБД буде отримано нову інформацію (наприклад, «результати сканування не виявили нових критичних вразливостей, і аномальної активності в логах не зафіксовано»), то поточна апостеріорна ймовірність (0.0748) стане новою апріорною ймовірністю для наступного циклу оцінки. Це дозволить суб'єкту кіберзахисту постійно уточнювати свої оцінки ризиків та адаптувати заходи з кіберзахисту.

_____