ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
02 червня 2026 року N 402

Методика
оцінювання ризиків кібербезпеки

I. Загальні положення

1. Ця Методика встановлює єдиний підхід до ідентифікації та оцінювання ризиків кібербезпеки для органів державної влади, інших державних органів, органів місцевого самоврядування, державних підприємствам, установ та організацій, які є власниками або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем (далі - системи), в яких обробляються державні інформаційні ресурси (далі - ДІР) або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом (далі - ІзОД), операторами критичної інфраструктури та власниками або розпорядниками об'єктів критичної інформаційної інфраструктури (далі - ОКІІ) та застосовується під час формування поточного та/або цільового станів кіберзахисту, розроблення планів кіберзахисту.

Власники або розпорядники системи можуть використовувати іншу методику оцінки ризиків кібербезпеки за умови наявності затвердженої власником або розпорядником системи власної методики оцінки ризиків кібербезпеки, яка розроблена відповідно до вимог і національних стандартів у сфері захисту інформації та кіберзахисту або стандартів, настанов, рекомендацій, аналітичних оглядів та інших документів, розроблених та прийнятих іноземними та міжнародними організаціями у сфері кібербезпеки.

2. У цій Методиці наведені нижче терміни вживаються в таких значеннях:

актив - будь-який матеріальний чи нематеріальний ресурс, який має визначену або потенційну цінність для об'єкта кіберзахисту, використовується в його діяльності та може зазнати впливу кіберзагроз;

вразливість - властивість активу або групи активів, яке може бути використане для реалізації однієї чи декількох кіберзагроз;

вплив (наслідки) - шкода, завдана об'єкту кіберзахисту внаслідок реалізації кіберзагрози (порушення конфіденційності, цілісності, доступності інформації; фінансові, репутаційні, операційні втрати, шкода національній безпеці тощо);

частота виникнення - оцінка того, наскільки часто в рік може виникати кіберзагроза.

Інші терміни вживаються у значеннях, наведених у Законах України "Про основні засади забезпечення кібербезпеки України", "Про Державну службу спеціального зв'язку та захисту інформації України", "Про захист інформації в інформаційно-комунікаційних системах", "Про критичну інфраструктуру", Загальних вимогах з кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року N 518, Національному плані реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженому постановою Кабінету Міністрів України від 26 листопада 2025 року N 1533, Мінімальних вимогах до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року N 373, Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженому постановою Кабінету Міністрів України від 16 травня 2023 року N 497.

3. Метою цієї Методики є встановлення порядку оцінки ризиків і прийняття обґрунтованих рішень на основі отриманих результатів оцінювання щодо впровадження заходів з кіберзахисту, пріоритизації ресурсів та формування планів для обробки ризиків кібербезпеки відповідно до вимог чинного законодавства.

4. Ця Методика призначена для використання власниками або розпорядниками системи, в яких обробляються ДІР або ІзОД, операторами критичної інфраструктури та власниками або розпорядниками ОКІІ (далі - суб'єкти кіберзахисту).

5. Методика передбачає застосування якісних і кількісних методів оцінювання ризиків кібербезпеки, зокрема кількісного методу, що ґрунтується на використанні теореми Баєса (Баєсівський метод).

6. Оцінювання ризиків кібербезпеки здійснюється не рідше одного разу на рік, а також у разі виникнення суттєвих змін в системах, сервісах або процесах обробки ДІР, ІзОД чи на ОКІІ.

II. Ідентифікація активів (групи активів)

1. Суб'єкт кіберзахисту формує вичерпний перелік активів, що може включати ДІР, ІзОД, іншу інформацію, яка потребує захисту, а також системи та їх складові (сервери, бази даних, мережеве обладнання тощо), що обробляють таку інформацію.

Активами можуть бути апаратне та програмне забезпечення, технологічні засоби, інформація, персонал, послуги, процеси та інші ресурси.

2. З метою спрощення процесу оцінювання ризиків кібербезпеки активи з подібними характеристиками, які піддаються однаковим кіберзагрозам, можуть об'єднуватися у групи.

3. Для кожного активу або групи активів призначається особа, яка відповідає за управління ризиками кібербезпеки відповідного активу (групи активів), включаючи їх обробку та моніторинг.

4. Кожному активу (групі активів) присвоюється рівень критичності, який визначається на основі таких факторів, які дозволяють об'єктивно класифікувати активи (групи активів) за рівнями критичності, що є основою для подальшої пріоритизації заходів із кіберзахисту:

рівень важливості для виконання функцій об'єкта кіберзахисту - оцінюється ступінь впливу активу на досягнення місії об'єкта, його стратегічних цілей (чим більше актив залучений у ключових процесах, тим вищий його рівень критичності);

законодавчі та нормативні вимоги - визначаються вимоги законодавства та нормативних документів щодо кіберзахисту інформації, що обробляється на активі (наприклад, ІзОД);

потенційний вплив на безперервність роботи - аналізується, наскільки втрата або порушення роботи активу може вплинути на безперервність критичних процесів;

фінансові, репутаційні та інші ризики, що мають значення для діяльності суб'єкта кіберзахисту, - оцінюється ймовірний фінансовий збиток, що може виникнути в результаті компрометації активу (витрати на відновлення, штрафи, втрата прибутку), а також можлива шкода для репутації об'єкта кіберзахисту та інші негативні наслідки, пов'язані з порушенням конфіденційності, цілісності та доступності інформації;

взаємозалежність активів - враховується, чи є актив ключовою ланкою в ланцюгу залежностей між іншими системами (вихід з ладу такого активу може спричинити каскадні порушення в роботі залежних систем).

III. Ідентифікація загроз та вразливостей

1. Для кожного критичного активу (групи активів) визначається перелік актуальних кіберзагроз. Джерелами інформації для ідентифікації таких загроз є, зокрема:

національні та міжнародні каталоги кіберзагроз, такі як IT-Grundschutz, NIST, ENISA, MITRE ATT&CK®;

дані, надані суб'єктами національної системи реагування на кіберінциденти, кібератаки та кіберзагрози;

результати проведення оцінювання стану кіберзахисту та проведення незалежного тесту (тестування на проникнення);

аналіз подій кібербезпеки та кіберінцидентів;

технічна документація виробників програмного забезпечення та обладнання;

публікації про кіберзагрози та вразливості у відкритих джерелах інформації та результати власного аналізу кіберзагроз;

особистий досвід суб'єкта кіберзахисту або дані, отримані від партнерів по співробітництву;

результати експертного обговорення із залученням фахівців з кібербезпеки, системних та інших адміністраторів, користувачів систем, що забезпечують реалізацію функціонального призначення активу.

2. Ідентифікація вразливостей, які можуть бути використані ідентифікованими кіберзагрозами, здійснюється на основі аналізу інформації з таких джерел:

результатів виявлення вразливостей, сканування інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем та мереж з метою виявлення вразливостей, які можуть мати значний вплив, пошуку та виявлення потенційної вразливості систем, електронних комунікаційних мереж, оцінки стану захищеності ДІР у системах та тестування на проникнення, проведення незалежного тесту (тестування на проникнення);

звітів виробників програмного забезпечення та обладнання про виявлені вразливості;

даних, отриманих від системи моніторингу подій та управління інформаційною безпекою;

результатів внутрішніх та зовнішніх аудитів кібербезпеки;

аналізу внутрішньої документації, включаючи політики безпеки, інструкцій та регламентів;

інформації з відкритих джерел інформації про вразливості;

звітів та рекомендацій уповноважених державних органів;

результатів аналізу існуючих засобів захисту та оцінка їх ефективності;

результати здійснення дослідником пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

IV. Якісний метод оцінювання ризиків кібербезпеки

1. Для кожної пари "кіберзагроза-вразливість" конкретного активу (групи активів) проводиться оцінка за двома параметрами:

оцінка впливу (наслідків) - визначається рівень потенційної шкоди у разі реалізації ризиків кібербезпеки (оцінка має враховувати не лише фінансові, а й операційні, репутаційні та безпекові наслідки для держави (рівні оцінювання впливу (наслідків) кіберзагрози на національному рівні наведено в додатку 1 до цієї Методики));

оцінка очікуваної частоти / ймовірності реалізації - визначається ймовірність реалізації загрози з урахуванням існуючих заходів захисту, рівня мотивації та можливостей потенційних зловмисників (відповідно до додатка 2 до цієї Методики).

2. Описові поля (графи), наведені в додатку 1 до цієї Методики ("Опис впливу на державні інформаційні ресурси та інформацію, вимоги щодо захисту якої встановлено законом") і в додатку 2 до цієї Методики ("Опис стану кіберзахисту"), можуть адаптуватися суб'єктом кіберзахисту з урахуванням його специфіки та практичних потреб.

3. Рівень ризиків кібербезпеки визначається шляхом поєднання результатів оцінювання впливу (наслідків) кіберзагрози (додаток 1) та оцінювання очікуваної частоти / ймовірності реалізації кіберзагрози (додаток 2).

Поєднання зазначених оцінок здійснюється шляхом визначення числового значення ризику, яке розраховується відповідно до Матриці ризиків кібербезпеки (додаток 3 до цієї Методики).

Отримане числове значення ризику відповідає одному із п'яти рівнів:

критичний (20 - 25) - неприйнятний ризик кібербезпеки, що відповідає надзвичайному та критичному рівню критичності кіберінциденту/кібератаки; вимагає негайного впровадження комплексних заходів для його зменшення та локалізації;

високий (15 - 19) - неприйнятний ризик кібербезпеки, що відповідає високому рівню критичності кіберінциденту/кібератаки; вимагає визначення та реалізації заходів з обробки ризиків кібербезпеки з чіткими термінами та відповідальних структурних підрозділів (посадових осіб) суб'єкта кіберзахисту; бездіяльність може призвести до серйозних порушень у сталому, надійному та штатному режимі функціонування систем;

середній (6 - 14) - прийнятний ризик кібербезпеки, що відповідає середньому рівню критичності кіберінциденту/кібератаки; не потребує додаткових негайних заходів, але підлягає регулярному перегляду в рамках загального управління ризиками; заходи безпеки, що вже впроваджені або передбачені планом кіберзахисту, забезпечують належний захист від більшості типових кіберзагроз;

низький (3 - 5) - мінімальний або незначний ризик кібербезпеки, що відповідає низькому рівню критичності кіберінциденту/кібератаки; не потребує додаткових заходів, крім стандартного операційного моніторингу та планових перевірок; існуючі заходи з кіберзахисту забезпечують винятково високий рівень захисту, і ймовірність реалізації кіберзагрози є вкрай малою;

дуже низький (0 - 2) - мінімальний або незначний ризик кібербезпеки, що відповідає некритичному рівню критичності кіберінциденту/кібератаки; не потребує додаткових заходів, крім стандартного операційного моніторингу та планових перевірок; існуючі заходи безпеки забезпечують винятково високий рівень захисту, і ймовірність реалізації загрози є вкрай малою.

V. Обробка ризиків кібербезпеки та звітування

1. Суб'єктом кіберзахисту забезпечується ведення переліку ризиків кібербезпеки за формою, визначеною у додатку 4 до цієї Методики. До переліку включаються всі ідентифіковані ризики кібербезпеки, які підлягають регулярному перегляду та актуалізації.

Для всіх ризиків кібербезпеки розробляється план обробки ризиків кібербезпеки, який може включати дії щодо:

зменшення (модифікації) ризику кібербезпеки - впровадження нових або посилення існуючих заходів захисту (технічних, організаційних);

прийняття ризику кібербезпеки - формалізоване, документально підтверджене та затверджене керівництвом суб'єкта кіберзахисту рішення не застосовувати заходів для зниження ризику. Таке рішення може бути ухвалене лише у випадках, коли витрати на впровадження заходів захисту не є пропорційними рівню потенційних збитків від реалізації кіберзагрози, або ефективні заходи невідомі, або частота виникнення / ймовірність реалізації кіберзагрози та рівень її впливу є прийнятними (незначними) для діяльності суб'єкта кіберзахисту;

уникнення ризику кібербезпеки - відмова від діяльності або використання активу (групи активів), що є джерелом ризику, шляхом реструктуризації відповідних робочих процесів або систем;

передача ризику кібербезпеки (розподіл ризиків кібербезпеки) - передача ризику третій стороні, наприклад, через страхування активів або за допомогою аутсорсингу;

моніторинг ризику кібербезпеки - усі ризики кібербезпеки, включаючи ті, що були прийняті, підлягають постійному контролю. Результати моніторингу та відомості про коригування заходів захисту вносяться до переліку ризиків кібербезпеки для забезпечення його актуальності.

2. За результатами оцінки складається звіт про оцінювання ризиків кібербезпеки (далі - звіт), який містить:

перелік та класифікацію активів (групи активів);

опис ідентифікованих ризиків кібербезпеки;

перелік ризиків кібербезпеки із зазначенням оцінок частоти виникнення/ймовірності, впливу та фінального рівня;

рекомендації та план обробки ризиків кібербезпеки.

3. За рішенням керівника суб'єкта кіберзахисту, звіт може бути доповнений іншими відомостями, необхідними для повного та обґрунтованого ухвалення рішень щодо управління ризиків кібербезпеки, з урахуванням специфіки діяльності суб'єкта кіберзахисту та поточних загроз.

4. Звіт є основою для подальшого планування робіт із кіберзахисту та для подальшого прийняття рішень щодо обробки ризиків кібербезпеки.

5. Форма звіту про оцінювання ризиків кібербезпеки та плану обробки ризиків кібербезпеки є довільною та визначається суб'єктом кіберзахисту. Для їх оформлення може використовуватися форма переліку ризиків кібербезпеки, наведена у додатку 4 до цієї Методики, з урахуванням її адаптації відповідно до змісту та призначення звіту або плану обробки ризиків кібербезпеки.

VI. Кількісний метод оцінювання ризиків кібербезпеки

1. Проведення кількісного аналізу ризиків кібербезпеки застосовується до всіх ризиків кібербезпеки, які були оцінені за критичним та високим рівнями. Застосування кількісного методу оцінювання до інших ризиків кібербезпеки здійснюється за рішенням керівника суб'єкта кіберзахисту.

2. Метою кількісного аналізу ризиків кібербезпеки є визначення їх фінансових показників, що дозволяє:

здійснювати порівняння та пріоритизацію критичних ризиків кібербезпеки; обґрунтовувати економічну доцільність витрат на впровадження заходів із кіберзахисту;

надавати керівництву суб'єкта кіберзахисту конкретні дані для ухвалення рішень щодо інвестицій у кібербезпеку.

3. Для кількісної оцінки ризиків кібербезпеки розраховуються річні очікувані втрати (РОВ) активу (групи активів) за формулою:

$$РОВ = ОРВ \times ОЧР, \text{ де} \quad (1)$$

ОРВ (очікувані разові втрати) - фінансові втрати, що виникають внаслідок одного інциденту;

ОЧР (очікувана частота реалізації) - прогнозована кількість реалізацій ризиків кібербезпеки протягом одного року (прогнозована кількість інцидентів протягом одного року).

4. Очікувана частота реалізації може базуватися на:

статистичних даних - звітах CERT-UA, Національного координаційного центру кібербезпеки, внутрішній статистиці інцидентів за попередні періоди та інших доступних джерелах;

експертній оцінці - враховуючи актуальність загроз, наявність вразливостей та привабливість активу (групи активів) для зловмисників.

5. Розрахунок ОРВ проводиться за формулою:

$$ОРВ = ВА \times КВ, \text{ де} \quad (2)$$

ВА (вартість активу (групи активів)) - сукупна вартість активу (групи активів);

КВ (коефіцієнт вразливості) - частка вартості активу (групи активів) (у відсотках, від 0 % до 100 %), яка буде втрачена внаслідок одного інциденту.

6. Вартість активу включає, але не обмежується:

балансовою вартістю обладнання та програмного забезпечення;

вартістю відновлення даних та працездатності системи (включаючи оплату праці фахівців, закупівлю нового програмного забезпечення/обладнання тощо);

втрати від переривання процесів, що виникає внаслідок неможливості надання послуг чи виконання функцій суб'єктом кіберзахисту;

вартістю компенсації збитків третім особам (включаючи штрафи за порушення законодавства про захист персональних даних тощо);

репутаційними втратами, що оцінюються експертно;

вартістю розслідування кіберінциденту;

іншими витратами.

Приклад оцінювання ризиків кібербезпеки за кількісним методом наведено в додатку 5 до цієї Методики.

7. Комплексний підхід до оцінки ризиків кібербезпеки поєднує якісний та кількісний методи. Якісний аналіз використовується для початкової ідентифікації та класифікації ризиків кібербезпеки, тоді як кількісний метод, що застосовується для ризиків кібербезпеки із високим і критичним рівнем, допомагає визначити їхні фінансові показники та обґрунтувати інвестиції у кібербезпеку.

Оскільки не можна точно визначити частоту виникнення кіберінцидентів/кібератак чи їхні наслідки, на практиці можна застосувати більш гнучкі методи такі як Баєсівські мережі довіри, метод імітаційного моделювання Монте-Карло, аналіз дерев подій та відмов, оцінка рентабельності інвестицій у кібербезпеку тощо.

VII. Баєсівський метод кількісної оцінки ризиків кібербезпеки

1. Для кількісного оцінювання ризиків кібербезпеки може застосовуватися Баєсівський метод, який передбачає оновлення значень ймовірностей реалізації ризиків на основі нової інформації про кіберінциденти, кіберзагрози або зміни стану захищеності систем.

2. Метод базується на теоремі Баєса та забезпечує адаптивне уточнення оцінок ризиків з урахуванням поточних умов функціонування і суттєвих змін у системах, сервісах або процесах обробки ДІР, ІзОД чи на ОКІІ.

3. Результатом цього процесу ϵ отримання апостеріорних ймовірностей, які надають більш точну оцінку ймовірності реалізації ризику кібербезпеки або успішної кібератаки. Метод дозволяє перейти від суб'єктивних експертних оцінок до точних числових значень, які відображають актуальний стан загроз та вразливостей.

4. При застосуванні Баєсівського методу апріорна ймовірність P(A) може визначатися на основі очікуваної частоти виникнення (реалізації) загрози, як ймовірність виникнення, принаймні однієї події протягом визначеного інтервалу часу (наприклад, року або місяця), з використанням відповідних математичних моделей розподілу.

5. Баєсівський метод передбачає оновлення оцінок ймовірності реалізації ризиків кібербезпеки на основі оновленої інформації про інциденти, результати сканування вразливостей або змін у профілі загроз, математичне представлення методу має такий вигляд:

$$P(A|B) = \frac{P(B|A) \times P(A)}{P(B)}, \text{ де} \quad (3)$$

P(A | B) - апостеріорна ймовірність: оновлена ймовірність події A (ризик кібербезпеки) після врахування оновленої інформації щодо ймовірності реалізації ризиків кібербезпеки B;

P(B | A) - ймовірність правдоподібності: ймовірність спостереження даних B за умови, що подія A відбулася. Цей показник кількісно оцінює, наскільки нові дані підтверджують гіпотезу про ризик;

P(A) - апріорна ймовірність: початкова оцінка ймовірності події A до отримання будь-яких нових даних. Ця ймовірність може ґрунтуватися на статистичних даних про кіберінциденти за попередні звітні періоди, експертних знаннях або попередніх дослідженнях;

P(B) - гранична правдоподібність (маргінальна ймовірність): загальна ймовірність отримання даних B незалежно від реалізації події A.

6. Значення граничної правдоподібності P(B) розраховується за допомогою закону повної ймовірності. Цей закон враховує всі можливі взаємозаперечні та вичерпні стани, в загальному - подія A та її доповнення - A (не A). Формула для обчислення P(B) має такий вигляд:

$$P(B) = P(B|A) \times P(A) + P\left(B\middle|\neg A\right) \times P(\neg A), \quad (4)$$

де P(B | ¬A) - ймовірність спостереження оновленої інформації B за умови, що подія A не відбулася. Цей показник у формулі є нормалізуючим фактором, який гарантує, що сума всіх можливих апостеріорних ймовірностей дорівнює 1, що робить P(A | B) дійсною ймовірністю.

Приклад застосування Баєсівського методу кількісної оцінки ризиків кібербезпеки для кіберзагрози об'єктового рівня наведено в додатку 6 до цієї Методики.

7. Послідовність дій для застосування Баєсівського методу дає змогу об'єктивно оновлювати оцінки ймовірності реалізації ризиків кібербезпеки на основі нових даних, отриманих у процесі кількісної оцінки ризиків кібербезпеки.

Апріорна ймовірність реалізації ризиків кібербезпеки встановлюється на початковому етапі аналізу, ґрунтуючись на наявних даних, статистиці, експертних оцінках та результатах попередніх досліджень. Ця ймовірність відображає поточний ступінь впевненості у реалізації ризиків кібербезпеки до того, як буде отримана оновлена інформація.

Здійснюються ідентифікація та збір об'єктивних даних, спостережень або інформації, які можуть вплинути на оцінку ймовірності ризиків кібербезпеки. Оновлена інформація щодо реалізації ризиків кібербезпеки повинна бути релевантна та зафіксована.

8. Далі проводиться оцінка двох ключових умовних ймовірностей, що базуються на експертних знаннях, статистиці та моделюванні:

ймовірність отримання оновленої інформації щодо реалізації ризиків кібербезпеки (P(A | B)), яка показує наскільки характерною є отримана інформація для конкретної кіберзагрози;

ймовірність отримання оновленої інформації за умови, що ризик не реалізувався (P(B | ¬A)), що враховує можливість появи аналогічних відомостей з інших причин (наприклад, технічні збої, що не пов'язані з атакою).

На основі початкової оцінки та цих показників за допомогою формули Баєса обчислюється уточнена ймовірність реалізації ризику. Вона є оновленою кількісною оцінкою рівня ризику, яка вже враховує отриману інформацію.

Наступним проводиться порівняння уточненої ймовірності з початковою. Це дозволяє визначити, яка саме інформація змінила рівень ризику (підвищили його, знизили чи залишили без змін) та наскільки суттєвим є вплив на загальний стан кібербезпеки.

9. На основі оновленої кількісної оцінки ризиків кібербезпеки приймаються обґрунтовані управлінські рішення щодо обробки ризику (зменшення, прийняття, уникнення, передача) та коригування планів заходів із забезпечення кібербезпеки.

У разі надходження нових релевантних доказів постеріорна ймовірність, отримана на поточному етапі, стає новою апріорною ймовірністю для наступного циклу оцінки, що забезпечує безперервне уточнення та підвищення точності оцінок ризиків кібербезпеки.

Приклади застосування Баєсівського методу кількісної оцінки ризиків кібербезпеки для кіберзагроз національного рівня наведено у додатку 7 до цієї Методики.

Приклад оцінювання ризиків кібербезпеки для кіберзагрози об'єктового рівня за якісним, кількісним та Баєсівським методом кількісної оцінки ризиків кібербезпеки наведено у додатку 8 до цієї Методики.

Директор Департаменту
кіберзахисту Адміністрації Держспецзв'язку **Дмитро ПАХОЛЬЧЕНКО**

Додаток 1
до Методики оцінювання ризиків кібербезпеки
(пункт 1 розділу IV)

Рівні
оцінювання впливу (наслідків) кіберзагрози на національному рівні

Рівень	Назва	Опис впливу на ДІР та інформацію, вимога щодо захисту якої встановлена законом, в системах, на ОКІІ, а також у сферах використання ДІР
5	Катастрофічний	Порушення функціонування систем та/або ОКІІ, що містять ДІР; значна шкода національній безпеці; тривале (понад 24 год) припинення надання життєво важливих функцій та/або послуг
4	Дуже високий	Значні репутаційні/фінансові втрати держави; суттєве порушення функціонування систем, які обробляють інформацію, що містять ДІР, ОКІІ (8 - 24 год); розголошення інформації, що становить державну таємницю
3	Високий	Локальне порушення конфіденційності, цілісності, доступності ДІР, систем, що містять ДІР, на ОКІІ; значні фінансові збитки; короткочасне (1 - 8 год) порушення надання життєво важливих функцій та/або послуг; несанкціонований доступ до ДІР та інформації з обмеженим доступом; витік персональних даних громадян
2	Середній	Незначні фінансові втрати; короткочасне зниження продуктивності функціонування систем, що містять ДІР, ОКІІ (до 1 год); необхідність у відновленні даних з резервних копій; локальний репутаційний збиток.
1	Незначний	Мінімальний вплив на функціонування систем, що містять ДІР, ОКІІ; відсутність фінансових збитків; інформація, що була скомпрометована, є публічною.

_____

Додаток 2
до Методики оцінювання ризиків кібербезпеки
(пункт 1 розділу IV)

Оцінювання
очікуваної частоти/ймовірності реалізації кіберзагрози

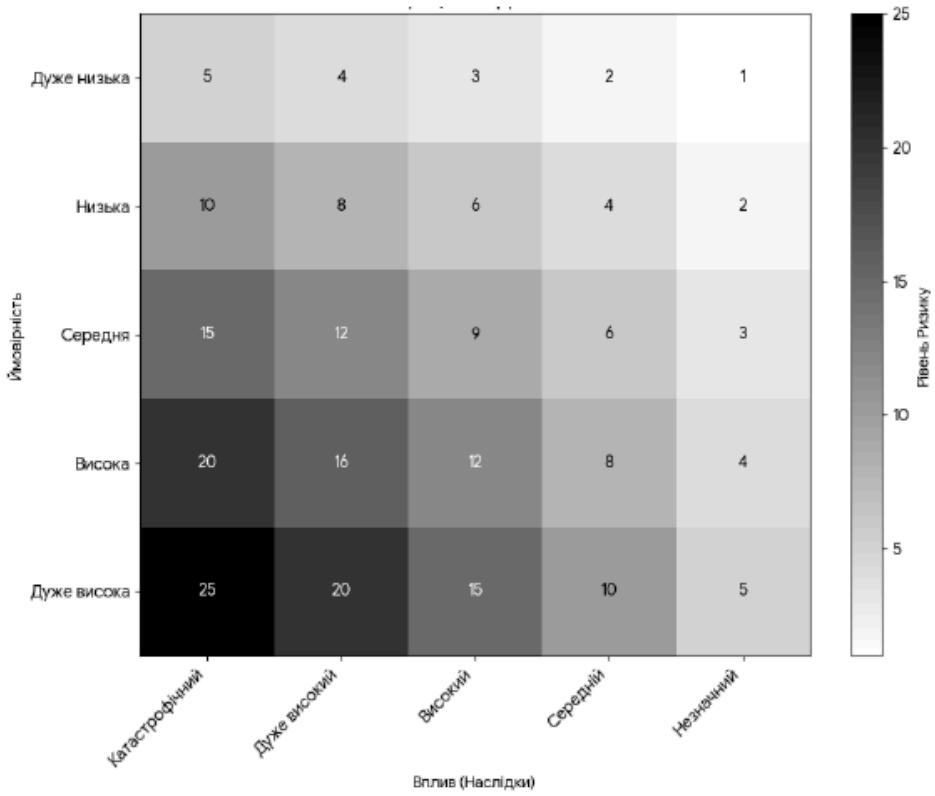
Категорія ймовірності (частота виникнення)	Бали (для якісного методу оцінювання ризиків)	Ймовірність/відсотки (для кількісного методу оцінювання ризиків)	Опис стану кіберзахисту

1	2	3	4
Дуже висока	5	0,8 - 1 80 - 100 %	Організаційний рівень: Політики кібербезпеки та плану реагування на інциденти немає. Відповідальність за безпеку не закріплена за конкретним підрозділом чи особою. Співробітники не проходять інструктажі та систематичні тренінги щодо кібергігієни. Технічний рівень: На критичних системах немає базових засобів захисту (антивірус, міжмережевий екран). Існують відомі, публічно доступні вразливості, які не виправлені. Після аудитів виявлені значні прогалини, які досі не усунуті.
Висока	4	0,6 - 0,8 60 - 80 %	Організаційний рівень: Політика кібербезпеки існує лише у формальному вигляді, але не застосовується на практиці. План реагування на інциденти або відсутній, або не тестується. Навчання проводяться несистематично і не охоплюють всіх співробітників. Технічний рівень: Оновлення ПЗ та систем безпеки виконується нерегулярно. Немає багатофакторної автентифікації для облікових записів з високими привілеями. Існують невиправлені критичні вразливості.
Середня	3	0,4 - 0,6 40 - 60 %	Організаційний рівень: Політика кібербезпеки розроблена та затверджена, але не повністю впроваджена. План реагування на інциденти існує, але може мати прогалини. Навчання проводяться періодично, але їх ефективність не оцінюється. Технічний рівень: Впроваджені стандартні засоби захисту, але в їх конфігурації чи моніторингу є недоліки. Зафіксовано поодинокі, але частково успішні спроби атак, які не призвели до значних наслідків.
Низька	2	0,2 - 0,4 20 - 40 %	Організаційний рівень: Існує комплексна, формалізована політика кібербезпеки. Процедури реагування на інциденти чітко визначені та регулярно тестуються. Навчання співробітників є обов'язковим і проводиться систематично. Технічний рівень: Впроваджено комплексні заходи захисту, як-от системи виявлення та запобігання вторгнень (IDS/IPS) та системи керування подіями безпеки (SIEM). Системи регулярно оновлюються. Аудити та пентести виявляють лише незначні вразливості.
Дуже низька	1	0 - 0,2 0 - 20 %	Організаційний рівень: Компанія має високий рівень зрілості у сфері кібербезпеки. Існує чітке управління ризиками. Застосовуються проактивні заходи, що дозволяють запобігати інцидентам. Персонал проходить постійне навчання та підвищення кваліфікації. Технічний рівень: Впроваджена архітектура "Zero Trust" та автоматизовані системи реагування на інциденти. Не зафіксовано відомих критичних вразливостей. Незважаючи на постійні спроби, успішних атак не було зафіксовано протягом тривалого часу (більше року).

Додаток 3
до Методики оцінювання ризиків кібербезпеки

(пункт 2 розділу IV)

Матриця
ризиків кібербезпеки



Додаток 4
до Методики оцінювання ризиків кібербезпеки
(пункт 1 розділу V)

Перелік ризиків кібербезпеки

Приклад заповнення форми

ID ризику	Актив	Кіберзагроза	Вразливість	Потенційний вплив	Рівень оцінювання	Ймовірність	Ймовірність	Рівень ризику	Обґрунтування	Стратегія обробки	Заплановані заходи	Відповідальний	Термін виконання	Статус виконання	Пріоритет	Рівень ризику	Коментарі/

					вання	(якісна)	(кількісна)	(початковий	початкового рівня		(план обробки)	на особа	нання	нання		(залишковий)	приміт-ки
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
R-001	Сервер БД (конфіденційні дані клієнтів)	Несанкціонований доступ (інсайдер)	Слабкі політики паролів, відсутність розмежування доступу	Витік даних, репутаційні втрати, штрафи	5 (Критичний)	Висока	00	Критичний	Високий ризик через критичність даних та слабкі засоби контролю	Зменшення	Впровадження MFA, посилення політик паролів, впровадження системи DLP	Начальник ІБ	30.09.2025	У процесі	Середній	Необхідне навчання персоналу	У процесі
R-002	Вебсайт (E-commerce платформа)	DDoS-атака	Недостатній захист від DDoS, відсутність балансувальника навантаження	Відмова в обслуговуванні, фінансові втрати	3 (Високий)	Середня	0.5	Високий	Значний вплив на робочий процес, існують базові, але не повноцінні засоби захисту	Зменшення	Підключення до провайдера DDoS-захисту, оптимізація мережевої інфраструктури	IT-директор	31.12.2025	Заплановано	Низький	Потрібно провести стрес-тестування	Заплановано
R-003	Робочі станції співробітників	Встановлення шкідливого ПЗ (троян)	Низький рівень обізнаності користувачів, відсутність EDR-рішення	Крадіжка облікових даних, блокування систем	3 (Високий)	Висока	0.7	Високий	Висока ймовірність через людський фактор, значний потенційний вплив	Зменшення	Регулярне навчання з кібергігієни (щоквартально), впровадження EDR-системи, жорсткіші політики встановлення ПЗ	HR-відділ, начальник ІБ	31.10.2025	У процесі	Середній	Моніторинг активності користувачів	У процесі
R-004	Застаріле ПЗ (внутрішній сервер)	Експлуатація відомих вразливостей	Неоновлюване ПЗ (Windows Server 2008), немає плану міграції	Повна компрометація сервера, втрата даних	5 (Високий)	Дуже висока	0.9	Критичний	Непідтримуване ПЗ створює величезну площу атаки	Уникнення	Міграція даних та функціоналу на новий, підтримуваний сервер з	IT-відділ	30.11.2025	Заплановано	Дуже низький	Необхідний резервний план на випадок	Заплановано

											актуальною ОС						
R-005	Корпоративний портал (інформація про проекти)	Несанкціонований перегляд даних	Слабкий контроль доступу на рівні папок, відсутність регулярного аудиту прав доступу	Витік комерційної таємниці, зниження конкурентоспроможності	2 (Середні)	Середня	0.4	Середній	Ризик є, але не такий критичний, як витік персональних даних	Прийняття	Вартість повного перегляду прав занадто висока на цьому етапі	Керівник відділу	Постійно	Прийнято	Середній	Ризик буде переглянуто при наступному циклі оцінки	Прийнято

Дата останнього оновлення: __.__.202__.

Відповідальний за перелік: _____

(власне ім'я, прізвище, посада, підрозділ, контактні дані (телефон, електронна пошта)).

_____

Додаток 5
до Методики оцінювання ризиків кібербезпеки
(пункт 6 розділу VI)

Приклад
оцінювання ризику кібербезпеки за кількісним методом

Ризик: "Тривала відмова у доступі до порталу надання електронних послуг через DDoS-атаку" (рівень за матрицею кіберризиків: критичний).

Розрахунок вартості активу (ВА):

вартість відновлення (робота інженерів): 100000 грн;

втрати від простою (24 години): 400000 грн;

репутаційні втрати (експертна оцінка): 500000 грн;

загальна ВА: 1000000 грн.

Розрахунок коефіцієнта вразливості (КВ):

кібератака не знищує дані, але призводить до простою та репутаційних втрат. Проводиться експертна оцінка, що один такий інцидент "коштує" 30 % загальної вартості активу;

КВ = 0,3 (або 30 %).

Розрахунок очікуваних разових втрат (ОРВ):

ОРВ = 1000000 грн × 0.3 = 300000 грн, що означає, що кожна успішна DDoS-атака коштуватиме організації 300000 грн.

Визначення очікуваної частоти реалізації (ОЧР):

на основі даних НКЦК при РНБО України та аналізу попередніх спроб атак очікується, що потужна атака такого типу може відбутися 1 раз на рік;

ОЧР: 1.0

Розрахунок річних очікуваних втрат (РОВ):

РОВ = 300000 грн × 1.0 = 300000 грн/рік;

бездіяльність щодо цього ризику в середньому обходитиметься суб'єкту кіберзахисту у 300000 грн на рік.

Аналіз "витрати-вигоди" та обґрунтування контрзаходів:

отриманий показник РОВ є основою для обґрунтування витрат на заходи захисту.

Пропозиція контрзаходу: упровадження хмарного сервісу захисту від DDoS-атак;

Вартість контрзаходу: 200000 грн/рік.

Перерахунок ризику після впровадження контрзаходу:

новий показник ОЧР (ймовірність успішної атаки) знижується до 0.1 (одна успішна атака раз на 10 років);

новий РОВ = 300000 грн (ОРВ) х 0.1 (новий ОЧР) = 30000 грн/рік.

Розрахунок економічного ефекту:

зменшення втрат: 300000 грн (РОВ до) - 30000 грн (РОВ після) = 270000 грн;

чиста вигода: 270000 грн (зменшення втрат) - 200000 грн (вартість захисту) = 70000 грн/рік.

Фінальне обґрунтування: інвестиція у сервіс захисту від DDoS у розмірі 200000 грн на рік є економічно доцільною, оскільки вона дозволяє запобігти очікуваним втратам у розмірі 300000 грн та забезпечує чисту річну вигоду у 70000 грн, значно підвищуючи при цьому стабільність надання послуг чи виконання функцій суб'єктом кіберзахисту.

Такі розрахунки проводяться до кожного активу або групи активів залежно від ступеня деталізації та вносяться до переліку ризиків (Додаток 5).

Запропонований стандартний метод кількісного аналізу (розрахунок річних очікуваних втрат) надає єдину, точкову оцінку ризику.

ПРИКЛАД

N	Назва ризику	Рівень за матрицею	Вартість активу (ВА)	Коефіцієнт вразливості (КВ)	Очікувані разові	Очікувана частота реалізації	Річні очікувані	Пропонований контрзахід	Вартість контрзаходу/рік	Новий ОЧР після впровадження	Новий РОВ після впровадження	Зменшення втрат	Чиста вигода/рік

		якісного оцінювання			втрати (ОРВ)	(ОЧР)/ ймовірність (ОЙР)	втрати (РОВ)						
1.	Тривала відмова у доступі до порталу надання електронних послуг через DDoS-атаку	Критичний	1000000 грн	0.3	300000 грн	1.0	300000 грн	Упровадження хмарного сервісу захисту від DDoS-атак	200000 грн	0.1	30000 грн	270000 грн	70000 грн
2.	Несанкціонований доступ до конфіденційної інформації через фішингову атаку	Високий	400000 грн	0.8	320000 грн	0.5	160000 грн	Упровадження регулярних навчань з кібергігієни для співробітників та використання додаткових інструментів фільтрації електронної пошти	50000 грн	0.1	32000 грн	128000 грн	78000 грн

Дата останнього оновлення: __.__.202__.

Відповідальний за перелік: _____

(власне ім'я, прізвище, посада, підрозділ, контактні дані (телефон, електронна пошта)).

_____

Додаток 6
до Методики оцінювання ризиків кібербезпеки
(пункт 5 розділу VII)

Приклад
застосування Баєсівського методу кількісної оцінки ризиків кібербезпеки для кіберзагрози об'єктового рівня

Сценарій. Оцінка ризику успішної фішингової атаки

1. Визначення ризику

Ризик (подія А) - це успішна фішингова атака, що призведе до компрометації облікових даних співробітника протягом наступного місяця.

2. Визначення апріорної ймовірності (P(A))

На основі історичних даних за минулий рік та експертних оцінок (наприклад, щорічні звіти про кіберзагрози, внутрішні аудити), припустимо, що апріорна ймовірність успішної фішингової атаки у організації становить 2 % (0.02). Це початкове переконання. Тобто, P(A) = 0,02 (ймовірність успішної фішингової атаки). Тоді, ймовірність того, що успішна фішингова атака не відбудеться P(¬A) = 1 - P(A) = 1 - 0,02 = 0,98.

3. Оновлення інформації щодо ймовірності реалізації ризиків кібербезпеки (B)

Розглянемо випадок коли ми отримуємо оновлену інформацію щодо ймовірності реалізації ризиків кібкрбезпеки (B): протягом останнього тижня було зафіксовано значне збільшення кількості вхідних електронних листів з підозрілими посиланнями, які були ідентифіковані системою фільтрації спаму як потенційні фішингові спроби.

4. Оцінка функції правдоподібності P(B | A) та P(B | ¬A)

Оцінка (P(B | A) та P(B | ¬A)), як правило здійснюється на основі експертної оцінки.

Припустимо P(B | A) є ймовірність спостереження збільшення підозрілих листів за умови, що успішна фішингова атака дійсно відбудеться (або є висока ймовірність її виникнення). Якщо фішингова атака неминуча, є висока ймовірність, що її передумовою буде збільшення таких спроб. Відповідно до висновків експертів ймовірність дорівнює 0,8 (80 %). Тоді ймовірність P(B | A) = 0,8.

Навіть без безпосередньої загрози успішної атаки, час від часу, наприклад, через загальний сплеск спаму або низькоякісні, неефективні спроби фішингу надходять підозрілі листи. Відповідно до оцінки експертів ймовірність спостереження збільшення підозрілих листів за умови, що успішна фішингова атака не відбудеться P(B | A) як **10 % (0.1)**. Тобто, P(B | ¬A) = 0,1 або **10 %.**

5. Обчислення граничної правдоподібності (маргінальної ймовірності) (P(B))

Це загальна ймовірність спостереження нової інформації (B) незалежно від того, чи відбудеться подія (A) чи ні.

$$P(B) = P(B \mid A) \times P(A) + P(B \mid \neg A) \times P(\neg A), \text{ тоді}$$

$$P(B) = (0{,}8 \times 0{,}02) \div 0{,}114 = 0{,}016 \div 0{,}114 \approx 0{,}1404$$

Отже, загальна ймовірність спостереження сплеску підозрілих фішингових листів становить 11.4 %.

6. Застосування формули Баєса для обчислення апостеріорної ймовірності (P(A | B))

Обчислимо оновлену ймовірність успішної фішингової атаки відповідно до оновленої інформації.

$$P(A \mid B) = \frac{P(B|A) \times P(A)}{P(B)}, \text{ тоді}$$

$$P(A \mid B) = (0.8 \times 0.02) \div 0.114 = 0.016 \div 0.114 \approx 0.1404.$$

В результаті отримання інформації про значне збільшення кількості підозрілих фішингових листів, оновлена апостеріорна ймовірність успішної фішингової атаки зросла з 2 % до приблизно 14.04 %.

7. Інтерпретація отриманих результатів

Нові дані суттєво підвищили оцінку ризику. Кількісна оцінка показує, що ймовірність успішної атаки зросла майже в 7 разів (14.04 % ÷ 2 % ≈ 7). Це свідчить, що суб'єкт кіберзахисту стикається з підвищеною загрозою, і можливо, необхідно вжити додаткових заходів безпеки (наприклад, вдосконалити інструктажі та тренінги щодо кібергігієни, тимчасово запровадити додаткові фільтри пошти тощо).

Додаток 7
до Методики оцінювання ризиків кібербезпеки
(пункт 6 розділу VII)

Приклад
застосування Баєсівського методу кількісної оцінки ризиків кібербезпеки для кіберзагрози національного рівня

Приклад розроблено з метою демонстрації послідовності дій щодо об'єктивного оновлення оцінок ймовірності реалізації кіберзагрози національного рівня на підставі отримання оновленої інформації.

1. Ідентифікація та формалізація ризику

Цільова подія (ризик A**):** Повномасштабна кібератака на об'єкти критичної інформаційної інфраструктури (ОКІІ) енергетичного сектору України з метою виведення з ладу систем управління технологічними процесами (АСУТП), що може призвести до масштабних та довготривалих перебоїв в енергопостачанні регіонів.

2. Встановлення апріорної (початкової) ймовірності (P(A))

2.1. Визначення апріорної (початкової) ймовірності

На підставі аналізу геополітичної ситуації, агресивної риторики з боку держав-агресорів, звітів про кіберактивність ворожих суб'єктів кіберпростору (зокрема, тих, що мають історію атак на енергетичні системи), а також оцінок НКЦК при РНБО України та Сил оборони України, припускається, що апріорна ймовірність повномасштабної кібератаки на ОКІІ енергетичного сектору становить P(A) = 0.1 (10 %).

2.2. Розрахунок ймовірності події, що доповнює

Ймовірність того, що ризик не реалізується (¬A), становить P(¬A) = 1 - P(A) = 1 - 0.1 = 0.9.

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

Підтвердження інформації:

Підтверджено інформацію, яка впливає на оцінку ймовірності реалізації ризику національного рівня: **підтвердження інформації** B**:** "Звіт розвідувальних даних, підтверджений кількома незалежними джерелами, про збільшення активності відомої APT-групи (Advanced Persistent Threat), пов'язаної з державою-агресором, яка спеціалізується на атаках на АСУ ТП енергетичного сектору, включаючи виявлення нових зразків шкідливого програмного забезпечення (далі - ШПЗ), призначених для компрометації промислових контролерів, та нецільові сканування мереж об'єктів енергетичної інфраструктури".

4. Оцінка релевантності оновленої інформації

4.1. Визначення ймовірності отримання оновленої інформації за умови реалізації ризику ($P(B \mid A)$**)**

Здійснено експертну оцінку умовної ймовірності отримання оновленої інформації B за умови, що повномасштабна кібератака на ОКІІ енергетичного сектору України вже готується або неминуча (A). Припускається, що у випадку такої підготовки або неминучості, ймовірність виявлення подібної активності з боку відомої APT-групи, призначеної для атаки, є дуже високою. Встановлено $P(B \mid A) = 0.95$ (95 %).

4.2. Визначення ймовірності отримання оновленої інформації за умови нереалізації ризику ($P(B \mid \neg A)$**)**

Здійснено експертну оцінку умовної ймовірності отримання оновленої інформації B за умови, що повномасштабна кібератака на ОКІІ енергетичного сектору не готується або не є неминучою ($\neg A$). Припускається, що навіть за відсутності прямої загрози повномасштабної атаки певна активність APT-груп може спостерігатися (наприклад, збір розвідувальних даних, тестування ШПЗ), але її інтенсивність та сфокусованість на конкретних цілях будуть значно меншими. Експертно встановлено, що $P(B \mid \neg A) = 0.15$ (15 %).

5. Обчислення апостеріорної ймовірності (P(A | B))

5.1. Обчислення граничної ймовірності отримання оновленої інформації ($P(B)$**):** згідно із Законом повної ймовірності:

$$P(B) = P(B \mid A) \times P(A) + P(B \mid \neg A) \times P(\neg A), \tag{1}$$

$$P(B) = (0{,}95 \times 0.1) + (0{,}15 \times 0.9) = 0{,}095 + 0{,}135 = 0{,}23 \tag{2}$$

5.2. Застосування Баєсівської формули:

$$P(A \mid B) = \frac{P(B|A) \times P(A)}{P(B)}, \tag{3}$$

$$P(A \mid B) = (0{,}95 \times 0{,}1) \div 0{,}23 = 0{,}095 \div 0{,}23 \approx 0{,}4130434783 \tag{4}$$

6. Інтерпретація та ітерація

6.1. Аналіз оновленої оцінки: апріорна ймовірність повномасштабної кібератаки на ОКІІ енергетичного сектору становила 0.1 (10 %). Після отримання оновленої інформації B (звіт розвідувальних органів про підвищену активність APT-групи) апостеріорна ймовірність ризику зросла до ≈ 0,413 (41,3 %).

6.2. Висновки щодо впливу оновленої інформації

Зростання ймовірності ризику з 10 % до понад 41 % є критичним і вказує на суттєве підвищення загрози повномасштабної кібератаки на енергетичний сектор України. Отримання оновленої інформації B є сильним індикатором безпосередньої підготовки до атаки.

6.3. Прийняття управлінських рішень

На підставі оновленої кількісної оцінки ризику, що вказує на високий (за якісною оцінкою) або критичний (за кількісною, враховуючи наслідки) рівень загрози, приймається рішення щодо негайної реалізації заходів з обробки ризику (зменшення/уникнення), що можуть включати:

а) негайне підвищення рівня готовності (готовності до реагування на інциденти) суб'єктів енергетичного сектору (впровадження посиленого моніторингу, переведення чергових змін у режим підвищеної готовності до реагування);

б) упровадження додаткових заходів кіберзахисту на ОКІІ (наприклад, посилення сегментації мереж АСУТП, оновлення сигнатур ШПЗ, проведення тестів на проникнення з акцентом на промислові системи);

в) оповіщення всіх відповідних державних органів та суб'єктів ОКІІ про підвищений рівень загрози та надання оперативних рекомендацій;

г) активація кризових планів реагування, включаючи перевірку планів відновлення після інцидентів та відпрацювання сценаріїв кібератак;

д) зміцнення міжнародного співробітництва з питань кіберрозвідки та обміну інформацією про загрози.

6.4. Динамічне оновлення оцінок (ітерація)

У разі отримання нової релевантної інформації (наприклад, зниження активності APT-групи після успішних контрзаходів, успішне блокування виявленого ШПЗ, або, навпаки, виявлення нових індикаторів компрометації) поточна апостеріорна ймовірність ($P(A \mid B) \approx 0.413$) буде використана як нова апріорна ймовірність для наступного циклу оцінки ризику. Це забезпечить безперервне уточнення та підвищення точності оцінок кіберризиків на національному рівні, дозволяючи адаптивно реагувати на динамічні зміни в кіберпросторі.

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 х 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 = **10000000 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 = 10000000 грн. × 0.9 = **9000000 грн.** Це означає, що кожна успішна компрометація СБД коштуватиме суб'єкту кіберзахисту 9000000 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**):**

$$РОВ = ОРВ \times ОЧР = 9000000 \text{ грн} \times 0.01 = 90000 \text{ грн/рік}. \quad (1)$$

Висновок кількісної оцінки: бездіяльність щодо цього ризику в середньому обходитиметься суб'єкта кіберзахисту у 90000 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 A)

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 А), 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 | ¬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 | 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 % (**90000 грн/рік.**) до майже 7.5 % (**673200 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.
