Co-funded by the
Erasmus+ Programme
of the European Union

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФРАСТРУКТУРИ ТА ТЕХНОЛОГІЙ

ФАКУЛЬТЕТ УПРАВЛІННЯ І ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ГІБРИДНІ ЗАГРОЗИ

Навчальний посібник
для здобувачів другого (магістерського)
рівня вищої освіти

Київ – 2024

Co-funded by the Erasmus+ Programme of the European Union

УДК 004.45
І74

Рекомендовано до друку Вченою радою
Державного університету інфраструктури та технологій
Міністерства освіти і науки України *(протокол № 12 від 28 червня 2024р.)*

РЕЦЕНЗЕНТИ:

Кравченко Ю.В., доктор технічних наук, професор, завідувач кафедри мережевих та інтернет технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Бідюк П.І., доктор технічних наук, професор, професор кафедри математичних методів системного аналізу ННК «ІПСА» Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Бондарчук А.П., доктор технічних наук, професор, директор навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій.

І74 Інформаційна безпека та гібридні загрози: навчальний посібник. Укл. Мухін В.Є., Завгородній В.В., Завгородня Г.А. Київ : ТОВ «ТРОПЕА», 2024. 104 с.
DOI: https://doi.org/10.32703/978-617-8268-36-7
ISBN 978-617-8268-36-7

Навчальний посібник присвячений всебічному розгляду проблем інформаційної безпеки в комп'ютерних системах, акцентуючи увагу на сучасних викликах та методах їх вирішення. Розглядаються питання прогнозування ризику виникнення небезпечних подій в умовах впливу гібридних загроз та методи передбачення наслідків небезпечних дій з боку зловмисників. Посібник розроблений для студентів, аспірантів, а також професіоналів, які працюють в галузі інформаційної безпеки та прагнуть глибше розібратися в тематиці ризиків та гідридних загроз у комп'ютерних системах. Навчальний посібник є цінним ресурсом для тих, хто прагне підвищити свою компетенцію в галузі інформаційної безпеки, розуміти ризики та гібридні загрози сучасних комп'ютерних систем, а також ефективно застосовувати знання на практиці.

Навчальний посібник підготовлено на основі матеріалів проєкту WARN «Академічна протидія гібридним загрозам» (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP), що співфінансується програмою Erasmus+ Європейського Союзу. Підтримка Європейською Комісією створення матеріалів, розміщених у даному навчальному посібнику, не є схваленням змісту, який відображає погляди лише авторів, і Комісія не несе відповідальності за будь-яке використання інформації, що міститься в ньому.

ISBN 978-617-8268-36-7 УДК 004.45

ЗМІСТ

ПЕРЕДМОВА

Гібридні загрози стають все більш поширеними в галузі інформаційної безпеки. Такі загрози включають в себе комбінацію різних методів, таких як кібератаки, дезінформація, вплив на громадську думку та інші техніки, що можуть використовуватися з метою досягнення стратегічних цілей.

Гібридні загрози можуть бути важко виявити та протистояти, оскільки вони поєднують в собі різні методи, які можуть використовуватися паралельно або послідовно. Наприклад, кібератаки можуть бути спрямовані на знищення або зміну інформації, яку потім використовують для поширення дезінформації через соціальні мережі та інші канали зв'язку.

Щоб захистити себе від гібридних загроз, необхідно розуміти їх сутність та ризики, які пов'язані з кожним методом, що використовується в загрозі. Також важливо забезпечити захист своїх комп'ютерних систем від кібератак, перевіряти джерела інформації, щоб уникнути дезінформації, і дотримуватися інших принципів кібербезпеки. Для більш ефективної боротьби з гібридними загрозами можна використовувати спеціалізовані програмні засоби та послуги зі збору та аналізу інформації, які допоможуть виявляти загрози та приймати своєчасні заходи для їх протидії. Для забезпечення кібербезпеки необхідно дотримуватися базових принципів, таких як використання складних та унікальних паролів, регулярне оновлення програмного забезпечення та антивірусів, та перевірка джерел інформації перед її поширенням.

У сучасному світі гібридні загрози використовуються в політичних та військових конфліктах, де вони можуть бути важливим інструментом для досягнення стратегічних цілей. Крім того, гібридні загрози можуть бути використані для налагодження шпигунської діяльності та отримання конфіденційної інформації.

Щоб бути готовим до протидії гібридним загрозам, необхідно вдосконалювати свої знання та навички в галузі кібербезпеки та вивчати нові методи протидії. Також важливо бути обережним при отриманні та поширенні інформації в соціальних мережах та інших медіа-каналах, а також вживати заходів забезпечення безпеки своєї комп'ютерної системи.

Національні уряди та міжнародні організації також займаються питанням протидії гібридним загрозам. Для цього створюються спеціальні центри з моніторингу та аналізу загроз, розробляються правила та рекомендації щодо кібербезпеки та проводяться різні навчальні заходи.

Одним з таких заходів є проєкт «Академічна протидія гібридним загрозам» (WARN) в межах Програми ЄС Еразмус+ за напрямом «Розвиток потенціалу вищої освіти» (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP). Вебсайт проєкту WARN: http://warn-erasmus.eu. У рамках реалізації саме цього проєкту був укладений даний навчальний посібник.

Отже, захист від гібридних загроз потребує комплексного підходу, що включає в себе як технічні, так і неконкретні заходи. Крім того, важливо пам'ятати, що ризики гібридних загроз можуть змінюватися з часом, тому важливо регулярно оновлювати свої знання та заходи щодо кібербезпеки.

РОЗДІЛ 1.
ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ

1.1. Проблема інтеграції з механізмами розподілених комп’ютерних систем
1.2. Проблема взаємодії з механізмами розподілених комп’ютерних систем
1.3. Проблема встановлення довіри між різними доменами та вузлами розподілених комп’ютерних систем
1.4. Системи безпеки розподілених комп'ютерних систем
1.5. Стандарти та керівні документи, що визначають вимоги до забезпечення безпеки інформації
1.6. Законодавча та нормативна база, що регулює питання інформаційної безпеки в Україні

Проблеми, пов'язані з забезпеченням інформаційної безпеки, є надзвичайно важливими в сучасному світі (рис. 1.1). Ці проблеми зустрічаються в усіх сферах життя, включаючи державну безпеку, бізнес, особисту безпеку та приватність [10].

Рис. 1.1. Проблеми, пов'язані з забезпеченням інформаційної безпеки

Однією з головних причин проблем забезпечення інформаційної безпеки є зростання кількості інформації, яка зберігається та обробляється в електронному вигляді. Це створює нові можливості для хакерів та кіберзлочинців, які намагаються отримати несанкціонований доступ до цієї інформації.

Іншою проблемою є відсутність належної уваги до інформаційної безпеки з боку користувачів, особливо в умовах розгортання гібридних воєн у глобальному інформаційному просторі. Це може стати наслідком недостатньої освіти або недостатнього розуміння ризиків, пов'язаних з використанням інформаційних технологій.

Нарешті, третьою проблемою є швидкий розвиток технологій та старіння систем захисту. Більшість компаній та організацій не можуть дотримуватися

вимог до безпеки, що змінюються, тому їхні системи захисту можуть стати вразливими перед новими загрозами і бути недостатньо ефективними у протидії гібридним загрозам.

З урахуванням цих проблем необхідно приділяти належну увагу забезпеченню інформаційної безпеки та вживати необхідних заходів для захисту конфіденційної інформації.

Умови гібридних загроз стали дедалі більш актуальними в сучасному світі, а проблеми забезпечення інформаційної безпеки стають все більш складними і різноманітними. Основними проблемами забезпечення інформаційної безпеки в умовах гібридних загроз є (рис. 1.2):

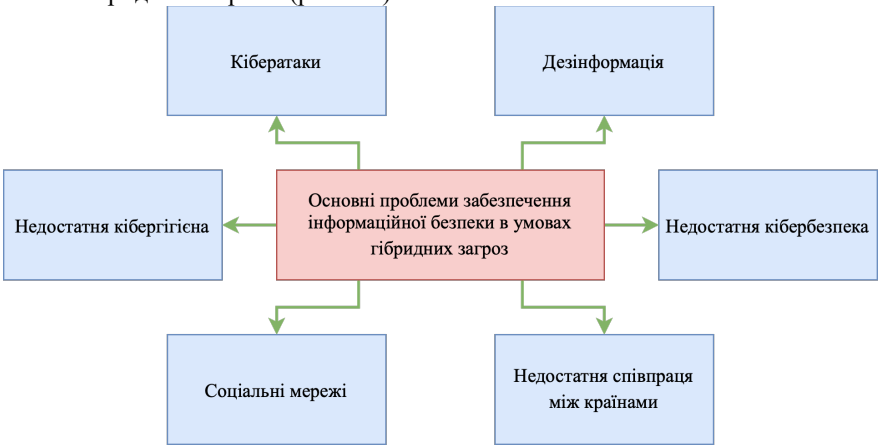

Рис. 1.2. Основні проблеми забезпечення інформаційної безпеки в умовах гібридних загроз

1. Кібератаки є одним з найбільш поширених методів атак на інформаційну безпеку. Умови гібридних загроз роблять їх більш складними, оскільки атаки можуть бути здійснені з різних джерел і використовувати різні методи. Крім того, вони можуть бути використані в комбінації з іншими методами, наприклад, з використанням дезінформації.

2. Дезінформація стає все більш поширеною в умовах гібридних загроз. За допомогою дезінформації можна дискредитувати дії влади, збільшити загрозу для національної безпеки і підривати довіру громадськості до владних структур. У таких умовах важливо забезпечити швидке реагування на дезінформацію і забезпечити доступ до достовірної інформації.

3. Недостатня кібербезпека може призвести до втрати даних і вразливості систем, які використовуються для зберігання і передачі інформації. Умови гібридних загроз можуть зробити кібербезпеку ще більш складною, оскільки можуть бути використані різні методи атак.

4. Недостатня співпраця між країнами може призвести до збільшення загроз і погіршення ситуації з інформаційною безпекою. В умовах гібридних загроз необхідна співпраця між країнами для обміну інформацією про можливі загрози та методи боротьби з ними. Також важливо співпрацювати в питаннях кібербезпеки, щоб забезпечити безпеку критичних інфраструктур та міжнародних мереж.

5. Соціальні мережі є джерелом великої кількості інформації і можуть бути використані як для поширення дезінформації, так і для збору інформації про користувачів з метою здійснення кібератак. Важливо забезпечити безпеку користувачів соціальних мереж і зменшити можливість використання цих мереж для дезінформації та кібератак.

6. Недостатня кібергігієна може призвести до небезпеки для інформаційної безпеки. Користувачі можуть стати жертвами фішингу, шпигунства або інших видів кібератак через недостатні знання про кібербезпеку. Умови гібридних загроз підсилюють ризики, тому важливо забезпечити навчання користувачів кібербезпеці та збільшити кіберграмотність громадськості.

Усі ці проблеми забезпечення інформаційної безпеки в умовах гібридних загроз потребують комплексного підходу до вирішення. Необхідно забезпечити широкомасштабну співпрацю між країнами, громадськістю, приватними та державними структурами, а також забезпечити безпеку користувачів.

1.1. Проблема інтеграції з механізмами розподілених комп'ютерних систем

Проблема інтеграції з механізмами розподілених комп'ютерних систем полягає в тому, що різні комп'ютерні системи можуть мати відмінні структури та протоколи комунікації, що ускладнює обмін даними та забезпечення сумісності між ними.

Інтеграція систем може включати в себе розробку та застосування проміжного програмного забезпечення, яке забезпечує зв'язок між системами, здійснює оцінку потенційних загроз та забезпечує зручний доступ до розподілених ресурсів. Однак, розробка такого програмного забезпечення може бути часомісткою та вимагати значних витрат [6].

Також, інтеграція з механізмами розподілених комп'ютерних систем може стикатися з проблемами безпеки. Зокрема, при обміні даними між різними системами можуть виникати проблеми з автентифікацією та авторизацією користувачів, а також забезпечення цілісності та конфіденційності даних.

Одним з можливих рішень проблеми інтеграції з механізмами розподілених комп'ютерних систем є застосування стандартів та протоколів комунікації, що забезпечують сумісність між різними системами. Наприклад, стандарт Web Services забезпечує зв'язок між різними системами через мережу Інтернет за допомогою протоколів SOAP та REST.

З метою протидії гібридним загрозам та захисту РКС розробляються відповідні засоби захисту, які інтегруються в програмно-апаратне забезпечення таких систем [1].

1.2. Проблема взаємодії з механізмами розподілених комп'ютерних систем

Для ефективної роботи засобів захисту РКС, необхідно забезпечити їх сумісність з іншими системами, що використовуються в організації. Також з огляду на широкомасштабну гібридну війну важливо забезпечити захист даних, що передаються між доменами, включаючи конфіденційні дані.

Підтримка безпеки в РКС також передбачає забезпечення захисту від різноманітних загроз, таких як віруси, троянські програми, хакерські атаки тощо. Для цього можуть використовуватись різні механізми, такі як брандмауери, антивіруси, інтеграція з системами моніторингу та аудиту безпеки.

Для ефективної роботи системи захисту РКС важливо забезпечити регулярне оновлення програмного забезпечення та встановлення необхідних патчів. Також необхідно проводити регулярні аудити та перевірки безпеки, щоб виявляти можливі вразливості та загрози та вчасно їх ліквідовувати.

Тобто, засоби захисту РКС мають забезпечувати захист від загроз на різних рівнях та забезпечувати безпеку взаємодії між доменами та вузлами. Для ефективної роботи системи захисту необхідно забезпечити сумісність з іншими системами, захист даних та регулярне оновлення та перевірки безпеки.

1.3. Проблема встановлення довіри між різними доменами та вузлами розподілених комп'ютерних систем

Встановлення довіри між різними доменами та вузлами РКС є ключовим елементом забезпечення безпеки системи в цілому. Це особливо важливо, оскільки в доменах РКС застосовуються різні технології безпеки, і механізми встановлення довіри повинні враховувати всі їх особливості для ефективної протидії гібридним загрозам.

Проблема довірчих відносин стає особливо актуальною у разі потреби управління сервісами РКС, що запускаються та керуються динамічно. Такі сервіси можуть виконувати різні завдання, такі як обробка даних з віддаленого сховища або синтез інформації, і їх запуск потребує встановлення довіри між різними доменами та вузлами РКС.

Окрім того, механізми встановлення довіри повинні забезпечувати можливість динамічної зміни рівня довіри відповідно до потреб конкретної сесії або запиту. Це забезпечує більш гнучке та ефективне управління безпекою РКС.

Усі ці фактори підкреслюють важливість ретельного проектування та розробки механізмів встановлення довіри в РКС для забезпечення комплексної та ефективної безпеки від гібридних загроз.

При встановленні довірчих відносин необхідно враховувати наступні аспекти (рис. 1.3) [3, 12]:

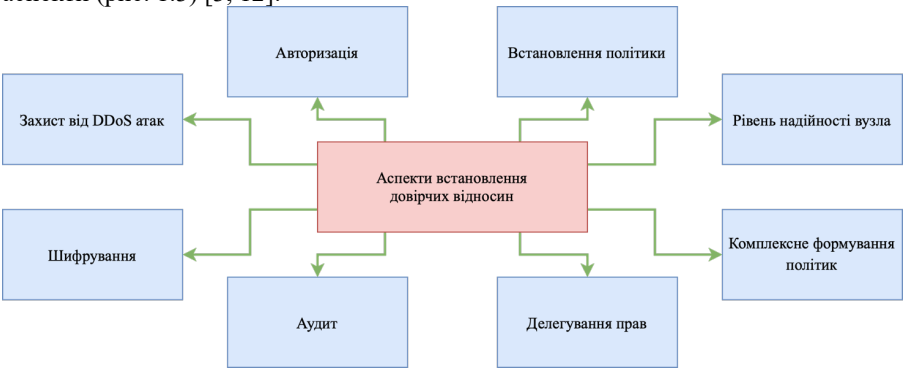

Рис. 1.3. Аспекти встановлення довірчих відносин

1. Авторизація – визначається ініціатор запуску сервісу, що має право на його використання.

2. Встановлення політики – суб'єкти повинні мати можливість створювати власні політики, визначаючи, які суб'єкти мають доступ до сервісів та які дії є допустимими. Локальна політика суб'єкта має відповідати політиці, яку підтримує РКС.

3. Рівень надійності вузла – перед ініціацією завдань у РКС суб'єкт може запросити оцінку рівня надійності вузлів РКС, яка включає наявність антивірусного захисту, міжмережевих екранів та використання VPN для обміну даними всередині РКС. Рівень надійності вузла визначається з урахуванням незалежних експертних оцінок за допомогою механізму акредитації.

4. Комплексне формування політик – політики безпеки для створених сервісів РКС створюються динамічно з урахуванням багатьох чинників: власника ресурсів, ініціатора запуску сервісу чи завдання, специфіки віртуальної системи, у якій реалізовано сервіс тощо.

5. Делегування прав – у деяких випадках тимчасові сервіси виконують дії від імені суб'єкта, що їх створив. Наприклад, обчислювальний процес може запитувати дані, що знаходяться в іншому домені РКС. У цьому випадку можуть не бути встановлені довірчі відносини між доменами [13].

6. Аудит – РКС повинна забезпечувати можливість аудиту доступу до сервісів. В умовах гібридних загроз це означає збір і аналіз інформації про доступ до сервісів з метою виявлення порушень політик безпеки або інших випадків невідповідності вимогам.

7. Шифрування – забезпечення конфіденційності інформації в РКС можна забезпечити за допомогою різних методів шифрування, наприклад, шифрування на рівні транспорту або застосування шифрування кінцевих точок.

8. Захист від DDoS атак – важливим аспектом безпеки є захист від DDoS атак, які можуть призвести до відмови в обслуговуванні сервісів. Для цього можуть застосовуватись різноманітні технології захисту, наприклад, механізми виявлення та фільтрації трафіку, використання хмарних технологій тощо.

Отже, при встановленні довірчих відносин в РКС необхідно враховувати багато аспектів, включаючи авторизацію, рівень надійності вузла, комплексне формування політик, делегування прав, аудит, шифрування та захист від DDoS атак.

Ці аспекти повинні бути взаємопов'язані та доповнювати один одного для забезпечення максимального рівня інформаційної безпеки в РКС в умовах гібридної війни.

1.4. Системи безпеки розподілених комп'ютерних систем

Системи безпеки розподілених комп'ютерних систем включають в себе механізми та процедури, які забезпечують конфіденційність, цілісність та доступність даних і ресурсів у розподіленому середовищі.

Для забезпечення безпеки розподіленої комп'ютерної системи можуть використовуватися різні методи і технології, такі як (рис. 1.4) [18]:

Рис. 1.4. Методи і технології для забезпечення безпеки розподіленої комп'ютерної системи

1. Використання брандмауера і системи виявлення вторгнень для захисту мережевого рівня від несанкціонованого доступу та атак.

2. Використання механізмів захисту операційної системи, таких як контроль доступу, авторизація та криптографічні методи.

3. Використання методів захисту додатків, таких як валідація введення, захист від SQL-ін'єкцій та захист від міжсайтового скриптування.

4. Захист баз даних від несанкціонованого доступу та викрадення даних, використовуючи методи шифрування даних, контроль доступу та моніторинг активності користувачів.

5. Контроль прав доступу користувачів до різних ресурсів системи та застосування різних рівнів авторизації та автентифікації.

6. Використання резервних копій для забезпечення можливості відновлення системи в разі випадкового видалення або випадкової пошкодження даних.

7. Постійний моніторинг стану безпеки системи та реагування на події, що можуть загрожувати безпеці системи.

Розробка та реалізація моделі безпеки розподіленої комп'ютерної системи є складним завданням, яке потребує великої уваги до деталей та знання з різних областей, таких як мережна безпека, безпека операційної системи, безпека додатків та баз даних, криптографія та інші. Крім того, важливо мати достатній рівень експертизи і досвіду для розуміння та оцінки різних загроз безпеці системи, використання найкращих практик та стандартів для їх запобігання, здійснення своєчасного реагування на загрози забезпечення інформаційної безпеки в умовах гібридної війни.

Окрім розробки та реалізації моделі безпеки, важливо забезпечити постійний моніторинг та аналіз стану безпеки системи. Це може включати моніторинг логів, виявлення та аналіз подій, аналіз ризиків та оцінку вразливостей системи. На основі такого аналізу можуть бути прийняті заходи для поліпшення безпеки системи та зменшення ризиків для її функціонування.

Також важливим аспектом безпеки розподіленої комп'ютерної системи є забезпечення безпеки користувачів. Це може включати реалізацію методів захисту від атак на користувачів, таких як соціальний інжиніринг та фішинг, а також забезпечення безпеки паролів та ідентифікаторів користувачів.

Оскільки РКС зазвичай складаються з багатьох компонентів, вони стають більш складними для забезпечення безпеки порівняно з централізованими системами. Для цього розробники мають дотримуватись рекомендацій та стандартів з безпеки, а також використовувати спеціалізовані інструменти для тестування та аналізу вразливостей системи. Крім того, в умовах постійної адаптації гібридних атак під конкретні вразливості системи, важливо постійно моніторити систему на предмет аномалій та інцидентів з метою своєчасної виявлення та реагування на них.

Таким чином, для формування концепції інформаційної безпеки РКС в умовах гібридних загроз необхідно підтримувати обмін політиками, оцінювати необхідний рівень безпеки та забезпечувати прозорість міжмережевих екранів. Більшість з цих вимог вже включені до стандарту OGF «Архітектура Відкритих Грід-систем», що базується на реалізації Globus Toolkit.

Застосування цього стандарту в РКС дозволяє підтримувати вимоги до обміну політиками та забезпечувати необхідний рівень безпеки. Крім того, забезпечення прозорості міжмережевих екранів здійснюється шляхом забезпечення можливості передачі даних через міжмережеві екрани без зміни політики безпеки.

1.5. Стандарти та керівні документи, що визначають вимоги до забезпечення безпеки інформації

У галузі забезпечення інформаційної безпеки існує багато стандартів та керівних документів, розроблених різними організаціями та компаніями з метою забезпечення безпеки інформації. Деякі з найбільш поширених та відомих стандартів та керівних документів в цій галузі включають (рис. 1.5) [5]:

1. ISO/IEC 27001 – цей стандарт встановлює вимоги до системи управління інформаційною безпекою, яка допомагає організаціям захистити свою інформацію від ризиків, таких як хакерські атаки, віруси та інші загрози.
2. NIST SP 800-53 – цей керівний документ містить каталог безпеки інформації, який описує вимоги до систем управління безпекою, що застосовуються в урядових установах США.
3. GDPR – це регулювання європейського союзу встановлює правила та вимоги щодо захисту персональних даних громадян ЄС, включаючи право на забування та право на доступ до власних даних.

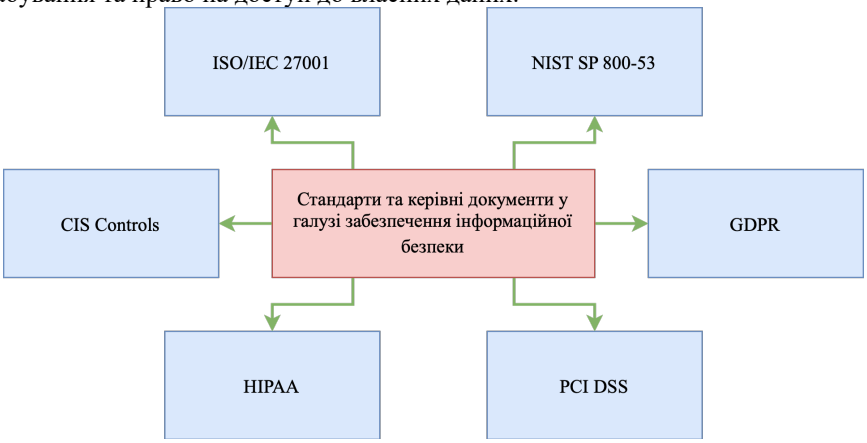

Рис. 1.5. Стандарти та керівні документи у галузі забезпечення інформаційної безпеки

4. PCI DSS – цей стандарт встановлює вимоги до захисту кредитної інформації, що збирається та обробляється відповідно до стандарту PCI.

5. HIPAA – цей закон США встановлює правила та вимоги щодо захисту медичної інформації та конфіденційності пацієнтів.

6. CIS Controls – цей керівний документ містить список з 20 контролів безпеки, які повинні бути впроваджені для захисту інформації та зменшення ризиків.

Ці стандарти та керівні документи допомагають організаціям впроваджувати ефективні та безпечні заходи для захисту інформації та зменшення ризиків її втрати чи пошкодження. Ці документи також допомагають створювати спільний стандарт та мову між різними організаціями, що дозволяє краще розуміти та оцінювати ризики та заходи для їх запобігання [7].

Крім того, окрім перелічених стандартів та документів, існує багато інших ресурсів, які допомагають організаціям забезпечувати безпеку своєї інформації. Наприклад, організації можуть використовувати різні інструменти та програми для виявлення та запобігання загроз безпеці, а також залучати консультантів з інформаційної безпеки для професійної оцінки ризиків та планування заходів.

Важливо зазначити, що забезпечення інформаційної безпеки є постійним процесом, який вимагає постійного оновлення та вдосконалення. У контексті попередження та протидії гібридним загрозам організації повинні забезпечувати регулярне оновлення своїх заходів забезпечення безпеки та використовувати нові технології та підходи для захисту своєї інформації від нових загроз та ризиків.

Одним із стандартів, які допомагають організаціям забезпечувати безпеку своєї інформації, є стандарт ISO 27001. Цей стандарт встановлює вимоги до системи управління інформаційною безпекою та надає рекомендації щодо її реалізації. Він допомагає організаціям створювати і розвивати систему управління інформаційною безпекою, а також контролювати та покращувати її ефективність.

Іншим важливим стандартом є стандарт PCI DSS (Payment Card Industry Data Security Standard), який встановлює вимоги до захисту інформації про платіжні картки. Цей стандарт використовується організаціями, які приймають платежі з використанням платіжних карток, та вимагає дотримання ряду заходів для захисту конфіденційної інформації про картки.

Крім стандартів, у багатьох країнах існують закони та регуляторні вимоги щодо захисту інформації. Наприклад, у Європейському Союзі діє Загальний регламент про захист персональних даних (GDPR), який встановлює вимоги до збору, обробки та зберігання персональних даних. У США існують закони, такі як HIPAA (Health Insurance Portability and Accountability Act) та Sarbanes-Oxley Act, які встановлюють вимоги до захисту конфіденційної інформації в різних галузях.

Отже, в галузі інформаційної безпеки існують різноманітні стандарти та документи, які допомагають організаціям забезпечувати захист своєї інформації та контролювати ризики. Ці стандарти та документи є важливим інформаційним

ресурсом для організацій, які хочуть забезпечити безпеку своєї інформації. Вони надають рекомендації щодо різних аспектів захисту інформації, від технічних заходів до процедур управління ризиками та контролю. Дотримання цих стандартів та регуляторних вимог може також допомогти організації уникнути штрафів, санкцій та репутаційних проблем.

Окрім стандартів та законів, у галузі інформаційної безпеки існують різноманітні керівні документи та ради, які надають поради та рекомендації щодо захисту інформації. Наприклад, Information Security Forum (ISF) – це міжнародна організація, яка займається дослідженнями та розробкою керівництва щодо захисту інформації. Вони надають своїм членам поради та рекомендації щодо стратегій безпеки, управління ризиками та технічного захисту інформації.

Іншими важливими керівними документами є різноманітні методичні рекомендації та практики, які розробляються організаціями, які займаються безпекою інформації. Наприклад, Center for Internet Security (CIS) розробляє практики та рекомендації щодо захисту інформації, які забезпечуються з використанням різних технічних засобів та процедур.

Важливу роль у процесі забезпечення безпеки інформації відводиться професійним організаціям, які надають консультації та підтримку у сфері інформаційної безпеки. Наприклад, International Association of Computer Science and Information Technology (IACSIT) є однією з найбільших професійних організацій, яка займається пропагуванням наукових досліджень у галузі інформаційної безпеки та забезпечує платформу для обміну досвідом та знаннями [16].

У зв'язку з розгортанням гібридних воєн у глобальному інформаційному просторі забезпечення інформаційної безпеки є важливим аспектом управління будь-якою організацією. Сучасні стандарти та керівні документи у цій галузі надають рекомендації та методики, які допомагають організаціям ефективно захищати свою інформацію від різних загроз. Крім того, важливу роль у цьому процесі відіграють професійні організації, які надають консультації та підтримку в сфері інформаційної безпеки.

1.6. Законодавча та нормативна база, що регулює питання інформаційної безпеки в Україні

Україна має законодавчу та нормативну базу в галузі інформаційної безпеки. Ця база включає закони, постанови, розпорядження та інші нормативні акти, які регулюють захист інформації в різних сферах життя, таких як державна безпека, оборона, економіка, наука та техніка [5].

В Україні існує ряд законів та нормативно-правових актів, які регулюють питання інформаційної безпеки. Нижче перераховані деякі з них:

1. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI.

2. Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII.

3. Закон України 2Про кібербезпеку» від 05.06.2018 р. № 2469-VIII.

4. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р. № 851-IV.

5. Національна стратегія забезпечення кібербезпеки України на період до 2020 року, затверджена Указом Президента України від 26.03.2013 р. № 126/2013.

6. Наказ Національного банку України «Про затвердження Положення про заходи щодо запобігання виникненню та виявленню та відновлення доступу до активів, які стали об'єктом кібератаки» від 26.04.2018 р. № 59.

7. Наказ Міністерства цифрової трансформації України «Про затвердження Типового положення про організацію захисту інформації в системах та мережах інформаційно-телекомунікаційного забезпечення державних органів» від 18.02.2021 р. № 190.

8. Постанова Кабінету Міністрів України «Про затвердження Положення про національний центр кібербезпеки» від 08.08.2018 р. № 641.

9. Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг «Про затвердження Переліку заходів щодо захисту критичних інформаційних інфраструктур» від 14.07.2020 р. № 1234.

10. Постанова Національної комісії з питань регулювання зв'язку та інформатизації «Про затвердження Положення про забезпечення кібербезпеки в телекомунікаційних системах» від 28.05.2019 р. № 331.

Ці законодавчі та нормативні акти регулюють питання захисту персональних даних, кібербезпеки, захисту інформації в державних системах, забезпечення безпеки в телекомунікаційних системах та інші аспекти інформаційної безпеки в Україні.

Дотримання цих правових актів є важливим для забезпечення безпеки та захисту інформації в Україні, оскільки забезпечення інформаційної безпеки є однією з основних складових національної безпеки.

Загалом, законодавча та нормативна база в галузі інформаційної безпеки в Україні є достатньою для забезпечення захисту інформації та забезпечення національної безпеки в цій сфері.

У зв'язку з тим, що інформаційні та кібернетичні атаки стають все більш складними з кожним роком, важливо постійно вдосконалювати стратегії для їх запобігання.

Ефективний захист від гібридних викликів і загроз, що намагаються зламати інформаційні системи, передбачає розробку та дотримання новітніх стратегій, процедур і правил, які базуються на використанні сучасних технологій та кращих світових практик.

Для досягнення результативності в боротьбі з гібридними загрозами, необхідно зосередитися на створенні та впровадженні типових політик, процедур та інструкцій для захисту інформаційних активів державних та приватних структур. Це дозволить забезпечити більш ефективний захист інформації від потенційних загроз та покращити загальний рівень безпеки інформаційних систем.

КОНТРОЛЬНІ ПИТАННЯ

1. Перелічіть проблеми пов'язані із забезпеченням інформаційної безпеки.
2. Які основні проблеми забезпечення інформаційної безпеки в умовах гібридних загроз?
3. У чому полягає проблема інтеграції з механізмами розподілених комп’ютерних систем?
4. У чому полягає проблема взаємодії з механізмами розподілених комп’ютерних систем?
5. У чому полягає проблема встановлення довіри між різними доменами та вузлами розподілених комп’ютерних систем?
6. Які аспекти необхідно враховувати при встановленні довірчих відносин?
7. Які методи і технології використовуються для забезпечення безпеки розподіленої комп'ютерної системи?
7. Перелічіть стандарти та керівні документи у галузі забезпечення інформаційної безпеки.
8. Які закони та нормативно-правові акти регулюють питання інформаційної безпеки в Україні?

ТЕСТИ

1. Яка з наведених проблем пов’язана із зростанням кількості інформації в електронному вигляді?
а) Збільшення вартості зберігання інформації
б) Збільшення можливостей для хакерів та кіберзлочинців
в) Зменшення обсягу конфіденційної інформації
г) Покращення безпеки даних

2. Що є однією з головних причин кіберзагроз в умовах гібридних воєн?
а) Недостатнє розуміння ризиків користувачами
б) Недостатня кількість фахівців з кібербезпеки
в) Перевантаженість систем захисту
г) Застарілі методи зберігання інформації

3. Що з наведеного є основним методом атак на інформаційну безпеку в умовах гібридних загроз?
а) Вірусні атаки
б) Кібератаки
в) Атаки через фізичний доступ до серверів
г) Зашифровані атаки

4. Яка проблема стосується використання дезінформації в умовах гібридних загроз?
а) Вона сприяє збільшенню довіри до державних органів
б) Вона знижує рівень національної безпеки
в) Вона підвищує ефективність оборони
г) Вона сприяє стабільності в державі

5. Що є важливим аспектом для зменшення ризиків використання соціальних мереж для дезінформації?
а) Збільшення кількості підписників
б) Захист користувачів від кібератак
в) Впровадження нових функцій
г) Створення державних акаунтів у соціальних мережах

6. Що є ключовою проблемою безпеки розподілених комп'ютерних систем?
а) Підвищення доступності системи
б) Взаємодія між різними доменами і вузлами
в) Підвищення продуктивності системи
г) Недостатнє шифрування даних

7. Яке рішення проблеми інтеграції розподілених систем може бути найефективнішим?
а) Використання приватних мереж
б) Використання проміжного програмного забезпечення
в) Видалення старих систем
г) Запровадження нових комп’ютерів

8. Що є прикладом механізму встановлення довіри між доменами РКС?
а) Ручна перевірка користувачів
б) Політики безпеки, які створюються динамічно
в) Повна ізоляція вузлів
г) Немає потреби у встановленні довіри

9. Який метод допомагає захистити дані в розподілених системах?
а) Шифрування на рівні транспорту

б) Знищення даних після обробки
в) Обмеження кількості користувачів
г) Використання простих паролів

10. Що є важливою умовою безпеки для запобігання DDoS атакам?
а) Використання хмарних технологій
б) Відключення мережі при атаці
в) Обмеження доступу до всіх ресурсів
г) Використання спільного обладнання для всіх служб

РОЗДІЛ 2.
АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Класифікація ризиків інформаційної безпеки
2.2. Фактори, які збільшують ризик

Аналіз загроз інформаційної безпеки – це процес виявлення, оцінки та розуміння можливих загроз, які можуть вплинути на безпеку інформації в комп'ютерних системах, мережах та інших інформаційних технологіях.

Загрози інформаційної безпеки можуть бути різними – від технічних проблем до зловмисних дій, спрямованих на крадіжку даних або завдання шкоди системам. Наприклад, до технічних проблем можна віднести некоректну роботу обладнання, падіння систем, помилки в програмному забезпеченні тощо. До зловмисних дій можна віднести кібератаки, віруси, хакерські атаки, фішингові атаки, вимагання викупу (рансомвари) та інші.

Аналіз загроз інформаційної безпеки включає в себе такі етапи (рис. 2.1):

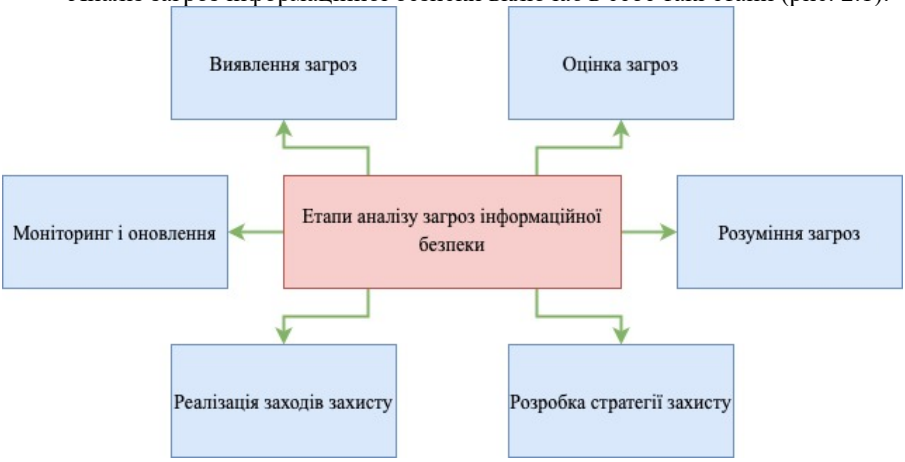

Рис. 2.1. Етапи аналізу загроз інформаційної безпеки

1. Виявлення загроз – процес виявлення можливих загроз для інформаційної безпеки в комп'ютерних системах і мережах.

2. Оцінка загроз – процес оцінки потенційного впливу загроз на безпеку інформації та визначення ризику.

3. Розуміння загроз – процес аналізу властивостей та взаємозв'язку загроз, що дозволяє зрозуміти їх природу та можливості.

4. Розробка стратегії захисту – процес розробки стратегій та заходів для запобігання або зменшення впливу загроз на безпеку інформації.

5. Реалізація заходів захисту – процес реалізації стратегій та заходів захисту для забезпечення безпеки інформації.

6. Моніторинг і оновлення – процес стеження за виникненням нових загроз та оновлення захисних заходів відповідно до зміни ситуації.

Для аналізу загроз інформаційної безпеки можуть використовуватися різні методи та інструменти, такі як аудит безпеки, сканування портів, тестування на проникнення, аналіз журналів подій, аналіз вразливостей та інші.

Важливо пам'ятати, що аналіз загроз інформаційної безпеки – це процес, який потребує постійного оновлення та вдосконалення, оскільки внаслідок розгортання гібридних воєн у глобальному інформаційному просторі нові загрози з'являються щодня. Тому, компанії та організації повинні постійно моніторити та оновлювати свої системи захисту, щоб захистити свої дані та інформацію від потенційних загроз.

2.1. Класифікація ризиків інформаційної безпеки

Класифікація ризиків інформаційної безпеки може бути здійснена на різних рівнях – від окремих інформаційних систем до комплексних інфраструктур.

На загальному рівні можна виділити такі типи ризиків інформаційної безпеки (рис. 2.2) [19]:

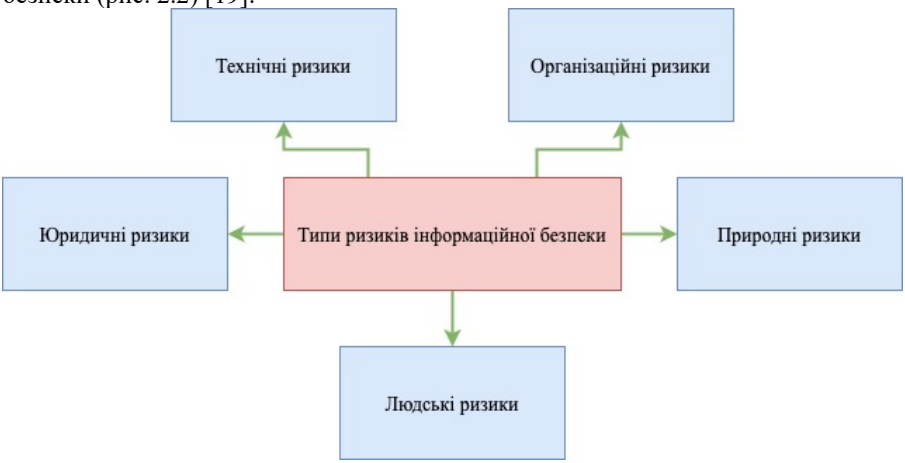

Рис. 2.2. Типи ризиків інформаційної безпеки

1. Технічні ризики – пов'язані з вразливостями апаратного та програмного забезпечення, можуть призвести до порушення конфіденційності, цілісності та доступності інформації.

2. Організаційні ризики – пов'язані зі зловживанням довіри працівників, недостатньою організацією процесів управління інформацією, недостатніми заходами безпеки.

3. Природні ризики – пов'язані зі стихійними лихами, техногенними катастрофами, пожежами тощо, які можуть призвести до втрати даних і порушення доступності інформації.

4. Людські ризики – пов'язані з недбалістю або недостатнім рівнем обізнаності працівників щодо правил і процедур інформаційної безпеки, які можуть призвести до втрати даних та інших проблем.

5. Юридичні ризики – пов'язані з порушенням законодавства в галузі інформаційної безпеки, які можуть призвести до штрафів або інших правових наслідків.

Крім того, на окремих рівнях можна виділити такі типи ризиків (рис. 2.3):

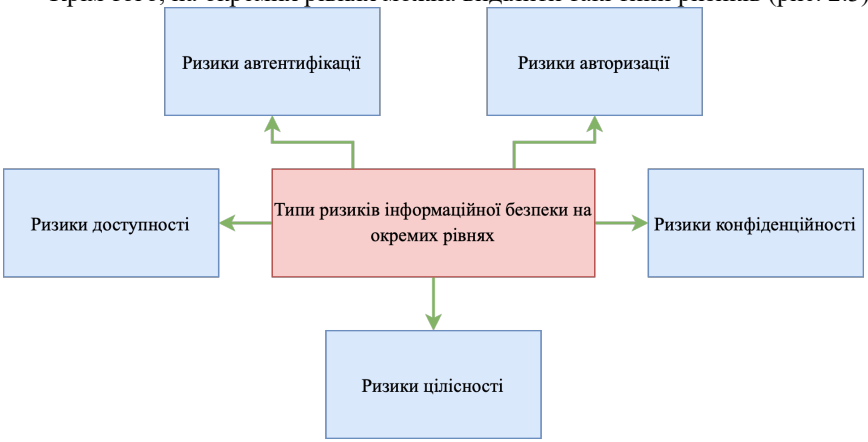

Рис. 2.3. Типи ризиків інформаційної безпеки на окремих рівнях

1. Ризики автентифікації – пов'язані з можливістю несанкціонованого доступу до інформації через слабкі паролі, недостатній контроль доступу, атаки фішингу тощо.

2. Ризики авторизації – пов'язані з можливістю несанкціонованої зміни або збереження даних чи виконання дій в інформаційній системі через недостатній контроль прав доступу.

3. Ризики конфіденційності – пов'язані з можливістю несанкціонованого доступу до конфіденційної інформації через недостатньо ефективні механізми шифрування, нестачу аудиту доступу тощо.

4. Ризики цілісності – пов'язані з можливістю несанкціонованої зміни або видалення інформації через недостатній контроль цілісності даних, атаки на криптографічні алгоритми, шкідливе програмне забезпечення тощо.

5. Ризики доступності – пов'язані з можливістю заборони доступу до інформації через атаки на мережу, дії зловмисників, програмні вади тощо.

Для кожного типу ризику можуть бути розроблені відповідні заходи забезпечення безпеки для зменшення ризику виникнення подій, що можуть спричинити втрату конфіденційної інформації або пошкодження системи. Таким чином, класифікація ризиків інформаційної безпеки є важливим інструментом для розуміння загального стану безпеки і визначення потреби в заходах щодо її підвищення.

Можна класифікувати ризики інформаційної безпеки за декількома критеріями (рис. 2.4) [7].

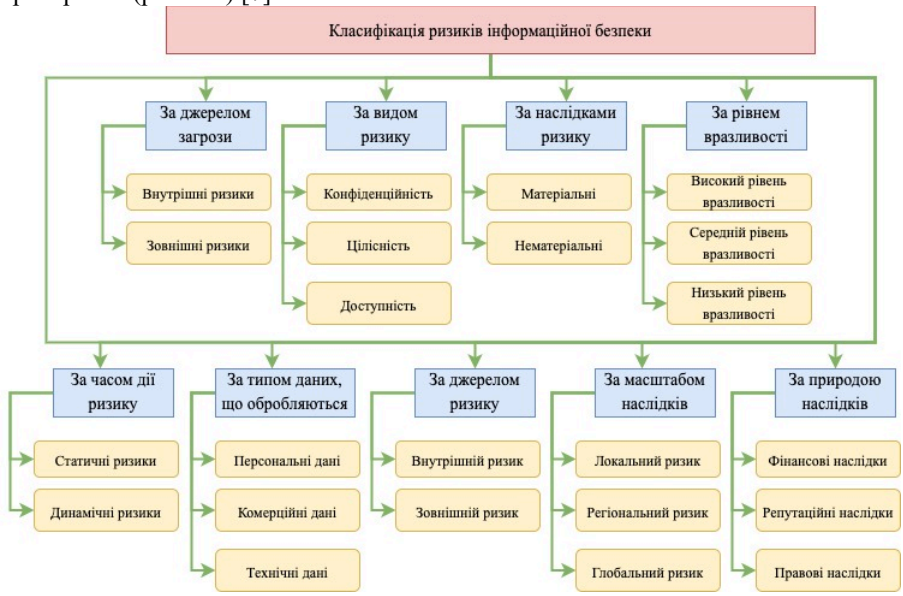

Рис. 2.4. Класифікація ризиків інформаційної безпеки

1. За джерелом загрози:

– Внутрішні ризики – пов'язані з діяльністю самої організації та її співробітників (наприклад, недбале ставлення до інформації, порушення правил безпеки тощо);

– Зовнішні ризики – пов'язані з діяльністю зовнішніх суб'єктів, які можуть завдати шкоди організації (наприклад, хакерські атаки, крадіжки даних тощо).

2. За видом ризику:

– Конфіденційність – ризик незаконного доступу до конфіденційної інформації;

– Цілісність – ризик порушення цілісності інформації, тобто її зміни або видалення без дозволу;

– Доступність – ризик обмеження доступу до інформації.

3. За наслідками ризику:

– Матеріальні – пов'язані з фінансовими втратами;

– Нематеріальні – пов'язані з втратою репутації, довіри клієнтів, порушенням законодавства тощо.

4. За рівнем вразливості:

– Високий рівень вразливості – пов'язаний зі складністю захисту від певних загроз;

– Середній рівень вразливості – пов'язаний з наявністю деяких заходів захисту, але зі слабкістю їх реалізації;

– Низький рівень вразливості – пов'язаний з високим рівнем захисту від певних загроз.

5. За часом дії ризику:

– Статичні ризики – що залежать від сталої конфігурації системи та відсутності нових загроз;

– Динамічні ризики – що залежать від появи нових загроз та внесення змін в систему.

6. За типом даних, що обробляються:

– Персональні дані – які пов'язані з особистою інформацією користувачів (ім'я, прізвище, адреса, номер телефону тощо);

– Комерційні дані – які пов'язані з фінансовою діяльністю організації (фінансові звіти, операційна інформація тощо);

– Технічні дані – які пов'язані з технічними параметрами системи (IP-адреси, MAC-адреси, конфігураційні дані тощо).

7. За джерелом ризику:

– Внутрішній ризик – виникає внаслідок дій або бездіяльності працівників або систем організації;

– Зовнішній ризик – виникає внаслідок дій зовнішніх осіб або впливу зовнішніх факторів, таких як природні лиха, кібератаки та інші.

8. За масштабом наслідків:

– Локальний ризик – впливає тільки на окремі компоненти системи або на обмежений регіон;

– Регіональний ризик – впливає на певний регіон або на певну групу користувачів;

– Глобальний ризик – впливає на весь обсяг діяльності організації.

9. За природою наслідків:

– Фінансові наслідки – збитки, що пов'язані з витратами на відновлення системи, компенсації клієнтам, штрафами та іншими витратами;

– Репутаційні наслідки – вплив на імідж організації, який може викликати втрату довіри клієнтів та інвесторів;

– Правові наслідки – можуть виникнути через порушення законодавства з питань інформаційної безпеки, що може призвести до судових позовів та інших юридичних наслідків.

Ці класифікації ризиків інформаційної безпеки допомагають керівникам інформаційної безпеки та іншим спеціалістам управляти ризиками, що пов'язані з обробкою інформації. При розробці стратегій і планів забезпечення інформаційної безпеки в умовах гібридної війни, класифікація ризиків є важливим інструментом для визначення основних загроз і захисту від них.

Також класифікація ризиків допомагає ідентифікувати різноманітні види ризиків, що пов'язані з інформаційною безпекою, та вживати заходів для запобігання їх виникненню. Знання про класифікацію ризиків допомагає забезпечити ефективний захист інформації та зменшити вплив можливих загроз на діяльність організації.

Важливим питанням є формулювання мінімальних умов, необхідних для визначення вимог до структури та змісту концепції інформаційної безпеки в умовах гібридних загроз. Ці умови мають базуватися на аналізі сучасних загроз та оцінках власних ризиків з метою оптимізації та підвищення ефективності побудови процесів забезпечення IT державних та приватних організацій.

Класифікація ризиків щодо об'єкту впливу негативних факторів – це процес ідентифікації та оцінки можливих загроз та небезпек, які можуть виникнути на об'єкті, та розподіл їх за рівнями серйозності та ймовірності.

Зазвичай ризики класифікують за наступними основними параметрами:

1. Ймовірність виникнення небезпеки або загрози.
2. Серйозність наслідків, які можуть виникнути у випадку реалізації ризику.

Залежно від цих параметрів, ризики можна розділити на наступні категорії (рис. 2.5):

– Високий ризик – це ризик з високою ймовірністю виникнення і серйозними наслідками в разі його реалізації. Цей тип ризику потребує негайних заходів для запобігання або мінімізації можливих наслідків.

– Середній ризик – це ризик з помірною ймовірністю виникнення і помірними наслідками в разі його реалізації. Цей тип ризику потребує уваги та контролю, але може бути управлений за допомогою регулярних перевірок та моніторингу.

– Низький ризик – це ризик з низькою ймовірністю виникнення та незначними наслідками в разі його реалізації. Цей тип ризику може бути забезпечений прийняттям заходів зі зменшення ймовірності виникнення небезпеки та моніторингу ситуації.

– Неприйнятний ризик – це ризик, який неможливо прийняти з точки зору безпеки об'єкту. Якщо такий ризик існує, то необхідно здійснити відповідні заходи для зменшення ймовірності його реалізації, які можуть включати зміну умов експлуатації, впровадження нових технологій або повну заміну об'єкту.

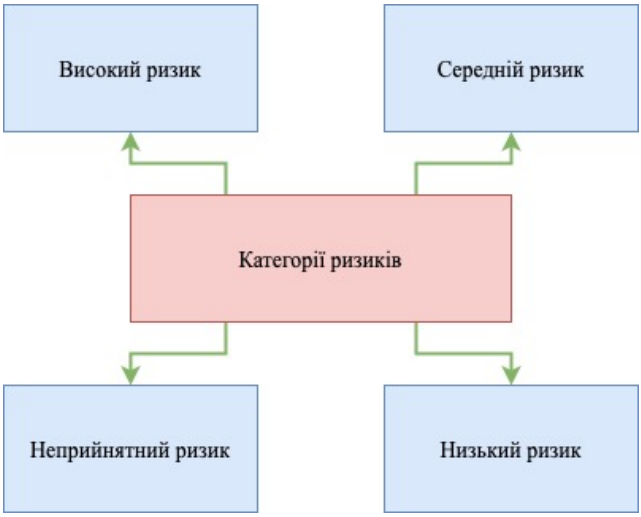

Рис. 2.5. Категорії ризиків

При класифікації ризиків, також можуть бути використані додаткові параметри, такі як [17]:

1. Термін дії ризику: короткострокові (до 1 року), середньострокові (від 1 до 3 років) та довгострокові (більше 3 років).

2. Джерело ризику: внутрішнє (пов'язане зі станом об'єкту, процесів та персоналу) або зовнішнє (пов'язане з природними чинниками, стихійними лихами, техногенними катастрофами, терористичними актами тощо).

Для класифікації ризиків можуть бути використані різні методи, наприклад, матриця ризиків, дерево ризиків, карта ризиків тощо. Важливо пам'ятати, що ідентифікація та класифікація ризиків – це лише початок процесу управління ризиками, і після цього необхідно розробляти та впроваджувати плани дій з метою запобігання або зменшення ризиків та їх наслідків.

Інвестиційні ризики пов'язані з можливими збитками, які можуть виникнути у зв'язку з інвестуванням коштів у певний проект, компанію або фінансовий інструмент. Такі ризики можуть виникнути через різні причини, такі як непередбачувані зміни ринку, низька прибутковість проекту або компанії, несприятливі зміни в законодавстві тощо.

Інноваційні ризики пов'язані з введенням на ринок нових продуктів, послуг або технологій. Такі ризики пов'язані з невизначеністю щодо прийняття нового продукту ринком, його популярності серед споживачів, конкуренції на ринку та іншими факторами.

Для того, щоб підвищити здатність протидіяти гібридним загрозам та зменшити ризики, пов'язані з прийняттям рішень, необхідно проводити

детальний аналіз можливих наслідків прийнятих рішень, розробляти плани та стратегії зменшення ризиків, а також використовувати методи експертної оцінки ризиків та моделювання сценаріїв розвитку подій.

Управління ризиками є важливою складовою діяльності будь-якої організації або системи. Необхідність в управлінні ризиками обумовлена збільшенням кількості та різноманітності можливих загроз, які можуть виникнути в процесі діяльності. Окрім того, управління ризиками дозволяє знизити витрати на захист від негативних наслідків, збільшити ефективність функціонування та збільшити стійкість до ризиків.

Для успішного управління ризиками необхідно визначити можливі загрози, оцінити їх вплив та імовірність настання, вжити заходів контролю та захисту від цих загроз та постійно відстежувати ризики для їх своєчасного усунення. Управління ризиками є елементом комплексної системи протидії гібридним загрозам, який вимагає залучення кваліфікованих фахівців та використання спеціальних інструментів та технологій.

2.2. Фактори, які збільшують ризик

Ризик-утворюючі фактори – це фактори, які можуть збільшувати ймовірність виникнення небажаного результату, події або стану. У контексті бізнесу, це можуть бути такі фактори, як (рис. 2.6):

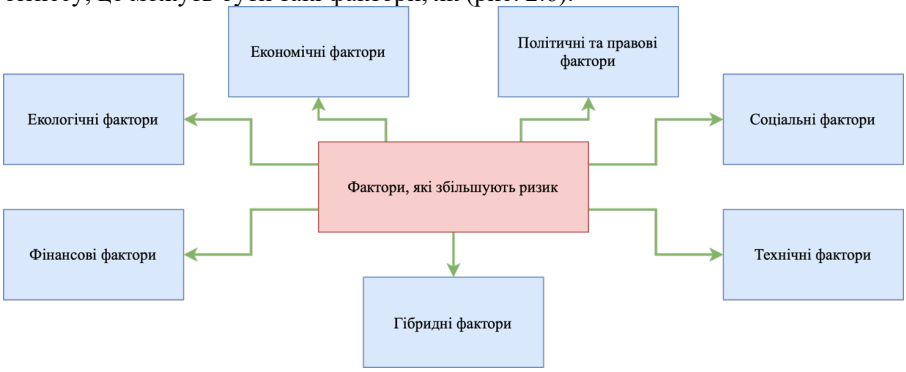

Рис. 2.6. Фактори, які збільшують ризик

1. Економічні фактори – зміни в економіці, такі як спад або зростання ринку, вартості сировини, курсу валют тощо.
2. Політичні та правові фактори – зміни у законодавстві, політична нестабільність, конфлікти з владою або регуляторами.
3. Соціальні фактори – зміни в поведінці споживачів, тенденції, нові технології та культурні зміни.

4. Технічні фактори – зміни в технології, розвиток нових матеріалів, винахід нових процесів.

5. Фінансові фактори – зміни у вартості активів, заборгованості, ліквідності тощо.

6. Екологічні фактори – забруднення навколишнього середовища, зміни клімату, природні катастрофи тощо.

7. Гібридні фактори: впливи, що породжуються з реалізацією гібридних загроз.

Усі ці фактори можуть вплинути на ризики, які пов'язані з діяльністю компанії, тому їх потрібно аналізувати і враховувати при прийнятті рішень.

Крім того, існують інші ризик-утворюючі фактори, які можуть вплинути на успішність бізнесу, наприклад (рис. 2.7):

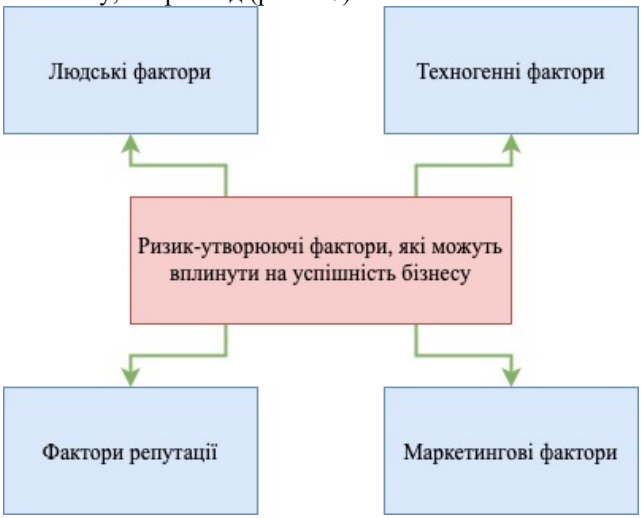

Рис. 2.7. Ризик-утворюючі фактори, які можуть вплинути на успішність бізнесу

1. Людські фактори – кадрові проблеми, конфлікти між працівниками, низька мотивація, недостатня кваліфікація персоналу.

2. Техногенні фактори – аварії, непередбачувані ситуації, збої в техніці та обладнанні.

3. Маркетингові фактори – конкуренція, необхідність зміни маркетингової стратегії, зміни в поведінці споживачів.

4. Фактори репутації – відгуки клієнтів, погана репутація бренду, негативна преса.

Зрозуміло, що ризик-утворюючі фактори можуть бути різними для кожної компанії, в залежності від її специфіки і галузі, у якій вона працює. Однак,

збільшення уваги до аналізу цих факторів може допомогти зменшити ризик та збільшити шанси на успіх [3].

Внутрішні ризик-утворюючі чинники можуть включати фактори, які пов'язані з конструкцією та функціонуванням самого об'єкта, його технічним станом, персоналом, який займається експлуатацією об'єкта, та інші аспекти, які можуть спричинити ризик. Зовнішні ризик-утворюючі чинники можуть включати фактори, які залежать від зовнішнього середовища, наприклад, погодні умови, вібрації від інших об'єктів, взаємодію з людьми та інші.

Локальні ризик-утворюючі фактори можуть бути пов'язані з конкретним видом ризику, наприклад, з діяльністю, яка відбувається на об'єкті. Інтегральні ризик-утворюючі фактори можуть включати фактори, які впливають на кілька видів ризику одночасно, наприклад, зміни у законодавстві або соціально-економічні фактори, які впливають на ефективність та дохідність організації.

Отже, знання та аналіз ризик-утворюючих факторів є дуже важливим для оцінки ризику та прийняття ефективних заходів для його запобігання та за рахунок цього підвищення можливості протистояти гібридним загрозам.

Для кожного об'єкта, що потенційно може стати джерелом ризику, важливо провести оцінку ризиків, що передбачає ідентифікацію всіх можливих ризиків та визначення їх впливу та ймовірності виникнення. Це дозволяє визначити ті ризики, які є найбільш значущими та розробити стратегії їх управління. Управління ризиками повинно бути системним та охоплювати всі етапи життєвого циклу об'єкта – від проектування та будівництва до експлуатації та видалення.

Важливо також враховувати взаємозв'язки між різними ризиками та їх можливі взаємовпливи. Наприклад, заходи щодо зниження одного виду ризику можуть призвести до збільшення іншого виду ризику.

В цілому, успішне управління ризиками потребує комплексного підходу, який охоплює не лише технічні, але й соціальні, економічні та екологічні аспекти. Такий підхід дозволяє забезпечити безпеку об'єкта та його користувачів, зменшити можливість виникнення аварій та інших негативних наслідків, а також забезпечити сталість функціонування об'єкта в умовах невизначеності та змін.

Один з ключових етапів управління ризиками – це розробка та впровадження плану управління ризиками, який повинен містити стратегії та заходи щодо запобігання ризикам, зменшення їх впливу та реагування на негативні наслідки.

Для ефективного управління ризиками необхідна система моніторингу та контролю, що дозволяє вчасно виявляти та вирішувати проблеми. Також важливо проводити регулярні перевірки ефективності заходів управління ризиками та вносити корективи у план управління ризиками в залежності від змін у умовах функціонування об'єкта.

Управління ризиками є важливим аспектом в багатьох галузях, таких як промисловість, транспорт, будівництво, медицина та інші. В сучасному світі, де

технології розвиваються все швидше та з'являються нові види ризиків, управління ризиками є особливо важливим для забезпечення безпеки в умовах гібридних загроз та сталості функціонування об'єктів у невизначених умовах.

КОНТРОЛЬНІ ПИТАННЯ

1. Назвіть етапи аналізу загроз інформаційної безпеки.
2. Які виділяють типи ризиків інформаційної безпеки?
3. Класифікуйте ризики інформаційної безпеки за різними критеріями.
4. Розкрийте та опишіть основні категорії ризиків.
5. Перелічіть фактори, які збільшують ризик.
6. Назвіть ризик-утворюючі фактори, які можуть вплинути на успішність бізнесу.

ТЕСТИ

1. Що включає в себе процес аналізу загроз інформаційної безпеки?
а) Виявлення загроз
б) Оцінка загроз
в) Розуміння загроз
г) Усі відповіді правильні

2. Який із наступних факторів є прикладом технічних ризиків інформаційної безпеки?
а) Недостатня організація процесів управління інформацією
б) Стихійні лиха
в) Вразливості апаратного та програмного забезпечення
г) Недбалість працівників

3. Який тип атак відноситься до зловмисних дій в контексті інформаційної безпеки?
а) Некоректна робота обладнання
б) Хакерські атаки
в) Падіння систем
г) Помилки в програмному забезпеченні

4. Який ризик пов'язаний з можливістю несанкціонованої зміни даних?
а) Ризик доступності
б) Ризик цілісності
в) Ризик конфіденційності
г) Ризик автентифікації

5. До якого типу ризиків відноситься можливість крадіжки даних через фішингові атаки?
а) Технічні ризики
б) Юридичні ризики
в) Людські ризики
г) Природні ризики

6. Що характеризує ризики високого рівня вразливості?
а) Високий рівень захисту від загроз
б) Складність захисту від певних загроз
в) Середній рівень захисту
г) Відсутність загроз

7. Що включає процес розробки стратегії захисту?
а) Аналіз вразливостей
б) Виявлення загроз
в) Розробка стратегій і заходів для запобігання або зменшення впливу загроз
г) Оцінка ризиків

8. Який ризик виникає внаслідок недбалого ставлення працівників до інформації?
а) Технічний ризик
б) Людський ризик
в) Природний ризик
г) Юридичний ризик

9. Що є важливою частиною моніторингу загроз інформаційної безпеки?
а) Виявлення нових загроз
б) Виявлення помилок в програмному забезпеченні
в) Тестування на проникнення
г) Оновлення апаратного забезпечення

10. До яких ризиків відносяться природні лиха, які можуть вплинути на інформаційну безпеку?
а) Людські ризики
б) Природні ризики
в) Організаційні ризики
г) Юридичні ризики

РОЗДІЛ 3.
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ

3.1. Концепції, в яких відображаються сучасні підходи до визначення ризику
3.2. Основні аспекти, що вивчаються в теорії ризиків
3.3. Норми та вимоги щодо керування ризиками
3.3.1. Стандарт ISO/IEC Guide 73
3.3.2. Стандарт управління ризиками AS/NZS 4360

Ризик-орієнтований підхід до забезпечення інформаційної безпеки полягає в оцінці ризику та впровадженні заходів, щоб зменшити його до прийнятного рівня. Цей підхід базується на принципі, що кожна організація має унікальні потреби з точки зору інформаційної безпеки, а отже, потребує індивідуальної оцінки ризиків та розробки відповідної стратегії захисту.

Оцінка ризиків включає в себе ідентифікацію потенційних загроз, оцінку їх вірогідності та наслідків для організації, а також визначення потенційних вразливостей в системах та інфраструктурі організації. Після оцінки ризиків розробляється стратегія захисту, яка може включати в себе різні заходи, такі як встановлення програмного та апаратного забезпечення, зміна процедур, навчання персоналу тощо.

При розробці стратегії захисту необхідно враховувати, що ризик може змінюватися з часом, тому важливо регулярно перевіряти та оновлювати стратегію захисту. Також необхідно забезпечити своєчасне виявлення та реагування на інциденти безпеки, що породжуються з реалізацією гібридних загроз.

Застосування ризик-орієнтованого підходу до забезпечення інформаційної безпеки допомагає організаціям зменшити ризик витоку чутливої інформації та інших кіберзагроз, підвищити рівень довіри клієнтів та збільшити стійкість бізнесу до інцидентів безпеки [1].

Крім того, ризик-орієнтований підхід до забезпечення інформаційної безпеки дозволяє ефективно використовувати ресурси організації, оскільки забезпечення повної безпеки може бути дуже дорогим. Використання ризик-орієнтованого підходу дозволяє організації визначити, які заходи безпеки є найбільш важливими та необхідними для забезпечення безпеки даних та інфраструктури.

Ще одним важливим аспектом ризик-орієнтованого підходу є те, що він сприяє створенню культури безпеки в організації у контексті попередження та протидії гібридним загрозам. Кожен працівник повинен бути свідомим своєї ролі в забезпеченні безпеки та повинен виконувати встановлені процедури та правила, щоб зменшити ризик для організації.

У світі, де у глобальному інформаційному просторі розгортаються гібридні війни, а кіберзагрози стають все більш складними та розповсюдженими, ризик-орієнтований підхід до забезпечення інформаційної безпеки є ключовим для забезпечення захисту та стійкості організації. Організації повинні розуміти, що забезпечення безпеки – це постійний процес, який потребує встановлення та оновлення заходів безпеки відповідно до ризиків та загроз, що змінюються.

3.1. Концепції, в яких відображаються сучасні підходи до визначення ризику

Сучасні концепції ризику відображаються в наступних підходах (рис. 3.1):

1. Концепція ризику як ймовірності відхилення фактичного результату від очікуваного. Цей підхід передбачає, що ризик – це відношення між очікуваною винагородою та можливими втратами.
2. Концепція ризику як можливості збитку або втрати. Цей підхід зосереджується на визначенні можливих втрат та збитків, що можуть статися в результаті діяльності.
3. Концепція ризику як систематичного та несистематичного ризику. Систематичний ризик відображає загальну нестабільність ринку, тоді як несистематичний ризик пов'язаний з конкретними компаніями або галузями.
4. Концепція ризику як загрози та небезпеки. Цей підхід передбачає визначення можливих загроз та небезпек, що можуть статися в результаті діяльності та розробка стратегій для зменшення цих ризиків.

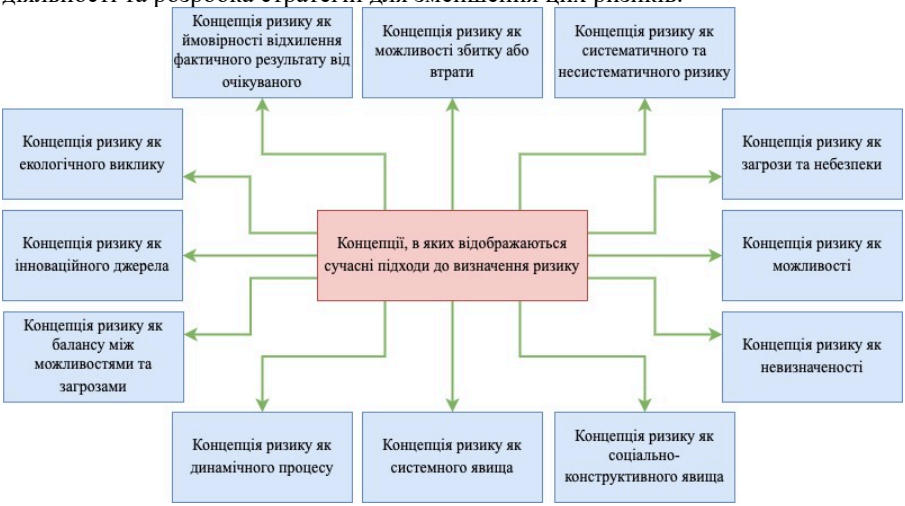

Рис. 3.1. Концепції, в яких відображаються сучасні підходи до визначення ризику

5. Концепція ризику як можливості. Цей підхід зосереджується на визначенні можливостей, які можуть виникнути в результаті діяльності, та розробці стратегій для їх максимізації.

6. Концепція ризику як невизначеності. Цей підхід розглядає ризик як невизначеність щодо майбутніх подій та результатів. Він визнає, що не завжди можна точно передбачити ймовірність та наслідки ризику, і намагається розробити стратегії для управління цією невизначеністю.

7. Концепція ризику як соціально-конструктивного явища. Цей підхід відзначає, що ризик є соціально сконструйованою концепцією, яка формується через взаємодію між людьми, організаціями та суспільством. Розуміння ризику залежить від культурних, соціальних та індивідуальних факторів.

8. Концепція ризику як системного явища. Цей підхід розглядає ризик як складну систему, де різні фактори та взаємозв'язки впливають на появу та розповсюдження ризикових подій. Він визнає, що ризики можуть мати широкий спектр наслідків та потенційно впливати на багатоаспектні системи.

9. Концепція ризику як динамічного процесу. Цей підхід відображає ризик як еволюційний процес, що змінюється з часом. Ризик може зростати або зменшуватися внаслідок змін у внутрішніх та зовнішніх умовах, технологічного розвитку, соціальних та економічних чинників.

10. Концепція ризику як балансу між можливостями та загрозами. Цей підхід відображає ризик як взаємодію між можливостями, які можуть призвести до успіху або переваг для організації, і загрозами, які можуть призвести до втрат або негативних наслідків. В управлінні ризиками важливо знайти оптимальний баланс між експлуатацією можливостей і мінімізацією загроз.

11. Концепція ризику як інноваційного джерела. Цей підхід розглядає ризик як можливість для інновацій та розвитку. Ризик може стимулювати організацію до впровадження нових ідей, технологій та стратегій, що сприяють її конкурентоспроможності та успіху на ринку.

12. Концепція ризику як екологічного виклику. Цей підхід визнає, що ризик може походити з екологічних факторів та може мати вплив на навколишнє середовище. Організації повинні враховувати екологічні аспекти ризику та розробляти сталі стратегії для його зменшення та управління.

Ці концепції ризику відображають сучасні підходи до розуміння та управління ризиками. Вони покривають широкий спектр аспектів, від економічних до соціальних та екологічних, і допомагають організаціям ефективно аналізувати, оцінювати та керувати ризиками в сучасному світі.

Загалом, при формуванні інформаційної безпеки в умовах гібридних загроз концепції ризику допомагають визначити можливість та наслідки ризику та виробити стратегії для його управління.

3.2. Основні аспекти, що вивчаються в теорії ризиків

Теорія ризиків вивчає, які наслідки можуть мати різні ризики на фінансові результати і поведінку людей. Основні об'єкти дослідження в теорії ризиків включають (рис. 3.2):

Рис. 3.2. Основні об'єкти дослідження в теорії ризиків

1. Ризикові події: це може бути будь-яка подія, яка може мати негативний вплив на фінансові результати, такі як невдачі в бізнесі, природні катастрофи, політична нестабільність тощо.

2. Ризикові фактори: це можуть бути різні чинники, які впливають на виникнення ризиків і на їх рівень, такі як волатильність ринку, ступінь впливу конкуренції на підприємство, ступінь складності операцій та інші.

3. Ризикові стратегії: це можуть бути різні стратегії, що допомагають зменшити ризики або вплинути на їх рівень, наприклад, страхування, диверсифікація портфелю, захист від валютних ризиків, зниження витрат тощо.

4. Ризикова поведінка: це можуть бути різні стратегії поведінки людей, які можуть зменшити або збільшити ризики, наприклад, відмова від інвестицій в ризикові активи, необґрунтована впевненість у своїх здібностях, недостатня інформованість тощо.

Також у теорії ризиків вивчаються поняття, такі як ризиковий капітал, ризикове управління, ризиковий аналіз тощо. В цілому, теорія ризиків створена для того, щоб допомогти людям зрозуміти, які ризики існують, як протистояти гібридним загрозам, як можна зменшити ризики таких загроз або управляти ними для досягнення інформаційної безпеки та фінансового успіху.

Так, основними суб'єктами безпеки в умовах розгортання гібридних воєн (згідно з рис. 3.1) є (рис. 3.3):

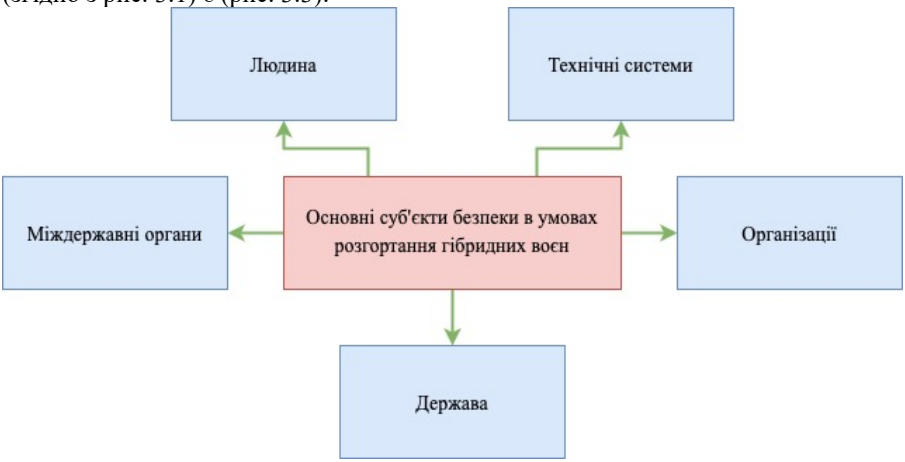

Рис. 3.3. Основні суб'єкти безпеки в умовах розгортання гібридних воєн

1. Людина – індивідуали, які можуть бути піддані впливу гібридних загроз, наприклад, кібератак, інформаційної пропаганди або психологічного впливу.

2. Технічні системи – це включає комп'ютерні мережі, інформаційні системи, телекомунікаційні мережі та інші технічні засоби, які можуть піддаватися атакам або маніпуляціям з боку супротивника.

3. Організації – це можуть бути державні та недержавні організації, включаючи військові, правоохоронні, політичні, економічні та соціальні структури. Гібридні загрози можуть спрямовуватися на ослаблення або підрив діяльності цих організацій.

4. Держава – держава як така може бути суб'єктом безпеки, оскільки вона відповідає за захист своїх громадян та території. Це включає діяльність державних органів, таких як військові, розвідувальні та правоохоронні служби, які працюють на захист державних інтересів.

5. Міждержавні органи – умови гібридної війни можуть створювати напруженість між державами або групами держав. Міждержавні органи, такі як міжнародні організації, союзи або альянси, можуть брати участь у забезпеченні безпеки та врегулюванні конфліктів.

Важливо відзначити, що в гібридних конфліктах, різні суб'єкти безпеки можуть взаємодіяти між собою, щоб забезпечити спільну безпеку. Наприклад, державні органи можуть співпрацювати з організаціями та технічними системами, щоб захистити свою територію та населення від гібридних загроз.

Заходи, які вживаються для забезпечення безпеки в умовах гібридної війни, можуть варіюватися в залежності від конкретної ситуації. Наприклад,

можуть бути вжиті заходи для забезпечення кібербезпеки, збільшення свідомості громадян про гібридні загрози, зміцнення оборонної потужності держави, розвитку нових технологій для виявлення та протидії гібридним загрозам.

Однак важливо зазначити, що забезпечення безпеки в умовах гібридних воєн є складним та багатоаспектним процесом, який потребує співпраці різних суб'єктів безпеки та використання різних стратегій та інструментів.

Крім того, важливо пам'ятати, що гібридна війна може мати не тільки військовий, але й економічний, інформаційний, політичний або культурний компоненти. Тому, для забезпечення повної безпеки, необхідно враховувати всі аспекти гібридної війни та вживати відповідні заходи щодо захисту від них.

Також важливо зазначити, що реагування на гібридну війну повинне бути комплексним та системним. Це означає, що вживані заходи повинні бути не тільки реактивними, але й проактивними та попереджувальними. Наприклад, можуть бути вжиті заходи щодо попередження кібератак, виявлення та аналізу гібридних загроз та забезпечення кібербезпеки [4].

У цілому, забезпечення безпеки в умовах гібридних воєн є важливою задачею, яка потребує співпраці та координації різних суб'єктів безпеки, використання різних стратегій та інструментів, а також реактивного та проактивного підходу.

3.3. Норми та вимоги щодо керування ризиками

Управління ризиками – це процес ідентифікації, оцінки та керування ризиками, які можуть вплинути на досягнення мети або успішність організації. У світі існує кілька стандартів в галузі управління ризиками, деякі з них наведені нижче (рис. 3.4) [18]:

1. ISO 31000:2018 «Управління ризиками. Принципи та загальні вимоги» – це міжнародний стандарт, який надає загальні принципи та вимоги щодо управління ризиками. Цей стандарт містить принципи управління ризиками, процес управління ризиками, оцінку ризиків, керування ризиками та моніторинг ризиків.

2. COSO ERM Framework – це стандарт, який використовується для оцінки та управління ризиками в організаціях. Цей фреймворк надає опис загальних принципів управління ризиками, визначення складності, інтерпретації та впровадження процесів управління ризиками.

3. PMI-RMP – це сертифікаційна програма, яка надає знання та навички управління ризиками для професійних менеджерів проектів. Цей стандарт містить принципи, процеси, інструменти та техніки, що використовуються для управління ризиками в проектах.

4. ISO/IEC 27005:2018 «Інформаційна технологія. Управління ризиками інформаційної безпеки» – це стандарт, який визначає процеси та методології управління ризиками інформаційної безпеки в інформаційній технології. Цей

стандарт визначає ризики, пов'язані з інформаційною безпекою, та надає методи оцінки, керування та моніторингу цих ризиків.

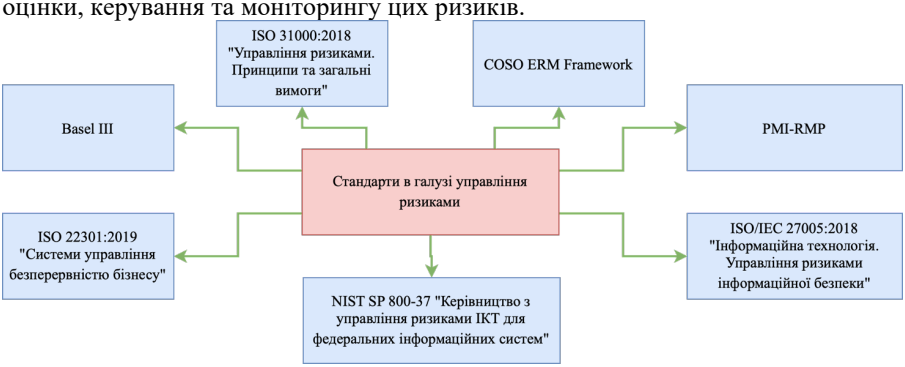

Рис. 3.4. Стандарти в галузі управління ризиками

5. NIST SP 800-37 «Керівництво з управління ризиками ІКТ для федеральних інформаційних систем» – це стандарт, розроблений Національним інститутом стандартів та технологій (NIST) США, який надає рекомендації щодо управління ризиками інформаційно-комунікаційних технологій (ІКТ) у федеральних інформаційних системах.

6. ISO 22301:2019 «Системи управління безперервністю бізнесу» – це стандарт, який надає вимоги та рекомендації щодо управління ризиками, пов'язаними з перервою в діяльності бізнесу, та відновленням діяльності після кризових ситуацій.

7. Basel III – це стандарт, що встановлює регулятивні вимоги до банківської діяльності та управління ризиками в банках. Він встановлює вимоги до капіталу, ліквідності та управління ризиками банків, що мають за мету зменшення ризиків для банків та фінансової стабільності в цілому.

Ці стандарти надають загальні принципи, методи та процеси для управління ризиками, що можуть бути застосовані в різних галузях. Обираючи стандарт для своєї організації, важливо враховувати її потреби та специфіку діяльності. ISO/IEC Guide 73 та AS/NZS 4360 є двома з основних стандартів в галузі управління ризиками.

3.3.1. Стандарт ISO/IEC Guide 73

Стандарт ISO/IEC Guide 73, повне найменування якого «Управління ризиками – Термінологія – Керівні принципи щодо використання в стандартах», встановлює термінологічні основи для управління ризиками. Цей стандарт визначає терміни, які використовуються в галузі управління ризиками, та встановлює загальні та керівні принципи для їх використання в різних

стандартах та регуляторних документах. Основною метою стандарту є забезпечення єдності та розуміння термінів, пов'язаних з управлінням ризиками, в усьому світі.Стандарт ISO/IEC Guide 73 включає наступні основні розділи:

– вступ, в якому описуються цілі та область застосування стандарту;

– розділ, присвячений основним термінам та визначенням в галузі управління ризиками;

– розділ, в якому описується процес управління ризиками та його основні елементи;

– розділ, присвячений загальним принципам управління ризиками та рекомендаціям щодо їх застосування;

– розділ, в якому обговорюються різні методи оцінки та аналізу ризиків;

– розділ, присвячений керівництву щодо використання термінології, встановленої в стандарті, в різних стандартах та регуляторних документах.

В цілому, стандарт ISO/IEC Guide 73 є важливим ресурсом для фахівців, які працюють в галузі управління ризиками, та дозволяє їм ефективно спілкуватися та співпрацювати в цій галузі в міжнародному масштабі.

3.3.2. Стандарт управління ризиками AS/NZS 4360

AS/NZS 4360 є стандартом з управління ризиками, який був розроблений в Австралії та Новій Зеландії. Цей стандарт був опублікований у 1995 році та розглядається як один з перших стандартів управління ризиками, який був розроблений на світовому рівні. Цей стандарт надає рекомендації та методологію для управління ризиками в будь-якій організації. Він визначає ризик як можливу втрату або шкоду, яка може виникнути, якщо не будуть прийняті необхідні заходи для її уникнення або зменшення до мінімуму.

Стандарт AS/NZS 4360 включає в себе процеси, які дозволяють організації ідентифікувати, оцінювати та управляти ризиками. Ці процеси включають в себе визначення контексту, установлення критеріїв оцінки ризиків, ідентифікацію ризиків, оцінку ризиків, управління ризиками, моніторинг та огляд.

Стандарт AS/NZS 4360 визначає процес управління ризиками, який включає наступні етапи:

1. Визначення контексту – визначення обставин, в яких діяльність відбувається, та ідентифікація факторів, які можуть впливати на досягнення цілей.

2. Оцінка ризиків – оцінка ймовірності виникнення ризиків та їх впливу на цілі.

3. Розроблення стратегії управління ризиками – визначення методів та засобів, які можуть бути використані для управління ризиками.

4. Реалізація стратегії управління ризиками – застосування засобів та методів, які були визначені на попередньому етапі.

5. Моніторинг та оцінка – визначення ефективності стратегії управління ризиками та оцінка нових ризиків, які можуть виникнути.

Стандарт AS/NZS 4360 дозволяє організаціям розуміти ризики та розробляти ефективні стратегії управління ними. Цей стандарт може бути використаний в різних галузях та діяльностях, включаючи бізнес, проектний менеджмент, гібридні конфлікти та державне управління.

AS/NZS 4360 підкреслює важливість управління ризиками для досягнення успіху в будь-якій організації, незалежно від її розміру чи галузі діяльності. Застосування стандарту AS/NZS 4360 дозволяє організаціям зменшити ризики та збільшити можливості для досягнення своїх цілей. Стандарти ISO/IEC Guide 73 і AS/NZS 4360 можуть використовуватися як окремо, так і разом для підвищення здатності протидіяти гібридним загрозам за рахунок забезпечення ефективного управління ризиками в організаціях. Наприклад, ISO/IEC Guide 73 може бути використаний для узагальнення термінів, пов'язаних з управлінням ризиками, а AS/NZS 4360 може бути використаний для надання процесу, який повинен бути виконаний для управління ризиками в організації.

КОНТРОЛЬНІ ПИТАННЯ

1. Розкрийте поняття основних сучасних концепцій, в яких відображаються сучасні підходи до визначення ризику.
2. Перелічіть основні об'єкти дослідження в теорії ризиків.
3. Які існують суб'єкти безпеки в умовах розгортання гібридних воєн?
4. Назвіть стандарти в галузі управління ризиками?
5. Перелічіть основні розділи стандарту ISO/IEC Guide 73.
6. Які етапи стандарту AS/NZS 4360 визначає процес управління ризиками?

ТЕСТИ

1. Що є основою ризик-орієнтованого підходу до забезпечення інформаційної безпеки?

а) Технологічні інновації
б) Оцінка ризиків та впровадження заходів для зменшення ризику
в) Соціальна взаємодія між організаціями
г) Маркетингова стратегія

2. Який підхід розглядає ризик як можливість виникнення збитків?

а) Ризик як ймовірність відхилення
б) Ризик як системне явище
в) Ризик як можливість збитку або втрати
г) Ризик як можливість

3. Що включає в себе процес оцінки ризику?
а) Виключно встановлення програмного забезпечення
б) Визначення вразливостей та загроз
в) Тільки оцінка фінансових втрат
г) Виключно оцінка ймовірності ризиків

4. Чому важливо регулярно оновлювати стратегію захисту?
а) Тому що загрози змінюються з часом
б) Тому що це вимагає законодавство
в) Для підвищення ефективності маркетингових кампаній
г) Щоб зберегти популярність компанії

5. Який стандарт регулює управління ризиками на міжнародному рівні?
а) ISO 9001
б) ISO 27001
в) ISO 31000
г) COBIT

6. Що відображає підхід до ризику як динамічного процесу?
а) Ризик не змінюється з часом
б) Ризик змінюється в залежності від внутрішніх та зовнішніх умов
в) Ризик можна повністю усунути
г) Ризик є непередбачуваним і некерованим

7. Яка концепція ризику зосереджується на взаємодії між можливостями та загрозами?
а) Ризик як невизначеність
б) Ризик як баланс між можливостями та загрозами
в) Ризик як інноваційне джерело
г) Ризик як можливість збитку

8. Що є основним об’єктом вивчення теорії ризиків?
а) Ризикова поведінка
б) Ризикові події
в) Економічні фактори
г) Стратегічне планування

9. Що є важливим аспектом забезпечення інформаційної безпеки в умовах гібридних загроз?
а) Регулярна оптимізація маркетингових стратегій
б) Встановлення мінімуму технічних заходів безпеки

в) Своєчасне виявлення та реагування на інциденти безпеки
г) Виключно технічні засоби безпеки

10. Яка концепція ризику визнає, що ризик є соціально-конструктивним явищем?
а) Ризик як систематичний та несистематичний
б) Ризик як соціально-конструктивне явище
в) Ризик як ймовірність відхилення
г) Ризик як інноваційне джерело

РОЗДІЛ 4.
АНАЛІЗ ТА ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1. Основні поняття аналізу ризиків інформаційної безпеки

Аналіз ризиків інформаційної безпеки – це процес виявлення, оцінки та управління ризиками, що пов'язані з інформаційною безпекою компанії. Для проведення аналізу ризиків інформаційної безпеки необхідно знати наступні поняття [25]:

1. Ризик – можливість того, що станеться небажана подія (інцидент), яка може призвести до негативних наслідків для інформаційної системи або організації в цілому.
2. Аналіз ризиків – процес виявлення, оцінки та управління ризиками, пов'язаними з інформаційною безпекою.
3. Загроза – потенційна можливість виникнення небажаної події, що може призвести до порушення безпеки інформації.
4. Вразливість – слабкі місця в системі захисту, які можуть бути використані зловмисниками для злому або знищення інформації.
5. Атака – спроба незаконного доступу до інформації або інших ресурсів компанії з метою їх злому, крадіжки або знищення.
6. Вразливість експлойта – використання зловмисником вразливості системи для злому або знищення інформації.
7. Ризиковий аналіз – оцінка можливих наслідків та ймовірності виникнення ризиків інформаційної безпеки.
8. Ризикове керівництво – процес управління ризиками, який передбачає вжиття заходів для зменшення ризиків та забезпечення безпеки інформації.
9. Класифікація ризиків – процес розподілу ризиків на категорії відповідно до їх характеру, можливих наслідків та імовірності виникнення.
10. Стійкість – здатність системи або організації відновлюватись після інцидентів, що стосуються безпеки інформації, і продовжувати свою роботу в обставинах, коли вони стають менш захищеними.
11. Безпека інформації – захист конфіденційності, цілісності та доступності інформації від несанкціонованого доступу, втручання та знищення.
12. Конфіденційність – забезпечення та збереження конфіденційності інформації, тобто забезпечення того, що інформація доступна тільки тим, кому вона призначена.

13. Цілісність – забезпечення та збереження цілісності інформації, тобто забезпечення того, що інформація не буде змінена без дозволу.

14. Доступність – забезпечення та збереження доступності інформації, тобто забезпечення того, що інформація буде доступна тим, хто має право на неї, у необхідний час.

15. Автентичність – забезпечення та збереження автентичності інформації, тобто забезпечення того, що інформація відповідає дійсності і не є підробкою.

Ці поняття допомагають зрозуміти, які ризики стосуються інформаційної безпеки, як їх оцінювати та управляти ними, а також які аспекти безпеки інформації необхідно захищати.

4.2. Етапи аналізу та оцінки ризиків

Аналіз та оцінка ризиків інформаційної безпеки – це процес ідентифікації та оцінки потенційних загроз інформаційній безпеці організації, її інфраструктурі, системам та даним, що зберігаються в цих системах. Цей процес допомагає організації розуміти можливість виникнення небезпеки, що може призвести до порушення конфіденційності, цілісності та доступності даних.

Процес аналізу та оцінки ризиків повинен включати наступні етапи (рис. 4.1) [18]:

Рис. 4.1. Етапи процесу аналізу та оцінки ризиків

1. Ідентифікація загроз – цей етап передбачає виявлення потенційних загроз інформаційній безпеці організації, що можуть призвести до втрати, руйнування, псування або незаконного доступу до даних.

2. Оцінка потенційного впливу – на цьому етапі необхідно визначити, який вплив може мати кожна з ідентифікованих загроз на інформаційну безпеку

організації. Наприклад, загроза вірусної атаки може призвести до втрати даних або порушення їх цілісності.

3. Визначення рівня ризику – на основі попередніх двох етапів можна визначити рівень ризику для кожної ідентифікованої загрози. Це допоможе організації прийняти рішення щодо необхідності прийняти заходи для захисту від цих загроз.

4. Вибір та реалізація заходів захисту – на цьому етапі організація вибирає заходи, які найбільш ефективні для запобігання виявленим загрозам. Це можуть бути технічні заходи (наприклад, встановлення файерволу або антивірусного програмного забезпечення), організаційні заходи (наприклад, політики безпеки, процедури контролю доступу) або навчання персоналу.

5. Моніторинг та аналіз ефективності заходів – після виконання заходів захисту необхідно провести моніторинг, щоб переконатися, що вони ефективні та забезпечують захист від ідентифікованих загроз. Якщо під час моніторингу буде виявлено нові загрози або проблеми з існуючими заходами захисту, організація повинна прийняти відповідні заходи для їх вирішення.

Аналіз та оцінка ризиків інформаційної безпеки – це постійний процес, оскільки загрози можуть змінюватися з часом, а гібридні атаки адаптуються під конкретні вразливості. Тому організації повинні проводити регулярний аналіз ризиків та вживати заходів захисту, щоб забезпечити безпеку своєї інформації.

До методичного апарату аналізу ризику можна віднести такі методи та інструменти (рис. 4.2) [10]:

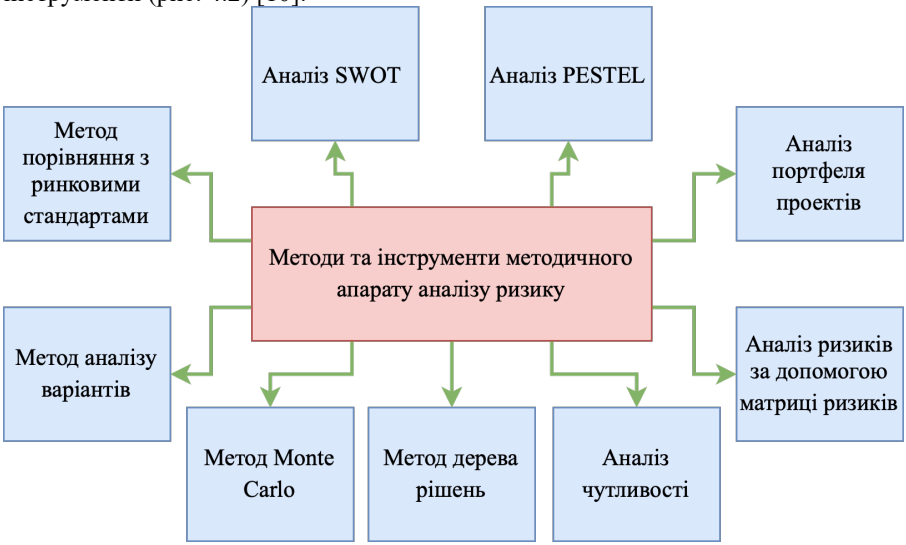

Рис. 4.2. Методи та інструменти методичного апарату аналізу ризику

1. Аналіз SWOT (Strengths, Weaknesses, Opportunities, Threats) – метод, що дозволяє оцінити сильні та слабкі сторони підприємства, а також можливості та загрози зовнішнього середовища.

2. Аналіз PESTEL (Political, Economic, Social, Technological, Environmental, Legal) – метод, що дозволяє оцінити вплив політичних, економічних, соціальних, технологічних, екологічних та правових факторів на діяльність підприємства.

3. Аналіз портфеля проектів – метод, що дозволяє відбирати та ранжувати проекти за рівнем ризику та доходності.

4. Аналіз ризиків за допомогою матриці ризиків – метод, що дозволяє оцінити величину ризику на основі його ймовірності та наслідків.

5. Аналіз чутливості – метод, що дозволяє визначити, як зміна параметрів впливає на ризик та доходність проекту.

6. Метод дерева рішень – метод, що дозволяє оцінити ризики та можливі наслідки прийняття різних рішень.

7. Метод Monte Carlo – метод, що дозволяє провести стохастичні симуляції для оцінки ризику та можливих наслідків.

8. Метод аналізу варіантів – метод, що дозволяє оцінити ризики та доходність різних варіантів дій та вибрати оптимальний.

9. Метод порівняння з ринковими стандартами – метод, що дозволяє порівняти величину ризику та доходність зі стандартами відповідного ринку.

Використання методичного апарату аналізу ризику дозволяє знизити ризик та підвищити ефективність діяльності в різних сферах. Крім того, цей апарат є важливим інструментом для прийняття обґрунтованих рішень та управління ризиками в умовах впливу гібридних загроз та невизначеності.

4.3. Типи та мета аналізу ризиків

Аналіз ризиків – це процес ідентифікації, оцінки та управління потенційними небажаними наслідками, які можуть виникнути в процесі виконання проекту або діяльності підприємства. Існують різні види аналізу ризиків, зокрема (рис. 4.3):

1. Кваліативний аналіз ризиків – оцінка ймовірності та впливу ризиків на проект або діяльність підприємства на основі досвіду, інтуїції та експертної оцінки.

2. Кількісний аналіз ризиків – оцінка ризиків на основі математичних моделей та статистичних методів. Цей вид аналізу дозволяє кількісно оцінити вплив ризиків та визначити оптимальні стратегії управління ризиками.

3. Аналіз імовірності та впливу – оцінка імовірності виникнення ризиків та їх впливу на проект або діяльність підприємства. Цей вид аналізу дозволяє визначити найбільш значущі ризики та зосередитися на них у процесі управління ризиками.

4. SWOT-аналіз – оцінка сильних та слабких сторін, можливостей та загроз, що відображаються на проекті або діяльності підприємства. SWOT-аналіз дозволяє визначити потенційні ризики та шляхи управління ними.

Рис. 4.3. Види аналізу ризиків

Завдання аналізу ризиків (рис. 4.4):

1. Ідентифікація потенційних ризиків, що можуть вплинути на проект або діяльність підприємства.
2. Оцінка ймовірності виникнення та впливу ризиків на проект або діяльність підприємства.
3. Визначення оптимальних стратегій управління ризиками, включаючи плани дій для зменшення ризиків, підвищення готовності до ризиків, або уникнення ризиків.
4. Визначення ризикових факторів, які впливають на кінцеві результати проекту або діяльності підприємства, і розробка плану управління цими факторами.
5. Моніторинг та оновлення аналізу ризиків протягом всього проекту або діяльності підприємства, з метою вчасного виявлення нових ризиків та адаптації стратегій управління ризиками.
6. Забезпечення комунікації та співпраці між всіма зацікавленими сторонами, щоб забезпечити ефективне управління ризиками та досягнення успішних результатів проекту або діяльності підприємства.

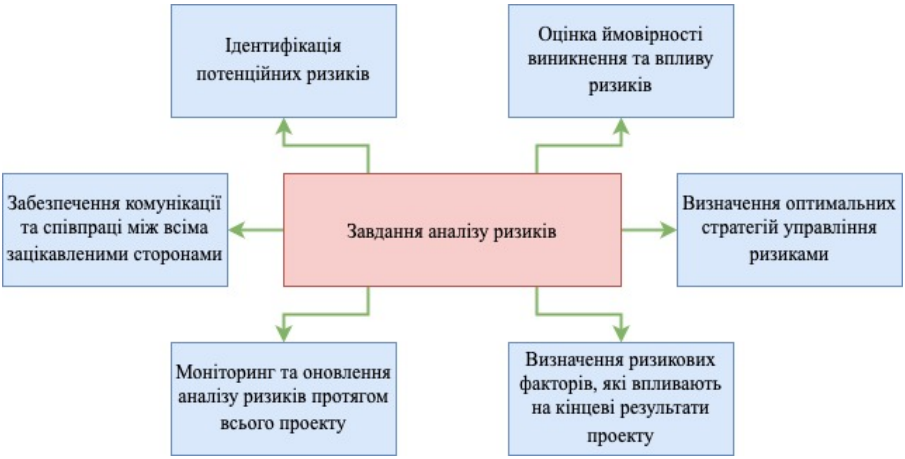

Рис. 4.4. Завдання аналізу ризиків

Аналіз ризиків дозволяє підвищити ефективність проекту або діяльності підприємства, зменшити ймовірність виникнення небажаних наслідків, підвищити можливості протистояти гібридним загрозам та забезпечити досягнення поставлених цілей.

4.4. Основні методи аналізу ризиків

Методи аналізу ризиків використовуються для ідентифікації та оцінки ризиків, що виникають у проектах, бізнес-планах, діяльності компаній та організацій. Для ефективного управління ризиками, важливо використовувати різні методи аналізу, які дозволяють виявляти та оцінювати можливі ризики та приймати рішення щодо їх управління.

Основні методи аналізу ризиків (рис. 4.5) [3]:

1. Аналіз SWOT – це метод, який використовується для ідентифікації сильних та слабких сторін проекту, а також можливих небезпек та можливостей. SWOT складається з аналізу чотирьох факторів: сильних сторін (Strengths), слабких сторін (Weaknesses), можливостей (Opportunities) та загроз (Threats).

2. Аналіз PEST – це метод, який використовується для вивчення зовнішнього середовища, у якому діє проект або організація. PEST означає: Політичні, Економічні, Соціальні та Технологічні аспекти. Аналіз PEST дозволяє виявити зміни у законодавстві, економічних умовах, технологіях та інших факторах, які можуть вплинути на проект.

3. Аналіз ризиків FMEA (Failure Mode and Effects Analysis) – це метод, який використовується для ідентифікації можливих несправностей в процесі роботи

та їх наслідків. Аналіз FMEA дозволяє виявити можливі проблеми та їх наслідки, що допомагає уникнути відповідних ризиків.

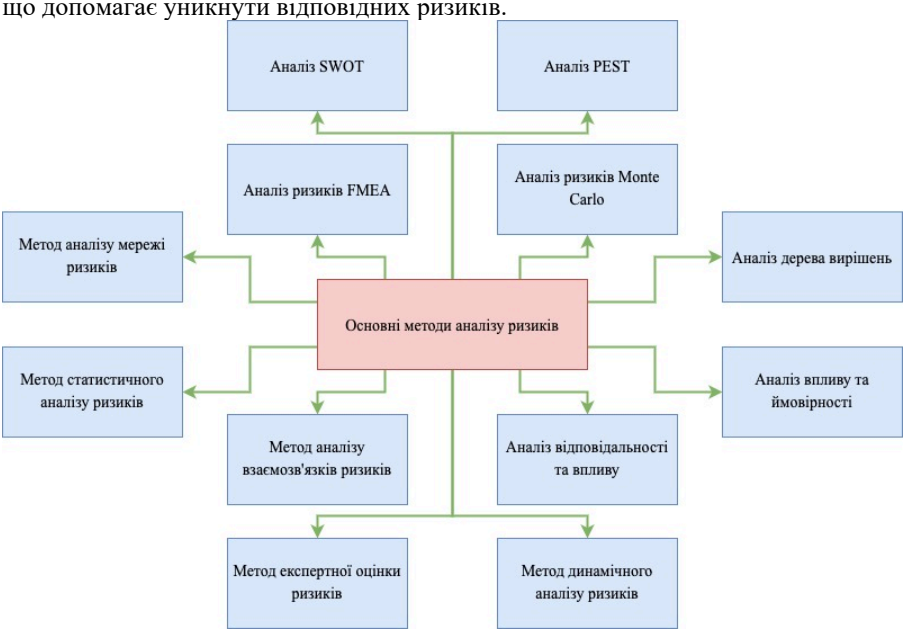

Рис. 4.5. Основні методи аналізу ризиків

4. Аналіз ризиків Monte Carlo – це метод, який використовується для визначення ймовірності відповідних результатів в залежності від різних варіантів випадкових подій або змінних. Цей метод дозволяє розрахувати ризики та оцінити вплив невизначеності на результати проекту.

5. Аналіз дерева рішень – це метод, який використовується для визначення ризиків та вибору оптимального рішення з багатьох можливих варіантів. Цей метод базується на побудові дерева рішень, яке містить всі можливі сценарії та їх вартість, і дозволяє оцінити ризики та вибрати найбільш ефективний варіант.

6. Аналіз впливу та ймовірності – це метод, який використовується для оцінки впливу та ймовірності виникнення ризиків. Для цього оцінюється важливість та вплив ризику на проект, а також ймовірність виникнення даного ризику. Цей метод дозволяє встановити пріоритетність ризиків та прийняти рішення щодо їх управління.

7. Аналіз відповідальності та впливу – це метод, який використовується для оцінки відповідальності та впливу на проект різних зацікавлених сторін. Для цього визначається список стейкхолдерів та їх вплив на проект, а також їхню

відповідальність за ризики. Цей метод дозволяє зрозуміти, які стейкхолдери можуть спричинити ризики та як їх вплив можна зменшити.

8. Метод динамічного аналізу ризиків – цей метод використовується для визначення ризиків, які можуть змінюватися з часом. Цей метод передбачає постійний моніторинг та аналіз ризиків, щоб вчасно реагувати на можливі проблеми.

9. Метод аналізу взаємозв'язків ризиків – цей метод використовується для визначення взаємозв'язків між різними ризиками та їх вплив на проект. Цей метод дозволяє враховувати можливість, що один ризик може призвести до появи іншого, або що відносно незначний ризик може мати серйозні наслідки в поєднанні з іншими ризиками.

10. Метод експертної оцінки ризиків – цей метод використовується для отримання оцінки ризиків від експертів відповідних галузей або фахівців у конкретній області. Цей метод дозволяє враховувати експертну думку, знання та досвід, щоб визначити ризики.

11. Метод аналізу мережі ризиків – цей метод використовується для визначення залежностей між різними ризиками та їх вплив на проект у вигляді мережі. Цей метод дозволяє враховувати можливість, що залежності між ризиками можуть вплинути на успішність проекту, тому що зниження ризиків в одній області може підвищити ризики в інших областях.

12. Метод статистичного аналізу ризиків – цей метод використовується для визначення ризиків на основі статистичних даних. Цей метод дозволяє враховувати історичні дані та інші статистичні фактори, щоб визначити ймовірність виникнення ризиків.

Ці методи можуть бути використані окремо або у комбінації для більш точного та повного аналізу ризиків в проекті. Крім того, важливо пам'ятати, що аналіз ризиків повинен бути постійним процесом, оскільки нові ризики можуть виникнути протягом всього життєвого циклу проекту. Тому після виявлення ризиків важливо розробити стратегії для управління ними, мінімізації їх впливу на проект та гарантій безпеки в умовах гібридних загроз.

Кожен з цих методів має свої переваги та недоліки, тому використання комбінації різних методів дозволяє отримати більш повну та точну картину ризиків та підходів до управління ними.

Деякі з методів управління ризиками включають [4]:

1. Передбачення ризиків – визначення можливих ризиків та їх вірогідності на ранніх етапах проекту.

2. Оцінка ризиків – оцінка впливу ризиків на проект та його цілі.

3. Розробка стратегій управління ризиками – визначення стратегій для зменшення впливу ризиків на проект.

4. Реалізація стратегій управління ризиками – здійснення стратегій для зменшення впливу ризиків на проект.

5. Моніторинг та контроль – відстеження ризиків протягом життєвого циклу проекту та здійснення необхідних корекцій.

Управління ризиками є важливим елементом успішного виконання будь-якого проекту, оскільки допомагає уникнути непередбачених проблем, знизити витрати та підвищити ефективність проекту. Однак, варто зазначити, що абсолютно неможливо передбачити всі можливі ризики, тому важливо мати здатність протистояти гібридним загрозам, готовість до непередбачених обставин та здатність швидко реагувати на них.

Ідентифікація, оцінювання та прогнозування ризиків для об'єктів та систем є важливими завданнями в багатьох галузях, включаючи фінанси, медицину, технології та інженерію. Математичні методи та моделі, які використовуються для цих завдань, можуть бути дуже різними, залежно від контексту застосування.

Одним з найбільш поширених методів є статистичний аналіз, який дозволяє оцінити ризики на основі даних, що зібрані про певний об'єкт або систему. Цей підхід може використовувати методи, такі як регресійний аналіз, кластерний аналіз та аналіз головних компонентів.

Інші методи включають моделювання ризиків, де математичні моделі використовуються для аналізу можливих наслідків різних сценаріїв. Це може включати методи, такі як математичні моделі марковських процесів, дерева рішень та байєсівські мережі.

Для складних систем, таких як мережі електропередачі, можуть використовуватись системні аналізи, які моделюють систему як набір взаємодіючих елементів. Це дозволяє оцінити ризики на основі взаємодії між елементами системи [24].

Ще одним підходом є використання методів штучного інтелекту, таких як нейронні мережі та генетичні алгоритми. Ці методи можуть використовуватись для аналізу складних даних та пошуку оптимальних рішень.

В кінці кінців, вибір конкретних математичних методів та моделей залежить від конкретного контексту застосування та доступності даних.

Також важливо враховувати те, що математичні моделі можуть мати свої обмеження та припущення, які не завжди можуть відповідати реальності. Наприклад, можуть бути проблеми з точністю даних, що використовуються для моделювання, або з недостатнім розумінням взаємодії між елементами системи.

Тому для успішної ідентифікації, оцінювання та прогнозування ризиків, важливо враховувати як математичні, так і не математичні фактори. Наприклад, для для виявлення та протидії гібридним загрозам експертне знання та досвід можна доповнити математичними методами та моделями, а також враховувати фактори, які можуть бути складними для врахування в математичних моделях.

Взагалі, ідентифікація, оцінювання та прогнозування ризиків є складними задачами, і вони вимагають ретельного аналізу та врахування різних факторів. Математичні методи та моделі можуть бути корисними інструментами для цих

завдань, але вони повинні використовуватися в контексті розуміння та експертизи з тієї галузі, де застосовуються.

4.5. Методи оцінки ризиків

Оцінка ризиків є важливою частиною багатьох бізнес-процесів. Для її здійснення існують різні методи, що можуть варіюватися залежно від сфери застосування і особливостей конкретної ситуації.

Один з методів оцінки ризиків – це аналіз ймовірності та впливу. Він базується на оцінці ймовірності настання певної події та на її впливі на бізнес-процес. Цей метод дозволяє зорієнтуватися в тому, наскільки серйозним може бути ризик та які заходи можна вжити для зменшення його впливу на бізнес.

Інший метод – аналіз відносних ризиків. Він полягає у порівнянні різних ризиків за їхньою серйозністю та вірогідністю настання. Цей метод дозволяє визначити найбільш значущі ризики та сконцентрувати зусилля на їхньому управлінні.

Крім того, існують інші методи оцінки ризиків, такі як дерево рішень, матриця ризиків тощо. Вибір методу залежить від конкретної ситуації та вимог замовника [19].

Ще один метод – SWOT-аналіз, який дозволяє оцінити сильні та слабкі сторони компанії, а також шанси та загрози на зовнішньому ринку. Цей метод використовується для стратегічного планування та може допомогти виявити можливості для розвитку компанії та уникнути ризиків.

Також, методи оцінки ризиків можуть бути розглянуті з різних поглядів, наприклад, з фінансового, екологічного, правового тощо. Кожен з цих підходів може мати свої особливості та відповідні методи оцінки.

У будь-якому випадку, оцінка ризиків є важливим етапом управління бізнес-процесами та дозволяє забезпечити забезпечення інформаційну безпеку та стійкість компанії в умовах гібридної війни. Правильний вибір методу та якісна оцінка ризиків допоможуть уникнути можливих негативних наслідків та досягти успіху в бізнесі.

Залежно від обсягу статистичних даних, методи імовірнісної оцінки показника ризику можуть мати різноманітні області застосування.

У випадку, коли обсяг даних досить великий, методи імовірнісної оцінки можуть бути застосовані для підтвердження або спростування гіпотез про показник ризику. Це може бути корисно в наукових дослідженнях, а також у фінансовій та медичній сферах, де точність оцінки ризику є критично важливою.

У випадку невеликого обсягу даних, методи імовірнісної оцінки можуть бути використані для створення прогнозів або передбачень про показник ризику. Це може бути корисно в бізнесі, де прогнозування ризику може допомогти у прийнятті важливих рішень у контексті попередження та протидії гібридним загрозам.

Отже, методи імовірнісної оцінки показника ризику можуть бути корисними в багатьох галузях, в залежності від обсягу статистичних даних, які використовуються для їх застосування.

Імовірнісна оцінка показника ризику залежить від обсягу статистичних даних, які використовуються для її розрахунку. Зазвичай, чим більший обсяг даних, тим точніша імовірнісна оцінка. Це пов'язано з тим, що більший обсяг даних дозволяє більш точно визначити статистичні параметри, які використовуються для розрахунку показника ризику.

Наприклад, якщо є дані про здоров'я людей, то більший обсяг даних дозволяє більш точно визначити ризики здоров'я, такі як ризик серцево-судинних захворювань, діабету, раку тощо. Також, чим більший обсяг даних, тим менше ймовірність випадкових помилок, які можуть вплинути на імовірнісну оцінку.

Проте, важливо зазначити, що при збільшенні обсягу даних може зростати складність обробки та аналізу даних, а також можуть виникнути проблеми зі збереженням та обробкою великих обсягів даних. Також, імовірнісна оцінка не завжди залежить виключно від обсягу даних, на неї можуть вплинути й інші фактори, такі як якість даних, методи аналізу тощо. Тому, при використанні методів імовірнісної оцінки показника ризику, необхідно враховувати всі фактори, які можуть вплинути на точність оцінки.

Методи імовірнісної оцінки показника ризику знаходять своє застосування в багатьох галузях, де важливим є прогнозування ризиків на основі даних. Залежно від наявності статистичних даних та рівня формалізації задачі, можна виділити наступні області застосування методів імовірнісної оцінки показника ризику:

1. Фінанси – управління ризиками в інвестиційному портфелі, оцінка кредитного ризику, ризикові моделі фінансових інструментів, оцінка фінансових ризиків.
2. Медицина – оцінка ризиків виникнення захворювань, прогнозування підвищення ризику побічних ефектів від лікування, оцінка ефективності лікарських засобів.
3. Технічні науки – оцінка ризику аварій на підприємствах, розробка систем автоматичного контролю ризиків, оцінка ефективності технічних рішень.
4. Соціальні науки – оцінка ризику прийняття рішень в умовах невизначеності, оцінка соціальних ризиків, аналіз ризиків державного управління.
5. Екологія – оцінка ризику впливу людської діяльності на довкілля, прогнозування екологічних катастроф, розробка заходів з мінімізації ризиків екологічної діяльності.

У випадках, коли є достатньо статистичних даних і задача має достатній рівень формалізації, методи імовірнісної оцінки показника ризику можуть бути дуже ефективними. Однак, коли дані обмежені або задача не формалізована

повністю, методи імовірнісної оцінки можуть бути менш ефективними, або потребувати додаткової експертної оцінки.

Наприклад, якщо задача полягає в оцінці ризику злочинної діяльності в певній області, інформація про кількість злочинів може бути обмеженою, і може бути важко визначити, які саме фактори впливають на ризик злочинної діяльності. У таких випадках можуть бути корисними інші методи оцінки ризику, такі як експертні оцінки або методи аналізу сценаріїв.

У загальному, методи імовірнісної оцінки показника ризику є важливим інструментом для багатьох галузей, де важливо прогнозувати та мінімізувати ризики на основі даних. Проте, варто зазначити, що вони не є універсальним рішенням для всіх задач, що породжуються з реалізацією гібридних загроз, і в деяких випадках можуть потребувати додаткової експертної оцінки або використання інших методів оцінки ризику.

КОНТРОЛЬНІ ПИТАННЯ

1. Дайте визначення основним поняттям для проведення аналізу ризиків інформаційної безпеки.
2. Навіть основні етапи процесу аналізу та оцінки ризиків.
3. Опишіть основні методи та інструменти методичного апарату аналізу ризику.
4. Які існують види аналізу ризиків?
5. Перелічіть основні завдання аналізу ризиків.
6. Опишіть основні методи аналізу ризиків.
7. Які існують методи оцінки ризиків?

ТЕСТИ

1. Що таке ризик в контексті інформаційної безпеки?

а) Можливість того, що станеться небажана подія, яка призведе до негативних наслідків

б) Позитивний результат роботи системи

в) Захищеність даних від зовнішніх атак

г) Ефективність захисту даних

2. Що є загрозою для інформаційної безпеки?

а) Використання антивірусного програмного забезпечення

б) Потенційна можливість виникнення небажаної події, що порушить безпеку інформації

в) Зашифрована передача даних

г) Контроль доступу до системи

3. Що таке вразливість?
а) Система захисту від загроз
б) Слабкі місця в системі, що можуть бути використані зловмисниками
в) Високий рівень захисту інформаційних систем
г) Безпека передачі даних через інтернет

4. Що означає термін «аналіз ризиків»?
а) Процес ідентифікації, оцінки та управління потенційними загрозами
б) Процес шифрування даних для їх захисту
в) Використання брандмауера для захисту мережі
г) Встановлення паролів на доступ до системи

5. Що таке конфіденційність в інформаційній безпеці?
а) Збереження доступності інформації для користувачів
б) Захист інформації від несанкціонованого доступу
в) Гарантія того, що дані будуть змінені лише з дозволу
г) Встановлення паролів для доступу до інформації

6. Що є прикладом атаки на інформаційну систему?
а) Спроба незаконного доступу до інформації з метою її знищення або зміни
б) Створення резервної копії даних
в) Оновлення антивірусного програмного забезпечення
г) Використання системи контролю доступу

7. Що таке стійкість інформаційної системи?
а) Здатність системи протистояти атакам без шифрування
б) Здатність системи відновлюватись після інцидентів і продовжувати роботу
в) Вміння користувачів захищати свої дані
г) Здатність системи працювати без збоїв упродовж 24 годин

8. Що входить до складу трикутника інформаційної безпеки?
а) Конфіденційність, доступність, зручність
б) Доступність, цілісність, автентичність
в) Конфіденційність, цілісність, доступність
г) Захищеність, надійність, швидкодія

9. Що таке кількісний аналіз ризиків?
а) Оцінка ризиків на основі математичних моделей та статистичних даних
б) Оцінка ризиків за допомогою експертних оцінок
в) Опис можливих ризиків у вигляді сценаріїв
г) Оцінка ризиків шляхом аналізу можливих атак на систему

10. Яка мета моніторингу заходів захисту?
а) Перевірити, чи всі користувачі мають доступ до системи
б) Виявити нові загрози або проблеми з існуючими заходами захисту
в) Забезпечити високошвидкісний доступ до інформації
г) Встановити нові паролі на всі системи

РОЗДІЛ 5.
ІДЕНТИФІКАЦІЯ ТА ОЦІНКА ЦІННОСТІ ІНФОРМАЦІЇ ЯК КЛЮЧОВОГО ФАКТОРУ РИЗИКУ

5.1. Інформація, яка обробляється інформаційними системами
5.2. Оцінка рівня безпеки інформаційних систем

Інформація є ключовим ресурсом для будь-якої організації та має велику цінність для її функціонування та розвитку. Однак, якщо інформація попадає в ненадійні руки або втрачається, це може призвести до серйозних наслідків для організації. Тому, ідентифікація та оцінка цінності інформації є ключовим фактором ризику для будь-якої організації з огляду на широкомасштабну гібридну війну.

Ідентифікація цінної інформації полягає у визначенні того, яка інформація є найбільш цінною для організації та як вона використовується. Наприклад, це може бути клієнтська база даних, комерційна інформація, технічні розробки або інтелектуальна власність. Важливо також визначити, яка саме інформація є конфіденційною та потребує додаткових заходів захисту.

Оцінка цінності інформації передбачає визначення ризиків, які можуть виникнути при її втраті або неправомірному використанні. Це можуть бути ризики для бізнесу, такі як втрата прибутку, конкурентний тиск або порушення репутації. Також можуть бути ризики для безпеки, такі як зловживання даними, крадіжка ідентифікаційної інформації або використання інформації для здійснення кібератак.

Для зменшення ризиків пов'язаних з використанням цінної інформації, організації повинні вживати заходів забезпечення безпеки даних, таких як шифрування, двофакторна автентифікація та моніторинг доступу до інформації. Також важливо регулярно оновлювати програмне забезпечення та обладнання, яке використовується для обробки цінної інформації, для запобігання використанню застарілих інструментів, які можуть містити вразливості.

Окрім технічних заходів, організації повинні звертати увагу на культуру безпеки даних серед своїх співробітників. В межах комплексної протидії гібридним загрозам це може включати проведення тренінгів та навчань з приводу правил зберігання та обробки інформації, а також розроблення політик безпеки даних, які передбачають внутрішні правила та процедури.

Також важливо мати плани відновлення після катастрофи та резервні копії даних, які забезпечать можливість відновити роботу системи у разі випадкової втрати даних або кібератаки.

Отже, ідентифікація та оцінка цінності інформації є ключовим фактором ризику для організації. Заходи забезпечення безпеки даних та культура безпеки даних серед співробітників можуть допомогти зменшити ризики пов'язані з використанням цінної інформації.

5.1. Інформація, яка обробляється інформаційними системами

Класифікація інформації за її цінністю є важливим етапом обробки даних в інформаційних системах. Зазвичай інформацію класифікують на три категорії залежно від її значення (рис. 5.1):

Рис. 5.1. Класифікація інформації за її цінністю

1. Критична інформація – це інформація, яка є надзвичайно важливою для підприємства або організації. Така інформація може стосуватись фінансів, власності, персоналу або бізнес-операцій. Невірна обробка або втрата цієї інформації може спричинити серйозні наслідки для діяльності організації.

2. Некритична інформація – це інформація, яка не має такого ж значення для організації, як критична інформація. Це може бути інформація про події, які відбуваються в компанії, але не стосуються її основної діяльності, наприклад, інформація про спортивні заходи або соціальні події.

3. Незначна інформація – це інформація, яка не має важливості для організації і може бути використана для загального інформування або розваг.

Класифікація інформації допомагає інформаційним системам забезпечувати адекватний рівень захисту інформації залежно від її значення та попереджувати можливі наслідки випадкової втрати або невірної обробки даних.

Інформація, яка обробляється інформаційними системами, може класифікуватися за її цінністю для організації або іншого користувача. Основні рівні класифікації інформації за її цінністю такі (рис. 5.2) [20]:

1. Відкрита інформація – це інформація, яка є загальнодоступною і не потребує додаткових заходів захисту. Це може бути інформація, яка доступна на публічних веб-сайтах, відкритих базах даних, газетах, журналах тощо.

2. Конфіденційна інформація – це інформація, яка містить обмежені доступом дані, що містять конфіденційні дані, такі як особисті дані, бізнес-секрети, фінансова інформація тощо. До такої інформації можуть мати доступ тільки авторизовані особи, які мають дозвіл на роботу з цією інформацією.

3. Секретна інформація – це інформація, яка містить дуже обмежений доступ та має ознаки національної важливості для держави. Це можуть бути військові та розвідувальні дані, державні таємниці, тощо. До такої інформації

можуть мати доступ лише спеціально авторизовані особи, які пройшли відповідну перевірку та мають відповідний дозвіл на роботу з цією інформацією.

Рис. 5.2. Основні рівні класифікації інформації за її цінністю

4. Критична інформація – це інформація, яка містить найбільш важливі та критичні для бізнесу чи держави дані. Це може бути, наприклад, інформація про системи безпеки, критичні інфраструктури, розклади польотів, місцезнаходження важливих осіб тощо. До такої інформації можуть мати доступ лише найвищі рівні управління та спеціально авторизовані особи зі статусом «потребує особливого захисту».

5. Некласифікована інформація – це інформація, яка не потребує класифікації за її цінністю, оскільки вона не містить конфіденційних або критичних даних і не становить загрози для безпеки організації або держави.

Для того, щоб протистояти гібридним загрозам та забезпечити належний захист інформації, необхідно визначити її рівень цінності та відповідний рівень захисту. Класифікація інформації за її цінністю допомагає встановити такі рівні та забезпечити відповідний захист від несанкціонованого доступу, втрати, руйнування або зміни інформації.

Також відома класифікація інформації, що називається «класифікацією за динамікою зміни цінності інформації з часом». Згідно з цією класифікацією, інформацію можна розділити на наступні категорії (рис. 5.3):

1. Нова інформація – інформація, яка щойно з'явилася, не мала часу на оцінку та аналіз і може мати значну цінність для прийняття рішень.

2. Стабільна інформація – інформація, яка не зазнає значних змін з часом і може бути корисною для прийняття рішень протягом тривалого періоду.

3. Застаріла інформація – інформація, яка втратила свою цінність через зміни в ситуації або надходження нової інформації.

4. Вторинна інформація – інформація, яка вже була використана для прийняття рішень, але може бути корисною для аналізу та вивчення досвіду.

Рис. 5.3. Класифікація інформації за динамікою зміни цінності інформації з часом

Для формування концепції інформаційної безпеки в умовах гібридних загроз класифікація інформації за динамікою зміни цінності з часом є важливою для розуміння того, як інформація може впливати на прийняття рішень в різних ситуаціях.

5.2. Оцінка рівня безпеки інформаційних систем

Оцінка рівня захищеності інформаційних систем повинна враховувати не тільки технічні заходи захисту, але й цінність оброблюваної інформації. Для цього необхідно провести аналіз можливих загроз та вразливостей інформаційної системи, вивчити форми і чинники впливу гібридної війни на стан і перебіг процесів, визначити рівень важливості різних типів інформації, що обробляється, та оцінити наслідки їх втрати або розголошення.

На основі цього аналізу можна розробити комплекс заходів захисту інформаційної системи, які будуть відповідати її рівню захищеності. При цьому важливо враховувати, що заходи захисту повинні бути пропорційними ризику втрати або розголошення інформації, а також вартості її відновлення або відшкодування.

Оцінка захищеності інформаційної системи повинна бути проведена регулярно, оскільки загрози та вразливості змінюються з часом. Крім того,

необхідно забезпечувати своєчасне оновлення заходів захисту відповідно до змін у загрозах та рівнях важливості інформації, що обробляється.

Окрім технічних заходів захисту, важливо також звернути увагу на культуру безпеки серед працівників, які мають доступ до інформаційної системи. Необхідно проводити навчання та тренінги з питань кібербезпеки, різних аспектів гібридної війни, підвищувати свідомість працівників щодо можливих загроз та вразливостей інформаційної системи, а також забезпечувати дотримання правил користування системою та інших політик безпеки.

Крім того, слід використовувати методи аудиту безпеки для виявлення можливих порушень у захисті інформаційної системи та її дієвості. Під час аудиту необхідно перевіряти відповідність заходів захисту встановленим вимогам та стандартам, а також забезпечувати виявлення та усунення вразливостей та можливих порушень безпеки.

Оцінка захищеності інформаційної системи повинна враховувати не тільки технічні заходи захисту, але й цінність оброблюваної інформації, культуру безпеки серед працівників та методи аудиту безпеки. Це дозволить забезпечити ефективний та пропорційний рівень захисту інформаційної системи від гібридних загроз та вразливостей.

Оцінка захищеності інформаційних систем з урахуванням цінності інформації, що обробляється, є важливою складовою безпеки інформаційної системи. Для здійснення оцінки захищеності необхідно виконати такі етапи (рис. 5.4):

Рис. 5.4. Етапи здійснення оцінки захищеності

1. Визначення критеріїв захищеності – у процесі визначення критеріїв захищеності необхідно враховувати всі аспекти безпеки інформації, такі як цілісність, конфіденційність, доступність, автентичність, надійність та інші.

2. Оцінка загроз – оцінка загроз допоможе визначити потенційні загрози для інформаційної системи, що можуть призвести до порушення безпеки та конфіденційності інформації.

3. Оцінка вразливостей – оцінка вразливостей допоможе визначити слабкі місця в інформаційній системі, які можуть бути використані зловмисниками для злому безпеки.

4. Визначення заходів захисту – враховуючи виявлені загрози та вразливості, необхідно визначити заходи захисту, які допоможуть зменшити ризики порушення безпеки інформаційної системи.

5. Оцінка ефективності заходів захисту – після впровадження заходів захисту необхідно перевірити їх ефективність і здатність до захисту інформації від потенційних загроз.

6. Проведення тестування на проникнення: – тестування на проникнення – це важливий етап в оцінці захищеності інформаційних систем. Цей процес допоможе виявити можливі вразливості інформаційної системи і перевірити ефективність заходів захисту.

7. Підтримка та оновлення – забезпечення безпеки інформаційної системи – це постійний процес. Тому необхідно забезпечити підтримку та оновлення системи, щоб забезпечити максимальний рівень безпеки та зменшити ризики порушення безпеки.

8. Систематична оцінка – оцінка захищеності інформаційної системи повинна бути проводитися систематично, з метою виявлення нових загроз та вразливостей і забезпечення максимального рівня безпеки.

Отже, оцінка захищеності інформаційної системи з урахуванням цінності інформації, що обробляється, є важливим етапом в забезпеченні безпеки інформації. Дотримання вищезазначених етапів допоможе забезпечити максимальний рівень безпеки, зменшити ризики порушення безпеки та дозволить реагувати на загрози забезпечення інформаційної безпеки в умовах гібридної війни.

КОНТРОЛЬНІ ПИТАННЯ

1. Перелічіть основні рівні класифікації інформації за її цінністю.
2. Наведіть приклади класифікації інформації за динамікою зміни цінності інформації з часом.
3. Що дозволяє забезпечити ефективний та пропорційний рівень захисту інформаційної системи від гібридних загроз та вразливостей?
4. Які існують етапи здійснення оцінки захищеності?

ТЕСТИ

1. Що таке критична інформація?
а) Інформація про спортивні події
б) Інформація, яка не має значення для організації
в) Інформація, яка є надзвичайно важливою для організації

г) Інформація, що доступна всім користувачам

2. Який захід може допомогти зменшити ризики втрати конфіденційної інформації?
а) Відкритий доступ до всіх файлів
б) Шифрування даних
в) Зберігання інформації без жодних заходів безпеки
г) Ігнорування захисту інформації

3. Що таке конфіденційна інформація?
а) Інформація про загальнодоступні новини
б) Дані, які мають обмежений доступ
в) Відкрита для всіх інформація
г) Інформація для розваг

4. Який рівень класифікації інформації потребує найвищого рівня захисту?
а) Відкрита інформація
б) Конфіденційна інформація
в) Секретна інформація
г) Некритична інформація

5. Що означає оцінка ризиків у контексті інформаційної безпеки?
а) Визначення важливості інформації для розваг
б) Оцінка можливих загроз при втраті інформації
в) Ігнорування загроз
г) Доступ до всіх даних для всіх працівників

6. Як часто слід проводити оцінку захищеності інформаційної системи?
а) Раз на 10 років
б) Після кожної зміни пароля
в) Регулярно
г) Лише після виявлення загрози

7. Що таке стабільна інформація?
а) Інформація, яка швидко змінюється
б) Інформація, що залишається корисною протягом тривалого часу
в) Інформація, яка втратила свою цінність
г) Інформація для розваг

8. Що таке резервне копіювання?
а) Процес видалення старих файлів
б) Процес створення копій даних для відновлення у разі втрати

в) Процес шифрування файлів
г) Зберігання даних без шифрування

9. Яка інформація вважається незначною для організації?
а) Фінансова інформація
б) Технічні розробки
в) Інформація про спортивні заходи
г) Інформація про клієнтів

10. Який захід допоможе захистити інформацію від кібератак?
а) Використання застарілого програмного забезпечення
б) Двофакторна автентифікація
в) Відкриття доступу до всіх даних для всіх співробітників
г) Ігнорування регулярних оновлень системи

РОЗДІЛ 6.
АНАЛІЗ ОСНОВНИХ ТА ГІБРИДНИХ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ

6.1. Прогнозування ризику виникнення небезпечних подій в умовах впливу гібридних загроз

6.2. Методи передбачення наслідків небезпечних дій з боку зловмисників, які здійснюють атаки

Інформаційні системи є важливим елементом сучасного суспільства, що використовується для забезпечення різних функцій, включаючи збір, обробку, зберігання та передачу інформації. Однак, інформаційні системи також піддаються різним загрозам та вразливостям, які можуть призвести до витоку конфіденційної інформації, порушення функціонування систем, а також інших негативних наслідків.

Основні загрози інформаційних систем (рис. 6.1) [1]:

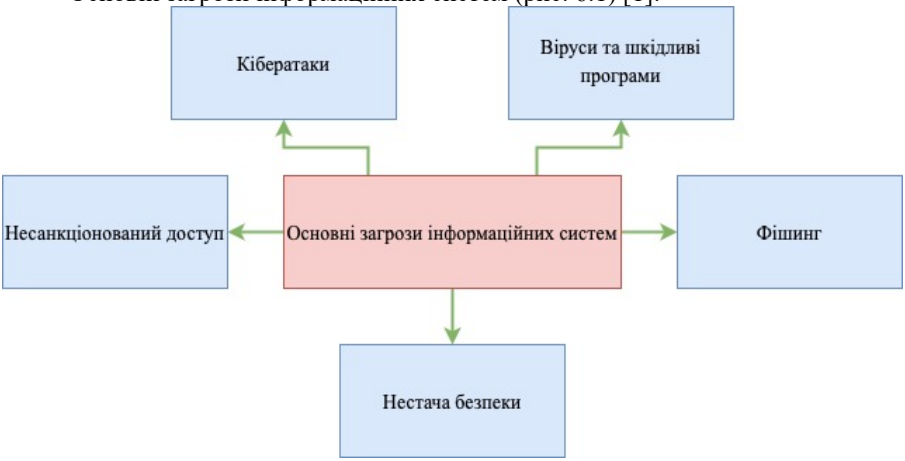

Рис. 6.1. Основні загрози інформаційних систем

1. Кібератаки – це зловживання комп'ютерних систем, мереж та програм, щоб завдати шкоди користувачам або організаціям.

2. Віруси та шкідливі програми – це програми, які розроблені для шкоди комп'ютерним системам і здатні поширюватися в мережі.

3. Фішинг – це метод атаки, який використовується для шахрайства, зокрема шляхом використання підробленої інформації для отримання доступу до конфіденційних даних.

4. Нестача безпеки – вразливості систем безпеки можуть бути використані для отримання несанкціонованого доступу до даних.

5. Несанкціонований доступ – це може бути викликано недостатньою системою автентифікації та авторизації, або через злам паролів.

Гібридні загрози інформаційних систем – це загрози, які поєднують у собі різні види атак, наприклад:

– фішингові атаки з використанням шкідливих програм;
– кібератаки з використанням шпигунського ПЗ;
– атаки на мережу з використанням дослідження директорій та розширень;
– атаки на мережу з використанням віддаленого доступу;
– атаки з використанням соціальної інженерії та шпигунських програм;
– атаки з використанням недоліків в програмному забезпеченні.

Для захисту інформаційних систем від цих загроз необхідно вживати комплексних заходів, таких як (рис. 6.2) [8]:

Рис. 6.2. Комплексні заходи, які необхідно вживати для захисту інформаційних систем від гібридних загроз

1. Забезпечення безпеки мережі – використання захисту мережевих пристроїв, таких як мережеві мережеві брандмауери, мережеві інтрузійні системи та системи виявлення інцидентів.

2. Захист програмного забезпечення – встановлення оновлень програмного забезпечення та антивірусних програм, виявлення та виправлення вразливостей.

3. Захист доступу – використання сильних паролів, двофакторної автентифікації, заборону доступу до конфіденційної інформації для зовнішніх користувачів.

4. Навчання персоналу – навчання користувачів інформаційних систем про методи захисту інформації, виявлення загроз та вчасне повідомлення про інциденти.

5. Відстеження інцидентів – встановлення системи відстеження та аналізу інцидентів, що допоможе вчасно виявляти та реагувати на гібридні та інші загрози.

6. Захист фізичного доступу – обмеження доступу до серверних кімнат та інших приміщень, де знаходяться комп'ютери та інші пристрої.

7. Захист даних – захист даних від несанкціонованого доступу за допомогою шифрування та інших методів захисту.

У контексті попередження та протидії гібридним загрозам врахування цих заходів допоможе зменшити ризик порушення безпеки інформаційної системи та зберегти конфіденційну інформацію в безпеці.

6.1. Прогнозування ризику виникнення небезпечних подій в умовах впливу гібридних загроз

Прогнозування можливості виникнення небезпечних подій в умовах впливу гібридних загроз є складним завданням, оскільки гібридні загрози можуть мати різноманітні форми і використовувати різні комбінації технологій та методів. Проте, деякі загальні підходи можуть допомогти в цьому процесі.

Один з підходів – це використання аналітики даних та машинного навчання для аналізу та моделювання можливих гібридних загроз. Цей підхід базується на використанні великої кількості даних про попередні атаки та інциденти для навчання моделей прогнозування ризику. Моделі можуть використовувати різноманітні джерела даних, такі як журнали подій, інформацію про кібербезпеку та відкриті дані з соціальних мереж, щоб прогнозувати можливі напади [2].

Інший підхід – це використання моніторингу в режимі реального часу для виявлення змін у поведінці користувачів та систем. Наприклад, це може включати моніторинг даних з мережі, системи виявлення вторгнень, моніторинг віддалених доступів, аналіз вмісту електронної пошти та інші технології. Цей підхід дозволяє виявляти підозрілу активність та реагувати на неї до того, як вона стане серйозною загрозою.

Крім того, важливо мати експертне знання та розуміння можливих гібридних загроз. Це може допомогти виявити підозрілу активність та надати контекст для аналізу даних. Експерти можуть використовувати свої знання та досвід для виявлення можливих комбінацій атак та їх відповідних наслідків. Наприклад, експерти можуть враховувати такі фактори, як мету нападу, тип цілі, тип атаки, що використовується, та інші чинники.

Крім того, для ефективного прогнозування можливих гібридних загроз важливо мати хорошу комунікацію та співпрацю між різними структурами та департаментами. Наприклад, кібербезпекові експерти, правоохоронні органи, військові та інші структури повинні обмінюватися інформацією та координувати свої дії для ефективної протидії гібридним загрозам [2].

Усі ці підходи можуть бути використані разом для створення більш точних та ефективних прогнозів можливих гібридних загроз. Однак, важливо розуміти, що гібридні загрози можуть бути дуже складними та вимагати розгляду багатьох

факторів, тому прогнозування можливих подій повинно бути підтримане постійним моніторингом та аналізом нових даних.

Основні методи прогнозування ризиків полягають у визначенні можливих наслідків, оцінці ймовірності їх виникнення та встановленні заходів для їх запобігання чи зменшення впливу.

Прогнозування ініціюючих подій – це процес передбачення майбутніх подій, які можуть вплинути на певну сферу життєдіяльності. Існує кілька підходів до прогнозування ініціюючих подій, які мають свої характеристики (рис. 6.3) [11]:

Рис. 6.3. Підходи до прогнозування ініціюючих подій

1. Статистичний підхід базується на аналізі статистичних даних, що дозволяє виявити тенденції та закономірності в розвитку подій. Для прогнозування використовуються математичні методи, такі як регресійний аналіз та часові ряди.

2. Експертний підхід базується на думках та оцінках експертів, які мають досвід у відповідній сфері. Експерти можуть використовувати свій досвід, знання та інтуїцію, щоб зробити прогноз.

3. Модельний підхід використовує математичні моделі для прогнозування ініціюючих подій. Моделі можуть бути стохастичними або детермінованими, залежно від того, чи враховуються в них випадкові фактори.

4. Гібридний підхід комбінує різні методи прогнозування, щоб отримати більш точний прогноз. Наприклад, можна використовувати статистичний підхід для аналізу даних та експертний підхід для оцінки важливості різних факторів.

У кожного підходу до прогнозування ініціюючих подій є свої переваги та недоліки, тому вибір підходу залежить від конкретної ситуації та мети прогнозування. Наприклад, для прогнозування економічних показників може бути використаний статистичний підхід, оскільки історичні дані про показники економіки є достатньо об'єктивними та доступними для аналізу. Для прогнозування соціальних подій, таких як зміна настроїв громадськості, може бути більш ефективним експертний підхід, оскільки експерти можуть врахувати більше кваліативних факторів, які не можуть бути виміряні статистично.

Незалежно від підходу, прогнозування ініціюючих подій має свої обмеження та ризики. Наприклад, прогноз може бути неточним через непередбачуваність незалежних факторів, а також може викликати негативну реакцію на ринках або серед громадськості, якщо прогноз виявиться неправильним.

Отже, вибір підходу до прогнозування ініціюючих подій повинен бути здійснений з урахуванням аспектів гібридної війни, конкретної ситуації, мети та обмежень прогнозування, а також оцінки ризиків та їх можливих наслідків.

Попередній прогноз небезпечних дій у комп'ютерній системі може містити різні показники, в залежності від його мети та обсягу.

Основними показниками можуть бути (рис. 6.4) [4]:

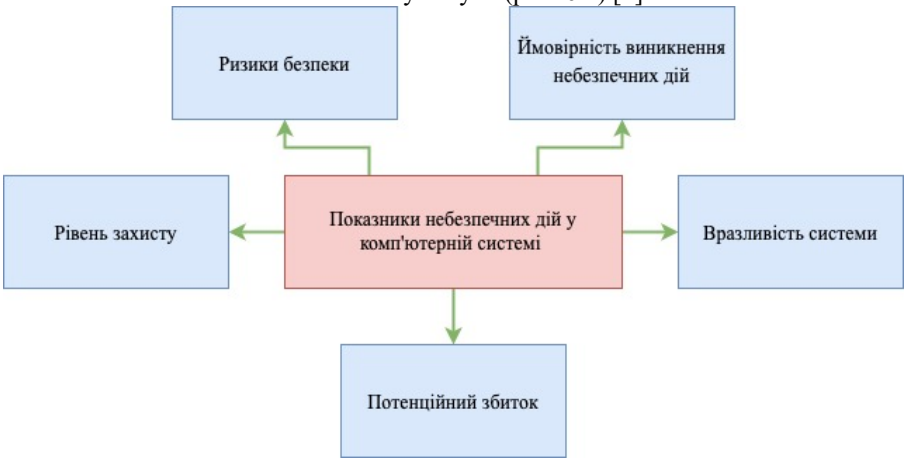

Рис. 6.4. Показники небезпечних дій у комп'ютерній системі

1. Ризики безпеки вказує на рівень загроз, які можуть виникнути в результаті небезпечних дій у комп'ютерній системі. Він може бути представлений у вигляді числа або категорії (наприклад, низький, середній, високий ризик).

2. Ймовірність виникнення небезпечних дій вказує на те, наскільки ймовірно виникнення небезпечних дій в комп'ютерній системі. Він також може бути представлений у вигляді числа або категорії.

3. Вразливість системи вказує на те, наскільки вразлива комп'ютерна система на певні види атак. Він може бути представлений у вигляді списку вразливостей або загальної оцінки вразливості системи.

4. Потенційний збиток вказує на те, який може бути збиток у разі виникнення небезпечних дій в комп'ютерній системі. Він може бути представлений у вигляді числа або категорії (наприклад, фінансовий, репутаційний збиток).

5. Рівень захисту вказує на те, наскільки ефективна система захисту комп'ютерної системи від небезпечних дій. Він може бути представлений у вигляді списку заходів захисту або загальної оцінки рівня захисту.

Ці показники можуть бути використані для виявлення та протидії гібридним загрозам та визначення стратегії захисту комп'ютерної системи. Однак, варто пам'ятати, що прогнозування небезпечних дій у комп'ютерній системі є складним процесом, оскільки він вимагає знань з кількох різних областей, таких як інформаційна безпека, кібербезпека, криптографія, програмування та інші. Тому важливо, щоб прогнозування небезпечних дій проводилося кваліфікованими фахівцями з достатнім рівнем знань та досвіду.

Для отримання більш точних результатів прогнозування можуть використовуватися різні методи та техніки, такі як аналіз загроз, ризик-аналіз, сканування вразливостей та інші. Також важливо регулярно проводити аудит безпеки комп'ютерної системи, оцінювати здатність протистояти гібридним загрозам та вчасно виявляти і усувати вразливості [13].

Отже, попередній прогноз небезпечних дій у комп'ютерній системі може містити різні показники, що дозволяють оцінювати рівень загроз та визначати стратегію захисту. Прогнозування небезпечних дій є важливим етапом у забезпеченні безпеки комп'ютерної системи та потребує високого рівня знань та досвіду від фахівців з інформаційної безпеки.

6.2. Методи передбачення наслідків небезпечних дій з боку зловмисників, які здійснюють атаки

Прогнозування наслідків небезпечних дій агентів вторгнень є важливим етапом в процесі забезпечення кібербезпеки. Для досягнення цієї мети використовуються різні методи прогнозування, такі як (рис. 6.5) [2]:

1. Метод аналізу ризиків включає оцінку потенційних загроз і виявлення вразливостей системи. Після цього визначається ризик і можливі наслідки, що виникають в результаті вторгнення.

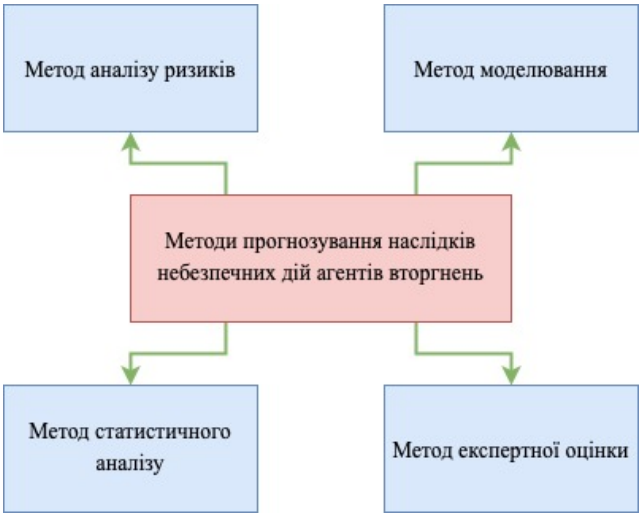

Рис. 6.5. Методи прогнозування наслідків небезпечних дій агентів вторгнень

2. Метод моделювання використовує математичні моделі для відображення поведінки зловмисника та його можливих наслідків. Такий підхід дозволяє відтворити різні сценарії вторгнень та здійснити їх аналіз.

3. Метод експертної оцінки передбачає залучення експертів, які мають досвід у виявленні загроз та оцінці наслідків вторгнення. Експерти надають свої рекомендації та прогнозують можливі наслідки.

4. Метод статистичного аналізу використовує статистичні дані для визначення ризику вторгнення та його наслідків. Часто використовуються дані про попередні вторгнення, щоб визначити шаблони та тренди.

Кожен з цих методів має свої переваги та недоліки, тому вибір методу залежить від конкретної ситуації та завдань. У кібербезпеці найчастіше використовують комбінацію різних методів для досягнення найкращих результатів.

Завдання оцінки та прогнозу небезпечних дій агентів вторгнень (інтрузів) є складними та вимагають забезпечення високої якості даних, аналізу та інтерпретації. Деякі з характеристик цих завдань включають (рис. 6.6) [2]:

1. Надійність даних – для оцінки та прогнозу небезпечних дій агентів вторгнень необхідно мати надійні дані про те, що сталося в минулому та що відбувається в даний момент. Це може включати дані про спроби вторгнення, виявлені вразливості системи та активність користувачів. Для забезпечення надійності даних можна використовувати різні джерела даних та методи перевірки.

Рис. 6.6. Характеристики завдань оцінки та прогнозу небезпечних дій агентів вторгнень

2. Аналітичні навички – оцінка та прогноз небезпечних дій агентів вторгнень потребує вмінь аналізувати великі обсяги даних та знаходити залежності та тенденції. Необхідні навички включають статистичний аналіз, машинне навчання та інші методи аналізу даних.

3. Знання про загрози – ефективна оцінка та прогнозування небезпечних дій агентів вторгнень потребує глибоких знань про різні типи загроз та їхні наслідки. Це може включати знання про різні види атак, шкідливі програми та інші методи вторгнень.

4. Експертиза в області кібербезпеки – оцінка та прогноз небезпечних дій агентів вторгнень потребує експертизи в області кібербезпеки. Це може включати знання про вимоги до захисту даних, технології захисту мереж та інші аспекти кібербезпеки.

5. Розуміння контексту – для ефективної оцінки та прогнозування небезпечних дій агентів вторгнень, необхідно розуміти контекст, в якому вони відбуваються. Це може включати розуміння бізнес-процесів, технічних систем та інфраструктури, а також соціальних та політичних факторів, що можуть впливати на дії агентів вторгнень.

6. Здатність до прогнозування – оцінка та прогноз небезпечних дій агентів вторгнень потребує здатності до прогнозування майбутньої діяльності. Це може включати розуміння тенденцій та патернів в активності вторгнення, а також вміння прогнозувати можливі наслідки.

7. Ефективність взаємодії – оцінка та прогноз небезпечних дій агентів вторгнень потребує ефективної взаємодії між різними командами та фахівцями.

Це може включати комунікацію між командами з інформаційної безпеки, мережевою інфраструктурою, експертами з даних та аналітиками.

8. Систематичний підхід – оцінка та прогноз небезпечних дій агентів вторгнень потребує систематичного підходу, який включає організацію даних, аналіз, взаємодію, оцінку та прогнозування. Це може включати використання різних методів та інструментів для збору та аналізу даних, моделювання та прогнозування на основі цих даних, та взаємодії між командами та фахівцями.

9. Використання інформаційних джерел – для оцінки та прогнозування небезпечних дій агентів вторгнень необхідно використовувати різні джерела інформації. Це можуть бути дані з моніторингу мережі, логів систем, відкритих та інших джерел.

10. Аналіз даних – для ефективної оцінки та прогнозування небезпечних дій агентів вторгнень потрібний аналіз даних. Це може включати використання аналітики даних, машинного навчання та інших методів для виявлення патернів та аномалій у поведінці вторгнення.

11. Експертна оцінка – експертна оцінка є важливим елементом при оцінці та прогнозуванні небезпечних дій агентів вторгнень. Експерти можуть надавати свої знання та досвід для розуміння складних аспектів вторгнення та розробки стратегій захисту.

12. Здатність до швидкої реакції – оцінка та прогноз небезпечних дій агентів вторгнень потребує здатності до швидкої реакції на виявлені загрози. Це може включати розробку планів дій, організацію протоколів безпеки та інші заходи для запобігання та ліквідації інцидентів.

13. Моніторинг та оновлення – оцінка та прогноз небезпечних дій агентів вторгнень є постійним процесом, який потребує моніторингу та оновлення. Система безпеки повинна бути постійно оновлюваною та адаптованою до нових загроз, щоб забезпечити ефективний захист.

14. Взаємодія зі стейкхолдерами – оцінка та прогноз небезпечних дій агентів вторгнень є процесом, який повинен включати взаємодію зі стейкхолдерами, такими як керівництво компанії, IT-відділ, безпекові служби та інші зацікавлені сторони. Це допоможе забезпечити згоду та співпрацю у визначенні загроз та розробці стратегій захисту.

15. Контроль та аудит – оцінка та прогноз небезпечних дій агентів вторгнень повинна підлягати контролю та аудиту, щоб забезпечити ефективність та відповідність вимогам безпеки. Це може включати перевірку відповідності політик безпеки, аналіз вразливостей та випробування систем безпеки.

Отже, характеристики завдань оцінки та прогнозу небезпечних дій агентів вторгнень включають в себе використання різних джерел інформації, аналіз даних, експертну оцінку, здатність до швидкої реакції, моніторинг та оновлення, взаємодію зі стейкхолдерами та контроль і аудит. Виконання цих завдань є важливим елементом забезпечення інформаційної безпеки як однієї з основних складових національної безпеки.

Так, прогнозування наслідків небезпечних дій агентів вторгнень є важливим завданням для забезпечення безпеки комп'ютерних систем. Агенти вторгнень можуть включати в себе шкідливі програми, які можуть використовувати вразливості в програмному забезпеченні, щоб отримати несанкціонований доступ до комп'ютерної системи, викрадати конфіденційну інформацію або завдати шкоди системі.

Прогнозування наслідків небезпечних дій агентів вторгнень дозволяє забезпечити ефективну реакцію на такі дії, виявити порушення безпеки на ранній стадії та запобігти виникненню серйозних проблем. Для прогнозування наслідків небезпечних дій агентів вторгнень використовуються різні методи, такі як аналіз вразливостей системи, моніторинг мережевої активності, виявлення аномальних дій та інші.

У контексті попередження та протидії гібридним загрозам, прогнозування наслідків небезпечних дій агентів вторгнень є необхідною складовою для забезпечення безпеки комп'ютерних систем і є важливим завданням для інформаційної безпеки в цілому.

КОНТРОЛЬНІ ПИТАННЯ

1. Які виділяють основні загрози інформаційних систем?
2. Які комплексні заходи необхідно вживати для захисту інформаційних систем від гібридних загроз?
3. Як відбувається прогнозування ризику виникнення небезпечних подій в умовах впливу гібридних загроз?
4. Які виділяють підходи до прогнозування ініціюючих подій?
5. Які показники небезпечних дій у комп'ютерній системі існують?
6. Опишіть методи прогнозування наслідків небезпечних дій агентів вторгнень.
7. Які виділяють характеристики завдань оцінки та прогнозу небезпечних дій агентів вторгнень?

ТЕСТИ

1. Що таке кібератака?
а) Неправомірне використання комп'ютерних систем для отримання вигоди
б) Зловживання комп'ютерних систем, мереж та програм для шкоди
в) Процес навчання користувачів інформаційних систем
г) Встановлення антивірусного програмного забезпечення

2. Яка з наведених програм є прикладом шкідливих програм?
а) Операційна система
б) Вірус

в) Офісний пакет
г) Браузер

3. Що таке фішинг?
а) Атака на комп'ютерну мережу
б) Метод шахрайства для отримання конфіденційних даних
в) Процес встановлення паролів
г) Захист інформаційних систем

4. Який захід є важливим для захисту доступу до інформаційних систем?
а) Використання слабких паролів
б) Двофакторна автентифікація
в) Відкритий доступ до даних
г) Використання загальних паролів

5. Яка з наведених дій є частиною захисту фізичного доступу?
а) Використання антивірусних програм
б) Обмеження доступу до серверних кімнат
в) Встановлення брандмауера
г) Моніторинг даних з мережі

6. Яка з нижче перерахованих методів використовується для прогнозування ризику виникнення небезпечних подій?
а) Статистичний підхід
б) Творчий підхід
в) Соціальний підхід
г) Візуальний підхід

7. Що є основним методом виявлення загроз у кібербезпеці?
а) Статистичний аналіз
б) Моніторинг в режимі реального часу
в) Використання антивірусних програм
г) Оцінка ринку

8. Який підхід комбінує різні методи прогнозування для отримання точніших результатів?
а) Статистичний підхід
б) Модельний підхід
в) Гібридний підхід
г) Експертний підхід

9. Що таке метод експертної оцінки у прогнозуванні загроз?

а) Оцінка на основі статистичних даних
б) Залучення фахівців для аналізу ситуації
в) Використання математичних моделей
г) Оцінка на основі попередніх інцидентів

10. Який метод передбачає використання даних з минулих атак для прогнозування ризику?
а) Метод моделювання
б) Метод аналізу ризиків
в) Метод статистичного аналізу
г) Метод експертної оцінки

РОЗДІЛ 7.
МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЇ

7.1. Методи управління ризиками захищеності

Управління ризиками захищеності (інформаційної безпеки) – це процес ідентифікації, аналізу, оцінки та контролювання ризиків, пов'язаних із захищеністю інформації в організації або підприємстві. Існує кілька методів управління ризиками захищеності, таких як (рис. 7.1) [21]:

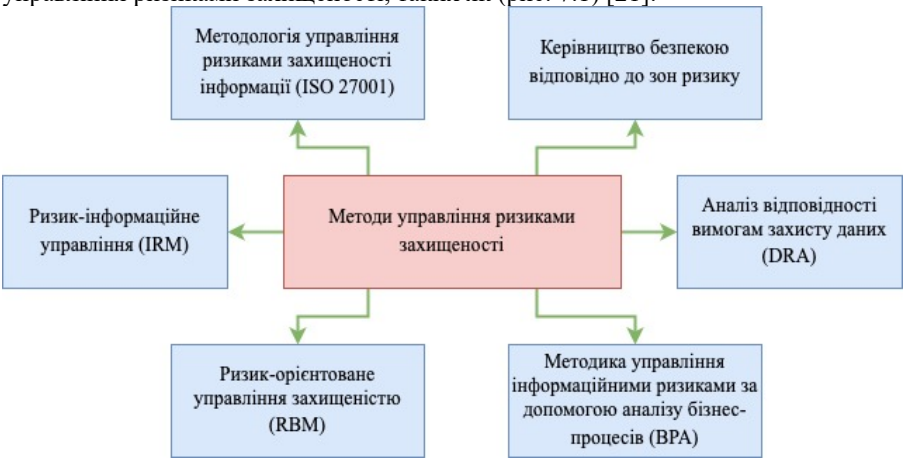

Рис. 7.1. Методи управління ризиками захищеності

1. Методологія управління ризиками захищеності інформації (ISO 27001) базується на стандарті ISO/IEC 27001:2013 і складається з шести етапів: контекст організації, управління ризиками, управління ризиками захищеності інформації, оцінка ризиків захищеності інформації, ризик-аналіз та виправлення, а також моніторинг та оцінка.

2. Керівництво безпекою відповідно до зон ризику полягає у визначенні зон ризику і прийнятті рішень щодо заходів захисту, які мають бути реалізовані в кожній зоні.

3. Аналіз відповідності вимогам захисту даних (DRA) заснований на виконанні аналізу захищеності даних, який дозволяє визначити ризики захисту та розробити план управління ними.

4. Методика управління інформаційними ризиками за допомогою аналізу бізнес-процесів (BPA) використовується для аналізу бізнес-процесів з метою виявлення ризиків захисту, пов'язаних з обробкою інформації.

5. Ризик-орієнтоване управління захищеністю (RBM) заснований на використанні ризик-орієнтованого підходу до управління захищеністю, де пріоритетним є аналіз та управління ризиками. Згідно з цим підходом, організація повинна визначити свої ресурси та цілі, а також оцінити ризики, що стануть перешкодою для досягнення цих цілей. Після цього, заходи захисту повинні бути призначені згідно з відповідністю виявлених ризиків.

6. Ризик-інформаційне управління (IRM) використовується для ідентифікації, оцінки та контролювання ризиків, пов'язаних з інформаційними технологіями. IRM дає можливість виявити ризики, пов'язані з інформаційною безпекою, і розробити заходи захисту для запобігання цим ризикам.

Використання будь-якого з цих методів залежить від контексту та потреб організації, яка здійснює управління ризиками захищеності. Однак, важливо мати на увазі, що з огляду на широкомасштабну гібридну війну управління ризиками захищеності повинно бути постійним процесом, оскільки загрози і ризики постійно змінюються [13].

EBIOS, MEHARI, OCTAVE, CRAMM та CORAS є методами управління ризиками захищеності, які зазвичай використовуються в інформаційній безпеці та при оцінці вразливостей систем. Кожен з цих методів має свою власну систему критеріїв та процедур, що дозволяє оцінити рівень ризику та розробити план дій для його зменшення.

COBRA та RiskWatch є програмними засобами управління ризиками, які дозволяють зібрати, аналізувати та оцінювати дані про ризики, пов'язані з інформаційною безпекою. Ці інструменти забезпечують більш ефективний процес управління ризиками, зменшуючи ймовірність виникнення проблем та покращуючи реагування на них.

Усі ці методи та інструменти є важливими компонентами для забезпечення безпеки та захищеності розподілених комп'ютерних систем і можуть надавати певні гарантії безпеки в умовах гібридних загроз. Вибір конкретного методу чи інструменту залежить від потреб та особливостей конкретної системи та оцінки ризиків, пов'язаних з її функціонуванням.

7.2. Метод EBIOS

Метод EBIOS (Expression des Besoins et Identification des Objectifs de Securite) – це методологія оцінки та управління ризиками в галузі інформаційної безпеки, розроблена у Франції. Вона дозволяє оцінити вразливості

інформаційної системи, визначити найбільш ймовірні загрози та розробити заходи щодо їх усунення. Метод EBIOS включає наступні етапи:

1. Визначення цілей безпеки – визначення цілей, які необхідно досягти в галузі інформаційної безпеки.
2. Ідентифікація активів – визначення інформаційних активів, які потрібно захистити.
3. Визначення загроз – визначення потенційних загроз інформаційної безпеки та оцінка їх впливу на активи.
4. Визначення вразливостей – визначення вразливостей інформаційної системи, які можуть бути використані зловмисниками для здійснення загроз.
5. Оцінка ризику – оцінка ймовірності виникнення загроз та їх впливу на активи, а також визначення рівня ризику.
6. Розробка заходів з управління ризиками – визначення заходів, які дозволять знизити ризик до прийнятного рівня.
7. Реалізація заходів з управління ризиками – впровадження заходів з управління ризиками та контроль їх ефективності.
8. Моніторинг та управління – моніторинг системи безпеки, аналіз результатів та коригування заходів за потреби.

Метод EBIOS дозволяє оцінити ризики інформаційної безпеки на різних рівнях – від окремих додатків і компонентів до цілої інформаційної системи. Він використовується в багатьох галузях, де важливо забезпечити високий рівень захисту інформації, таких як фінансові установи, державні структури, телекомунікаційні компанії, тощо.

Однією з переваг методу EBIOS є його гнучкість і адаптабельність до конкретних потреб організації. Метод можна адаптувати до різних моделей оцінки ризиків, що дозволяє вибрати оптимальний підхід для конкретної ситуації та підвищує можливості протистояти гібридним загрозам.

Також важливим є те, що метод EBIOS спрощує взаємодію між різними відділами організації, які займаються питаннями інформаційної безпеки. Це досягається за рахунок використання спільного мовлення та стандартів для опису процесів оцінки та управління ризиками.

Загалом, метод EBIOS є ефективним інструментом для управління ризиками в галузі інформаційної безпеки. Він дозволяє забезпечити високий рівень захисту інформації, знизити ризик її втрати або пошкодження, а також зберегти репутацію та довіру клієнтів.

7.3. Метод MEHARI

Методологія MEHARI (Model for Evaluation of the Human Factors in Risk Analysis) – це метод оцінки ризиків, створений в Європі для оцінки ризиків в галузі інформаційної безпеки [12].

Вона була створена з метою поліпшення розуміння ризиків, пов'язаних з людським фактором в галузі інформаційної безпеки, а також для оцінки цих ризиків. MEHARI включає кроки, такі як оцінка вразливостей, оцінка загроз, оцінка ризиків та прийняття рішень щодо управління ризиками.

Цей метод допомагає виявити вразливості та ризики, пов'язані з людським фактором, такі як помилки, недоліки навчання, неправильне використання систем тощо. Він також дозволяє визначити відповідні заходи щодо управління ризиками, які можуть включати зміни в політику безпеки, процедури, вимоги до навчання тощо.

MEHARI може використовуватися як окремо, так і в поєднанні з іншими методами оцінки ризиків. Він широко використовується в Європі, особливо в державному секторі та секторі фінансових послуг, і є корисним інструментом для оцінки ризиків в галузі інформаційної безпеки, пов'язаних з людським фактором.

MEHARI дозволяє враховувати особливості людського фактора в оцінці ризиків. Наприклад, він дозволяє оцінити вплив соціального і культурного середовища на поведінку користувачів, що може впливати на ризик безпеки інформації, яка потребує захисту від гібридних викликів і загроз, що в свою чергу вимагає вироблення механізмів їх чіткої ідентифікації та протидії. Також метод дозволяє враховувати вплив недосвідченості користувачів, їхнього рівня знань та інших факторів, які можуть призвести до виникнення ризиків безпеки.

Крім того, MEHARI дозволяє використовувати різноманітні моделі, які відображають вплив різних факторів на безпеку інформації, що дозволяє більш точно оцінювати ризики та приймати обґрунтовані рішення щодо їх управління.

Важливо зазначити, що MEHARI не є універсальним методом оцінки ризиків, і не підходить для всіх випадків. Він спрямований переважно на оцінку ризиків, пов'язаних з людським фактором в галузі інформаційної безпеки. Однак, він може бути використаний в поєднанні з іншими методами оцінки ризиків для отримання більш повної карти ризиків та їх управління. Метод MEHARI (Method for Harmonized Risk Assessment in ICT Environments) – це методологія оцінки ризиків інформаційно-комунікаційних технологій (ІКТ). Основні модулі цієї методології включають наступне (рис. 7.2):

1. Керування проектом та опис системи – цей модуль визначає мету оцінки ризиків, створює проект, визначає опис системи та визначає, які активи слід оцінювати.

2. Ідентифікація загроз – в цьому модулі визначаються потенційні загрози, які можуть вплинути на систему. Це можуть бути загрози, пов'язані з людьми, технологіями, природними катастрофами, технічними помилками тощо.

3. Визначення вразливостей – в цьому модулі визначаються вразливості системи, тобто слабкі місця, які можуть бути використані для атаки.

4. Оцінка ризиків – в цьому модулі оцінюються ризики, які виникають внаслідок поєднання загроз і вразливостей. В результаті цієї оцінки ризиків

визначається ймовірність виникнення загрози та наслідки, які можуть відбутися у зв'язку з реалізацією цієї загрози.

Рис. 7.2. Основні модулі методу MEHARI

5. Управління ризиками – в цьому модулі визначаються заходи з мінімізації ризиків, тобто способи зменшення ймовірності виникнення загроз та наслідків їх реалізації.

6. Розробка плану безпеки – цей модуль включає розробку плану безпеки, який описує, як будуть впроваджені заходи з мінімізації ризиків та забезпечення безпеки ІКТ.

7. Аудит – цей модуль відповідає за періодичну перевірку системи на відповідність плану безпеки, оцінку ефективності заходів з мінімізації ризиків та виявлення нових загроз та вразливостей, що можуть виникнути.

8. Моніторинг – цей модуль включає в себе періодичний моніторинг заходів з мінімізації ризиків та плану безпеки, щоб переконатися, що вони дієві та залишаються актуальними у середовищі, що змінюється.

Кожен з цих модулів є важливим етапом процесу оцінки ризиків інформаційно-комунікаційних технологій і допомагає сформувати концепцію інформаційної безпеки в умовах гібридних загроз, забезпечити повну і точну оцінку ризиків та ефективне управління ними.

7.4. Метод OCTAVE

Метод OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) є систематичним підходом до оцінки загроз, активів та вразливостей, що використовується для забезпечення безпеки інформаційних систем. Він був розроблений Центром безпеки інформаційних технологій (CERT) в Карнегі-Меллонському університеті.

Метод OCTAVE представляє собою комбінацію процесів, методик і інструментів, які допомагають оцінити рівень безпеки інформаційної системи та розробити план дій щодо усунення виявлених вразливостей та загроз.

Основні етапи методу OCTAVE включають в себе (рис. 7.3):

1. Формування команди проекту – команда проекту повинна включати представників різних відділів організації, відповідальних за безпеку інформації.

2. Визначення цінних активів – необхідно визначити, які активи є критичними для бізнесу, щоб сконцентруватися на їх захисті.

Рис. 7.3. Основні етапи методу OCTAVE

3. Визначення загроз – необхідно проаналізувати можливі загрози, які можуть вплинути на цінні активи.

4. Визначення вразливостей – необхідно визначити вразливості інформаційної системи, які можуть бути використані зловмисниками для атаки.

5. Оцінка ризиків – необхідно оцінити рівень ризику для кожної загрози та вразливості.

6. Розробка плану дій – на основі результатів оцінки ризиків необхідно розробити план дій щодо усунення виявлених вразливостей та загроз.

7. Реалізація плану дій – необхідно провести заходи, передбачені планом дій, та регулярно перевіряти ефективність застосованих заходів.

Метод OCTAVE може бути застосований для оцінки ризиків безпеки інформаційних систем будь-яких масштабів та складності. Він дозволяє оцінювати загрози, які можуть походити як з зовнішнього, так і з внутрішнього середовища організації, та визначати вразливості інформаційної системи.

Метод OCTAVE може бути використаний як окремий інструмент для оцінки ризиків, або у поєднанні з іншими методами, такими як ISO 27001, NIST або COBIT. Він може бути застосований як у великих, так і в малих організаціях, які мають обмежені ресурси для забезпечення безпеки інформаційної системи.

Основна перевага методу OCTAVE полягає в тому, що він дозволяє оцінити ризики з точки зору бізнесу, тобто зрозуміти, які цінні активи можуть

бути під загрозою і як це може вплинути на діяльність організації. Крім того, метод OCTAVE дозволяє визначати пріоритети заходів щодо захисту інформаційної системи на основі оцінки ризиків і за рахунок цього підвищує можливості протистояти гібридним загрозам.

7.5. Метод CRAMM

Метод CRAMM (CCTA Risk Analysis and Management Method) – це метод оцінки ризиків, який був розроблений Центром комп'ютерної техніки та автоматизації Великобританії (CCTA) в 1980-х роках. Цей метод дозволяє оцінити ризики, пов'язані з інформаційною безпекою, та розробити плани з управління цими ризиками.

Метод CRAMM складається з наступних етапів (рис. 7.4):

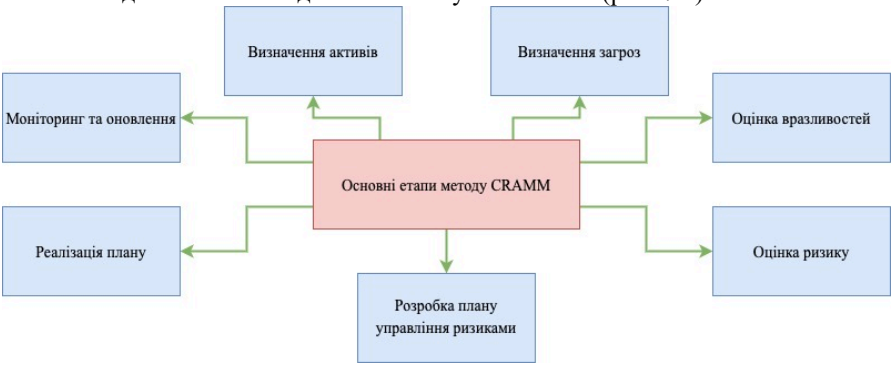

Рис. 7.4. Основні етапи методу CRAMM

1. Визначення активів – визначення тих об'єктів, які потрібно захистити, наприклад, комп'ютерів, мереж, баз даних тощо.
2. Визначення загроз – визначення потенційних загроз безпеці для активів, наприклад, зламу, вірусів, несанкціонованого доступу тощо.
3. Оцінка вразливостей – визначення вразливостей, які можуть бути використані зловмисниками для атак на активи.
4. Оцінка ризику – визначення ймовірності виникнення загрози та її наслідків, а також ймовірності наявності вразливостей, які можуть бути використані зловмисниками. На основі цих оцінок визначається рівень ризику.
5. Розробка плану управління ризиками – розробка плану з управління ризиками на основі оцінок ризиків. План може включати рекомендації з захисту активів, забезпечення безпеки мережі, організаційних заходів тощо.
6. Реалізація плану – впровадження рекомендацій та заходів, які були визначені в плані управління ризиками.

7. Моніторинг та оновлення – постійне відстеження вразливостей та загроз, а також оновлення плану управління ризиками.

Метод CRAMM є одним з найбільш ефективних методів оцінки ризиків в інформаційній безпеці. Він дозволяє оцінити потенційні загрози безпеці та визначити оптимальні стратегії управління ризиками та забезпечення інформаційної безпеки в умовах гібридної війни.

Одна з переваг методу CRAMM полягає в тому, що він дозволяє оцінювати ризики в контексті конкретного бізнес-середовища, в якому діє організація. Це дозволяє збільшити точність оцінки ризиків та розробки плану управління ризиками.

Крім того, метод CRAMM має широкий спектр застосування, включаючи в себе оцінку ризиків в інформаційних системах, оцінку ризиків в бізнес-процесах та оцінку ризиків в сфері зберігання та обробки конфіденційної інформації.

Однак, для успішної реалізації методу CRAMM необхідно мати досвід та кваліфікацію в області інформаційної безпеки. Крім того, процес оцінки ризиків може займати багато часу та ресурсів, що може бути важким для менших організацій.

7.6. Метод CORAS

Метод CORAS (Risk Assessment of Security Critical Systems) – це методологія оцінки ризиків безпеки інформації, яка призначена для використання при проектуванні та розробці критично важливих систем безпеки.

Метод CORAS розроблений в Норвегії у 90-х роках минулого століття і з того часу був застосований в різних проектах, включаючи проекти, пов'язані з інформаційною безпекою, автоматизацією процесів та управлінням ризиками. Він може бути використаний як на початку життєвого циклу проекту, так і в процесі його розвитку. Основні етапи методу CORAS наступні (рис. 7.5) [9]:

1. Аналіз контексту – визначення цілей та обмежень оцінки ризиків, встановлення границь системи, що вивчається, та ідентифікація загроз безпеки, що можуть вплинути на систему.
2. Моделювання – розробка моделі системи та її контексту з використанням спеціальних графічних засобів для ідентифікації потенційних загроз та їх впливу на систему.
3. Ідентифікація загроз – збір та аналіз інформації про можливі загрози безпеки для системи.
4. Оцінка ризиків – визначення потенційного впливу кожної загрози на систему, а також вірогідності її виникнення. Це дозволяє розрахувати загальний ризик для системи.
5. Управління ризиками – розробка планів дій для зменшення виявлених ризиків безпеки та виконання заходів для їх усунення або зменшення.

Рис. 7.5. Основні етапи методу CORAS

6. Документування – документування всіх етапів процесу оцінки ризиків та результатів оцінки ризиків.

7. Аналіз результатів – аналіз результатів оцінки ризиків та вирішення, чи є необхідність в додаткових заходах для забезпечення безпеки системи.

Ці етапи повторюються для кожної загрози безпеки та допомагають забезпечити безпеку критичної системи.

Метод CORAS базується на аналізі потенційних загроз та вразливостей, що породжуються з реалізацією гібридних загроз, а також на оцінці ймовірності та наслідків можливих атак на систему. Він включає кроки, такі як визначення об'єктів загроз, визначення вразливостей, визначення потенційних атак та визначення наслідків цих атак.

Основним результатом методу CORAS є матриця ризиків, яка показує ймовірність та наслідки можливих атак на систему. Це дозволяє розробникам приймати обґрунтовані рішення про те, які заходи безпеки необхідно реалізувати для мінімізації ризиків.

Метод CORAS може бути використаний в поєднанні з іншими методами оцінки ризиків і є одним з інструментів, які можуть допомогти в забезпеченні безпеки критично важливих систем.

Одним з важливих аспектів методу CORAS є його фокус на системному підході до оцінки ризиків. Метод CORAS дозволяє зосередитися на аналізі всієї системи, включаючи її компоненти та зв'язки між ними. Це допомагає виявити потенційні вразливості та загрози, які можуть бути невидимими при поверхневому аналізі.

Ще однією перевагою методу CORAS є його гнучкість. Метод може бути адаптований до різних типів проектів та систем безпеки. Наприклад, його можна використовувати для оцінки ризиків в інформаційних системах, мережах, програмних додатках, технічних системах тощо.

Крім того, метод CORAS може бути використаний для оцінки ризиків на різних етапах життєвого циклу проекту. Наприклад, він може бути використаний на етапі проектування для виявлення потенційних ризиків та визначення заходів безпеки, які необхідно реалізувати. Або він може бути використаний на етапі експлуатації системи для оцінки існуючих ризиків та визначення необхідності внесення змін в систему. Нарешті, метод CORAS допомагає виявляти недоліки та проблеми в системах безпеки, що може призвести до покращення їх ефективності та забезпечення більш високого рівня безпеки з метою комплексної протидії гібридним загрозам.

Метод CORAS (Corrective Security Actions) є методом оцінки безпеки системи, який дозволяє виявити слабкі місця та потенційні загрози, та розробити коригувальні заходи для їх запобігання. Нижче наведено приклад реалізації методу CORAS з урахуванням агентів вторгнень та слабких місць у системі розмежування доступу суб'єктів системи [14]:

1. Оцінка загроз та слабких місць – для оцінки загроз та слабких місць у системі розмежування доступу суб'єктів системи можна використовувати різні методи, наприклад, аналіз потенційних вразливостей, оцінка ризиків, аналіз реалізації доступу до ресурсів тощо.

2. Виявлення агентів вторгнень – для виявлення агентів вторгнень у систему можна використовувати різні методи, наприклад, моніторинг системних журналів, аналіз мережевого трафіку, використання системи детекції вторгнень тощо.

3. Розробка коригувальних заходів – після оцінки загроз та слабких місць та виявлення агентів вторгнень необхідно розробити коригувальні заходи, щоб запобігти можливим вторгненням та захистити систему. До таких заходів можуть відноситись:

– підвищення рівня безпеки системи шляхом встановлення оновлень та патчів для програмного забезпечення та операційної системи;

– проведення навчання та підвищення свідомості користувачів щодо безпеки даних та захисту системи;

– встановлення додаткових механізмів автентифікації та авторизації користувачів;

– встановлення механізмів моніторингу доступу та аудиту дій користувачів у системі;

– зменшення повних прав доступу до системи у користувачів та створення обмеженого доступу залежно від ролі та обов'язків користувача;

–реалізація механізмів виявлення та обробки вторгнень у систему, включаючи детекцію та реагування на аномальну активність в системі, встановлення механізмів антивірусного захисту та файерволів;

– встановлення систем моніторингу та аналізу мережевого трафіку, що дозволить виявляти аномальну активність, яка може бути пов'язана з вторгненням у систему.

4. Реалізація коректив заходів – після розробки коректив заходів необхідно реалізувати їх у системі. Для цього можна використовувати різні засоби, наприклад, встановлювати оновлення та патчі для програмного забезпечення, налаштовувати механізми автентифікації та авторизації, створювати обмежені ролі користувачів та налаштовувати механізми моніторингу та аналізу мережевого трафіку.

5. Оцінка ефективності коректив заходів – після реалізації коректив заходів необхідно оцінити їх ефективність та вплив на безпеку системи. Для цього можна використовувати різні методи, наприклад, тестування безпеки системи, моніторинг системних журналів та мережевого трафіку, аналіз відгуків користувачів тощо.

У цілому, реалізація методу CORAS з урахуванням агентів вторгнень та слабких місць у системі розмежування доступу суб'єктів системи з метою підвищення здатності протидіяти гібридним загрозам може значно покращити безпеку системи та запобігти можливим вторгненням.

КОНТРОЛЬНІ ПИТАННЯ

1. Які методи управління ризиками захищеності вам відомі?
2. Перелічіть основні етапи методу EBIOS.
3. Опишіть основні модулі методу MEHARI.
4. Які основні етапи методу OCTAVE вам відомі?
5. Опишіть основні етапи методу CRAMM.
6. Які основні етапи методу CORAS вам відомі?

ТЕСТИ

1. Який з методів управління ризиками базується на стандарті ISO/IEC 27001?

а) MEHARI
б) COBRA
в) EBIOS
г) ISO 27001

2. Що є основною метою аналізу відповідності вимогам захисту даних (DRA)?

а) Оцінка загроз
б) Аналіз захищеності даних
в) Створення плану реагування
г) Визначення контексту організації

3. Який метод управління ризиками використовує аналіз бізнес-процесів?

а) MEHARI
б) BPA
в) CRAMM
г) EBIOS

4. Який підхід до управління захищеністю заснований на аналізі ризиків та пріоритетах?
а) BPA
б) RBM
в) OCTAVE
г) COBIT

5. Що є ключовим етапом методу EBIOS?
а) Визначення зон ризику
б) Оцінка ризиків
в) Визначення бізнес-процесів
г) Впровадження плану захисту

6. Що враховує методологія MEHARI при оцінці ризиків?
а) Активи організації
б) Людський фактор
в) Технологічні інновації
г) Фінансові ризики

7. Який метод оцінки ризиків був розроблений у Франції?
а) EBIOS
б) ISO 27001
в) MEHARI
г) COBIT

8. Яке завдання виконується на першому етапі методу OCTAVE?
а) Визначення активів
б) Визначення загроз
в) Формування команди проекту
г) Аналіз вразливостей

9. Яка з наступних програм є засобом управління ризиками інформаційної безпеки?
а) COBRA
б) BPA
в) RBM
г) ISO 27001

10. Яка методологія використовується для оцінки ризиків в галузі інформаційних технологій?

а) CRAMM
б) MEHARI
в) EBIOS
г) RiskWatch

РОЗДІЛ 8.
КОМПЛЕКСНИЙ ПІДХІД ДО ПРОЕКТУВАННЯ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

8.1. Встановлення довіри між компонентами системи
8.2. Центри сертифікації з відкритими ключами
8.3. Методи оцінки довіри до інших користувачів у системі на основі їхньої репутації
8.4. Порівняння різних методів та інструментів для аналізу та управління ризиками в галузі кібербезпеки

8.1. Встановлення довіри між компонентами системи

У сучасному світі розподілені комп'ютерні системи використовуються для різноманітних цілей, таких як обробка великих обсягів даних, забезпечення комунікації між вузлами мережі, зберігання інформації тощо. Проте, зростаюча кількість даних та збільшення кількості вузлів в мережі ставлять перед розподіленими комп'ютерними системами нові завдання та проблеми.

Однією з таких проблем є питання встановлення довіри між вузлами мережі. У розподілених системах можуть бути вузли з різними рівнями довіри, тобто вузли, які можуть надавати надійну інформацію та вузли, які можуть бути підозрілими на відправку неправдивої інформації. Тому, для забезпечення інформаційної безпеки в умовах гібридної війни необхідно використовувати моделі встановлення довіри.

Одна з найпоширеніших моделей встановлення довіри – модель Web of Trust (WoT), яка використовується у системах електронної пошти та інших мережевих протоколах. У цій моделі вузли мережі мають рейтинг довіри, який визначається на основі рейтингів вузлів, які вже є довіреними. Таким чином, WoT створює ієрархію довіри, де вузли з найвищим рівнем довіри є надійними джерелами інформації.

Іншою моделлю встановлення довіри є модель Public Key Infrastructure (PKI), яка використовується для забезпечення безпеки в інтернеті. У PKI вузли мережі мають публічні ключі, які дозволяють встановлювати довірність комунікації між вузлами. У цій моделі, довіру вузлів підтверджує третя довірена сторона, така як сертифікаційний центр (Certification Authority), яка видає сертифікати на підтвердження відповідності публічного ключа вузла. Дані сертифікати дозволяють віртуальним вузлам мережі перевіряти автентичність та цілісність інформації, яку вони отримують.

Крім WoT та PKI існує ще безліч інших моделей встановлення довіри, таких як модель відкритого ключа (OpenPGP), модель транзакційної довіри (Trust Transaction Model), модель децентралізованої довіри (Decentralized Trust

Model) тощо. Вибір моделі залежить від конкретних потреб та вимог до безпеки конкретної розподіленої системи [22].

У контексті попередження та протидії гібридним загрозам, встановлення довіри між вузлами є важливою задачею в розподілених комп'ютерних системах. Для цього використовуються різні моделі встановлення довіри, які дозволяють забезпечити безпеку та відсіяти недовірені джерела інформації.

У розподілених комп'ютерних системах моделі встановлення довіри використовуються для забезпечення безпеки та надійності обміну даними між різними вузлами системи. Основними моделями встановлення довіри є (рис. 8.1):

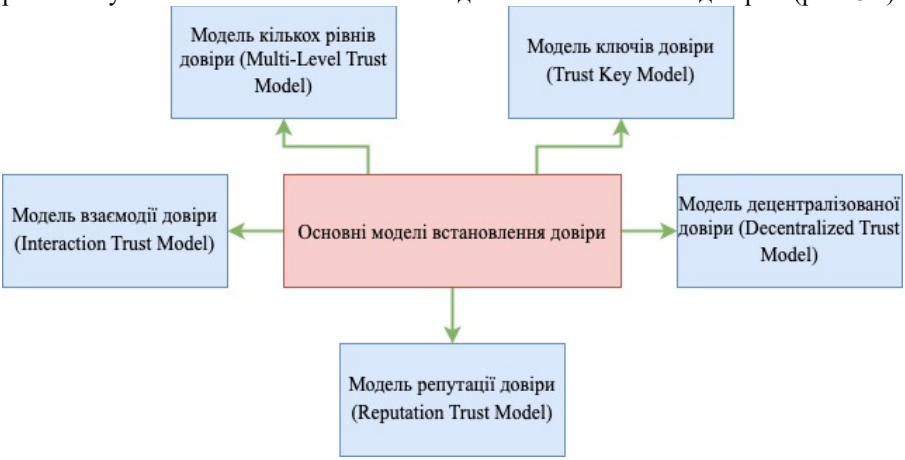

Рис. 8.1. Основні моделі встановлення довіри

1. Модель кількох рівнів довіри (Multi-Level Trust Model) – ця модель використовується для забезпечення безпеки в системах, що мають багато рівнів доступу. Кожен рівень має свою власну систему довіри, яка визначає, хто має доступ до різних ресурсів.

2. Модель ключів довіри (Trust Key Model) – ця модель використовується для забезпечення безпеки при обміні даними між різними вузлами. Кожен вузол має свій власний ключ довіри, який використовується для перевірки цифрових підписів на повідомленнях, які надсилаються від інших вузлів.

3. Модель децентралізованої довіри (Decentralized Trust Model) – ця модель використовується для забезпечення безпеки в розподілених системах, які не мають централізованого управління. У цій моделі кожен вузол має свою власну систему довіри, і взаємодіє з іншими вузлами, щоб встановити довіру до них.

4. Модель репутації довіри (Reputation Trust Model) – ця модель використовується для забезпечення безпеки в розподілених системах, які мають багато вузлів і велику кількість користувачів. У цій моделі кожен вузол має свою власну репутацію, яка визначається на основі дій, які він виконує в системі.

Репутація використовується для встановлення довіри до вузлів, які мають найбільшу репутацію в системі.

5. Модель взаємодії довіри (Interaction Trust Model) – ця модель використовується для забезпечення безпеки в системах, де взаємодіють різні вузли з різними рівнями довіри. У цій моделі довіра встановлюється на основі інтеракцій між вузлами, наприклад, на основі аналізу поведінки вузлів в системі.

Кожна з цих моделей має свої переваги та недоліки, і вибір моделі залежить від конкретних потреб та характеристик розподіленої системи. В будь-якому випадку, встановлення довіри – це важлива складова безпеки в розподілених комп'ютерних системах, і важливо забезпечити використання ефективної моделі встановлення довіри для нейтралізації негативних інформаційних впливів, забезпечення безпеки та надійності обміну даними між вузлами системи.

8.2. Центри сертифікації з відкритими ключами

Центри сертифікації з відкритими ключами є основою для створення моделей довіри в інформаційній безпеці. Вони використовуються для підтвердження автентичності та надійності електронних документів та повідомлень, що передаються через відкриті мережі. Такі центри забезпечують видання та розповсюдження цифрових сертифікатів, які встановлюють певний рівень довіри до електронної інформації, що передається за допомогою відкритих ключів.

Моделі довіри на основі центрів сертифікації з відкритим ключем (ЦСК) є широко використовуваним методом для забезпечення безпеки в інтернеті та інших мережевих засобах зв'язку.

ЦСК використовуються для видання цифрових сертифікатів, що підтверджують автентичність та валідність відкритих ключів, використовуваних для шифрування і розшифрування даних та для цифрового підпису. ЦСК мають велику вагу у забезпеченні довіри в інтернет-комунікаціях, оскільки вони підтверджують автентичність ключів та визначають, хто може використовувати ці ключі для шифрування та розшифрування даних або підпису документів.

Однак, такі системи можуть бути піддані гібридним атакам, а також технічній складності процесу створення сертифікатів та їх розповсюдження.

Основні складові моделі довіри на основі ЦСК включають (рис. 8.2) [12]:

1. Видача сертифікатів – процес створення та підпису сертифікатів ЦСК для визначення відкритих ключів, які можуть бути використані для шифрування та розшифрування даних або для цифрового підпису.

2. Перевірка сертифікатів – процес перевірки валідності сертифікатів ЦСК та їх відповідність ключам, використовуваним у комунікації.

3. Відкликання сертифікатів – процес відкликання вже виданих сертифікатів ЦСК, що вже не мають бути використовувані в наслідок підозрілих або зловмисних дій.

4. Управління ключами – процес керування ключами ЦС.

5. Довіра – процес встановлення довіри до сертифікатів та ЦСК, що використовується у комунікації.

Рис. 8.2. Основні складові моделі довіри на основі центрів сертифікації з відкритим ключем

Для забезпечення безпеки та довіри до системи ЦСК, важливо, щоб процеси видання, перевірки та управління сертифікатами були добре організовані та забезпечували високий рівень безпеки.

Додатково, необхідно забезпечити захист від атак, таких як підроблення сертифікатів, MITM (Man-in-the-middle), фішинг, шпигунство тощо.

Наприклад, одним зі способів забезпечення безпеки може бути використання криптографічних алгоритмів та протоколів, таких як TLS / SSL (Transport Layer Security / Secure Sockets Layer), що забезпечують шифрування даних у мережі та перевірку валідності сертифікатів.

Крім того, можуть бути встановлені процедури валідації, що забезпечують ідентифікацію власника ключів перед виданням сертифікату, і система відкликання, що дозволяє швидко скасовувати небезпечні сертифікати.

Загалом, моделі довіри на основі ЦСК є важливим елементом забезпечення безпеки у сучасних мережевих засобах зв'язку, які можуть бути піддані впливу гібридних загроз, та потребують ретельного планування, розгляду та реалізації з метою забезпечення безпеки та довіри в мережевій комунікації.

Метод взаємного розпізнавання (англ. cross-recognition) є технікою машинного навчання, яка використовується для класифікації об'єктів на основі їх опису з використанням зразків з інших класів. Цей метод можна використовувати для вирішення задач розпізнавання образів та класифікації даних. У процесі взаємного розпізнавання використовуються алгоритми

машинного навчання, які тренуються на підмножинах даних з кожного класу, після чого вони тестуються на інших підмножинах даних з тих самих та з інших класів. Наприклад, якщо ми маємо набір даних з різних категорій тварин, ми можемо тренувати класифікатор на деякій підмножині категорій, а потім використовувати його для класифікації зображень тварин з інших категорій.

Перевагами методу взаємного розпізнавання є його ефективність у випадку, коли класифікатор тренується на обмеженому обсязі даних, а також здатність до класифікації нових даних з використанням зразків з інших класів. Однак цей метод може бути менш точним, ніж методи, які тренуються на повному наборі даних [15].

Список довіри до сертифікатів (Certificate Trust List, CTL) – це список сертифікатів, які відповідають вимогам безпеки і яким можна довіряти для встановлення безпечного з'єднання. CTL є складовою частиною криптографічної інфраструктури веб-серверів, браузерів та інших програм, що використовують криптографію для забезпечення безпеки. CTL включає список кореневих сертифікатів, яким можна довіряти, а також сертифікатів проміжних центрів сертифікації (Intermediate Certificate Authority), які є посередниками між кореневими сертифікатами та сертифікатами веб-сайтів.

Браузери та інші програми використовують CTL для перевірки та довіри до сертифікатів, використовуваних для забезпечення безпечного з'єднання з веб-сайтами. Якщо сертифікат не входить до CTL, програми можуть виводити попередження про потенційну небезпеку встановлення з'єднання з цим сайтом.

CTL зазвичай оновлюються періодично, щоб включати нові кореневі та проміжні сертифікати та виключати застарілі сертифікати.

Метод який використовує сертифікат акредитації називається взаємним визнанням сертифікатів і ґрунтується на взаємній довірі між різними центрами сертифікації (ЦС). Коли центр сертифікації видав сертифікат, його можна засвідчити іншими довіреними ЦС у відповідних умовах. Це означає, що сертифікат, виданий одним ЦС, може бути прийнятий іншим ЦС без додаткової перевірки підписувача.

В умовах розгортання гібридних воєн взаємне визнання сертифікатів дає можливість зменшити навантаження на систему сертифікації та поліпшити її ефективність. Цей метод є популярним у світі та використовується в багатьох відкритих та комерційних системах, які вимагають безпечної електронної комунікації.

8.3. Методи оцінки довіри до інших користувачів у системі на основі їхньої репутації

Моделі довіри на основі репутаційних механізмів – це методи оцінки довіри до інших користувачів у системі на основі їхньої репутації, яка вимірюється на основі їхньої попередньої поведінки.

Ці моделі використовуються в соціальних мережах, електронній комерції, відкритих ринках, а також в інших контекстах, де важливо оцінювати довіру до невідомих користувачів. Наприклад, на електронних ринках, покупці можуть використовувати репутаційні механізми, щоб визначити, наскільки довіряти продавцю перед тим, як купувати товар.

Одна з найбільш поширених моделей довіри на основі репутації – це модель «expectation-confirmation», яка оцінює довіру на основі порівняння очікувань користувача щодо поведінки іншого користувача з їхньою фактичною поведінкою [9].

Інша модель – модель «багатоваріантної репутації», оцінює репутацію користувача на основі багатьох факторів, таких як кількість транзакцій, їхній тип, рейтинг відгуків та інші параметри.

Незалежно від використаної моделі, для успішного застосування репутаційного механізму важливо визначити правильні фактори, які впливають на репутацію користувача, а також забезпечити надійність даних, що використовуються для її оцінки.

Додатково, для формування довіри в багаторівневих мережах використовуються спеціальні механізми, такі як механізм динамічного управління довірою (Dynamic Trust Management), який дозволяє оцінювати довіру до суб'єктів, зокрема, в багаторівневих мережах з різними рівнями доступу [44]. У цьому механізмі використовуються різні методи оцінки довіри, включаючи збір статистики від суб'єктів та аналіз їх поведінки.

Однією з причин низької ефективності протидії гібридним загрозам та одним з найбільш важливих викликів у формуванні довіри є проблема атак на систему, що включає в себе атаки на протоколи довіри та атаки на самі дані. Для запобігання цим атакам запропоновано використання різних технік, таких як криптографічні методи, а також методи обробки даних, які дозволяють виявляти та відновлювати пошкоджені дані.

Отже, формування довіри є важливим елементом в будь-якій мережі, де взаємодіють різні суб'єкти, і цей процес може бути реалізований за допомогою різних методів та механізмів, які забезпечують визначення репутації суб'єктів та оцінювання рівня їх довіри в мережі.

8.4. Порівняння різних методів та інструментів для аналізу та управління ризиками в галузі кібербезпеки

Методи та засоби аналізу та управління ризиками захищеності є надзвичайно важливими для забезпечення безпеки інформації в сучасному цифровому середовищі. Порівняльна оцінка цих методів та засобів може допомогти вибрати найефективніші з них для конкретної ситуації.

Основні методи та засоби аналізу та управління ризиками захищеності, які використовуються в сучасному цифровому середовищі, включають (рис. 8.3) [2]:

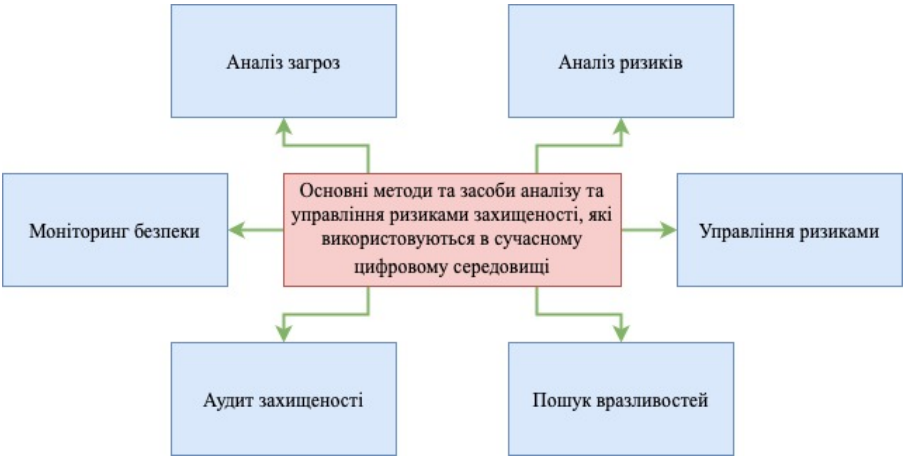

Рис. 8.3. Основні методи та засоби аналізу та управління ризиками захищеності, які використовуються в сучасному цифровому середовищі

1. Аналіз загроз використовується для визначення потенційних загроз безпеці інформації, їх впливу на систему та оцінки ризиків. Аналіз загроз зазвичай базується на переліку потенційних загроз та їх опису, що дозволяє виявити потенційні проблеми та прийняти заходи щодо зменшення ризику.

2. Аналіз ризиків використовується для оцінки ризиків, пов'язаних з інформаційною системою, та визначення ефективних заходів з їх зменшення. Аналіз ризиків зазвичай включає оцінку ймовірності виникнення загрози та її впливу на систему, а також визначення рівня ризику та вибір оптимального варіанту дії.

3. Управління ризиками використовується для прийняття рішень щодо зменшення ризику та підвищення захищеності інформаційної системи. Управління ризиками може включати в себе заходи з попередження виникнення загроз, захист від відомих загроз, виявлення та реагування на інциденти, а також відновлення системи після виникнення проблем.

4. Пошук вразливостей використовується для виявлення вразливостей в інформаційній системі та забезпечення їх виправлення. Пошук вразливостей зазвичай включає сканування системи для виявлення вразливостей, тестування на проникнення та аналіз заходів з захисту.

5. Аудит захищеності використовується для оцінки ефективності заходів з захисту та виявлення потенційних проблем у системі захисту. Аудит захищеності зазвичай включає перевірку політик захисту, наявності технічних засобів захисту, встановлення відповідних метрик безпеки та оцінку відповідності стандартам безпеки.

6. Моніторинг безпеки використовується для постійного відстеження стану безпеки інформаційної системи та виявлення можливих проблем. Моніторинг безпеки зазвичай включає в себе відстеження змін в системі, перевірку логів подій та сповіщення про можливі інциденти.

Порівняльна оцінка цих методів та засобів показує, що кожен з них має свої переваги та недоліки. Наприклад, аналіз загроз дозволяє ідентифікувати потенційні проблеми та знаходити їх рішення, але не дає повного уявлення про ступінь ризику. Управління ризиками забезпечує комплексний підхід до захисту інформаційної системи з метою забезпечення інформаційної безпеки в умовах гібридної війни, але вимагає значних витрат на реалізацію та підтримку заходів з захисту.

Пошук вразливостей та аудит захищеності забезпечують виявлення потенційних проблем, але не гарантують повної захищеності системи від атак.

Моніторинг безпеки дозволяє постійно відстежувати стан системи та вчасно виявляти можливі загрози, але може бути витратним у плані ресурсів та часу.

При оцінці методів та засобів аналізу та управління ризиками захищеності важливо враховувати контекст використання та мету оцінки. Наприклад, для великих корпорацій з значною кількістю даних та великою кількістю співробітників може бути необхідним використовувати більш складні та витратні методи та засоби аналізу та управління ризиками, ніж для менших компаній.

Також важливо враховувати, що жоден метод або засіб не може гарантувати повної захищеності інформаційної системи. Тому розумним є комбінування різних методів та засобів, щоб забезпечити комплексний підхід до захисту інформаційної системи від потенційних загроз.

Нарешті, важливо враховувати, що заходи з захисту мають бути постійно оновлюваними та адаптованими до змін в технологіях та враховуючи гібридні загрози. Тому, для успішного управління ризиками захищеності, потрібно мати якісну систему моніторингу та оцінки ефективності заходів з захисту та регулярно оновлювати політики та процедури безпеки відповідно до нових загроз та вимог.

Оцінка основних параметрів методів та засобів аналізу та управління ризиками захищеності може бути проведена з різних поглядів, але найбільш звичним підходом є порівняння їх за такими параметрами, як ефективність, складність, вартість та простота використання. Для цього можна розглянути такі методи та засоби (рис. 8.4) [23]:

1. Аудит захисту інформації є дуже ефективним, оскільки дозволяє виявляти вразливості в системі захисту інформації та допомагає уникнути ризиків її порушення. Однак, він може бути дуже складним та коштовним у використанні.

Рис. 8.4. Методи та засоби аналізу та управління ризиками захищеності

2. Перевірка на проникнення полягає в тестуванні системи захисту на наявність вразливостей шляхом спроби проникнення. Він може бути дуже ефективним, але його використання може бути дуже складним та витратним у часі та коштах.

3. Ризик-аналіз полягає в ідентифікації потенційних ризиків та оцінці ймовірності їх реалізації та впливу на систему захисту. Його можна використовувати для планування заходів зі зменшення ризиків. Він досить ефективний та простий у використанні, але може бути складним у виконанні та вимагати певного рівня експертизи.

4. Управління доступом полягає в обмеженні доступу до системи захисту лише належним особам та обмеження їх прав доступу. Він є досить ефективним та простим у використанні, але може вимагати певних технічних знань.

5. Захист від вторгнень полягає в захисті системи захисту від вторгнень, шляхом виявлення та блокування шкідливих програм та активностей. Він може бути дуже ефективним, але вимагає постійного моніторингу та оновлення захисних механізмів.

6. Захист від DDoS-атак полягає в захисті системи від деніал-оф-сервіс (DDoS) атак, що відбуваються шляхом переповнення ресурсів системи та зупинки її роботи. Він може бути дуже ефективним, але вимагає певного рівня технічних знань та спеціального програмного забезпечення.

Загалом, кожен з методів та засобів має свої переваги та недоліки, і вибір того, який краще використовувати, залежить від конкретних потреб та обставин. Однак, зазвичай, комбінація декількох методів та засобів може бути найбільш ефективним підходом до аналізу та управління ризиками захищеності.

КОНТРОЛЬНІ ПИТАННЯ

1. Які моделі встановлення довіри вам відомі?
2. Поясніть поняття та призначення центрів сертифікації?
3. Назвіть складові моделі довіри на основі центрів сертифікації з відкритими ключами.
4. У чому полягає суть методу взаємного розпізнавання? Для вирішення яких задач він використовується?
5. Що таке список довіри до сертифікатів? Як він використовується?
6. На чому ґрунтується метод взаємного визнання сертифікатів?
7. Які вам відомі моделі довіри на основі репутаційних механізмів?
8. Перелічіть засоби управління ризиками захищеності інформаційної безпеки.

ТЕСТИ

1. Яка з наведених моделей встановлення довіри використовується для забезпечення безпеки в системах з багатьма рівнями доступу?
а) Модель ключів довіри
б) Модель репутації довіри
в) Модель кількох рівнів довіри
г) Модель взаємодії довіри

2. Яка модель довіри підтверджується третьою довіреною стороною, такою як сертифікаційний центр?
а) Web of Trust
б) Public Key Infrastructure
в) Модель відкритого ключа
г) Модель репутації довіри

3. Що використовується для підтвердження автентичності вузлів у моделі PKI?
а) Публічні ключі
б) Приватні ключі
в) Репутація вузла
г) Рейтинг довіри

4. Яка з моделей довіри базується на репутації вузла?
а) Модель ключів довіри
б) Модель взаємодії довіри
в) Модель репутації довіри
г) Public Key Infrastructure

5. Яка модель довіри використовується в системах, що не мають централізованого управління?
а) Модель децентралізованої довіри
б) Public Key Infrastructure
в) Модель кількох рівнів довіри
г) Web of Trust

6. Що є головною функцією сертифікаційного центру в моделі PKI?
а) Видання сертифікатів
б) Відкликання ключів
в) Керування паролями
г) Перевірка даних

7. Який із методів використовується для шифрування даних і встановлення довіри в інтернет-комунікаціях?
а) Протоколи TLS/SSL
б) Модель кількох рівнів довіри
в) Динамічне управління довірою
г) Відкриті бази даних

8. Яка з моделей довіри встановлюється на основі аналізу поведінки вузлів?
а) Модель кількох рівнів довіри
б) Модель взаємодії довіри
в) Модель репутації довіри
г) Модель ключів довіри

9. Який метод використовується для взаємного визнання сертифікатів між різними сертифікаційними центрами?
а) Cross-recognition
б) Web of Trust
в) Відкликання сертифікатів
г) Криптографічний алгоритм

10. Яка з моделей довіри є децентралізованою і не покладається на третю довірену сторону?
а) Public Key Infrastructure
б) Web of Trust
в) Модель кількох рівнів довіри
г) Модель репутації довіри

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. Київ : Інтертехнологія, 2009. 164 с.

2. Бурячок, В.Л., Толубко, В.Б., Хорошко, В.О., Толюпа, С.В. 2015. Інформаційна та кібербезпека: соціотехнічний аспект: підручник, Київ ДУТ, 2015: 15.

3. Дубов, Д.В. 2014. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ, НІСД, 2014: 210.

4. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. Житомир : Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

5. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. Одеса : Фенікс, 2015. 264 с.

6. Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. Х. : Вид. ХНЕУ, 2013. 476 с.

7. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. К. : ДУТ-КНУ, 2016. 178 с.

8. Міжнародна інформаційна безпека: теорія і практика // Макаренко Є.А., Рижков М.М., Ожеван М.А., Кучмій О.П., Фролова О.М. / Підручник. Київ: Центр вільної преси, 2016. 418 с.

9. Андриевский Т. Гибридная война: сущность и базовые стратегии / Т. Андриевский. Desecuritate. 2017. No 1(3). С. 158-166.

10. Бурячок В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / В. Л. Бурячок // Сучас. спеціал. техніка. 2011. No 3 (26). С. 104-114.

11. Курбан О. В. Основи сучасної національної інформаційної безпеки України / О. В. Курбан // Вісн. ХДАК. 2017. Вип. 50. С. 55-62.

12. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві / І. В. Феськов // Актуал. пробл. політики. 2016. Вип. 58. С. 66-76.

13. Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K., & McCue, M. (2018). Addressing hybrid threats. Swedish Defence University. ISBN 978-91-86137-73-1. URL: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-Addressing-HybridThre-ats.pdf

14. Business community and hybrid threats: Report of Pasi Eronen Foundation for Defense of Democracies. Helsinki, 2018. URL : https://view.24mags.com/mobi-lev/bbc-43250c51aa3c0b599cb18066f3c#/page=1

15. Harjanne A., Muilu E., Pääkkönen J., Smith H. (2018) Helsinki in the era of hybrid threats – Hybrid influencing and the city. Helsinki, Finland: Hybrid CoE. URL:

https://www.hybridcoe.fi/wp-content/uploads/2020/07/Helsinki-in-the-era-of-hybrid-thre-ats-–-Hybrid-influencing-and-the-city_ENG.pdf

16. EU Security Union Strategy: connecting the dots in a new security ecosystem. ULR : https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_13-79/IP_20_1379_EN.pdf

17. JOINT STAFF WORKING DOCUMENT. Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. Brussels, 24.7.2020.SWD(2020) 153 final. URL : https://www.europarl.europa.eu/RegData/docs_a-utres_institutions/commission_europeenne/swd/2020/0152/COM_SWD(2020)0152_EN.pdf

18. Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi: 10.2760/44985, JRC123305. URL : https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

19. Лалак О. А. Ризики і виклики кібербезпеки: досвід України та Польщі / О. А. Лалак, L. Klich // Міжнародні відносини. Серія "Політичні науки". 2017. No 13. [Електронний ресурс]. Режим доступу: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3001

20. Шорошев В. Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах. Сб. Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, вып.3, 2001. С. 86-90.

21. Сопілко І. М. Становлення мережевого суспільства та питання кібербезпеки / І. М. Сопілко // Юрид. вісн. 2016. No 1 (38). С. 79-85.

22. Четверик Г. Г. Напрямки реалізації державної політики у сфері кібернетичної безпеки / Г. Г. Четверик // Вісн. Дніпропетр. ун-ту. Політологія. 2012. No 9/2. Вип. 22. С. 241-246.

23. Закон України Про криптографічний та технічний захист інформації [Електронний ресурс]. Режим доступу : https://ips.ligazakon.net/document/NT1819

24. Глосарій гібридних загроз. [Електронний ресурс]. Режим доступу: https://warn-erasmus.eu/ua/glossary/

25. Європейський центр з протидії гібридним загрозам Hybrid CoE. [Електронний ресурс]. Режим доступу: https://www.hybridcoe.fi/

Co-funded by the
Erasmus+ Programme
of the European Union

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ГІБРИДНІ ЗАГРОЗИ

Навчальний посібник
для здобувачів другого (магістерського)
рівня вищої освіти

Підп. до друку 01.10.2024. Формат вид. 60x80 1/16
Папір офсет. № 1. Офс. друк. Гарн. «Times New Roman Cyr»
Ум. друк. арк. 6,18. Обл.-вид.арк. 6,08.
Наклад 300 прим. Зам. 208

Віддруковано в типографії
ТОВ «ТРОПЕА»,
м. Київ, 2024