УДК 001.8:[004.056.5:334.724.6-021.412.1](477)
DOI: 10.31673/2409-7292.2024.030001

Шульга В. П., Іванченко Є. В., Вишневська Н. С., Бербер А. С.

ДОСЛІДЖЕННЯ МЕТОДІВ ТА МОДЕЛЕЙ ОЦІНЮВАННЯ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Дослідження “Методи та моделі оцінювання кіберзахисту критичної інфраструктури держави” зосереджується на аналізі різних методів оцінки ризиків кібербезпеки з метою їх застосування до захисту національної критичної інфраструктури. Робота оцінює придатність існуючих методів на основі критеріїв, таких як ідентифікація ризиків, реагування на кіберінциденти, відновлення стану кібербезпеки, кіберахист та кіберстійкість. Розглядаються методики як FMEA, HAZOP, Checklist, SWIFT та інші, аналізуючи їх здатність ідентифікувати потенційні загрози, реагувати на актуальні кіберінциденти, забезпечувати швидке відновлення операцій та зміцнювати загальну стійкість системи до майбутніх атак. Крім теоретичного огляду, робота включає практичний аспект, де за допомогою кейс-стаді на реальних системах критичної інфраструктури аналізується ефективність різних методів і стратегій. Дослідження також пропонує нові підходи та моделі, що могли б покращити інтеграцію та виконання заходів кібербезпеки, враховуючи комплексний характер кіберзагроз. Завдяки багатогранному аналізу, робота висвітлює критичні аспекти в оцінці та управлінні ризиками, що дозволяє формулювати рекомендації для поліпшення заходів захисту критичної інфраструктури. Це дослідження має велике значення для розробників політик, експертів у галузі кібербезпеки та керівників критичних інфраструктур, оскільки надає глибокий аналіз та порівняльну оцінку методів оцінки ризиків, вказуючи на їхні сильні та слабкі сторони в контексті різних аспектів кібербезпеки.

Ключові слова: Кібербезпека, кіберстійкість, критична інфраструктура, захист інформації, кібератака, кіберризики, кіберзагроза, кіберінциденти, методи та моделі.

Вступ

В сучасному світі, де залежність від інформаційних технологій зростає з кожним днем, захист критичної інфраструктури від кібератак стає пріоритетом для держав по всьому світу. Критична інфраструктура, яка включає енергетичні системи, транспортні мережі, водопостачання та інші життєво важливі служби, є основою для забезпечення національної безпеки, економічного добробуту та здоров'я населення. Останні інциденти показують, що кіберзагрози можуть спричинити не лише економічні втрати, а й реальну шкоду фізичній інфраструктурі та людським життям [1]. Так, для забезпечення неохідного рівня кіберзахисту ресурсів інформаційних систем, а саме розробки ефективних методів, моделей та систем оцінювання рівня кіберзахисту критичної інфраструктури є актуальною задачею.

Мета роботи

Метою роботи є дослідження методів, моделей та систем оцінювання рівня кіберзахисту критичної інфраструктури держави. Для досягнення поставленої мети необхідно визначити множину критеріїв, що відповідають класам кіберзахисту [6]. Це дасть можливість проаналізувати представлені методи та моделі на відповідність класам кіберзахисту відповідно до наказу Адміністрації Держспецзв’язку від 06.10.2021 № 601 “Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури” [6] та аналізу поняття кіберстійкості критичної інфраструктури [50], а також для її подальшого використання при вирішенні поставлених задач сфери кібербезпеки та захисту інформації.

Основна частина

Такі методи, як аналіз вразливостей, оцінка ризиків та розробка стратегій відновлення, допомагають знижувати потенційні наслідки кіберінцидентів. Це дослідження спрямоване на дослідження різних підходів та методів, зокрема FMEA, HAZOP, та SWIFT, для їх застосування в контексті кібербезпеки критичної інфраструктури [2].

В [7] автор монографії виділяє наступні методи оцінювання ризиків: Brainstorming, Structure d or semi-structure d interviews, Delphi method, Checklist, PHA, HAZOP, HACCP, Toxic it y assessment, SWIFT, Scenario analysis, FMEA, Fault tree analysis, Event tree analysis, Cause and consequence analysis, Cause-and-effec tanalysis, LOPA, Decision tree, HRA, Bowtie analysis,

Monte Carlo simulation, Consequence/probabilit ymatrix, Cost/benefitanalysis, MCDA. Було проведено аналіз цих методів на відповідність класам кібербезпеки відповідно до наказу [6].

Метод мозкового штурму (Brainstorming) використовується в кібербезпеці для вирішення різноманітних завдань, зокрема у процесах ідентифікації ризиків та розробки стратегій відновлення після інцидентів. Під час ідентифікації ризиків кібербезпеки, Brainstorming дозволяє учасникам ефективно генерувати ідеї, що виявляють нові та недооцінені загрози, що є критично важливим у динамічному полі кіберзагроз. Для розробки механізмів кіберзахисту, цей метод сприяє обговоренню та випробуванню стратегій захисту, що підвищує резильєнтність систем. Хоча мозковий штурм безпосередньо не застосовується для виявлення кіберінцидентів, він корисний для планування систем виявлення та моніторингу, дозволяючи визначити ключові показники для контролю аномалій. У контексті реагування на кіберінциденти, метод сприяє швидкій розробці стратегій реагування, обговоренню негайних дій для мінімізації наслідків атак, а також плануванню довгострокових заходів для запобігання подальшим інцидентам. Мозковий штурм також є корисним для визначення стратегій відновлення та посилення кібербезпеки після атаки, зокрема через відновлення критичних служб та впровадження змін для підвищення загальної стійкості системи. У загальному контексті кіберстійкості, цей метод сприяє створенню культури безперервного вдосконалення захисних механізмів та підготовки персоналу, що забезпечує ефективне реагування на майбутні загрози[7, 8].

Методика структурованих та напівструктурованих інтерв'ю (Structured or semi-structured interviews) використовується в кібербезпеці для детального збору інформації від експертів, працівників та інших стейкхолдерів. Цей підхід є особливо корисним для глибокого аналізу специфічних аспектів кібербезпеки та кіберризиків. У контексті ідентифікації ризиків кібербезпеки, структуровані інтерв'ю дозволяють зібрати спеціалізовані знання та досвід від експертів, які мають глибоке розуміння потенційних загроз і вразливостей системи. Це сприяє виявленню складних і часто ігнорованих аспектів безпеки, які не можуть бути автоматично виявлені за допомогою традиційних інструментів. Щодо кіберзахисту, застосування цих інтерв'ю допомагає виявити потреби у зміцненні захисту та розробці більш ефективних стратегій захисту. Через деталізовані відповіді, організації можуть краще розуміти, які заходи безпеки найбільш ефективні та як їх слід інтегрувати у загальну систему захисту. Структуровані інтерв'ю також важливі для виявлення кіберінцидентів, оскільки вони можуть забезпечити розуміння шляхів, якими загрози можуть проявитися, та індикаторів, на які потрібно звернути увагу при моніторингу систем. Реагування на кіберінциденти, інтерв'ю з відповідальними особами та командами IT-безпеки допомагають оцінити ефективність протоколів реагування та ідентифікувати потреби для їх вдосконалення. Для підвищення кіберстійкості організації, систематичний збір і аналіз даних через інтерв'ю сприяє розробці стратегій, які підвищують загальну здатність організації витримувати і адаптуватися до кіберзагроз [7, 9].

Метод Делфі, відомий своїм структурованим комунікаційним процесом для збору думок експертів, ефективно застосовується у сфері кібербезпеки, охоплюючи широкий спектр активностей від ідентифікації ризиків до вдосконалення кіберстійкості. Цей метод дозволяє експертам незалежно оцінювати потенційні загрози та ризики, після чого їхні відгуки агрегуються для формування узгодженого бачення критичних ризиків. Такий підхід допомагає виявляти нові та недооцінені загрози, які можуть бути пропущені при менш систематизованих підходах. У контексті кіберзахисту, Делфі сприяє розробці ефективних стратегій, залучаючи експертів для оцінки та вдосконалення захисних технологій та методів. Хоча метод не призначений для безпосереднього виявлення кіберінцидентів, він може використовуватися для оцінки ефективності існуючих методів виявлення та моніторингу, допомагаючи виявити потенційні покращення в цих процесах. Метод Делфі також є корисним для планування реагування на інциденти та відновлення після них, залучаючи експертів для розробки планів

дій та оцінки довгострокових заходів для запобігання подальшим інцидентам. Це сприяє визначенню найефективніших стратегій і тактик реагування, що базуються на згоді серед провідних фахівців. Метод Делфі важливий для підвищення кіберстійкості, оскільки допомагає формулювати стратегії, які зміцнюють здатність організації витримувати та адаптуватися до кіберзагроз на основі консенсусу експертів [7, 10, 11].

Метод використання контрольних списків (Check lists) у кібербезпеці дозволяє систематизувати процеси перевірки та забезпечення відповідності до стандартів безпеки. Цей інструмент є особливо корисним у різних аспектах кіберзахисту завдяки своїй здатності надати чіткі та послідовні напрямки для оцінювання та покращення безпеки систем. Контрольні списки використовуються для ідентифікації ризиків кібербезпеки, забезпечуючи швидкий і точний збір інформації про потенційні вразливості та загрози. Вони дозволяють фахівцям з кібербезпеки оцінити, чи були впроваджені необхідні заходи безпеки та чи дотримуються процедури, зазначені в політиках безпеки. У контексті кіберзахисту контрольні списки можуть бути інтегровані в повсякденні операції для постійного моніторингу та оцінки стану захисту інфраструктури. Це допомагає забезпечити, захищеність всіх системних компонентів відповідно до останніх стандартів та практик. У процесі виявлення кіберінцидентів контрольні списки можуть використовуватися для перевірки відповідності індикаторів компрометації IOC та інших сигналів тривоги, що дозволяє оперативно ідентифікувати потенційні загрози та реагувати на них. Контрольні списки зміцнюють кіберстійкість організації, дозволяючи систематично перевіряти відповідність і виконання заходів безпеки [7, 12, 13]

Метод PHA (Попередній Аналіз Небезпек) є важливим інструментом в кібербезпеці, який забезпечує ретельний аналіз потенційних ризиків на ранніх етапах проектування та впровадження систем. Цей метод ефективно використовується для ідентифікації ризиків кібербезпеки, оскільки дозволяє виявити, оцінити та впорядкувати загрози з метою їх подальшої нейтралізації або зменшення. Аналіз, який виконується за допомогою PHA, сприяє розробці комплексних заходів кіберзахисту, дозволяючи планувати впровадження технологій та стратегій, які ефективно захищають від виявлених загроз. PHA також сприяє виявленню та реагуванню на кіберінциденти. Цей метод не є прямим інструментом для моніторингу або виявлення інцидентів у реальному часі, він забезпечує базу для розуміння потенційних напрямків атак та слабких місць у системі, що допомагає формувати реакцію на інциденти, засновану на попередньому розумінні ризиків. Використання PHA для планування відновлення після кіберінцидентів дозволяє створювати деталізовані процедури та протоколи, які оптимізують процес відновлення систем та мінімізують час простою. Загалом, PHA значно підвищує кіберстійкість організації, забезпечуючи системний підхід до управління ризиками та розробки заходів кіберзахисту. Цей метод дозволяє не тільки реагувати на поточні загрози, а й адаптуватися до змінюваних умов кіберпростору, підвищуючи гнучкість і готовність до майбутніх викликів [7, 14].

Метод HAZOP (Hazard and Operability Study) є технікою, яка спочатку розроблялася для хімічної інженерії, але з часом знайшла застосування в кібербезпеці завдяки своєму систематичному підходу до ідентифікації ризиків. Цей метод аналізує можливі відхилення в роботі системи від норми, що дозволяє виявляти потенційні ризики або недоліки в безпеці. Використання HAZOP в кібербезпеці стає особливо ефективним при оцінці складних інформаційних систем та мереж, де потрібно розглянути широкий спектр потенційних загроз та вразливостей. Застосування HAZOP для ідентифікації ризиків кібербезпеки дозволяє організаціям проводити глибокий аналіз можливих небезпек, які можуть виникнути через неправильне конфігурування системи або через зовнішні атаки. Основна перевага цього методу полягає в його здатності допомагати у виявленні не лише відомих загроз, але й потенційних, які можуть не бути очевидними на перший погляд. Задля вдосконалення кіберзахисту, HAZOP може використовуватися для планування заходів з підвищення безпеки,

© Шульга, В. П., Іванченко, Є. В., Вишневська, Н. С., & Бербер, А. С. (2024). Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 3(59), 6–19. https://doi.org/10.31673/2409-7292.2024.030001.

виявлення слабких місць у безпеці, та розробки відповідних заходів реагування. Такий підхід допомагає забезпечити, що системи є максимально захищеними від можливих атак та відмов. HAZOP також корисний у процесах виявлення кіберінцидентів, оскільки дозволяє командам кібербезпеки розробляти детальні процедури для виявлення і реагування на аномалії у системі, що можуть свідчити про безпекові інциденти. Використання цього методу в контексті відновлення після кіберінцидентів сприяє розробці ефективних стратегій швидкого відновлення операційного стану систем, мінімізуючи час простою та фінансові втрати. Метод HAZOP сприяє розробці довгострокових стратегій зміцнення інфраструктури та процесів, а також допомагає формувати культуру безперервного аналізу та вдосконалення систем безпеки. Це забезпечує організації засоби для адаптації до змінюваних умов та нових загроз, зміцнюючи їх здатність захищати критичні активи в довгостроковій перспективі.[7, 15]

Метод HACCP (Hazard Analysis and Critical Control Points) широко використовується у харчовій промисловості для ідентифікації, оцінки та контролю небезпек, що можуть вплинути на безпеку продуктів харчування. Хоча цей метод зазвичай асоціюється з харчовою галуззю, його підходи можуть бути адаптовані та використані в контексті кібербезпеки для забезпечення системного управління ризиками. Використання HACCP у кібербезпеці може включати розробку схеми, яка допоможе в ідентифікації критичних точок у IT-інфраструктурі, де потенційні ризики або вразливості можуть негативно вплинути на оперативну діяльність організації. Наприклад, можна визначити критичні точки даних, де інформація зберігається або обробляється, та розробити заходи для їх захисту. Цей метод також сприяє кращому розумінню та реагуванню на кіберінциденти, оскільки дозволяє командам кібербезпеки розробляти детальні процедури для моніторингу та реагування на інциденти в цих критичних точках. Контрольні точки, визначені за методом HACCP, можуть стати фокусом для моніторингу аномалій, що дозволяє більш ефективно виявляти та усувати загрози. У контексті відновлення після кіберінцидентів, HACCP може допомогти в плануванні відновлення, вказуючи на критичні аспекти системи, які потребують негайної уваги, щоб мінімізувати час простою та вплив на бізнес-процеси. Такий підхід сприяє більш структурованому та ефективному процесу відновлення. Останнім часом підвищення кіберстійкості стає ключовим елементом стратегічного планування безпеки в багатьох організаціях. Застосування методу HACCP у цій області може допомогти встановити систему постійного оцінювання та вдосконалення заходів безпеки, що є фундаментом для забезпечення довгострокової кіберстійкості [7, 16].

Ідентифікація токсичних даних або діяльності може бути корисною для підвищення кібербезпеки, особливо в великих організаціях, де об'єм даних та інтеракції може ускладнити моніторинг безпеки. Використання аналогії оцінки токсичності може допомогти в розробці систем, здатних ідентифікувати та реагувати на потенційно шкідливі або “заражені” ділянки даних, які можуть спричинити зловмисні дії або витік інформації. Що стосується заходів кіберзахисту, розробка механізмів для виявлення та нейтралізації “токсичних” аспектів в IT-інфраструктурі може покращити загальний стан кібербезпеки. Наприклад, оцінка токсичності може виявити програмне забезпечення з високим рівнем ризику або ненадійні джерела, які часто є цілями для кібератак. В контексті відновлення після кіберінцидентів, методи оцінки токсичності можуть бути використані для визначення обсягу пошкоджень або “забруднення” системи після атаки, а також для розробки стратегій дезінфекції та відновлення чистоти даних. Підвищення кіберстійкості за допомогою аналогії оцінки токсичності включає створення довгострокових стратегій для виявлення та мінімізації ризиків від “токсичних” аспектів у кіберпросторі, що забезпечує тривалу захищеність систем та даних [7, 17].

Метод SWIFT (Structured What-If Technique) є ефективним інструментом аналізу, призначеним для ідентифікації потенційних ризиків у системах або процесах шляхом структурованого обговорення сценаріїв “що, якщо”. Ця техніка в кібербезпеці дозволяє оцінити можливі наслідки різних відхилень у роботі системи, виявляючи таким чином

© Шульга, В. П., Іванченко, Є. В., Вишневська, Н. С., & Бербер, А. С. (2024). Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 3(59), 6–19. https://doi.org/10.31673/2409-7292.2024.030001.

потенційні уразливості і вектори атак, що ще не були розглянуті. SWIFT сприяє розробці міцніших систем кіберзахисту, оскільки дозволяє ідентифікувати та розробляти стратегії мінімізації ризиків для критичних точок системи. Це, в свою чергу, допомагає підвищити загальну безпеку інформаційних систем та забезпечити більш ефективний захист від можливих кібератак. Важливим аспектом SWIFT є його здатність адаптуватися та застосовуватися в різних умовах і ситуаціях, що робить його особливо цінним для організацій, які хочуть проводити регулярні перевірки безпеки своїх систем. SWIFT також є інструментом, який можна використовувати під час планування відповідей на інциденти та відновлення після них, дозволяючи організаціям розробляти детальні плани дій на випадок реалізації виявлених ризиків. Це забезпечує більшу підготовку і здатність швидко реагувати на інциденти, мінімізуючи потенційні збитки та сприяючи швидкому відновленню нормальної роботи систем. За цим методом, організації можуть значно покращити свою кіберстійкість, використовуючи SWIFT для регулярного оновлення і тестування своїх захисних механізмів, що є ключем до розробки адаптивної і відповідальної стратегії кібербезпеки [7, 18].

Метод сценарного аналізу є потужним інструментом у галузі кібербезпеки, який дозволяє організаціям оцінювати потенційні ризики та наслідки різних гіпотетичних подій. Цей метод передбачає розробку докладних сценаріїв, які імітують можливі атаки або безпекові порушення, щоб краще зрозуміти, як організація може реагувати на них і які стратегії можуть бути найбільш ефективними для запобігання або мінімізації шкоди. Сценарний аналіз допомагає у виявленні і оцінюванні ризиків кібербезпеки, забезпечуючи розуміння можливих слабких місць в IT-інфраструктурі. Цей метод сприяє розробці комплексних стратегій кіберзахисту, виходячи з аналізу різних “якби” ситуацій, які можуть включати різні види кібератак або технічні неполадки. В результаті, команди кібербезпеки можуть розробити ефективні плани дій і процедури реагування, які будуть оптимізовані для найгірших можливих сценаріїв. Крім того, сценарний аналіз важливий для планування відновлення після кіберінцидентів. Через моделювання різних сценаріїв атак і порушень, організації можуть розробити більш ефективні стратегії для швидкого відновлення систем і мінімізації часу простою. Це також допомагає визначити найбільш критичні активи та процеси, які потребують найвищого рівня захисту. У контексті підвищення кіберстійкості, сценарний аналіз є ключовим для розробки стратегій, що дозволяють організаціям не тільки захищатися від потенційних атак, але й адаптуватися до змінних умов і вимог у сфері кібербезпеки. Цей метод допомагає забезпечити, що політики і процедури безпеки є гнучкими та можуть бути швидко оновлені відповідно до нових загроз[7, 19].

Метод FMEA (Failure Modes and Effects Analysis) є стратегічним підходом у кібербезпеці, який допомагає виявляти потенційні способи відмов системи та аналізувати наслідки цих відмов. Основна мета FMEA — визначення критичних точок відмови в IT-інфраструктурі та програмному забезпеченні, щоб зменшити ризики, пов'язані з безпекою даних та систем. Використання FMEA в кібербезпеці дозволяє організаціям систематично оцінювати кожен компонент системи на предмет потенційних відмов та розробляти відповідні стратегії запобігання. Це включає аналіз можливих причин відмови, оцінку їх імовірності та впливу на систему, а також розробку рекомендацій для вдосконалення кіберзахисту. Такий підхід дозволяє виявляти вразливості на ранніх стадіях розробки або впровадження систем, тим самим знижуючи ймовірність серйозних інцидентів та зменшуючи потенційні збитки. Застосування FMEA також ефективне у плануванні відповіді на інциденти та відновленні системи після атак. Аналізуючи потенційні режими відмови та їхні наслідки, організації можуть розробити більш дієві плани реагування, що враховують всі аспекти відновлення операцій і мінімізації простоїв. Крім того, систематичне застосування FMEA підвищує загальну кіберстійкість організації, забезпечуючи постійне оновлення захисних заходів та поліпшення процедур безпеки. Це створює фундамент для прогресивного управління ризиками та адаптації до постійно змінюваних умов у сфері кібербезпеки [7, 20].

© Шульга, В. П., Іванченко, Є. В., Вишневська, Н. С., & Бербер, А. С. (2024). Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 3(59), 6–19. https://doi.org/10.31673/2409-7292.2024.030001.

Методи Fault Tree Analysis (FTA) та **Event Tree Analysis** (ETA) використовуються для систематичного аналізу причин та наслідків потенційних відмов або інцидентів у системах. Ці методи широко застосовуються у кібербезпеці для детального розуміння та управління ризиками. Fault Tree Analysis (FTA) є методом, який зосереджується на аналізі кореневих причин відмов системи. FTA використовує деревоподібну структуру для визначення ланцюжка подій, які можуть призвести до небажаних результатів, таких як технічні збої або безпекові порушення. Цей метод дозволяє ідентифікувати критичні точки відмов, оцінювати ймовірність їх виникнення та розробляти стратегії для зменшення ризику. FTA корисний при розробці систем, що вимагають високого рівня надійності та безпеки, оскільки допомагає інженерам кібербезпеки зрозуміти можливі шляхи втручань або відмов і відповідно реагувати на них. Event Tree Analysis (ETA) доповнює FTA, фокусуючись на наслідках ініціюючих подій, які можуть привести до різних варіантів розвитку подій. Цей метод використовується для моделювання наслідків потенційних інцидентів, що дозволяє аналізувати різні результати на основі вжитих заходів безпеки. ETA допомагає оцінити ефективність запобіжних заходів та систем відновлення після відмов, надаючи організаціям інформацію для покращення планів реагування на інциденти та підвищення загальної стійкості системи.[7, 21]

Методи аналізу причин та наслідків (Causeand Consequence Analysis) та аналізу причинно-наслідкових зв’язків (Cause-and-Effect Analysis) є ключовими інструментами в галузі управління ризиками та кібербезпеки. Ці методи допомагають організаціям розуміти, яким чином різні фактори впливають на безпеку системи, та як потенційні інциденти можуть призводити до конкретних наслідків. Аналіз причин та наслідків в кібербезпеці зосереджений на виявленні можливих небажаних подій, визначенні їхніх причин та аналізі потенційних наслідків. Цей метод включає в себе систематичний розгляд усіх можливих сценаріїв, коли безпекові заходи можуть зазнати невдачі, та вивчення результатів таких відмов. Це дозволяє компаніям розробляти більш ефективні стратегії реагування на інциденти та вживати превентивних заходів для мінімізації ризиків. Аналіз причинно-наслідкових зв’язків, також відомий як “Діаграма Ісікави” або “Fishbone diagram”, допомагає ідентифікувати первинні та вторинні причини потенційних проблем у системах кібербезпеки. Цей метод забезпечує візуалізацію, яка допомагає аналітикам зрозуміти, як різні елементи системи взаємодіють та які фактори можуть призвести до відмов. Використання такого підходу сприяє глибокому аналізу кореневих причин проблем, що у свою чергу дозволяє виробляти більш ефективні рішення для підвищення надійності та безпеки [7, 22].

Метод LOPA (Layer of Protection Analysis) є важливим інструментом в області управління ризиками, який дозволяє компаніям оцінювати ефективність різних шарів захисту в їхніх системах кібербезпеки. Методом LOPA можна ідентифікувати та аналізувати можливі сценарії ризику, що мають місце внаслідок відмов безпекових заходів, та оцінювати, чи достатні наявні шари захисту для їх запобігання або пом'якшення. Використання LOPA в кібербезпеці зосереджується на кількісному аналізі ризиків, який дозволяє оцінити ймовірність різних загроз та потенційні наслідки інцидентів, зважаючи на існуючі захисні механізми. Цей метод особливо корисний при розробці комплексних інформаційних систем, де потрібно гарантувати, що критичні компоненти захищені відповідно до рівня ризику. LOPA допомагає також у плануванні відповіді на інциденти та відновленні системи після атак, оскільки дає змогу організаціям переконатися, що всі необхідні заходи запобігання враховані та достатньо ресурсів виділено для найбільш вразливих ділянок. Підхід LOPA сприяє також розробці ефективних стратегій мінімізації ризиків, що забезпечує організаціям можливість більш точно відповідати на потенційні загрози [7, 23].

Метод Decision Tree (древо рішень) використовується в кібербезпеці для визначення оптимальних стратегій реагування на різноманітні безпекові ситуації. Цей інструмент дозволяє аналізувати можливі наслідки рішень, що приймаються на основі систематичного відображення усіх альтернативних варіантів і їхніх потенційних результатів. Використовуючи

© Шульга, В. П., Іванченко, Є. В., Вишневська, Н. С., & Бербер, А. С. (2024). Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 3(59), 6–19. https://doi.org/10.31673/2409-7292.2024.030001.

дерева рішень, аналітики можуть визначити, як різні рішення можуть вплинути на безпеку системи, зменшити ризики або оптимізувати ресурси. Ідентифікація ризиків кібербезпеки: Decision Tree дозволяє ідентифікувати потенційні загрози та оцінити ризики, пов'язані з кібербезпекою. Використовуючи дерево рішень, можна систематично розглядати всі можливі сценарії і визначити, які заходи потрібно вжити для запобігання втрати даних або атак. Кіберзахист: В рамках підготовки захисних механізмів, DecisionTree може допомогти планувати та імплементувати заходи безпеки з урахуванням різних атак або непередбачених подій. Це дозволяє організаціям бути більш гнучкими у своїх стратегіях та швидко адаптуватися до змін у загрозах. Відновлення після кіберінцидентів: Застосування дерева рішень допомагає в плануванні відновлення операцій після інцидентів. Аналіз різних шляхів відновлення дає змогу вибрати найбільш ефективний варіант, що забезпечує мінімальний час простою та оптимальне використання ресурсів. Підвищення кіберстійкості: Використання DecisionTree сприяє розробці довгострокових стратегій, які зміцнюють кіберстійкість організацій. Цей метод допомагає оцінити ефективність різних заходів безпеки і виявити потреби в подальших інвестиціях у кібербезпеку [7, 24]

Метод HRA (Human Reliability Analysis) зосереджується на аналізі вірогідності помилок з боку людини та на оцінці потенційних наслідків цих помилок для систем безпеки. У контексті кібербезпеки, HRA допомагає розуміти, як людські фактори, такі як помилки операторів, недбалість або недостатня підготовка, можуть впливати на безпеку інформаційних систем. Цей підхід дає можливість виявити і мінімізувати ризики, пов’язані з людською діяльністю, і сприяє розробці більш ефективних процедур і політик управління кібербезпекою. Застосування HRA в кібербезпеці дозволяє аналізувати, як помилки користувачів або адміністраторів можуть призвести до втрати даних, несанкціонованого доступу, або інших безпекових порушень. Використання цього методу допомагає ідентифікувати найбільш критичні аспекти системи, які вразливі до людських помилок, і розробляти заходи для їх захисту, наприклад, через покращення інтерфейсів, навчання та розробку більш чітких процедур роботи. Крім того, HRA може сприяти в плануванні відповідей на інциденти та відновлення після них, визначаючи, як дії людей під час кризи можуть покращити або погіршити ситуацію. Аналізуючи потенційні людські помилки під час інцидентів, можна розробити ефективніші плани реагування, що враховують людський фактор. У контексті підвищення кіберстійкості, HRA допомагає організаціям створювати більш надійні системи, мінімізуючи ризики, що виникають через людські помилки. Це створює більш стійку обстановку, де ризики контролюються на всіх рівнях взаємодії користувачів [7, 25].

Метод Bow Tie Analysis використовується для візуалізації потенційних причин та наслідків ризикових подій, формуючи діаграму, яка нагадує форму метелика. В кібербезпеці цей метод дозволяє детально розглянути як можливі загрози, так і стратегії їх запобігання, забезпечуючи чітке уявлення про зв’язки між вразливостями, загрозами, наслідками і контрзаходами. Ідентифікація ризиків кібербезпеки: Bow Tie Analysis дозволяє виявити і візуалізувати критичні ризики, які можуть вплинути на систему. За допомогою цього методу аналітики можуть визначити не тільки потенційні джерела загроз, але й наслідки, що можуть виникнути в разі реалізації цих загроз. Це сприяє глибшому розумінню зв’язків між можливими причинами і їх впливом на систему. Використання BowTieAnalysis сприяє розробці більш ефективних стратегій кіберзахисту, забезпечуючи збалансоване бачення як загроз, так і контрзаходів. Аналіз допомагає планувати адекватні заходи щодо зниження ризику і запобігання можливим інцидентам, розробляючи захисні механізми на кожному етапі потенційної атаки. Bow Tie Analysis може використовуватися для планування відновлення системи після інцидентів, визначаючи ключові дії, необхідні для відновлення нормального функціонування. Це включає аналіз наслідків інцидентів та визначення оптимальних шляхів мінімізації шкоди та швидкого реагування. Через свою здатність до комплексного аналізу причин та наслідків, Bow Tie Analysis допомагає в розробці стратегій, які підвищують загальну

© Шульга, В. П., Іванченко, Є. В., Вишневська, Н. С., & Бербер, А. С. (2024). Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 3(59), 6–19. https://doi.org/10.31673/2409-7292.2024.030001.

кіберстійкість організації. Він забезпечує організації засобами для неперервного моніторингу та оцінки ефективності імплементованих заходів безпеки [7, 26].

Метод Monte Carlo Simulation використовується у кібербезпеці для моделювання різноманітних безпекових сценаріїв, дозволяючи оцінити ймовірності різних наслідків на основі статистичного аналізу. Цей метод особливо корисний для оцінки ризиків, які важко кількісно оцінити через їхню невизначеність та залежність від великої кількості змінних. Monte Carlo Simulation дозволяє симулювати різні сценарії атак або відмов, використовуючи випадково згенеровані вхідні дані для визначення ймовірності виникнення різних подій. Це допомагає виявити потенційні вразливості та оцінити потенційний вплив на системи та дані. Також Monte Carlo дозволяє аналізувати ефективність різних стратегій безпеки, моделюючи вплив різних заходів захисту на зменшення ризиків. Метод може допомогти оцінити, як зміни у конфігурації безпеки можуть вплинути на зниження ймовірності успішних кібератак. Симуляції Monte Carlo можуть бути використані для планування відновлення після інцидентів, дозволяючи аналізувати різні стратегії відновлення та оцінювати їхню ймовірну ефективність в реальних умовах. Сприяє розробці комплексних стратегій, що покращують загальну кіберстійкість організацій, дозволяючи моделювати різні загрози та вплив впроваджених заходів безпеки на довгострокову перспективу [7, 27].

Метод Consequence / Probability Matrix є фундаментальним інструментом у кібербезпеці для оцінки ризиків, де він дозволяє класифікувати та пріоритизувати ризики на основі їх імовірності та потенційних наслідків. Ця матриця є важливою для управління ризиками, оскільки надає зрозуміле візуальне представлення рівнів ризику, що допомагає приймати обґрунтовані рішення щодо заходів безпеки. Систематично оцінювати й категоризувати потенційні загрози, ранжуючи їх за рівнем серйозності від низького до високого та від низької до високої імовірності. Це дозволяє кібербезпековим командам виявляти, які загрози потребують негайної уваги та ресурсів для мінімізації. Використовуючи дані матриці, можна розробити більш цілеспрямовані стратегії безпеки, що фокусуються на найбільш критичних загрозах. Аналіз допомагає визначити необхідність вжиття певних заходів безпеки, зокрема, коли потенційні наслідки можуть бути катастрофічними. Матриця допомагає планувати відновлення операцій після інцидентів, дозволяючи аналізувати сценарії, які мають високі наслідки та високу ймовірність. Знання про можливі наслідки сприяє кращому розумінню того, які системи або активи потребують додаткових ресурсів для швидкого відновлення. Нарешті, метод допомагає в розробці довгострокових стратегій для покращення кіберстійкості організації. Регулярний перегляд і оновлення матриці забезпечують, що заходи безпеки завжди відповідають поточному рівню ризику [7, 28].

Метод Cost / Benefit Analysis (CBA) в кібербезпеці використовується для оцінки вартості запровадження заходів безпеки порівняно з перевагами, які ці заходи можуть принести. Це критично важливо для управління ресурсами та обґрунтування інвестицій у безпеку, забезпечуючи, що вкладені кошти ефективно знижують ризики або відшкодовують можливі збитки. CBA допомагає організаціям вирішити, скільки коштів варто інвестувати в конкретні заходи безпеки. Аналіз включає порівняння потенційних втрат від інцидентів кібербезпеки з витратами на впровадження та підтримку безпекових технологій та процедур. CBA дозволяє кібербезпековим командам пріоритизувати проекти на основі їхньої вартості та користі. Це допомагає оптимізувати розподіл бюджету кібербезпеки, зосереджуючи зусилля на найбільш ефективних заходах, які можуть запобігти найсерйознішим загрозам. CBA також використовується для оцінки потенційних наслідків кіберінцидентів, що дозволяє розробляти більш ефективні стратегії відновлення. Через аналіз можливих збитків та вартості заходів для їх уникнення або мінімізації, організації можуть краще планувати, як відновити операції з мінімальними втратами. Регулярне проведення CBA допомагає організаціям визначати слабкі місця у своїх захисних стратегіях і вчасно адаптуватися до змінюваного ландшафту загроз. Це

сприяє розвитку більш стійких інформаційних систем, які ефективно протистоять новим і еволюціонуючим загрозам [7, 29].

Метод MCDA (Multi-Criteria Decision Analysis) є інструментом для прийняття рішень, що базується на аналізі декількох критеріїв одночасно. У контексті кібербезпеки, MCDA може використовуватися для оцінки та порівняння різних заходів безпеки, враховуючи множину аспектів, таких як вартість, ефективність, вплив на продуктивність, і ризики. Цей метод дозволяє керівникам і фахівцям з кібербезпеки приймати зважені та обґрунтовані рішення, оптимізуючи захисні стратегії відповідно до комплексної оцінки їх потенціалу та витрат. MCDA допомагає оцінити і порівняти різні технології та методики безпеки, враховуючи їх комплексний вплив на організацію. Наприклад, аналізуючи новітні захисні технології, можна одночасно оцінювати їх вартість, складність інтеграції, очікуване зниження ризику, та вимоги до обслуговування. MCDA дозволяє кібербезпековим командам приймати рішення про розподіл ресурсів, зважаючи на обмеження бюджету та потреби у захисті. Метод сприяє прийняттю рішень, які забезпечують максимальний захист при оптимальних витратах.У ситуаціях, коли необхідно швидко відновити системи після кібератак, MCDA може допомогти оцінити різні стратегії відновлення, враховуючи їх швидкість впровадження, вартість та ефективність. Використання MCDA сприяє розробці стратегій, які підвищують загальну кіберстійкість організації. Метод дозволяє врахувати довгострокові переваги та недоліки різних підходів до захисту інформаційних систем [7, 30].

Аналіз графів атак (Attack Graph Analysis) – один із методів оцінки кібербезпеки, який допомагає визначити потенційні шляхи, за допомогою яких зловмисники можуть проникнути в систему чи мережу, і виявляти вразливі місця, для здійснення атак. Аналіз графів атак дозволяє виявляти потенційні ризики і уразливості в системі, оцінювати їхню важливість і ймовірність експлуатації, дозволяє розробити ефективні стратегії захисту на основі аналізу шляхів атак і вразливих точок, також можуть допомогти у визначенні характерних ознак атак і налаштуванні систем моніторингу для своєчасного виявлення інцидентів. Цей метод дозволяє планувати ефективні дії для реагування на інциденти шляхом визначення можливих сценаріїв атак і заходів для їхньої нейтралізації. допомагає визначити ключові компоненти, які потребують відновлення після атаки, і розробити плани відновлення. Також аналіз графів атак дозволяє оцінювати стійкість системи до атак і визначати заходи для підвищення її кіберстійкості [31, 32, 33].

Байєсівські мережі (BN) головним чином зосереджені на оцінці та ідентифікації ризиків для оцінки вразливості (Identification of Cybersecurity Risks): BN ефективні у виявленні та оцінці ризиків кібербезпеки. За рахунок моделювання різних факторів ризику та їх взаємозалежності, BN допомагають розуміти ймовірності і вплив різних загроз на кібербезпеку, але їх можна застосувати і до наступних критеріїв, а саме: виявлення кіберінцидентів шляхом моделювання нормальної та аномальної поведінки системи. Імовірнісні міркування допомагають визначити аномалії, які можуть вказувати на кіберінцидент.BN сприяють загальній кіберстійкості, надаючи повне розуміння ризиків, можливостей виявлення та стратегій реагування. Цей цілісний підхід гарантує, що система зможе протистояти кіберінцидентам і ефективно відновлюватися після них. Можна сказати, що байєсівські мережі ефективні у виявленні ризиків кібербезпеки, виявленні кіберінцидентів і реагуванні на кіберінциденти. Також BN підтримують кіберзахист, відновлення статусу кібербезпеки та кіберстійкість завдяки комплексній оцінці ризиків і можливостям імовірнісного обґрунтування [34, 35, 36, 37].

Загальна система підрахунку вразливостей (Common Vulnerability Scoring System CVSS) – це важлива структура, яка надає стандартизований спосіб оцінки важливості вразливостей безпеки програмного забезпечення. Його основна роль полягає у створенні послідовного та об’єктивного методу оцінки впливу вразливості. Оцінюючи основні атрибути вразливості, включаючи можливість її використання, вплив на цілісність системи, доступність

© Шульга, В. П., Іванченко, Є. В., Вишневська, Н. С., & Бербер, А. С. (2024). Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 3(59), 6–19. https://doi.org/10.31673/2409-7292.2024.030001.

і конфіденційність, а також рівень привілеїв, необхідних для використання. Ці фактори поєднуються, для створення числового балу, який відображає важливість вразливості. Потім цю оцінку можна використовувати для спрямування та визначення пріоритетності заходів щодо реагування та пом'якшення наслідків [38].

Common Weakness Enumeration (CWE) - це стандартизований список помилок програмного забезпечення, який використовується для ідентифікації, визначення та уникнення потенційних уразливостей в програмному забезпеченні. CWE створюється спільними зусиллями між комерційними, громадськими та урядовими організаціями задля покращення безпеки програмного забезпечення. CWE каталогізує слабкі місця на основі їх характеристик, надаючи спільну мову для опису вразливостей, що дозволяє стандартизувати підходи до їх виявлення і усунення. Кожна слабкість у CWE має унікальний ідентифікатор опис та приклади реалізації. CWE забезпечує структурований підхід до виявлення і класифікації слабких місць, що дозволяє ідентифікувати потенційні ризики, допомагає у розробці захисних заходів для усунення або зменшення впливу слабких місць, надає інформацію про характерні ознаки експлуатації слабких місць, що може бути використано для налаштування систем моніторингу та виявлення інцидентів. Інформація про вразливості та рекомендації щодо їх усунення, надані CWE, допомагають у швидкому реагуванні на інциденти. За допомогою CWE можна визначити необхідні кроки для усунення слабких місць і відновлення безпечного стану системи після інциденту. Також CWE сприяє підвищенню стійкості систем до атак шляхом впровадження передових практик та рекомендацій щодо безпеки [39].

Factor Analysis of Information Risk (FAIR) міжнародна визнана стандартна модель для кількісного оцінювання інформаційних та операційних ризиків. FAIR розроблена з метою допомогти організаціям зрозуміти та керувати ризиками, пов'язаними з інформаційною безпекою. Основні концепції FAIR включають ідентифікацію активів, визначення загроз, оцінку вразливостей та розрахунок потенційних втрат [7, 39].

Game Theory in Cybersecurity. Використання теорії ігор для аналізу стратегічної взаємодії між атакуючими та захисниками системи. Так Автори [40] запропонували підхід з використанням теорії ігор який покращує розуміння складних проблем і сприяє розробці ефективних рішень у сфері кібербезпеки. Він оцінює ефективність різних стратегій безпеки. Цей стратегічний підхід використовує некорпоративну гру, яка базується на змішаних стратегіях. Автори [40] визначили сценарій для ігор з одночасними ходами, оцінивши значення для різних елементів гри. Аналізуючи поведінку як зловмисника, так і захисника, запропоновали ігровий підхід, який може допомогти галузям розробити ефективніші та ефективніші стратегії безпеки. Крім того, цей підхід забезпечує розуміння складних викликів кібербезпеки [40].

Марківські ланцюги та теорія черг (Markov Chains and Queuing Theory) є потужними інструментами для моделювання та аналізу динамічних систем, у яких майбутній стан системи залежить лише від її поточного стану, що робить їх майже ідеальними для оцінки ризиків та керування вразливими місцями в IT-системах. Так Марківські ланцюги дозволяють оцінити ймовірність переходу системи у вразливий стан, що допомагає ідентифікувати ризики, Аналізувати перехід між станами, допомагає оцінити ефективність заходів захисту та визначити, які дії можуть зменшити ймовірність експлуатації вразливостей, Теорія черг дозволяє моделювати процес виявлення інцидентів, визначати ефективність моніторингових систем та оптимізувати їх роботу, моделювання процесів обробки інцидентів (черги) допомагає оцінити, наскільки швидко система може реагувати на загрози і які ресурси потрібні для цього, Марківські ланцюги дозволяють аналізувати стійкість системи до атак, оцінюючи ймовірність переходу в критичний стан і швидкість відновлення [41].

Національна база даних вразливостей (National Vulnerability Database, NVD) – це ресурс для оцінки та управління кібербезпекою. NVD містить інформацію про вразливості, яка

© Шульга, В. П., Іванченко, Є. В., Вишневська, Н. С., & Бербер, А. С. (2024). Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 3(59), 6–19. https://doi.org/10.31673/2409-7292.2024.030001.

збирається та публікується Національним інститутом стандартів і технологій США (NIST), надає стандартизовані описи вразливостей, методи їх оцінки та засоби для їхньої ідентифікації та усунення. Оцінка вразливостей здійснюється за допомогою Common Vulnerability Scoring System (CVSS), що дозволяє визначити критичність вразливості на основі різних критеріїв. NVD надає актуальну інформацію про відомі вразливості, що дозволяє організаціям ідентифікувати потенційні ризики в їхніх системах. Завдяки NVD можна отримати рекомендації щодо усунення вразливостей та впровадження відповідних заходів захисту. NVD містить рекомендації щодо швидкого усунення вразливостей, що допомагає у реагуванні на інциденти. Інформація про патчі та виправлення дозволяє швидко відновити систему до безпечного стану після інциденту. Регулярне оновлення інформації та впровадження рекомендованих заходів сприяє підвищенню стійкості систем до атак [42].

Fuzzy Logic for Vulnerability Assessment – це метод, який застосовує нечітку логіку для оцінки вразливостей у кібербезпеці. Нечітка логіка дозволяє обробляти неточні, невизначені або нечіткі дані, що особливо корисно в умовах, де ризики і загрози важко визначити [43].

Модель CIA (конфіденційність, цілісність та доступність) наводиться як простий і зрозумілий спосіб управління кібербезпекою, акцентуючи на трьох основних цілях. Критика цієї моделі полягає в її надмірній спрощеності та неуваги до інших важливих аспектів кібербезпеки, таких як аутентичність [43, 44].

Теорія мотивації захисту (PMT) та Теорія стримування демонструють [43, 45], як психологічні чинники можуть впливати на рішення людей щодо захисту від кіберзагроз. PMT пояснює, як сприйняття загрози та ефективності заходів захисту впливає на поведінку людей, тоді як Теорія стримування фокусується на впливі покарання на стримування кіберзлочинців від проведення зловмисних дій [43, 45].

Critical Security Controls (CIS Controls) – це набір найкращих методів кібербезпеки, призначених для покращення безпеки організації шляхом усунення найбільш поширених і критичних кіберзагроз. Цей підхід визначає пріоритетність заходів безпеки, дозволяючи організаціям ефективно керувати ресурсами та зусиллями для досягнення найвищого рівня захисту, а саме ідентифікація та інвентаризація активів дозволяє виявити пристрої та програми, які застосовуються і визначає, які з них можуть становити потенційні ризики; управління вразливостями виявляє тонкі місця та допомагає розробити плани для їх усунення, що знижує ризик успішних атак; контроль привілейованого доступу: встановлює правила, що лише уповноважені користувачі мають доступ до важливих ресурсів, зменшуючи вірогідність зловживань; безперервний моніторинг за рахунок виявлення аномалій у реальному часі, дозволяє швидко реагувати на потенційні загрози; захист даних: Визначення та захист конфіденційних даних, забезпечення їх цілісності та доступності. навчання та підвищення обізнаності: забезпечення навчання працівників про кіберзагрози та методи захисту, що знижує ймовірність людських помилок, пріоритезація заходів: завдяки CIS Controls організація має зосередитися на критичних аспектах безпеки, це дозволяє ефективно використовувати ресурси, стандартизація підходів: використання стандартизованих методів забезпечення безпеки створює уніфікований підхід до кібербезпеки в організації, спрощення процесів: задля спрощення впровадження заходів безпеки, контролі CIS мають адекватні інструкції та рекомендації [46].

Nessus сканер вразливостей, завдяки якому можна виявити тонкі місця в мережі, автоматизувати оцінювання на певний момент часу, задля швидкого виявлення та виправлення вразливості, зокрема недоліки програмного забезпечення, відсутні виправлення, зловмисне програмне забезпечення та неправильні конфігурації, у різноманітних операційних системах, пристроях і програмах [47].

Open VAS сканер вразливостей. Можливість неавтентифікованого та автентифікованого тестування, низка високорівневих та низькорівневих Інтернет протоколів та промислових

протоколів, налаштування продуктивності для широкомасштабного сканування та потужну внутрішню мову програмування для реалізації будь-якого типу тесту на вразливості [48].

Qualys – комплексна хмарна платформа, розроблена для керування вразливістю та кібербезпеки. Надає набір інструментів для виявлення, оцінки, пріоритезації та усунення вразливостей, повну інформацію про захищеність у різноманітних IT-активах. До характеристик Qualys можна віднести управління, виявлення та реагування на вразливості (VMDR), виявлення та реагування на загрози, керування виправленнями, безперервний моніторинг [49].

Узагальнена порівняльна характеристика розглянутих методів наведена у Табл. 1.

Таблиця 1.

Порівняльна характеристика методів та моделей оцінювання кіберзахисту критичної інфраструктури держави

Номер джерела	Заходи кіберзахисту					
	Ідентифікація ризиків кібербезпеки	Кіберзахист	Виявлення кіберінцидентів	Реагування на кіберінциденти	Відновлення стану кібербезпеки	Кіберстійкість
[7, 8]	+	+	-	-	+	+
[7, 9]	+	+	-	-	+	+
[7, 10]	+	+	-	-	-	+
[7, 11]	+	+	+	+	+	+
[7, 12]	+	+	-	-	-	+
[7, 13]	+	+	-	-	-	+
[7, 14]	+	-	-	-	-	-
[7, 15]	+	-	-	-	-	-
[7, 16]	+	+	-	+	-	+
[7, 17]	+	+	-	+	+	+
[7, 18]	+	+	-	+	+	+
[7, 19]	+	+	-	+	+	+
[7, 20]	+	+	-	+	+	+
[7, 21]	+	+	-	+	+	+
[7, 22]	+	+	-	-	+	+
[7, 23]	+	-	-	-	-	-
[7, 24]	-	+	+	+	+	+
[7, 25]	+	+	-	+	+	+
[7, 26]	-	+	-	-	+	+
[7, 27]	-	+	-	-	-	+
[7, 28]	+	+	-	-	+	+
[7, 29]	+	+	-	-	+	+
[7, 30]	+	+	-	-	+	+
[31, 32, 33]	+	+	+	+	+	+
[34, 35, 36, 37]	+	+	+	+	+	+
[38]	+	+	+	+	+	+
[39]	+	-	+	-	-	+
[40]	+	+	-	-	-	+
[43]	+	+	+	+	+	+
[41]	+	+	+	+	+	+
[42]	+	+	+	+	+	+
[43, 44]	+-	+-	+-	+-	+-	+-
[43, 45]	+	+-	+	+-	+-	+-
[46]	+	+	+	+	+	+
[47]	+	+	-+	+	-+	-+
[48]	+	+	+	+	+	+
[49]	+	+	+	+	+	+

© Шульга, В. П., Іванченко, Є. В., Вишневська, Н. С., & Бербер, А. С. (2024). Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 3(59), 6–19. https://doi.org/10.31673/2409-7292.2024.030001.

Висновок

Таким чином, проведено дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави, які на підставі сформованої множини критеріїв та класів кіберзахисту, дають можливість оцінити методи та моделі оцінювання кіберзахисту критичної інфраструктури держави для їх подальшого використання при вирішенні задач кібербезпеки та захисту інформації.

Перелік посилань

1. Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1, NIST Cybersecurity Framework, [online], https://doi.org/10.6028/NIST.CSWP.04162018, https://www.nist.gov/cyberframework (Accessed April 18, 2024)

2. European Union Agency for Cybersecurity (ENISA), “Threat Landscape Report 2020,” режим доступу https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

3. The Cybersecurity and Infrastructure Security Agency (CISA), “GuidelinesforSecuringtheCyberInfrastructure,” режим доступу: https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/laws-and-regulations/cybersecurity-and-infrastructure-security-agency-guidance

4. Schneier, Bruce, “Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World” (W.W. Norton & Company, 2015).

5. IBM X-Force Threat Intelligence Index 2024. https://www.ibm.com/reports/threat-intelligence

6. Наказ Адміністрації Держспецзв’язку від 06.10.2021 № 601 “Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури” (зі змінами)

7. Гончар, С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури: монографія / С.Ф. Гончар. – К.: Альфа Реклама, 2019. – 176 с. ISBN 978-966-288-263-6

8. ISO/IEC 27005:2022 URL https://www.iso.org/standard/80585.html

9. Patton, Michael Quinn. QualitativeResearchandEvaluationMethods. 3 ed, SagePublications, 2002.

10. Gene Rowe, George Wright, The Delphi technique as a forecasting tool: issues and analysis, International Journal of Forecasting, Volume 15, Issue 4, 1999, Pages 353-375, ISSN 0169-2070

11. Linstone, Harold & Turoff, Murray. (1975). The Delphi Method: Techniques and Applications. 10.2307/3150755.

12. NIST SP 800-53 Rev. 5 URL https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

13. ISO/IEC 27001:2022 URL https://www.iso.org/standard/27001

14. Roland, Harold E., and Brian. Moriarty. System Safety Engineering and Management / Harold E. Roland, Brian Moriarty. 2nd edition. NewYork: Wiley, 1990. Web.

15. Fthenakis, Vasilis & Trammell, Steven. (2003). Reference Guide for Hazard Analysis in PV Facilities.

16. Pasman, Hans. (2015). Risk Analysis and Control for Industrial Processes – Gas, Oiland Chemicals; A System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events.

17. A. Alahmari and B. Duncan, “CybersecurityRiskManagementinSmallandMedium-SizedEnterprises: A SystematicReviewofRecentEvidence,” 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), Dublin, Ireland, 2020, pp. 1-5, doi: 10.1109/CyberSA49311.2020.9139638.

18. Guidelines for Hazard Evaluation Procedures (3rd ed.). Wiley. Retrievedfrom https://www.perlego.com/book/1008408/guidelines-for-hazard-evaluation-procedures-pdf (Published 2011)

19. Hassani, Bertrand K. Scenario Analysis in Risk Management: Theory and Practice in Finance, 2016. Internet resource.

20. Schneider, H. (1996). Failure Mode and Effect Analysis: FMEA From Theory to Execution. Technometrics, 38(1), 80. https://doi.org/10.1080/00401706.1996.10484424

21. Rausand, Marvin and Høyland, Arnljot. System Reliability Theory: Models, Statistical Methods and Applications. Hoboken, NJ: Wiley-Interscience, 2004.

22. Bahr, N.J. (2015). System Safety Engineering and Risk Assessment: A Practical Approach, Second Edition (2nd ed.). CRC Press. https://doi.org/10.1201/b17854

23. Murphy, John & Chastain, Wayne & Bridges, William. (2009). CCPS Guidelines for Independent Protection Layers and Initiating Events. Process Safety Progress. 28. 374 - 378. 10.1002/prs.10356.

24. Han, Jiawei & Kamber, Micheline & Pei, Jian. (2012). Data Mining: Concepts and Techniques. 10.1016/C2009-0-61819-5.

25. Boyless, James. (1988). Human reliability: Analysis, prediction, and prevention of human errors. International Journal of Industrial Ergonomics - INT J IND ERGONOMIC. 2. 165-166. 10.1016/0169-8141(88)90048-0.

26. Clothier, Reece & Walker, Rodney. (2014). The Safety Risk Management of Unmanned Aircraft Systems. 10.1007/978-90-481-9707-1_39.

27. Nan Chenand L. Jeff Hong. 2007. Monte Carlo simulation in financial engineering. In Proceedings of the 39th conference on Wintersimulation: 40 years! The best is yet to come (WSC '07). IEEE Press, 919–931.

28. Pritchard, PMP, PMI-RMP, EVP, C.L. (2015). Risk Management: Concepts and Guidance, Fifth Edition (5th ed.). Auerbach Publications. https://doi.org/10.1201/9780429438967

29. Boardman, Anthony & Greenberg, David & Vining, Aidan & Weimer, David. (2018). Cost-Benefit Analysis: Concepts and Practice, 5th edition.

30. Glaser, Bodo. (2002). Multiple Objectives in Dynamic Decision Making. 10.1007/978-3-642-56100-9_7.

31. Steven Noel, Sushil Jajodia, Lingyu Wang, Anoop Singhal. Measuring security risk of networks using attack graphs. International Journal of Next-Generation Computing. 2010/7/14, P 135-147.

32. Survey of Attack Graph Analysis Methods from the Perspective of Data and Knowledge Processing Jianping Zeng, Shuang Wu, Chengrong Wu. Published in Secur. Commun. Networks 26 December 2019.

33. Yuri Diogenes Erdal Ozkaya Cybersecurity – Attack and Defense Strategies// Published by Packt Publishing Ltd. Livery Place 35 Livery Street Birmingham B3 2PB, UK, 2018, P 368.

34. Dawood Behbehani, Nikos Komninos, Khalid Al-Begain, Muttukrishnan Rajarajan Journalof Cloud Computing, volume12, Articlenumber: 79 (2023).

35. Helger Lipmaa, Aikaterini Mitrokotsa, Raimundas Matulevičius Cloud Enterprise Dynamic Risk Assessment (CEDRA): a dynamic risk assessment using dynamic Bayesian networks for cloud environment, Bayesian Network Models in Cyber Security: A Systematic Review, November 2017, DOI:10.1007/978-3-319-70290-2_7, Inbook: Secure IT Systems (pp.105-122), Chapter: 7, Publisher: Springer.

36. Optimal monitoring and attack detection of networks modeled by Bayesian attack graphs, Armita Kazeminajafabadi & Mahdi Imani, Cybersecurity volume 6, Articlenumber: 22 (2023).

37. Bayesian Network Models in Cyber Security: A Systematic Review, November 2017, DOI:10.1007/978-3-319-70290-2_7, Inbook: Secure IT Systems (pp.105-122), Chapter: 7, Publisher: Springer, Editors: Helger Lipmaa, Aikaterini Mitrokotsa, Raimundas Matulevičius.

38. Tuxcare URL https://tuxcare.com/blog/the-transition-to-cvss-v4-0-what-you-need-to-know/

39. Attack.mitre URL https://attack.mitre.org/

40. Ravdeep Kour, Ramin Karim, Pierre Dersin Game Theory and Cyber Kill Chain: A Strategic Approach to Cybersecurity January 2024, DOI:10.1007/978-3-031-39619-9_33, In book: International Congress and Workshop on Industrial AI and eMaintenance 2023 (pp.451-463).

41. Paul A Gagniuc, "Markov Chains: From Theory to Implementation and Experimentation", 2017, p 235.

42. Information Technology LaboratoryNationalVulnerabilityDatabase URL https://nvd.nist.gov/

43. Іванченко, Є. В., Корченко, О. Г., Бакалинський, О. О., Мялковський, Д. В., Верба, Д. В., Зубков, Д. А., Юдіна, Д. О. Модель системи характеристик даних для оцінювання заходів кіберзахисту в Україні. Український науковий журнал інформаційної безпеки: том. 30 № 1, (2024), 95-99 с.

44. CIA triad (confidentiality, integrityandavailability) https://www.techtarget.com /whatis/definition/Confidentiality-integrity-and-availability-CIA.

45. Теорія мотивації захисту. URL https://open.ncl.ac.uk/theories/10/protection-motivation-theory (дата звернення 08.07.2024).

46. Critical Security Controls (CIS Controls). URL: www.cisecurity.org/

47. Nessus Professional. URL: www.tenable.com (дата звернення 08.07.2024)

48. OpenVAS. URL:www.openvas.org. (дата звернення 08.07.2024)

49. The Qualys Enterprise Tru Risk TM Platform. URL: www.qualys.com. (дата звернення 08.07.2024).

50. Іванченко, Є., Корченко, О., Заріцький, О., Зибін, С., Вишневська, Н. Аналіз поняття кіберстійкості критичної інфраструктури. Захист інформації. Том 25, №4, жовтень-грудень 2023, 221-233.

Надійшла 04.07.2024