УДК 004.9.005.95 DOI: https://doi.org/10.33099/2304-2745/2022-1-74/69-77

Рибидайло А. А., кандидат технічних наук, старший науковий співробітник (0000-0002-6156-469X)
Федорієнко В. А., кандидат технічних наук (0000-0002-0921-3390)
Кульчицький О. С (0000-0002-4901-0192)
Обозненко Є. Г. (0000-0003-3617-8604)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Підходи до оцінювання захищеності інформаційної інфраструктури Міністерства оборони України

Резюме. Розглянуто підходи до оцінювання стану захищеності інформаційної інфраструктури та методика експрес-оцінювання загального рівня захищеності системи. Наведено приклад формалізації процесу оцінювання показників захищеності інформаційної інфраструктури Міністерства оборони України.

Ключові слова: інформаційна інфраструктура; стан захищеності інформаційної інфраструктури; показники рівня захищеності; граф атак; методика оцінювання показників захищеності.

Постановка проблеми. За напрямом створення інформаційної інфраструктури (ІІС) у Міністерстві оборони (МО) України на сьогодні розроблено та затверджено Міністром оборони України 22 грудня 2015 року Концепцію створення ІІС Міністерства оборони України. Видання Концепції створення ІІС Міністерства оборони України стало першим кроком, який обумовив стратегію та принципи створення ІІС Міністерства оборони України відповідно до засад державної політики у сфері інформатизації.

Інформаційна інфраструктура МО (англ. information infrastructure) – комплекс програмно-технічних засобів, організаційних систем і нормативних баз, який забезпечує організацію взаємодії інформаційних потоків, функціонування та розвиток засобів інформаційної взаємодії й інформаційного простору воєнного відомства. Технологічно, у класичному розумінні, інфраструктура являє собою: обчислювальне обладнання; лінії зв'язку; системи енергозабезпечення; системи кондиціонування тощо.

У період розвитку локальних і глобальних мереж поняття технологічної інфраструктури залишилося незмінним, однак ускладнилася структура її елементів через збільшення числа елементів, зв'язків між ними, ускладнення внутрішньої структури елементів, перерозподілу функцій між ними.

Забезпечення функціонування ІІС означає підтримання стану її компонент, що дає змогу своєчасно і якісно виконувати визначені функціональні завдання, зокрема *забезпечення інформаційної безпеки*.

Інформаційна безпека (information security) – збереження конфіденційності, цілісності та доступності інформації. *Конфіденційність* (англ. confidentiality) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем. *Цілісність* (англ. integrity) – означає неможливість модифікації неавторизованим користувачем. *Доступність* (англ. availability) – властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, у необхідний для нього час.

Тобто, інформаційна безпека – це стан захищеності ІІС. Показники безпеки ІІС характеризують здатність системи забезпечити конфіденційність і цілісність інформації, захист її від несанкціонованого доступу сторонніми особами, які мають за мету зламування, зміни або знищення інформації.

На сьогодні актуальним є питання оцінювання стану захищеності ІІС для обґрунтованого прийняття відповідних заходів щодо підтримання його на визначеному рівні.

Аналіз останніх досліджень і публікацій. Окремі питання захисту складових інформаційної інфраструктури висвітлені у роботах [1–5]. Зокрема у роботах [1–3] розглянуті питання:

оцінювання кіберзагроз у момент прийняття рішень щодо використання новітніх технологій;

планування відновлення систем захисту у разі реалізації кібератак і створення шляхів щодо відновлення даних;

перевірка здатності забезпечення повного захисту та відновлення пошкоджених

або "слабких" місць інформаційної інфраструктури.

У роботах [4, 5] розтлумачені основні принципи і способи захисту інформації в елементах інформаційної інфраструктури.

Аналіз означених джерел та інших наукових робіт дає змогу дійти висновку про те, що питання захищеності інформаційної інфраструктури досить ретельно пропрацьовано. Проте функціонування інформаційної інфраструктури МО України має певні особливості, які полягають у необхідності забезпечення надійного захисту інформації, яка циркулює у телекомунікаційній мережі, від несанкціонованого доступу та викривлення. Це зумовлює актуальність дослідження стану захищеності ІІС МО України та обґрунтування підходу до оцінювання визначених характеристик захищеності.

Мета статті – обґрунтування підходу до оцінювання характеристик стану захищеності інформаційної інфраструктури Міністерства оборони України.

Виклад основного матеріалу. Інформаційна інфраструктура включає (рис. 1):

інформаційно-телекомунікаційні системи (ІТС) та мережі зв'язку;

засоби інформатизації – ІАС, АСУ;

електронні інформаційні ресурси (ЕІР);

систему забезпечення та персонал, який спроможний забезпечувати якісне функціонування інформаційної інфраструктура МО.

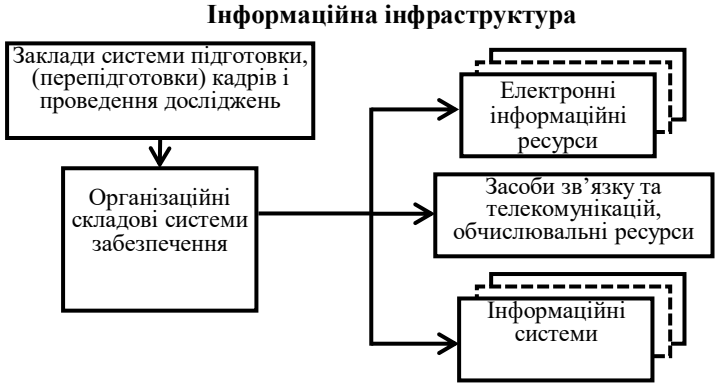

Рис. 1. Структурна схема інформаційної інфраструктури

Завдання організаційних складових системи забезпечення функціонування ІІС:

формування та забезпечення зберігання інформаційних ресурсів;

забезпечення доступу до систем зв'язку та інформаційних ресурсів;

надання інформаційних послуг користувачам Єдиного інформаційного середовища МО України;

забезпечення визначеного рівня захищеності ІІС (інформаційна безпека);

підготовка та перепідготовка кадрів, проведення наукових досліджень.

На сьогодні сформульовано три базові принципи інформаційної безпеки, завданнями якої є забезпечення:

цілісності даних – захист від збоїв, що ведуть до втрати інформації або її знищення;

конфіденційності інформації;

доступності інформації для авторизованих користувачів.

Інформаційна безпека досягається використанням набору технологій, стандартів і методів управління, які необхідні для захисту інформації. *Мета інформаційної безпеки* – забезпечити безперервність функціонування інформаційної інфраструктури і захистити дані та інфраструктуру від випадкового або навмисного втручання, що може стати причиною втрати даних або їх несанкціонованої зміни.

Для оцінювання стану захищеності ІІС використовується незалежне тестування на проникнення (тести подолання захисту). Суть зазначеного підходу полягає в санкціонованій спробі обійти існуючий комплекс засобів захисту ІІС МО України. Під час тестування аудитор виступає як зловмисник, мотивований на порушення інформаційної безпеки мережі.

Крім топології мережі та характеристик хостів (*хост* – будь-який комп'ютер, підключений до локальної або глобальної мережі), *вхідними даними* системи аналізу захищеності є:

граф атак з урахуванням вузьких місць у топології ІІС;

залежність сервісів (використовуються для визначення поширення шкоди);

модель порушника;

події, які відбуваються в системі;

слабкі місця системи, які визначаються на основі стандарту “Загальне перерахування слабких місць” (Common Weaknesses Enumeration, CWE).

Довідка. *Граф атак* – це граф, що представляє можливі послідовності дій порушника задля досягнення загроз (цілей). Такі послідовності дій називаються *трасами* (шляхами) атак.

Під *елементарною атакою* (atomic attack) розуміють використання порушником уразливості. Прикладом елементарної атаки, наприклад, є переповнення буфера служби SSH, що дає змогу віддалено отримати права адміністратора системи.

SSH (англ. Secure Shell – “безпечна оболонка”) – мережевий протокол прикладного рівня, який дає змогу виробляти віддалене управління операційною системою та тунелювання TCP-з’єднань (наприклад, для передавання файлів).

До *вихідних даних*, одержуваних унаслідок роботи системи аналізу захищеності, відносяться:

обчислені показники захищеності;

варіанти реагування, набір рекомендованих контрзаходів.

У межах цієї статті розглядається лише перша група вихідних даних, зокрема, показники захищеності.

Під час застосування показників захищеності враховуються можливі режими роботи системи: реального часу (online) та статичний (offline).

Перший накладає обмеження на час обчислень, що призводить до необхідності їх спрощення. Однак він дає змогу враховувати поточну безпекову ситуацію (події, конфігурацію системи тощо) і більш точно визначати напрямок розвитку атаки. *Другий* не має часових обмежень. У цьому разі можуть використовуватися історичні дані, і повністю будуватися та аналізуватись загальний граф атак і залежність сервісів. Такий режим дає змогу здійснювати повніше оцінювання.

На основі наведених аспектів можна виділити такі рівні системи оцінювання захищеності з відповідними показниками:

топологічний рівень;

рівень графу атак,

рівень порушника;

рівень подій

рівень системи.

Показники топологічного рівня визначаються адміністратором з урахуванням топології системи. Пропонується використовувати такі показники: вразливість хоста, критичність хоста, вразливість хоста до атак нульового дня.

На рівні графу атак використовуються показники ймовірності атаки та збитків від атаки.

На рівні порушника вводиться залежність від профілю порушника (включаючи його розташування та навички), що дає змогу сформувати профільний граф атак [6], який включає лише ті атаки, які може реалізувати цей порушник.

Рівень подій є актуальним у разі роботи системи оцінювання захищеності в реальному часі. Він дає змогу відстежувати розвиток атаки і профіль порушника відповідно до подій. При появі нових подій можна коригувати поточне місце порушника (хост і права доступу) на графі атак і можливі шляхи атаки (включаючи найбільш ймовірні), і отримувати таким чином точніше уявлення про розвиток атаки.

На рівні системи визначається загальний рівень захищеності системи та поверхня атаки.

Найбільш поширеними методиками оцінювання стану захищеності ІІС (ризику) є:

1) статична методика експрес-оцінювання рівня захищеності;

2) методика оцінювання рівня ризику атаки інформаційної інфраструктури;

3) методика, заснована на історичних даних.

У статті детально розглядається лише перша методика стосовно її адаптації до воєнного відомства. Інші дві методики розглядаються оглядово.

Методика експрес-оцінювання поєднує якісний і кількісний підходи до оцінювання ризиків та дає змогу визначити загальний рівень захищеності системи. Ризик визначається як результат імовірності загрози та наслідків її реалізації для системи.

Методика експрес-оцінювання включає визначення рівнів критичності хостів та атакуючих дій, обчислення шкоди від реалізації атакуючих дій, на їх основі знаходиться збиток від реалізації загроз і складність їх реалізації, потім обчислюється рівень ризику для всіх загроз і на його основі загальний рівень захищеності системи. На рис. 2 зображені основні етапи методики і відповідні показники захищеності.

Основною особливістю методики експрес-оцінювання, що базується на поведінці системи, є факт її орієнтованості на роботу в реальному часі.

У межах цієї методики обчислюються як показники рівня системи, так і додаткові показники захищеності, які не використовуються під час визначення інтегрального показника, але корисні для розуміння поточної ситуації.

Рис. 2. Основні етапи методики експрес-оцінювання рівня

Основні метрики захищеності та значна частина допоміжних метрик розраховуються на базі підходу CVSS (Common Vulnerability Scoring System – загальна система оцінювання вразливостей) [7].

Індекси *CVSS* поділені на три основні групи:

базові – визначають критичність вразливості та атакуючої дії, що реалізує цю вразливість;

часові – визначають актуальність уразливості в заданий час;

індекси, пов'язані з робочим оточенням – використовуються організаціями для розміщення пріоритетів під час планування дій щодо усунення вразливостей.

Індекси CVSS для атакуючих дій, що використовують різні вразливості програмного та апаратного забезпечення, можуть бути взяті безпосередньо із зовнішніх баз даних уразливостей, наприклад, бази *NVD* [8].

Розрахунок показників рівня системи

Показники рівня системи:

критичність (*Criticality)* хостів *h – C(h)*;

рівень критичності (*Severity)* атакуючих дій *a – S(a)*;

розмір збитків (*Mortality)* під час реалізації атаки з урахуванням критичності хоста – *M(a,h)*;

складність доступу (*Access Complexity)* для атакуючій дії *a – Ac(a)*, траси *S – Ac(S)* та загрози *(Threat, T) – Ac(T)*;

реалізованість (*Realization)* загрози *T – R(T)*;

рівень ризику *(Risk Level)* загрози *T – Rl(T)*;

рівень захищеності (*Security Level)* мережі, що аналізується – *Sl.*

Порядок розрахунку рівня захищеності системи передбачає виконання таких кроків.

1. Критичність хоста визначається проєктувальником (адміністратором) аналізованої комп'ютерної мережі на власний розсуд за трирівневою шкалою (*Високий, Середній, Низький*).

Максимальний рівень критичності встановлений для хостів, неправильне функціонування (або повне припинення функціонування) яких призводить до неможливості використання ресурсів мережі. Далі у бік зменшення рівня критичності йдуть робочі сервери, функціонування яких (кожного окремо) є дуже важливою складовою успішної роботи воєнного відомства. Мінімальний рівень критичності мають персональні робочі станції, порушення у роботі яких незначно впливають на процеси функціонування організації загалом.

2. Розрахунок критичності атакуючої дії $S(a)$ здійснюється на основі Національної бази вразливостей (NVD – National Vulnerability Database) з використанням узагальненої оцінки критичності атакуючої дії (*Base Score* – базовий бал) *Bs(a)* за допомогою підходу CVSS таким чином:

$$S(a)=\begin{cases} Низька, Bs(a)\in[0-3,9] \\ Середня, Bs(a)\in[4-6,9] \\ Висока, Bs(a)\in[7-10] \end{cases}.$$

Довідка. *NVD* включає бази даних контрольних списків безпеки, недоліків програмного забезпечення, пов'язаних з безпекою, неправильних конфігурацій, назв продуктів і показників впливу. Крім надання списку поширених уразливостей і ризиків (CVE), NVD оцінює вразливості за допомогою Загальної системи оцінювання вразливостей (CVSS), заснованої на наборі рівнянь з використанням таких показників, як складність доступу та доступність засобу захисту.

CVE (*Common Vulnerabilities and Exposures* – список поширених уразливостей і ризиків) – унікальна ідентифікація вразливостей та зв'язування конкретних версій кодових баз (наприклад, програмного забезпечення та спільних бібліотек) із цими вразливостями.

3. Розмір збитків, викликаних успішною реалізацією атакуючої дії з урахуванням рівня критичності атакованого хоста, розраховується згідно з Табл. 1.

Таблиця 1

Критичність хоста	**Рівень критичності атакуючої дії**		
	Високий	**Середній**	**Низький**
Високий	Високий	Високий	Середній
Середній	Високий	Середній	Низький
Низький	Середній	Низький	Низький

Розмір шкоди для хоста *h* з урахуванням його критичності, викликаного успішною реалізацією загрози, визначається її останньою атакуючою дією: $M(T)=M(a_T,h_T)$, де a_T – остання атакуюча дія в загрозі, h_T – хост, на який спрямована дія a_T.

Розмір збитків *M(T)* під час реалізації загрози *T* можна охарактеризувати таким чином:

Високий – зупинення критично важливих підрозділів, що призводить до суттєвих збитків для інформаційної інфраструктури, втрати функціональності;

Середній – короткочасне переривання роботи критичних процесів або систем, що призводить до функціональних обмежень в одному підрозділі;

Низький – перерва в роботі, що не викликає відчутних функціональних обмежень.

Проте можлива ситуація, коли порушником під час реалізації загрози було завдано набагато більшої шкоди комп'ютерної мережі, ніж розрахована за останньою атакуючою дією. Для врахування цієї ситуації необхідно ввести метрики максимального розміру шкоди під час реалізації траси *S* та загрози *T*, що розраховуються формулами:

$$M^{\max}(S)=\max_i\left(M(a_i,h_i)\right), i\in[1,N_S], a_i\in S,$$

$$M^{\max}(T)=\max_i\left(M(S_i)\right), i\in[1,N_T], S_i\in T,$$

де N_S – довжина траси (кількість атакуючих дій у трасі);

N_T – кількість трас, які реалізують загрозу *T*.

Для отримання якісної <u>*оцінки рівня ризику загрози*</u> необхідно оцінити ступінь можливості її реалізації (*Realization), R(T)* та скористатися методикою *FRAP* (Facilitated Risk Analysis Process – спрощений процес аналізу ризиків [9]) з використанням отриманого раніше розміру збитків *(Mortality)* під час реалізації загрози *M(T)*.

4. Для визначення <u>*ступеня можливості реалізації загрози*</u> використовується індекс *CVSS* "складність у доступі" з множини базових індексів *CVSS*, що задаються для кожної атакуючої дії у графі атак [6, 10]. Можливими значеннями цього індексу є:

Високий – існують умови на доступ, наприклад, специфічні часові рамки, специфічні обставини (специфічна конфігурація сервісу), взаємодія з людиною, що здійснює атаку;

Низький – немає специфічних умов доступу, тобто використання вразливості можливе завжди.

Тоді індекс "складність у доступі" для траси атак обчислюватиметься за формулою

$$Ac(S)=\begin{cases}Високий, \forall k\in[1,N]\ Ac(a_k)=Високий\\ Низький, \forall k\in[1,N]\ Ac(a_k)=Низький\end{cases}, S=\{a_i\}_{i=1}^{N},$$

де *S* – сценарій (траса) атаки;

N – довжина траси (кількість дій).

Розрахунок цього індексу для загрози (сукупності різних трас, які мають однакові першу та останню вершини) проводиться за формулою

$$Ac(T)=\begin{cases}Високий, \forall k\in[1,N_S]\ Ac(S_k)=Низький\\ Низький, \forall k\in[1,N_S]\ Ac(S_k)=Високий\end{cases},$$

де $T=\{S_k\}_{k=1}^{N_S}$ – загроза;

N_S – кількість різних трас, що реалізують загрозу *T*;

$S_k=\{a_i\}_{i=1}^{N_k}$ – траса атаки; N_k – кількість дій у трасі.

Тоді ступінь можливості реалізації загрози *T* розраховуватиметься за формулою

$$R(T)=\begin{cases} Високий,\ Ac(T)=Низький \\ Низький,\ Ac(T)=Високий \end{cases}.$$

5. Оцінка рівня ризику загрози формується відповідно до правила, яке задається матрицею ризиків (Табл. 2).

Таблиця 2

Ступінь можливості реалізації загрози	**Рівень серйозності (критичності) загрози**		
	Високий	**Середній**	**Низький**
Високий	**A**	**B**	**C**
Низький	**B**	**C**	**D**

Отримана оцінка рівня ризику може інтерпретуватися так:

Рівень A – пов'язані з ризиком дії (наприклад, упровадження нових засобів захисту інформації або усунення вразливостей) мають бути виконані негайно та обов'язково;

Рівень B – пов'язані з ризиком дії мають бути вжиті;

Рівень C – потрібен моніторинг ситуації (але безпосередніх заходів щодо протидії загрозі вживати, можливо, не треба);

Рівень D – ніяких дій у даний момент робити не потрібно.

Зважаючи на отримані якісні оцінки рівня ризику для всіх загроз ***рівень захищеності аналізованої інформаційної інфраструктури*** визначається таким чином:

$$Sl=\begin{cases} Зелений, \forall i\in[1,N]\ Rl(T_i)=D \\ Жовтий, \forall i\in[1,N]\ Rl(T_i)\le C \\ Оранжевий, \forall i\in[1,N]\ Rl(T_i)\le B \\ Червоний, \forall i\in[1,N]\ Rl(T_i)=A \end{cases}, \text{ де } D<C<B<A;\ N_T \text{ – кількість усіх загроз.} \quad (1)$$

Наведений порядок оцінювання рівня захищеності інформаційної інфраструктури дає змогу дійти висновку, що показник Sl характеризує лише якісний стан рівня захищеності. Проте під час потрапляння показника Sl в зони *A-C* мають бути вжиті певні міри захисту ІІС. Для застосування обґрунтованих заходів потрібно розрахувати додаткові показники захищеності для розуміння поточної ситуації і формування відповідних заходів.

До додаткових показників відносяться:

вразливість хоста;

слабкість хоста;

вразливість хоста до атак нульового дня;

відсоток систем без відомих критичних уразливостей;

поверхня атаки.

Для розрахунку вразливості та слабкості хоста використовується CVSS-підхід [7], а порядок розрахунку наведено у статті [11].

Для обчислення *вразливості хоста до атак нульового дня* використовується правило, яке засноване на припущенні, що чим слабший хост, тим вища ймовірність наявності на ньому невідомих уразливостей.

Довідка. "Нульовий день" – це загальний термін, що описує нещодавно виявлені вразливості у системі безпеки, які можуть бути використані зловмисниками для атаки на систему. Термін "нульовий день" показує, що постачальник або розробник щойно дізналися про вразливість, і вони мають "нуль днів" на її виправлення. Атака нульового відбувається внаслідок використання зловмисниками вразливості до того, як розробникам вдалося її виправити.

Поверхня атаки визначається як усі можливі шляхи розвитку атаки, з поточного становища порушника на графі атак та його навичок.

Відсоток хостів без відомих критичних уразливостей (під критичними розуміються вразливості, для яких базова оцінка CVSS "Висока") визначається так:

$$\left(K_{нку}/K\right)\cdot 100\%,$$

де $K_{нку}, K$ – кількість хостів без відомих критичних уразливостей і загальна кількість хостів відповідно.

Додаткові показники стосуються визначення стану захищеності хостів та на основі їх аналізу дають змогу застосувати певні заходи як для підвищення захищеності окремих (критичних) хостів, так і взагалі ІІС.

Розглянемо приклад формалізації процесу оцінювання показників захищеності ІІС МО України на базі застосування методики експрес-оцінювання.

Процес оцінювання якості функціонування конкретної складової (послуги) ІІС МО України можна подати у вигляді кортежу [12]

$$R = \left\langle M,\ K(t), U_{R_{in}}(t),\ D_R, U_{R_{out}}(t) \right\rangle,$$

де M – мета оцінювання;

$K(i)$ – показники якості системи (послуги), які потрібно оцінити;

$U_{R_{in}}(t)$ – вектор вхідних даних;

D_R – правило (оператор, алгоритм, методика тощо), за яким розраховуються показники якості;

$U_{R_{out}}(t)$ – вектор показників, які характеризують результати оцінювання;

t – дата здійснення контролю поточного стану системи (послуги).

Структурна схема методичного підходу оцінювання інтегрального показника захищеності ІІС та показників вразливості обраних хостів наведена на рис. 3.

Основні етапи оцінювання показників захищеності ІІС МО України можна визначити у такий спосіб:

Етап 1. *Визначення мети оцінювання*. Мета оцінювання – дослідження різних загроз безпеки та визначення "вузьких місць" (хостів, відповідальних за більшу кількість трас атак і вразливостей) для ухвалення рішення про необхідність реагування на основі застосування обґрунтованих контрзаходів.

Етап 2. *Вибір критеріїв* – інтегральний показник стану захищеності ІІС МО України та часткові показники захищеності хостів.

Як інтегральний показник використовується рівень захищеності аналізованої інформаційної інфраструктури *Security Level* (Sl) Для більш повного розуміння поточної ситуації розраховуються часткові показники:

вразливість хоста *Vulnerability* $V(h_k)$, h_k – k-й хост системи (k – номер хоста в системі $k = \overline{1,K}$);

слабкість хоста $W(h_k)$;

вразливість хоста до атак нульового дня $Z\_V(h_k)$;

відсоток хостів без відомих критичних уразливостей $\left(K_{нку}/K\right)\cdot 100\%$, $K_{нку}, K$ – кількість хостів без відомих критичних уразливостей та загальна кількість хостів відповідно.

Етап 3. *Структуризація даних*. *Вхідними даними* для розрахунків є:

кількість хостів K, які заплановані для оцінювання;

граф атак – формується з використанням методик, які містяться у актуалізованих базах даних та знань;

послідовність атаки на кожний з K хостів, які заплановано для перевірки з урахуванням даних про відомі місця їх вразливості i_k, $i_k = \overline{1, I_k}$, I_k – кількість слабких місць на k-му хості.

Правила розрахунку показників захищеності наведені у цій статті. До того ж використовується підхід *CVSS*.

Вихідні дані – обчислені показники захищеності:

$$Vulnerability(h_k);\quad Weakness(h_k);$$

$$Z\_Vulnerability(h_k);\ \left(K_{нку}/K\right)\cdot 100\%.$$

Етап 4. *Розроблення моделі оцінювання* – складається алгоритм оцінювання, результатом реалізації якого є вимір стану захищеності ІІС – вибираються відповідні шкали вимірів показників і привласнюється розраховане значення показників на цих шкалах. Усім досліджуваним властивостям системи (послуги) привласнюється певне значення на цих шкалах.

Етап 5. *Практична реалізація алгоритму* – усі досліджувані показники якості системи (послуги) порівнюються з базовими показниками і залежно від міри розходження формуються управлінські рішення стосовно утримання значень показників властивостей системи (послуги) або їх поліпшення.

Методика оцінювання рівня ризику атаки інформаційної інфраструктури. У загальному вигляді методика розрахунку містить кілька етапів. Рівень ризику атаки визначається як добуток імовірності успішної реалізації атаки на шкоду у разі успішної реалізації атаки. Імовірність успішної реалізації атаки визначається зважаючи на навички порушника (визначаються на основі рівня складності реалізованих атакуючих дій), надійності інформації про події безпеки (властивість системи виявлення вторгнень), критичності атаки (визначається на основі базової оцінки *CVSS*) та потенціалу атаки (визначається як відношення вже реалізованих кроків атаки до загальної кількості кроків в атаці). Збиток у разі успішної реалізації атаки включає власну шкоду (визначається на основі CVSS) та поширену шкоду (визначається з використанням залежностей сервісів). Отриманий у результаті рівень ризику використовується для прийняття рішення про необхідність реагування.

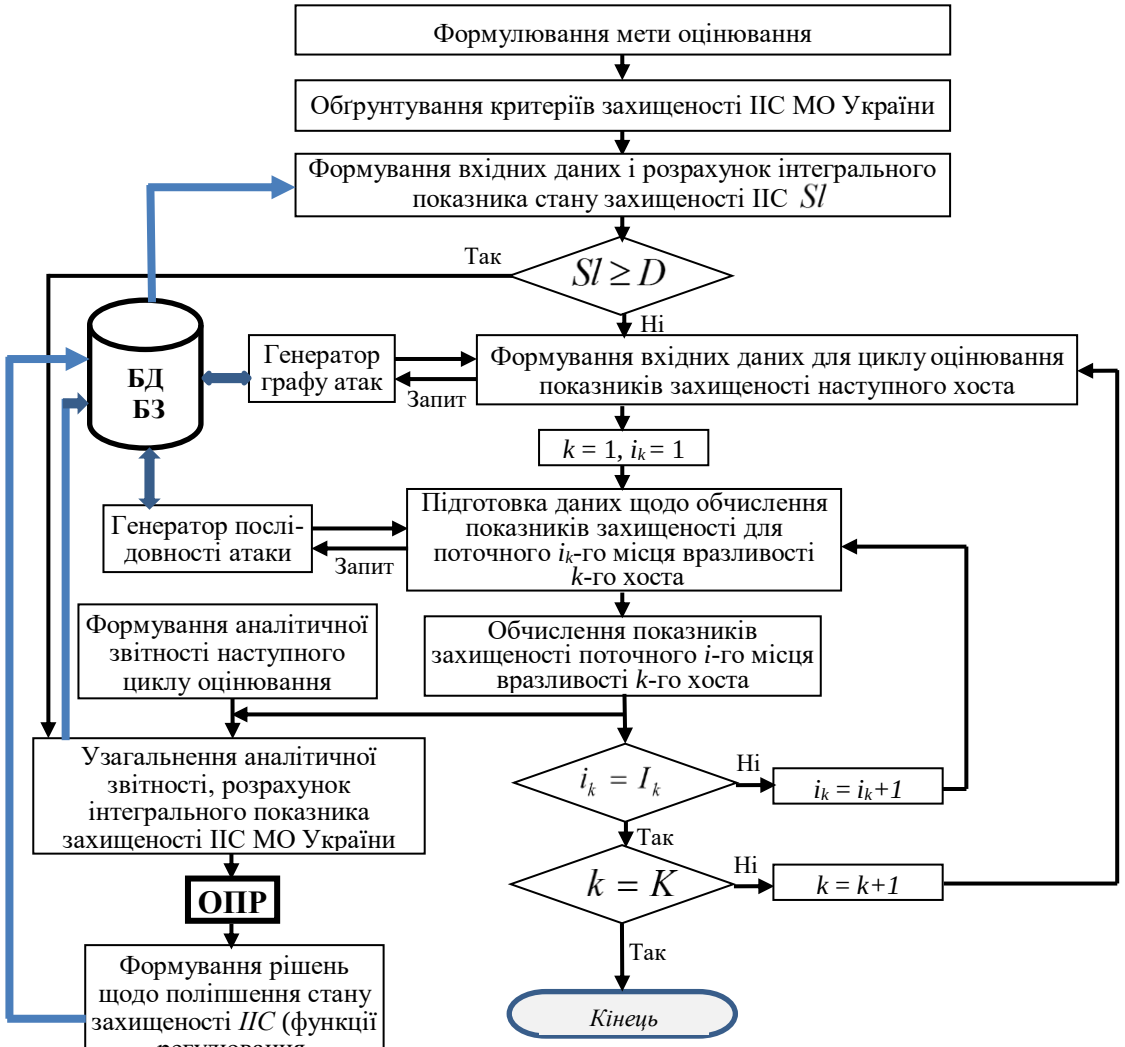

Рис. 3. Структурна схема методичного підходу оцінювання стану захищеності ІІС МО України

Методика, заснована на історичних даних, відрізняється від методики оцінювання рівня ризику інформаційної інфраструктури тим, що під час обчислення ймовірності атаки використовуються дані про попередні інциденти.

Висновки. Аналіз сучасних методик оцінювання характеристик стану захищеності інформаційної інфраструктури показав, що процедура оцінювання передбачає використання значної кількості апробованих стандартів і підходів (CVE, CVSS, NVD, FRAP, CWE, CWSS). Отже, для моніторингу рівня захищеності ІІС МО України потрібне залучення певної кількості фахівців. Це завдання має вирішуватись системою забезпечення функціонування ІІС.

Окремі дослідження доцільно присвятити розробленню методик формування графу і послідовності атак для практичної реалізації відповідних генераторів.

Запропонований методичний підхід дає змогу за наявності актуальних баз знань і даних автоматизувати процедури оцінювання стану захищеності ІІС МО України взагалі, та визначати часткові характеристики ризиків для елементів ІІС для забезпечення надійного захисту інформації, яка циркулює у телекомунікаційній мережі воєнного відомства.

Надалі доцільно здійснити детальний аналіз інших методик оцінювання рівня ризику атаки інформаційної інфраструктури для формування загальної методики моніторингу стану захищеності ІІС МО України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. Київ : НІСД, 2011. 30 с.
2. Інформаційна та кібербезпека: соціотехнічний аспект / В. Л. Бурячок, В. Б. Толубко,

В. О. Хорошко, С. В. Толюпа. Львів : Магнолія-2006, 2018. 320 с.
3. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві. *Економіка промисловості*. 2010. № 3. С. 123–129.
4. Радковець Ю. І., Левченко О. В., Косогов О. М. Погляди на створення системи інформаційної безпеки України та її Збройних Сил. *Наука і оборона*. 2014. № 1. С. 38–41.
5. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. *Сучасний захист інформації*. 2015. № 4. С. 86–90.
6. Котенко И. В., Степашкин М. В., Богданов В. С. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности. *Тр. СПИИРАН*. 2006. № 3, Т. 2. С. 30–49.
7. Common Vulnerability Scoring System. 2021. URL: https://ru.wikipedia.org/wiki/Common (дата звернення: 04.01.2022).
8. Сапожников А. Общий обзор реестров и классификаций уязвимостей (CVE, OSVDB, NVD, Secunia). *Информационная безопасность*. 2015. URL: https://safe-surf.ru/specialists/article/5228/607311/ (дата звернення: 04.01.2022).
9. Коротнев К. Методики управления рисками информационной безопасности и их оценки. *Отчет о глобальных рисках для человечества 2018* : Всемирный экономический форум в Давосе. 2018. URL: https://safe-surf.ru/specialists/article/5194/587935/ (дата звернення: 08.01.2022).
10. Колтик М. А. Характеристика особенностей построения модели угроз и нарушителей информации для объекта испытаний с использованием онтологии проведения испытаний КСЗИ. *"ИПС" НАН Украины*. 2015. № 1. С. 38–41.
11. Дойникова Е. В. Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов. *Тр. СПИИРАН*. 2013. № 3 (26). С. 123–129.
12. Прокопенко О. С., Рибидайло А. А. Модель управління кар'єрою військовослужбовців. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 3(70). С. 91–100.

Стаття надійшла до редакційної колегії 14.02.2022

Approaches to assessing the security of the information infrastructure of the Ministry of Defense of Ukraine

Annotation

Information infrastructure Ministry of Defense (MD) is a set of software and hardware, organizational systems and regulatory frameworks, which provides the organization of interaction of information flows, operation and development of information interaction and information space of the military department.

Ensuring the functioning of information infrastructure (IIS) means maintaining the state of its components, which allows timely and high-quality performance of certain functional tasks, in particular, information security.

Today, the issue of assessing the state of protection of IIS is relevant for the reasonable adoption of appropriate measures to maintain it at a certain level.

The purpose of the article is to substantiate the approach to assessing the characteristics of the state of protection of information infrastructure of the Ministry of Defense of Ukraine.

Analysis of modern methods of assessing the characteristics of the security of information infrastructure showed that the assessment procedure involves the use of a significant number of tested standards and approaches (CVE, CVSS, NVD, FRAP, CWE, CWSS). Therefore, monitoring the level of protection of the Ministry of Defense of Ukraine requires the involvement of a certain number of specialists. This task should be solved by the system of ensuring the functioning of the IIS.

The proposed methodological approach allows, in the presence of relevant knowledge bases and data to automate procedures for assessing the security of the IIS of the Ministry of Defense of Ukraine in general, and determine partial risk characteristics for elements of IIS to ensure reliable protection of information circulating in the telecommunications network of the military department.

In the future, it is advisable to analyze the methods of assessing the level of risk of information infrastructure attacks and assessing the level of risk of information infrastructure based on historical data to form a general methodology for monitoring the security of the Ministry of Defense of Ukraine.

Keywords: information infrastructure; the state of security of information infrastructure; indicators of the level of protection; count of attacks; methods of assessing security indicators.