УДК 621.391:004.056.53 (045)

МЕТОД МЕРЕЖЕВО-ЦЕНТРИЧНОГО МОНІТОРИНГУ КІБЕРІНЦИДЕНТІВ В СУЧАСНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Олександр Корченко, Віктор Гнатюк, Євгенія Іванченко, Сергій Гнатюк, Нургуль Сейлова

Процес впровадження інформаційно-комунікаційних технологій у більшості сфер сьогоденного суспільного життя спрямований на підвищення ефективності бізнес-процесів. Проте наявність уразливостей та кіберзагроз породжує кіберінциденти, для локалізації та нейтралізації яких необхідні ефективні методи виявлення, ідентифікації, оброблення та розслідування. Одним із підходів є застосування мережево-центричної концепції, яка орієнтована на протидію виникненню та ліквідації наслідків кіберінцидентів за допомогою засобів, об'єднаних інформаційними мережами в єдину систему. У роботі, на базі цієї концепції, запропоновано метод мережево-центричного моніторингу кіберінцидентів, який реалізується у 8 етапів: класифікація кібератак, виявлення типу кібератаки, категоризація кіберінцидентів, формування множини правил екстраполяції кіберінцидентів, визначення об'єктів захисту, визначення впливу кіберінцидентів на складові інформаційно-телекомунікаційних систем, визначення найбільш критичних складових інформаційно-телекомунікаційних систем, ранжування ступенів небезпеки кіберінцидентів. Цей метод дозволяє визначити найбільш важливі об'єкти захисту, а також прогнозувати категорії кіберінцидентів, які виникнуть внаслідок реалізації кібератаки, та їх рівень небезпеки (критичності). Крім того, цей метод та сформовані на його основі інструментальні засоби будуть корисними для команд реагування на кіберінциденти типу CERT/CSIRT для ефективної обробки кіберінцидентів (зокрема диспетчеризації) та адекватного на них реагування, а також для підрозділів, на які покладаються обов'язки щодо захисту інформаційно-телекомунікаційних систем як в межах підприємства, так і в межах держави.

Ключові слова: *кіберінцидент, інформаційно-телекомунікаційна система, мережево-центрична концепція, моніторинг, критичність, база KDD 99, CERT/CSIRT.*

Вступ. З огляду на динаміку розвитку та глобалізацію інформаційно-комунікаційних технологій (ІКТ), процес впровадження та використання ІКТ у більшості сфер сьогоденного суспільного життя набув неабиякої актуальності. Цей процес включає в себе: розвиток засобів інтерактивної комунікації та інформаційного обміну (соціальні мережі; електронний поштовий обмін; обмін миттєвими повідомленнями; відеозв'язок та Інтернет-телефонія); інформатизацію та автоматизацію виробничих процесів і більшості сфер суспільного життя (побудова локальних (корпоративних) обчислювальних мереж; систематизація інформації в базах даних; платформи для сумісної роботи користувачів; загальний доступ до ресурсів; VoIP та відеозв'язок; електронний документообіг; система управління взаємовідносинами з клієнтами (CRM); система планування ресурсів підприємства (ERP); система управління інформаційною безпекою; контроль та управління доступом); послуги Інтернет-банкінгу, електронну комерцію, миттєве переведення коштів тощо. Усі зазначені процедури, функціонування яких забезпечується ІКТ, є доволі критичними навіть для пересічного громадянина, в першу чергу, з точки зору інформації, яка в них циркулює. Виникнення *кіберінцидентів* (подій, які можуть порушити кібербезпеку (конфіденційність, цілісність та доступність інформації у кіберпросторі) [1]) і, як наслідок, порушення штатного режиму функціонування всієї системи можуть призвести до значних матеріальних збитків. Під виявленням, ідентифікацією, обробленням та розслідуванням кіберінцидентів будемо розуміти процеси відповідно до міжнародного стандарту [2].

Аналіз досліджень та постановка задачі. Сьогодні відомо багато робіт присвячених дослідженню систем виявлення несанкціонованих дій в ІКТ, наприклад, у [3] проведено порівняльний аналіз систем виявлення вторгнень (IDS) з використанням віртуальних приманок (Honeypot) останнього покоління Honeynet GenIII (Autograph, PADS, PAYL, COVERS, DIRA, DOME, Minos, Paid, Vigilante, HoneyStat тощо), що мають різні механізми виявлення атак та працюють з різними вхідними даними. Робота [4] містить ґрунтовний аналіз систем та засобів управління кризовими ситуаціями у різних галузях, що включає в себе прогнозування, ідентифікацію, оцінку кризових ситуацій та реагування на них. Хоча більшість розглянутих систем і базуються на застосуванні давачів (сенсорів) і зібраної статистики, проте такі системи не можливо використовувати в кіберпросторі з метою управління інформаційною (кібернетичною) безпекою, так як вони не оперують з реальними параметрами кіберпростору. З огляду на це, не є можливим прогнозування враження кіберінцидентами і конкретних складових інформаційно-телекомунікаційних систем (ІТС), як компонентів

кіберпростору і, як наслідок, не можливе управління протидією (контрзаходами) та ліквідацією наслідків різних категорій кіберінцидентів.

Мережево-центрична (Network-centric) теорія управління виникла у військовому середовищі не стільки в процесі теоретичних досліджень [5, 6], скільки внаслідок систематичного аналізу результатів впровадження в збройні сили нових бойових засобів і підвищення рівня освіченості особового складу. Останнім часом термін «мережево-центричний» все частіше використовується в різних галузях (цивільних), пов'язаних з використанням мережевих ІКТ у сфері управління, наприклад у [7] пропонується мережево-центричне управління кластерами ІКТ, у [8] розроблено універсальне програмоване комп'ютерне середовище мережево-центричного управління, а в [9] розглядається мережево-центричний підхід до ліквідації наслідків надзвичайних ситуацій. Проте, не зважаючи на очевидну аналогію із зазначеними галузями системи управління кіберінцидентами, на сьогодні відсутня загальна концепція і відповідні методи, моделі та системи мережево-центричного управління кіберінцидентами. З огляду на це, **метою** роботи є розробка методу мережево-центричного моніторингу кіберінцидентів, який на основі обробки динамічно змінюваних параметрів кіберпростору дозволить визначати об'єкти захисту та прогнозувати рівень небезпеки кіберінцидентів.

Концепція мережево-центричного моніторингу кіберінцидентів. Протидія виникненню та ліквідації наслідків кіберінцидентів за допомогою засобів, об'єднаних інформаційними мережами в єдину систему включає в себе: 1) постійний комп'ютерний моніторинг потенційно небезпечних місць та об'єктів для визначення необхідних заходів щодо ліквідації наслідків кожного виду можливих кіберінцидентів; 2) здійснення необхідних заходів з підготовки до боротьби з наслідками можливих груп кіберінцидентів; 3) формування цілей паралельної ліквідації можливих видів кіберінцидентів, їх синхронізацію, узгодження і ранжування; 4) реалізація паралельних стратегій цілей, їх синхронізацію і взаємодію використовуваних ресурсів; 5) формування можливого набору паралельних оперативних впливів, їх диспетчеризацію, синхронізацію і маневрування ресурсами в динаміці управління.

Відповідно до [9] у широкому розумінні під *моніторингом* розуміють систематичне накопичення та обробку даних про стан і динаміку зміни параметрів аналізованого об'єкта або процесу і представлення результатів у зручному для керівника або експерта вигляді. Завданням моніторингу при комплексному управлінні підготовкою до ліквідації наслідків різних категорій кіберінцидентів є своєчасна оцінка виникнення загроз кожної категорії кіберінцидентів, аналіз динаміки їх розвитку та їх комплексна оцінка. У динаміці це збір та аналіз даних про втрати від кіберінцидентів. *Мережево-центрична система моніторингу* об'єднує засоби моніторингу всіх рівнів і напрямків управління в єдине ціле. Вона повинна забезпечувати доведення всієї необхідної інформації до адресатів в реальному часі або близькому до нього в міру її отримання та, що дуже важливо, використовуючи інформацію, отриману на всіх рівнях і напрямах управління. Такий підхід дозволяє різко поліпшити розуміння сформованої ситуації керівниками усіх ступенів, підвищити рівень взаємодії і здійснювати синхронізацію зусиль по горизонталі і вертикалі управління. Необхідно зазначити, що порушення хоча б одного з перерахованих принципів може привести до серйозних ускладнень. Мережево-центрична концепція орієнтована не тільки на ефективне управління наявними технічними, фінансовими та іншими засобами, а й на досягнення інформаційної переваги в економіці, політиці, соціальній сфері і т.д., забезпечуючи здатність системи оперативно адаптуватися до швидкоплинної обстановки і переносити функції стратегічного та оперативного управління по вертикалі і горизонталі відповідно до потреб сформованої обстановки. Для цього мережево-центричний моніторинг повинен забезпечувати в реальному часі комплексний багаторівневий аналіз потоків окремих малоінформативних, а часто і суперечливих, первинних відомостей про появу нових об'єктів або процесів, а також динаміку зміни параметрів. Система повинна вміти змінювати логіку аналізу сформованої обстановки в міру зміни джерел інформації та отриманих нових даних про ситуацію. Вихід з ладу однієї або кількох локальних підсистем моніторингу не повинен призвести до колапсу всього мережево-центричного моніторингу.

При роботі команд реагування на кіберінциденти типу CERT/CSIRT [10] відповідно до зазначеної концепції встановлено послідовність (рис. 1): в ІТС відбувається певна *подія інформаційної безпеки* $E_1 \dots E_n$ (відповідно до [2] під подією інформаційної безпеки будемо розуміти ідентифіковану поведінку системи, сервісу чи мережі, яка вказує на можливе порушення інформаційної безпеки, політики, вихід з ладу засобів контролю чи

раніше невідома ситуація, яка може мати відношення до інформаційної безпеки), спричинена як *кібератаками* $CA_1 \dots CA_n$ [11], так і ненавмисними діями, що надходить на *сенсори* $S_1 \dots S_n$ (сенсорами у мережево-центричній системі моніторингу кіберінцидентів можуть бути джерела надходження інформації, зокрема системи виявлення / попередження вторгнень IDS/IPS, системи контролю цілісності, міжмережеві екрани, honeypot системи, системи аналізу уразливостей, експлойти, операційні системи, різні додатки (у тому числі спеціалізовані системи виявлення кіберінцидентів типу SIEM), антивірусні та антиспамові системи, звернення користувачів у системах типу Service Desk чи Help Desk тощо), що ідентифікують та фіксують кіберінциденти $I_1 \dots I_n$ за певним набором їх параметрів, порівнюючи з відповідними шаблонами.

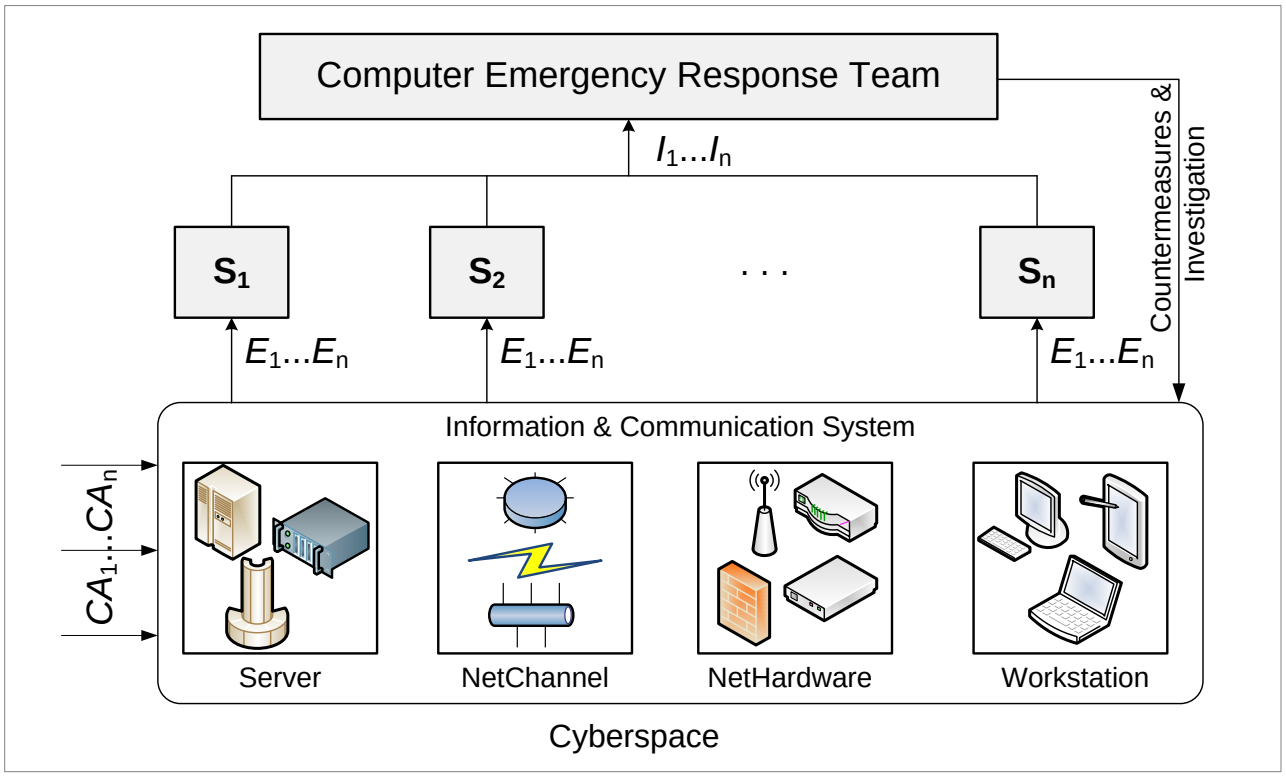


Рис. 1. Схема реалізації концепція мережево-центричного моніторингу кіберінцидентів

Мережево-центричний моніторинг визначається тим, що для кожної системи менеджменту кіберінцидентів формується мережа агентів (сенсорів). Загальну систему менеджменту кіберінцидентів регіону чи держави можна відобразити як складну мережу взаємопов'язаних центрів (команд) кампусного типу (рис. 2) [2], кожен з яких має можливість: мати чітко сформульовану мету функціонування; діяти відповідно до закладених при його створенні правил і алгоритмів; керувати базою даних, що містить необхідну йому інформацію; вміти використовувати результати моніторингу, реагуючи на них своїми діями; проявляти власну ініціативу; посилати і отримувати повідомлення від інших систем і вступати з ними у взаємодію.

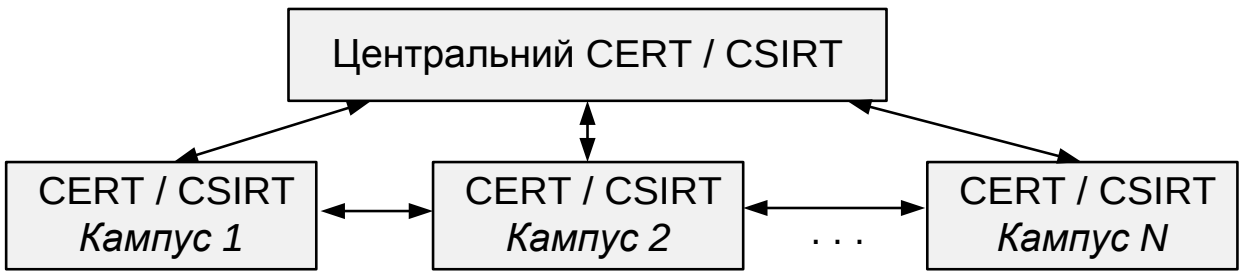


Рис. 2. Схема реалізації CERT/CSIRT кампусного типу

Побудована таким чином мережево-центрична система дозволяє зв'язати в єдиний інтерфейс управління, моніторингу і вироблення управляючих рішень всіх абонентів (посадових осіб), що

входять до її складу структурних підрозділів, програмні продукти, Web сторінки, мультимедіа, а також необхідні персональні дані для їх використання різними програмними застосунками незалежно від місцезнаходження абонентів мережі. При цьому обов'язковим є дотримання *основних принципів мережево-центричного управління* [9]: 1) всі елементи системи прив'язані до єдиного координатно-тимчасового поля, тобто діють в єдиному просторі станів; 2) дані для спільного використання надаються своєчасно і безперебійно; постійна підтримка систематичності спостережень за станом системи та потенційно-небезпечними об'єктами; 3) забезпечення своєчасності отримання, комплексності оброблення та використання поточної інформації, що надходить і зберігається; 4) система повинна бути самоорганізуючою, тобто здатна підтримувати, відновлюватись і адаптувати до нових умов свою структуру і поведінку, зокрема бути стійкою до часткових відмов вузлів мережі і ліній зв'язку; 5) система повинна бути відкритою, тобто обмінюватися ресурсами з середовищем тощо.

Метод мережево-центричного моніторингу кіберінцидентів. На основі зазначеної концепції метод мережево-центричного моніторингу кіберінцидентів у загальному вигляді базується на такій послідовності подій (рис. 3): ідентифіковані та класифіковані на декількох рівнях кібератаки (на основі порівняння поточних параметрів з параметрами, занесеними до баз шаблонів атак, наприклад *KDD 99* (2 рівні класифікації), *CAPEC* (4 рівні класифікації) тощо [12-14]) можуть спричинити кіберінциденти, які відносяться до однієї з категорій (у різних галузях ці категорії можуть бути різними, наприклад CERT-UA [15] визначає 7 категорій інцидентів, зазначених на рис. 3). Кіберінцидент, який може виникнути в результаті реалізації атаки, може потенційно нанести шкоду складовим *ITC* (сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле [16]), яких, наприклад, відповідно до [15] можна виділити 4. Визначення складових ІТС, які потребують захисту (об'єктів захисту) дозволить мінімізувати вплив на них кіберінцидентів. Крім того, у випадку одночасного виникнення інцидентів важливо спрогнозувати рівень їх небезпеки для більш ефективної обробки та адекватного реагування (розслідування) командами CERT/CSIRT.

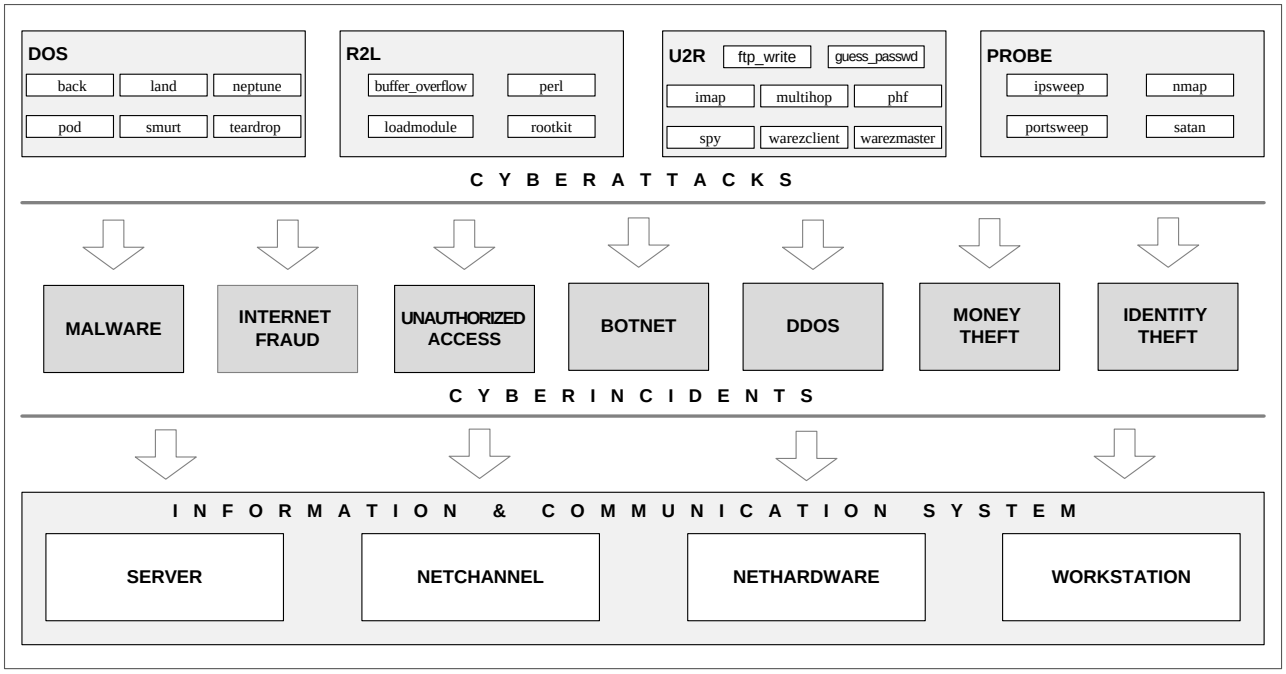


Рис. 3. Схема роботи методу мережево-центричного моніторингу кіберінцидентів у загальному вигляді

Запропонований метод мережево-центричного моніторингу кіберінцидентів реалізується у 8 етапів: класифікація кібератак, виявлення типу кібератаки, категоризація кіберінцидентів, формування множини правил екстраполяції кіберінцидентів, визначення об'єктів захисту, визначення впливу кіберінцидентів на складові ІТС, визначення найбільш критичних складових ІТС, ранжування ступенів небезпеки кіберінцидентів.

Етап 1 – Класифікація кібератак. Для реалізації цього етапу задамо множину еталонів параметрів кібератак **CA** , які можуть виникнути в ІТС:

$$\{\bigcup_{i=1}^{n}\mathbf{CA_i}\}=\{\mathbf{CA}_1,\mathbf{CA}_2,...,\mathbf{CA}_n\}, \quad (1)$$

де $\mathbf{CA_i}\subseteq\mathbf{CA}$, $(i=\overline{1,n})$, n – кількість кібератак, а

$$\mathbf{CA_i}=\{\bigcup_{j=1}^{m_i}\mathbf{CA_{ij}}\}=\{\mathbf{CA_{i1}},\mathbf{CA_{i2}},\ldots,\mathbf{CA}_{im_i}\}, \quad (2)$$

при цьому $\mathbf{CA_{ij}}$ $(j=\overline{1,m_i})$ – підмножини підкласів кібератак.

Зважаючи на (2) запишемо вираз (1) наступним чином:

$$\{\bigcup_{i=1}^{n}\mathbf{CA_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{CA_{ij}}\}\}= \quad (3)$$

$$=\{\{\mathbf{CA}_{11},\mathbf{CA}_{12},\ldots,\mathbf{CA}_{1m_1}\},\{\mathbf{CA}_{21},\mathbf{CA}_{22},\ldots,\mathbf{CA}_{2m_2}\},\ldots,\{\mathbf{CA}_{n1},\mathbf{CA}_{n2},\ldots,$$
$$\mathbf{CA}_{nm_n}\}\},\ (j=\overline{1,m_i}).$$

Підмножини підкласів кібератак $\mathbf{CA_{ij}}\subseteq\mathbf{CA_i}$ визначимо як:

$$\mathbf{CA_{ij}}=\{\bigcup_{s=1}^{r_{ij}}\mathbf{CA_{ijs}}\}=\{\mathrm{CA}_{ij1},\mathrm{CA}_{ij2},\ldots,\mathrm{CA}_{ijr_j}\}, \quad (4)$$

де CA_{ijs} $(s=\overline{1,r_{ij}})$ – параметри, що характеризують кібератаку $\mathbf{CA_{ij}}$; r_{ij} – кількість таких параметрів.

Тоді вираз (3) з урахуванням (4) отримає наступний вигляд

$$\{\bigcup_{i=1}^{n}\mathbf{CA_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{CA_{ij}}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_{ij}}CA_{ijs}\}\}\}=$$
$$=\{\{\{CA_{111},CA_{112},...,CA_{11r_1}\},\{CA_{121},CA_{122},...,CA_{12r_2}\},...,\{CA_{1m_11},CA_{1m_12},...,CA_{1m_1r_{m1}}\}\},$$
$$\{\{CA_{211},CA_{212},...,CA_{21r_1}\},\{CA_{221},CA_{222},...,CA_{22r_2}\},...,\{CA_{2m_21},CA_{2m_22},...,CA_{2m_2r_{m2}}\}\}, \quad (5)$$
$$...,$$
$$\{\{CA_{n11},CA_{n12},...,CA_{n1r_1}\},\{CA_{n21},CA_{n22},...,CA_{n2r_2}\},...,\{CA_{nm_n1},CA_{nm_n2},...,CA_{nm_nr_{mn}}\}\}\}.$$

Наприклад, використовуючи базу KDD 99, яка містить 5 млн. наборів параметрів кібератак та нормальної поведінки, при $n=4$, згідно виразу (1) отримаємо наступне:

$$\{\bigcup_{i=1}^{4}\mathbf{CA_i}\}=\{\mathbf{CA}_1,\mathbf{CA}_2,\mathbf{CA}_3,\mathbf{CA}_4\}=$$
$$=\{\mathbf{CA_{DOS}},\mathbf{CA_{R2L}},\mathbf{CA_{U2R}},\mathbf{CA_{PROBE}}\}= \quad (6)$$
$$=\{\mathbf{DOS},\mathbf{R2L},\mathbf{U2R},\mathbf{PROBE}\}.$$

де $\mathbf{CA}_1=\mathbf{CA_{DOS}}=\mathbf{DOS}$, $\mathbf{CA}_2=\mathbf{CA_{R2L}}=\mathbf{R2L}$, $\mathbf{CA}_3=\mathbf{CA_{U2R}}=\mathbf{U2R}$, $\mathbf{CA}_4=\mathbf{CA_{PROBE}}=\mathbf{PROBE}$ – класи кібератак з бази KDD 99. Розглянемо детальніше класи кібератак (табл. 1).

Таблиця 1

Кібератаки з KDD 99

Клас	Підклас
1. DOS	1.1. BACK, 1.2. LAND, 1.3. NEPTUNE, 1.4. POD, 1.5. SMURT, 1.6. TEARDROP
2. R2L	2.1. BUFFER_OVERFLOW, 2.2. PERL, 2.3. LOADMODULE, 2.4. ROOTKIT
3. U2R	3.1. FTP_WRITE, 3.2. GUESS_PASSWD, 3.3. IMAP, 3.4. MULTIHOP, 3.5. PHF, 3.6. SPY, 3.7. WAREZCLIENT, 3.8. WAREZMASTER
4. PROBE	4.1. IPSWEEP, 4.2. NMAP, 4.3. PORTSWEEP, 4.4. SATAN

Під зазначеними у табл. 1 класами відповідно до [15] будемо розуміти наступне:

*1. Denial of Service (**DOS**)* – кібератаки відмови систем від обслуговування, яка характеризується генеруванням великого об'єму трафіку, що призводить до перевантаження і блокування серверу (включає 6 підкласів кібератак);

*2. Remote to User (**R2L**)* – кібератаки, що характеризуються одержання доступу нелегітимним (незареєстрованим) користувачем несанкціонованого віддаленого доступу до інформації управління (включає 4 підкласи кібератак);

*3. User to Root (**U2R**)* – кібератаки, що передбачають несанкціоноване розширення повноважень нелегітимних (незареєстрованих) користувачів до рівня локального суперкористувача (адміністратора) (включає 8 підкласів кібератак);

*4. Probing (**PROBE**)* – кібератаки сканування портів з метою одержання конфіденційної інформації (включає 4 підкласи кібератак).

Використовуючи вираз (2), та дані з табл. 1, наприклад при $m_1 = 6,\ m_2 = 4,\ m_3 = 8,\ m_4 = 4$, отримаємо:

$$\mathbf{CA}_1 = \{\bigcup_{j=1}^{6} \mathbf{CA_{ij}}\} = \{\mathbf{CA_{1,1}}, \mathbf{CA_{1,2}}, \ldots, \mathbf{CA}_{1,6}\} =$$
$$= \{\mathbf{CA_{DOS,1}}, \mathbf{CA_{DOS,2}}, \ldots, \mathbf{CA_{DOS,6}}\} = \quad (7)$$
$$= \{\mathbf{DOS}_{BACK}, \mathbf{DOS}_{LAND}, \mathbf{DOS_{NEPTUNE}}, \mathbf{DOS_{POD}}, \mathbf{DOS_{SMURT}}, \mathbf{DOS}_{TEARDROP}\} =$$
$$= \mathbf{\{BACK, LAND, NEPTUNE, POD, SMURT, TEARDROP\}},$$

де $\mathbf{CA}_{1,1} = \mathbf{CA_{DOS,1}} = \mathbf{DOS}_{BACK} = \mathbf{BACK}$, $\mathbf{CA}_{1,2} = \mathbf{CA_{DOS,2}} = \mathbf{DOS}_{LAND} = \mathbf{LAND}$, $\mathbf{CA}_{1,3} = \mathbf{CA_{DOS,3}} = \mathbf{DOS_{NEPTUNE}} = \mathbf{NEPTUNE}$, $\mathbf{CA}_{1,4} = \mathbf{CA_{DOS,4}} = \mathbf{DOS_{POD}} = \mathbf{POD}$, $\mathbf{CA}_{1,5} = \mathbf{CA_{DOS,5}} = \mathbf{DOS_{SMURT}} = \mathbf{SMURT}$, $\mathbf{CA}_{1,6} = \mathbf{CA_{DOS,6}} = \mathbf{DOS}_{TEARDROP} = \mathbf{TEARDROP}$ – підкласи кібератак класу **DOS** відповідно до бази KDD 99 (табл. 1).

$$\mathbf{CA}_2 = \{\bigcup_{j=1}^{4} \mathbf{CA_{ij}}\} = \{\mathbf{CA_{1,1}}, \mathbf{CA_{1,2}}, \mathbf{CA_{1,3}}, \mathbf{CA}_{1,4}\} =$$
$$= \{\mathbf{CA}_{\mathrm{R2L},1}, \mathbf{CA}_{\mathrm{R2L},2}, \mathbf{CA}_{\mathrm{R2L},3}, \mathbf{CA}_{\mathrm{R2L},4}\} = \quad (8)$$
$$= \{\mathrm{R2L}_{BUFFER\_OVERFLOW}, \mathrm{R2L}_{PERL}, \mathrm{R2L}_{LOADMODULE}, \mathrm{R2L}_{ROOTKIT}\} =$$
$$= \mathbf{\{BUFFER\_OVERFLOW, PERL, LOADMODULE, ROOTKIT\}},$$

де $\mathbf{CA}_{1,1} = \mathbf{CA}_{\mathrm{R2L},1} = \mathrm{R2L}_{BUFFER\_OVERFLOW} = \mathbf{BUFFER\_OVERFLOW}$, $\mathbf{CA_{1,2}} = \mathbf{CA}_{\mathrm{R2L},2} = \mathrm{R2L}_{PERL} = \mathbf{PERL}$, $\mathbf{CA_{1,3}} = \mathbf{CA}_{\mathrm{R2L},3} = \mathbf{LOADMODULE}$, $\mathbf{CA}_{1,4} = \mathbf{CA}_{\mathrm{R2L},4} = \mathrm{R2L}_{ROOTKIT} = \mathbf{ROOTKIT}$ – підкласи кібератак класу R2L відповідно до бази KDD 99 (табл. 1).

$$\mathbf{CA}_3 = \{\bigcup_{j=1}^{8} \mathbf{CA_{ij}}\} = \{\mathbf{CA_{1,1}}, \mathbf{CA_{1,2}}, \ldots, \mathbf{CA}_{1,8}\} =$$
$$= \{\mathbf{CA}_{\mathrm{U2R},1}, \mathbf{CA}_{\mathrm{U2R},2}, \ldots, \mathbf{CA}_{\mathrm{U2R},8}\} = \quad (9)$$
$$= \{\mathrm{U2R}_{FTP\_WRITE}, \mathrm{U2R}_{GUESS\_PASSWD}, \mathrm{U2R}_{IMAP}, \mathrm{U2R}_{MULTIHOP},$$
$$\mathrm{U2R}_{PHF}, \mathrm{U2R}_{SPY}, \mathrm{U2R}_{WAREZCLIENT}, \mathrm{U2R}_{WAREZMASTER}\} =$$
$$= \mathbf{\{FTP\_WRITE, GUESS\_PASSWD, IMAP, MULTIHOP,}$$
$$\mathbf{PHF, SPY, WAREZCLIENT, WAREZMASTER}\},$$

де $\mathbf{CA}_{1,1} = \mathbf{CA}_{\mathrm{U2R},1} = \mathrm{U2R}_{FTP\_WRITE} = \mathbf{FTP\_WRITE}$, $\mathbf{CA}_{1,2} = \mathbf{CA}_{\mathrm{U2R},2} = \mathrm{U2R}_{GUESS\_PASSWD} = \mathbf{GUESS\_PASSWD}$, $\mathbf{CA}_{1,3} = \mathbf{CA}_{\mathrm{U2R},3} = \mathrm{U2R}_{IMAP} = \mathbf{IMAP}$, $\mathbf{CA}_{1,4} = \mathbf{CA}_{\mathrm{U2R},4} = \mathrm{U2R}_{MULTIHOP} = \mathbf{MULTIHOP}$, $\mathbf{CA}_{1,5} = \mathbf{CA}_{\mathrm{U2R},5} = \mathrm{U2R}_{PHF} = \mathbf{PHF}$, $\mathbf{CA}_{1,6} = \mathbf{CA}_{\mathrm{U2R},6} = \mathrm{U2R}_{SPY} = \mathbf{SPY}$, $\mathbf{CA}_{1,7} = \mathbf{CA}_{\mathrm{U2R},7} = \mathrm{U2R}_{WAREZCLIENT} = \mathbf{WAREZCLIENT}$, $\mathbf{CA}_{1,8} = \mathbf{CA}_{\mathrm{U2R},8} = \mathrm{U2R}_{WAREZMASTER} = \mathbf{WAREZMASTER}$ – підкласи кібератак класу U2R відповідно до бази KDD 99 (табл. 1).

$$\mathbf{CA}_4 = \{ \bigcup_{j=1}^{4} \mathbf{CA_{ij}} \} = \{ \mathbf{CA_{1,1}}, \mathbf{CA_{1,2}}, \mathbf{CA_{1,3}}, \mathbf{CA}_{1,4} \} =$$
$$= \{ \mathbf{CA}_{\mathrm{PROBE},1}, \mathbf{CA}_{\mathrm{PROBE},2}, \mathbf{CA}_{\mathrm{PROBE},3}, \mathbf{CA}_{\mathrm{PROBE},4} \} = \quad (10)$$
$$= \{\mathbf{PROBE_{IPSWEEP}}, \mathbf{PROBE_{NMAP}}, \mathbf{PROBE_{PORTSWEEP}}, \mathbf{PROBE_{SATAN}}\} =$$
$$= \{\mathbf{IPSWEEP}, \mathbf{NMAP}, \mathbf{PORTSWEEP}, \mathbf{SATAN}\},$$

де $\mathbf{CA}_{1,1} = \mathbf{CA}_{\mathrm{PROBE},1} = \mathbf{PROBE_{IPSWEEP}} = \mathbf{IPSWEEP}$, $\mathbf{CA_{1,2}} = \mathbf{CA}_{\mathrm{PROBE},2} = \mathbf{PROBE_{NMAP}} = \mathbf{NMAP}$, $\mathbf{CA_{1,3}} = \mathbf{CA}_{\mathrm{PROBE},3} = \mathbf{PROBE_{PORTSWEEP}} = \mathbf{PORTSWEEP}$, $\mathbf{CA}_{1,4} = \mathbf{CA}_{\mathrm{PROBE},4} = \mathbf{PROBE_{SATAN}} = \mathbf{SATAN}$ – підкласи кібератак класу **PROBE** відповідно до бази KDD 99 (табл. 1).

Кожна з атак, яка відноситься до одного із зазначених класів, представляється у вигляді кортежу параметрів [13]:

$$< D, PT, S, F, SB, DB, L, WF, U, H, NFL, LI, NC, RS, SA, NR, NFC, NS, NAF, NOC, IHL,$$
$$IGL, C, SC, SR, SSR, RR, SRR, SSER, DSR, SDHR, DHC, DHSC, DHSSR, DHDSR, DHSSPR, \quad (11)$$
$$DHSDHR, DHSR, DHSSR, DHRR, DHSRR > .$$

Усі параметри наведеного кортежу поділяються на 4 категорії [12, 13]: 1. Характеристики індивідуальних TCP-з'єднань (табл. 2); 2. Характеристики контенту (табл. 3); 3. Характеристики трафіку з використанням two-second time window (табл. 4); 4. Характеристики кінцевого хоста (табл. 5).

Таблиця 2

Опис характеристик індивідуальних TCP-з'єднань

Код	Назва	Опис	Тип даних
D	duration	тривалість з'єднання (в секундах)	неперервні
PT	protocol_type	тип протоколу, тобто tcp, udp тощо	дискретні
S	service	цільовий сервіс, що використовується, тобто http, telnet тощо	дискретні
SB	src_bytes	кількість байтів, переданих від джерела до приймача за одне з'єднання	неперервні
DB	dst_bytes	кількість байтів, переданих від приймача до джерела за одне з'єднання	неперервні
F	flag	статус з'єднання: нормальне, помилка	дискретні
L	land	якщо джерело та приймач має однакові номери портів, то параметр набуває значення «1», якщо не однакові – «0»	дискретні
WF	wrong_fragment	загальна кількість пошкоджених фрагментів у конкретному з'єднанні	неперервні
U	urgent	кількість термінових пакетів у конкретному з'єднанні. Терміновий пакет – це пакет, в якому активований біт терміновості URG	неперервні

Таблиця 3

Опис характеристик контенту

Код	**Назва**	**Опис**	**Тип даних**
H	hot	кількість «гарячих» індикаторів, що вміщує контент, наприклад, проникнення до системних директорій, створення та виконання програм	неперервні
NFL	num_failed_logins	кількість невдалих спроб авторизації	неперервні
LI	logged_in	статус авторизації: «1» – авторизація пройшла успішно, «0» – невдало	дискретні
NC	num_compromised	кількість скомпрометованих умов	неперервні
RS	root_shell	«1», якщо отримано права адміністратора, «0» – якщо ні	дискретні
SA	su_attempted	«1», якщо була спроба отримати або отримано права адміністратора, «0» – якщо ні	дискретні
NR	num_root	кількість адміністративного доступу, або кількість операцій, що виконуються від імені адміністратора в конкретному з'єднанні	неперервні
NFC	num_file_creations	кількість операцій створення файлів в конкретному з'єднанні	неперервні
NS	num_shells	кількість запитів на надання доступу до оболонки адміністрування	неперервні
NAF	num_access_files	кількість операцій над файлом контролю доступу	неперервні
NOC	num_outbound_cmds	кількість вихідних команд у ftp сесії	неперервні
IHL	is_hot_login	«1», якщо авторизація належить «гарячому» списку, тобто адміністраторам, «0» – якщо ні	дискретні
IGL	is_guest_login	«1», якщо авторизація належить гостьовому запису, «0» – якщо ні	дискретні

Таблиця 4

Опис характеристик трафіку з використанням two-second time window

Код	**Назва**	**Опис**	**Тип даних**
C	count	кількість під'єднань до цільового хоста протягом часового інтервалу в 2 с.	неперервні
SR	serror_rate	% з'єднань з помилкою типу SYN для даного хоста джерела	неперервні
RR	rerror_rate	% з'єднань з помилкою типу REJ для даного хоста джерела	неперервні
SSR	same_srv_rate	% з'єднань зі службою	неперервні
DSR	diff_srv_rate	% з'єднань з різними службами	неперервні
SC	srv_count	кількість під'єднань до поточної служби (номеру порта) за останні 2 с.	неперервні
SSER	srv_serror_rate	% з'єднань з помилкою типу SYN для даної служби джерела	неперервні
SRR	srv_rerror_rate	% з'єднань з помилкою типу REJ для даної служби джерела	неперервні
SDHR	srv_diff_host_rate	% з'єднань з різними хостами	неперервні

Використовуючи вирази (3-5) сформуємо значення $r_{ij}(i=\overline{1,n},\ j=\overline{1,m_i})$. Наприклад, для бази KDD 99 згідно таблиці 1-5 $r_{ij}=41(i=\overline{1,4},\ m_1=6,\ m_2=4,\ m_3=8,\ m_4=4)$. Якщо в якості **CA** виберемо множину еталонів параметрів з KDD 99, то $\mathbf{CA}=\mathbf{CA}_{KDD}$ і тоді отримаємо:

$$CA_{KDD} = \{\bigcup_{i=1}^{4} CA_i\} = \{\bigcup_{i=1}^{4}\{\bigcup_{j=1}^{m_i} CA_{ij}\}\} = \{\bigcup_{i=1}^{4}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{41} CA_{ijs}\}\}\} =$$

$$= \{\{\{CA_{1,1,1}, CA_{1,1,2}, ..., CA_{1,1,r_1}\}, \{CA_{1,2,1}, CA_{1,2,2}, ..., CA_{1,2,r_2}\}, ..., \{CA_{1,m_1,1}, CA_{1,m_1,2}, ..., CA_{1,m_1,r_{m1}}\}\},$$
$$\{\{CA_{2,1,1}, CA_{2,1,2}, ..., CA_{2,1,r_1}\}, \{CA_{2,2,1}, CA_{2,2,2}, ..., CA_{2,2,r_2}\}, ..., \{CA_{2,m_2,1}, CA_{2,m_2,2}, ..., CA_{2,m_2,r_{m2}}\}\}, ...,$$
$$\{\{CA_{n,1,1}, CA_{n,1,2}, ..., CA_{n,1,r_1}\}, \{CA_{n,2,1}, CA_{n,2,2}, ..., CA_{n,2,r_2}\}, ..., \{CA_{n,m_n,1}, CA_{n,m_n,2}, ..., CA_{n,m_n,r_{mn}}\}\}\} =$$

$$= \{\{\{CA_{1,1,1}, CA_{1,1,2}, ..., CA_{1,1,41}\}, \{CA_{1,2,1}, CA_{1,2,2}, ..., CA_{1,2,41}\}, ..., \{CA_{1,6,1}, CA_{1,6,2}, ..., CA_{1,6,41}\}\},$$
$$\{\{CA_{2,1,1}, CA_{2,1,2}, ..., CA_{2,1,41}\}, \{CA_{2,2,1}, CA_{2,2,2}, ..., CA_{2,2,41}\}, ..., \{CA_{2,4,1}, CA_{2,4,2}, ..., CA_{2,4,41}\}\},$$
$$\{\{CA_{3,1,1}, CA_{3,1,2}, ..., CA_{3,1,41}\}, \{CA_{3,2,1}, CA_{3,2,2}, ..., CA_{3,2,41}\}, ..., \{CA_{3,8,1}, CA_{3,8,2}, ..., CA_{3,8,41}\}\},$$
$$\{\{CA_{4,1,1}, CA_{4,1,2}, ..., CA_{4,1,41}\}, \{CA_{4,2,1}, CA_{4,2,2}, ..., CA_{4,2,41}\}, ..., \{CA_{4,4,1}, CA_{4,4,2}, ..., CA_{4,4,41}\}\}\} =$$

$$= \{\{\{ CA_{DOS,1,1}, CA_{DOS,1,2}, ..., CA_{DOS,1,41} \}, \{ CA_{DOS,2,1}, CA_{DOS,2,2}, ..., CA_{DOS,2,41} \}, ..., \{ CA_{DOS,6,1},$$
$$CA_{DOS,6,2}, ..., CA_{DOS,6,41} \}\},$$
$$\{\{ CA_{R2L,1,1}, CA_{R2L,1,2}, ..., CA_{R2L,1,41} \}, \{ CA_{R2L,2,1}, CA_{R2L,2,2}, ..., CA_{R2L,2,41} \}, ..., \{ CA_{R2L,4,1},$$
$$CA_{R2L,4,2}, ..., CA_{R2L,4,41} \}\},$$
$$\{\{ CA_{U2R,1,1}, CA_{U2R,1,2}, ..., CA_{U2R,1,41} \}, \{ CA_{U2R,2,1}, CA_{U2R,2,2}, ..., CA_{U2R,2,41} \}, ..., \{ CA_{U2R,8,1},$$
$$CA_{U2R,8,2}, ..., CA_{U2R,8,41} \}\},$$
$$\{\{ CA_{PROBE,1,1}, CA_{PROBE,1,2}, ..., CA_{PROBE,1,41} \}, \{ CA_{PROBE,2,1}, CA_{PROBE,2,2}, ..., CA_{PROBE,2,41} \}, ...,$$
$$\{ CA_{PROBE,4,1}, CA_{PROBE,4,2}, ..., CA_{PROBE,4,41} \}\} =$$

$$= \{\{\{ DOS_{BACK,1}, DOS_{BACK,2}, ..., DOS_{BACK,41} \}, \{ DOS_{LAND,1}, DOS_{LAND,2}, ..., DOS_{LAND,41} \}, ...,$$
$$\{ DOS_{TEARDROP,1}, DOS_{TEARDROP,2}, ..., DOS_{TEARDROP,41} \}\},$$
$$\{\{ R2L_{BUFFER\_OVERFLOW,1}, R2L_{BUFFER\_OVERFLOW,2}, ..., R2L_{BUFFER\_OVERFLOW,41} \}, \{ R2L_{PERL,1},$$
$$R2L_{PERL,2}, ..., R2L_{PERL,41} \}, ...,$$
$$\{ R2L_{ROOTKIT,1}, R2L_{ROOTKIT,2}, ..., R2L_{ROOTKIT,41} \}\}, \quad (12)$$
$$\{\{ U2R_{FTP\_WRITE,1}, U2R_{FTP\_WRITE,2}, ..., U2R_{FTP\_WRITE,41} \}, \{ U2R_{GUESS\_PASSWD,1},$$
$$U2R_{GUESS\_PASSWD,2}, ..., U2R_{GUESS\_PASSWD,41} \}, ...,$$
$$\{ U2R_{WAREZMASTER,1}, U2R_{WAREZMASTER,2}, ..., U2R_{WAREZMASTER,41} \}\},$$
$$\{\{ PROBE_{IPSWEEP,1}, PROBE_{IPSWEEP,2}, ..., PROBE_{IPSWEEP,41} \},$$
$$\{ PROBE_{NMAP,1}, PROBE_{NMAP,2}, ..., PROBE_{NMAP,41} \}, ...,$$
$$\{ PROBE_{SATAN,1}, PROBE_{SATAN,2}, ..., PROBE_{SATAN,41} \}\} =$$

$$= \{\{\{ DOS_{BACK,D}, DOS_{BACK,PT}, ..., DOS_{BACK,DHSRR} \}, \{ DOS_{LAND,D},$$
$$DOS_{LAND,PT}, ..., DOS_{LAND,DHSRR} \}, ...,$$
$$\{ DOS_{TEARDROP,D}, DOS_{TEARDROP,PT}, ..., DOS_{TEARDROP,DHSRR} \}\},$$
$$\{\{ R2L_{BUFFER\_OVERFLOW,D}, R2L_{BUFFER\_OVERFLOW,PT}, ...,$$
$$R2L_{BUFFER\_OVERFLOW,DHSRR} \}, \{ R2L_{PERL,D}, R2L_{PERL,PT}, ..., R2L_{PERL,DHSRR} \}, ...,$$
$$\{ R2L_{ROOTKIT,D}, R2L_{ROOTKIT,PT}, ..., R2L_{ROOTKIT,DHSRR} \}\},$$
$$\{\{ U2R_{FTP\_WRITE,D}, U2R_{FTP\_WRITE,PT}, ..., U2R_{FTP\_WRITE,DHSRR} \}, \{ U2R_{GUESS\_PASSWD,D},$$
$$U2R_{GUESS\_PASSWD,PT}, ..., U2R_{GUESS\_PASSWD,DHSRR} \}, ...,$$
$$\{ U2R_{WAREZMASTER,D}, U2R_{WAREZMASTER,PT}, ..., U2R_{WAREZMASTER,DHSRR} \}\},$$
$$\{\{ PROBE_{IPSWEEP,D}, PROBE_{IPSWEEP,PT}, ..., PROBE_{IPSWEEP,DHSRR} \},$$
$$\{ PROBE_{NMAP,D}, PROBE_{NMAP,PT}, ..., PROBE_{NMAP,DHSRR} \}, ...,$$
$$\{ PROBE_{SATAN,D}, PROBE_{SATAN,PT}, ..., PROBE_{SATAN,DHSRR} \}\} =$$

$$= \{\{\{ BACK_D, BACK_{PT}, ..., BACK_{DHSRR} \}, \{ LAND_D, LAND_{PT}, ..., LAND_{DHSRR} \}, ...,$$
$$\{ TEARDROP_D, TEARDROP_{PT}, ..., TEARDROP_{DHSRR} \}\},$$
$$\{\{ BUFFER\_OVERFLOW_D, BUFFER\_OVERFLOW_{PT}, ..., BUFFER\_OVERFLOW_{DHSRR} \},$$
$$\{ PERL_D, PERL_{PT}, ..., PERL_{DHSRR} \}, ...,$$
$$\{ ROOTKIT_D, ROOTKIT_{PT}, ..., ROOTKIT_{DHSRR} \}\},$$
$$\{\{ FTP\_WRITE_D, FTP\_WRITE_{PT}, ..., FTP\_WRITE_{DHSRR} \},$$
$$\{ GUESS\_PASSWD_D, GUESS\_PASSWD_{PT}, ..., GUESS\_PASSWD_{DHSRR} \}, ...,$$
$$\{ WAREZMASTER_D, WAREZMASTER_{PT}, ..., WAREZMASTER_{DHSRR} \}\},$$
$$\{\{ IPSWEEP_D, IPSWEEP_{PT}, ..., IPSWEEP_{DHSRR} \}, \{ NMAP_D, NMAP_{PT}, ..., NMAP_{DHSRR} \}, ...,$$
$$\{ SATAN_D, SATAN_{PT}, ..., SATAN_{DHSRR} \}\},$$

Таблиця 5

Опис характеристик кінцевого хоста

Код	Назва	Опис	Тип даних
DHC	dst_host_count	кількість з'єднань з хостом	неперервні
DHSC	dst_host_srv_count	кількість з'єднань зі службою	неперервні
DHSSR	dst_host_same_srv_rate	% з'єднань з цією службою на даному хості	неперервні
DHDSR	dst_host_diff_srv_rate	% з'єднань з різними службами на даному хості	неперервні
DHSSPR	dst_host_same_src_port_rate	% з'єднання з цим хостом при поточному номері порта джерела	неперервні
DHSDHR	dst_host_srv_diff_host_rate	% з'єднань зі службою різних хостів	неперервні
DHSR	dst_host_serror_rate	% з'єднань з помилкою типу SYN для цього хоста приймача	неперервні
DHSSR	dst_host_srv_serror_rate	% з'єднань з помилкою типу SYN для цієї служби приймача	неперервні
DHRR	dst_host_rerror_rate	% з'єднань з помилкою типу REJ для цієї хоста приймача	неперервні
DHSRR	dst_host_srv_rerror_rate	% з'єднань з помилкою типу REJ для цієї служби приймача	неперервні

де $\mathbf{CA_{1,1,1}} = \mathbf{CA_{DOS},_{1,1}} = \mathbf{DOS_{BACK},_{1}} = \mathbf{DOS_{BACK},_{D}} = \mathbf{BACK}_{D}$, $\mathbf{CA_{1,1,2}} = \mathbf{CA_{DOS},_{1,2}} = \mathbf{DOS_{BACK},_{2}} = \mathbf{DOS_{BACK},_{PT}} = \mathbf{BACK}_{PT}$, $\mathbf{CA_{1,1,r_1}} = \mathbf{CA_{1,1,41}} = \mathbf{CA_{DOS},_{1,41}} = \mathbf{DOS_{BACK},_{41}} = \mathbf{DOS_{BACK},_{DHSRR}} = \mathbf{BACK}_{DHSRR}$, … , $\mathbf{CA_{n,m_n,1}} = \mathbf{CA_{4,4,1}} = \mathbf{CA_{PROBE},_{4,1}} = \mathbf{PROBE_{SATAN},_{1}} = \mathbf{PROBE_{SATAN,}}_{D} = \mathbf{SATAN}_{D}$, $\mathbf{CA_{n,m_n,2}} = \mathbf{CA_{4,4,2}} = \mathbf{CA_{PROBE},_{4,2}} = \mathbf{PROBE_{SATAN},_{2}} = \mathbf{PROBE_{SATAN,}}_{PT} = \mathbf{SATAN}_{PT}$, $\mathbf{CA_{n,m_n,r_{mn}}} = \mathbf{CA_{4,4,41}} = \mathbf{CA_{PROBE},_{4,41}} = \mathbf{PROBE_{SATAN},_{41}} = \mathbf{PROBE_{SATAN,}}_{DHSRR} = \mathbf{SATAN}_{DHSRR}$ - підмножини параметрів підкласів кібератак.

Відповідно до множини еталонів параметрів (8) сформуємо множину поточних параметрів $\mathbf{SP}$, зафіксованих сенсорами за часовий проміжок τ:

$$\mathbf{SP}^{\tau} = \{\bigcup_{z=1}^{q} \mathbf{SP}_z^{\tau}\} = \{SP_1^{\tau}, SP_2^{\tau}, ..., SP_q^{\tau}\}, \quad (13)$$

де $(z = \overline{1,q})$, q – кількість поточних параметрів.

Для прикладу, використовуючи вираз (13) для часткового випадку [13], де $r_{ij} = q = 41(\forall i,j)$ з урахуванням (11), отримаємо:

$$\mathbf{SP}^{\tau} = \{\bigcup_{z=1}^{41} \mathbf{SP}_z^{\tau}\} = \{SP_1^{\tau}, SP_2^{\tau}, ..., SP_{41}^{\tau}\} = \{D^{\tau}, PT^{\tau}, ..., DHSRR^{\tau}\}. \quad (14)$$

Етап 2 – Виявлення типу кібератаки. Для порівняння зафіксованих сенсорами поточних параметрів з параметрами еталонних кібератак введемо логічну функцію еквівалентності:

$$E(x,y) = \begin{cases} 1, при\ x = y, \\ 0, при\ x \neq y. \end{cases} \quad (15)$$

Наприклад, за часовий проміжок $\tau = 1$ до системи надходить набір сигнатур параметрів, виміряних давачами в ІТС (опис параметрів наведено у табл. 2-5):

$\mathbf{SP^1}$={184, tcp, telnet, SF, 1511, 2957, 0, 0, 0, 3, 0, 1, 2, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0.00, 0.00, 0.00, 0.00, 1.00, 0.00, 0.00, 1, 3, 1.00, 0.00, 1.00, 0.67, 0.00, 0.00, 0.00, 0.00}.

Категоризація кібератак відбувається шляхом співставлення вхідних даних $\mathbf{SP}$ з шаблонами атак (згідно (12)), порівнюючи за кожним з наведених в (11) параметрів із використанням функції еквівалентності (15). У результаті чого було класифіковано кібератаку класу *R2L* підкласу *buffer_overflow*.

Етап 3 – Категоризація кіберінцидентів. Для реалізації цього етапу задамо множину кіберінцидентів $\mathbf{I}$, які можуть виникнути в результаті реалізації кібератак CA:

$$\mathbf{I} = \{\bigcup_{i=1}^{n} \mathbf{I}_i\} = \{\mathbf{I}_1, \mathbf{I}_2, ..., \mathbf{I}_n\}, \ (i = \overline{1,n}), \qquad (16)$$

де n – кількість можливих видів кіберінцидентів.

Для прикладу, відповідно до найбільш розповсюджених видів сучасних комп'ютерних загроз згідно [11] під категоріями кіберінцидентів будемо розуміти (табл. 6):

Таблиця 6

Категорії кіберінцидентів згідно CERT-UA

Код	Категорія	Короткий опис	Дефініція
MW	Malware	Враження ГТС вірусами та ін. шкідливим програмним забезпеченням	Один із найбільш розповсюджених способів ураження є drive-by завантаження – ураження комп'ютера при відвідуванні користувачем шкідливого веб-сайту. Віруси: мережеві хробаки (networm) підклас вірусів, що інфікують комп'ютери та шукають способи для розповсюдження по мережі, створюючи свої копії; троянські програми (trojan) програми, призначенні для прихованого (під виглядом чогось іншого) проникнення до системи, зазвичай, зі зловмисними намірами; руткіти (rootkit) набір програм, призначених для приховування факту «присутності» зловмисників у системі (комп'ютері); клавіатурні шпигуни (keylogger) забезпечують фіксацію всіх переривань, що надходять у систему вводу під час натискання клавіш на клавіатурі; рекламні системи (adware) шкідливе програмне забезпечення, призначене для нав'язування реклами, шляхом, як приклад, блокування дій користувача за допомогою «випливаючого вікна», що містить рекламні матеріали)
IF	Internet Fraud	Реалізація Інтернет-шахрайства	Фішинг (phishing) атака полягає у спонуканні користувача ввести свої аутентифікаційні дані (логін, пароль, банківську інформації) та іншу інформацію шляхом запевнення останніх щодо достовірності та справжності хибних (спеціально створених для цього) мережевих ресурсів (в тому числі просто посилань, за якими потрібно перейти), таких як пошта, веб-сайти, призначені для Інтернет-банкінгу, сторінки авторизації у соціальних мережах тощо; вішинг (vishing) вид шахрайства, що полягає в отриманні у користувача під час телефонної розмови, шляхом використання різних методів переконання, необхідної зловмиснику інформації. Один із різновидів «соціальної інженерії»
UA	Unauthorized Access	НСД до інформаційних ресурсів та ГТС	Цілеспрямована хакерська атака – дії, що спрямовані на порушення штатного режиму функціонування системи, порушення доступності її сервісів (компонентів), отримання несанкціонованого доступу до конфіденційної інформації, порушення цілісності інформації тощо; дефейс атака полягає у зміні змісту головної сторінки вебсайту, в результаті чого при його відвідуванні замість звичного контенту відображається щось інше (написи «hacked by», нецензурні або провокаційні фрази/малюнки тощо)
BN	Botnet	Бот-мережі	Сукупність комп'ютерів, уражених шкідливим програмним забезпеченням, ресурси яких (як інформаційні, так і виробничі) через спеціальні командно-контрольні сервери (C&C) несанкціоновано використовуються зловмисниками (ZeuS, SpyEye, Carberp, Rustock, Kelihos, Pandora, BlackEnergy)
DD	DDoS	Реалізація DDoS-атаки	Розподілена мережева атака, яка за допомогою численної кількості джерел має на меті порушити доступність сервісу (автоматизованої системи) шляхом вичерпання його обчислювальних ресурсів
MT	Money Theft	Крадіжка коштів	Незаконне заволодіння коштами особи, що реалізується зловмисниками з використанням ресурсів кіберпростору
IT	Identity Theft	«Крадіжка особистості»	Несанкціоноване заволодіння персональними даними особи, що дозволяє зловмиснику здійснювати діяльність (підписувати документи, отримувати доступ до ресурсів, користуватися послугами тощо) від її імені (як один із механізмів підтвердження автентичності особи може використовуватись електронний цифровий підпис)

Отже, використовуючи вираз (16) та дані з табл. 6, при $n = 7$ отримаємо:

$$\mathbf{I} = \{\bigcup_{i=1}^{7} \mathbf{I_i}\} = \{I_1, I_2, I_3, I_4, I_5, I_6, I_7\} = \\ = \{I_{MW}, I_{IF}, I_{UA}, I_{BN}, I_{DD}, I_{MT}, I_{IT}\} = \\ = \{MW, IF, UA, BN, DD, MT, IT\}, \quad (17)$$

де $I_1 = I_{MW} = MW$, $I_2 = I_{IF} = IF$, $I_3 = I_{UA} = UA$, $I_4 = I_{BN} = BN$, $I_5 = I_{DD} = DD$, $I_6 = I_{MT} = MT$, $I_7 = I_{IT} = IT$ – категорії кіберінцидентів.

Етап 4 – Формування множини правил екстраполяції кіберінцидентів. Для реалізації цього етапу необхідно сформувати множину базових правил **R** [6]:

$$\mathbf{R} = \{\bigcup_{i=1}^{g} \mathbf{R_i}\} = \{\mathbf{R_1}, \mathbf{R_2}, ..., \mathbf{R}_g\}, (i = \overline{1,g}), \quad (18)$$

де g – кількість базових правил.

Аналогічно підходу, описаному в [17-20], на базі експертного оцінювання (що не вимагає великих часових затрат на формування статистичних даних) формується множина правил (17), що встановлює зв'язки між підкласом реалізованої кібератаки **CA** та категорією кіберінцидента **I**.

Використовуючи підкласи кібератак (етап 1), реалізація яких може призвести до виникнення кіберінцидентів (етап 3) та зважаючи на (17) експерти розраховують значення ймовірностей $PR_{CA_1 I_1} \dots PR_{CA_m I_n}$ (нормоване від 0 до 1 або у відсотках**)** виникнення кіберінциденту при реалізації конкретного класу кібератаки (19):

$$PR = \begin{vmatrix} PR_{CA_1 I_1} & PR_{CA_1 I_2} & \dots & PR_{CA_1 I_n} \\ PR_{CA_2 I_1} & PR_{CA_2 I_2} & \dots & PR_{CA_2 I_n} \\ \dots & \dots & \dots & \dots \\ PR_{CA_m I_1} & PR_{CA_m I_2} & \dots & PR_{CA_m I_n} \end{vmatrix}. \quad (19)$$

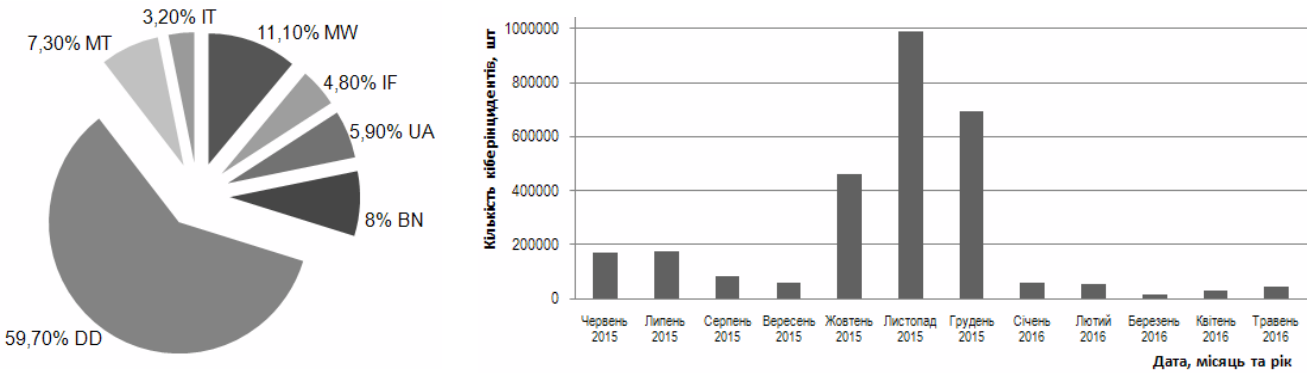
Таким чином, використовуючи статистику, що описує емпіричні дані щодо виникнення кіберінцидентів у результаті реалізації кібератак, експертами формуються значення ймовірності $PR_{CA_1 I_1} \dots PR_{CA_m I_n}$, а також відповідна множина правил **R** (17), які представляються у такому вигляді:

$$R_g = (PR_{CA_m}^{I_n} \geq PR_{lim}) \rightarrow I_n, \quad (20)$$

де PR_{lim} - це граничне значення ймовірності, за якого експерт впевнений у виникненні кіберінциденту **I** внаслідок реалізації кібератаки **CA** (визначається на основі аналізу статистики кіберінцидентів).

Наприклад, при m=22 (етап 1), n=7 (етап 3) експерти на базі статистики кіберінцидентів вітчизняного оператора стільникового зв'язку за останній рік (рис. 4) заповнюють матрицю (19) встановлюючи зв'язок між підкласом визначеної на етапі 2 кібератаки *buffer_overflow* і категоріями кіберінцидентів, які були визначені (17) на етапі 3 (табл. 7). Таким чином, формуються ймовірності $PR_{buffer\_overflow}^{MW}, PR_{buffer\_overflow}^{IF}, \dots, PR_{buffer\_overflow}^{IT}$ з огляду на часовий проміжок τ, в який була реалізована кібератака *buffer_overflow*. Далі, на основі аналізу статистичних даних встановлюється граничне значення ймовірності настання кіберінциденту PR_{lim} (для цього експерт аналізує атаки, які відбувались одночасно і визначає їх диференційований вплив на настання кіберінциденту). Отже, для зазначеного прикладу при $PR_{lim} = 0{,}15$ вираз (20) можна представити у такому вигляді:

$$R_1 = (PR_{buffe\_overflow}^{MW} > 0{,}15) \rightarrow MW;$$
$$R_2 = (PR_{buffe\_overflow}^{UA} > 0{,}15) \rightarrow UA;$$
$$R_3 = (PR_{buffe\_overflow}^{BN} > 0{,}15) \rightarrow BN.$$



а) *б)*

Рис. 4. Статистика кіберінцидентів, представлена за категоріями (а) та датою виникнення (б)

Таблиця 7

Приклад оцінки ймовірності виникнення кіберінциденту при реалізації кібератаки

Кіберінцидент / Кібератака	MW	IF	UA	BN	DD	MT	IT
buffer_overflow	0,18	0,01	0,52	0,21	0,06	0,015	0,005

Зважаючи на сформовані правила R_1, R_2, R_3 можна зробити висновки, що реалізована часовий проміжок τ кібератака *buffer_overflow* може призвести до виникнення трьох категорій інцидентів: Malware (18%), Unauthorized Access (52%) та Botnet (21%). Далі ці дані використовуються для визначення впливу кіберінцидентів на об'єкти захисту (етап 6).

Етап 5 – Визначення об'єктів захисту. Для визначення об'єктів захисту сформуємо їх множину **O:**

$$\mathbf{O} = \{\bigcup_{i=1}^{n} \mathbf{O}_i\} = \{O_1, O_2, ..., O_n\}, (i = \overline{1,n}), \quad (21)$$

де n – кількість об'єктів захисту.

Наприклад, у якості об'єктів захисту можуть бути складові ІТС. Таким чином, вхідними даними на цьому етапі є категорії кіберінцидентів (визначені на 3 етапі методу) та складові ІТС (складові ІТС можна визначити згідно [11]). ІТС є середовищем в якому можуть виникнути кіберінциденти, типовий склад ІТС згідно [11] наведено у табл. 8:

Таблиця 8

Набір складових ІТС згідно CERT-UA

Код	Складова ІТС	Короткий опис	Дефініція
SV	Server	Серверне обладнання	Комп'ютери з підвищеною продуктивністю та технічними характеристиками; зазвичай призначені для надання одного або декількох специфічних сервісів, на кшталт електронного поштового обміну, баз даних, IP-телефонії, файлового сховища тощо
NC	NetChannel	Середовище передачі даних	Оптоволоконні лінії, кабелі типу «звита пара», телефонні кабелі, бездротові канали передачі даних (Wi-Fi, Wi-MAX, Bluetooth)
NH	NetHardware	Активне мережеве обладнання і обладнання зв'язку	Комутатори, маршрутизатори, модеми, бездротові точки доступу, телефонія), а також пристрої захисту (міжмережеві екрани, системи виявлення/попередження вторгнень тощо
WS	WorkStation	Автоматизовані робочі місця співробітників	Стаціонарні комп'ютери, ноутбуки, мобільні пристрої

Отже, використовуючи вираз (21) та дані з табл. 8, при $n = 4$ отримаємо:

$$\mathbf{O} = \{\bigcup_{i=1}^{4} \mathbf{O}_i\} = \{\mathbf{O_1}, \mathbf{O_2}, \mathbf{O_3}, \mathbf{O_4}\} = \quad (22)$$

$$= \{\mathbf{O_{SV}}, \mathbf{O_{NC}}, \mathbf{O_{NH}}, \mathbf{O_{WS}}\} = \{\mathbf{SV}, \mathbf{NC}, \mathbf{NH}, \mathbf{WS}\},$$

де $\mathbf{O_1} = \mathbf{O_{SV}} = \mathbf{SV}, \mathbf{O_2} = \mathbf{O_{NC}} = \mathbf{NC}, \mathbf{O_3} = \mathbf{O_{NH}} = \mathbf{NH},$ $\mathbf{O_4} = \mathbf{O_{WS}} = \mathbf{WS}$ – об'єкти захисту (складові ІТС).

Етап 6 – Визначення впливу кіберінцидентів на складові ІТС. Для визначення впливу кіберінцидентів, категоризованих на етапі 3, на складові ІТС, які визначались на етапі 5, експертам пропонується поставити бальну оцінку U впливу кіберінциденту на складову ІТС (23). Кіберінцидент, що має більший вплив, отримує нижчий бал (1,2), менш впливовий — більший (3,4):

$$U = \begin{vmatrix} U_{O_1 I_1} & U_{O_1 I_2} & \dots & U_{O_1 I_n} \\ U_{O_2 I_1} & U_{O_2 I_2} & \dots & U_{O_2 I_n} \\ \dots & \dots & \dots & \dots \\ U_{O_m I_1} & U_{O_m I_2} & \dots & U_{O_m I_n} \end{vmatrix}. \quad (23)$$

Наприклад, при $m = 4$ (етап 5), $n = 7$ (етап 3) експерти заповнюють табл. 9 встановлюючи зв'язок між складовою ІТС і категорією кіберінциденту.

Таблиця 9

Оцінка впливу кіберінцидентів на складові ІТС

Складові ІТС	Оцінки за видами кіберінцидентів						
	MW	IF	UA	BN	DD	MT	IT
SV	2	3	2	1	1	4	4
NC	3	4	4	2	2	4	4
NH	3	4	3	3	3	3	3
WS	1	1	1	1	1	1	1

Вихідними даними є оцінки впливу категорій кіберінцидентів на складові ІТС. Таким чином, при виникненні зазначених трьох категорій кіберінцидентів найбільшого впливу зазнають такі складові ІТС як WorkStation та Server.

Етап 7 – Визначення найбільш критичних складових ІТС. Вхідними даними на цьому етапі є складові ІТС (етап 5). Цей етап реалізується у два кроки:

Крок 1 – Виставлення бальних оцінок експертами. Експерти визначають дані $U_{O_1I_1} \dots U_{O_mI_n}$ (23), проставляючи у кожній клітинці один із знаків: «важливіший» (>), «менш важливий» (<) і «еквівалентний» (=). Визначення найбільш критичної складової ІТС може бути здійснено, наприклад, *методом попарних порівнянь* (основною його перевагою є можливість зосередження уваги експертів на двох об'єктах в певний момент часу – ця перевага проявляється зі збільшенням кількості об'єктів оцінювання), а кількість таблиць має відповідати кількості експертів. Крім того, для визначення найбільш критичної складової ІТС можна використати один з наведених в [21] методів: ранжирування, множинних порівнянь, дельфійський метод, метод нормалізації, метод вектору переваг, метод кластерного аналізу, метод рангових перетворень, метод апроксимації функції корисності тощо.

У табл. 9 кожного k-го експерта замінюється знаки співвідношення на значення (бал) r_{ij}^k за правилом:

$$r_{ij}^k = \begin{cases} 1, якщо\ a_i > a_j, \\ 2, якщо\ a_i = a_j, \\ 3, якщо\ a_i < a_j, \end{cases} \quad (24)$$

де a_i, a_j - складові ІТС, що порівнюються.

Крок 2 – Узгодження суджень експертів. Після цього проводиться узгодження матриць кожного експерта R^k, в результаті формується зведена матриця колективної переваги [9]. Узгодження може проводитися за різними алгоритмами. У табл. 9 використовувалася трибальна шкала (<, >, =). Можуть бути використані шкали більшої бальності. У разі порушення транзитивності переваг може виникнути ситуація, коли матриця R^* не є ранжуванням, тобто не дозволяє визначити переваги. Тоді будується таке ранжування R, яке є найближчим до групової думки. Позначивши через $d(R,R^*)$ відстань між R і R^*, отримаємо вимогу $d(R,R^*)min$. Груповий вибір R^* визначається умовою:

$$\sum_{k=1}^{K} d(R^*,R^k) = \min_{R \in R(n)} \sum_{k=1}^{K} d(R,R^k). \quad (25)$$

Підраховується бал WC кожного критерію як сума r_{ij}^k (може бути і якийсь інший алгоритм, важливо, щоб він відображав «ваги» критеріїв, зазначених експертами при парних порівняннях критеріїв) та визначається місце критерію в ранжуванні RC. Табл. 10 заповнюється на основі узгоджених оцінок експертів стосовно найбільш критичних складових ІТС.

Таблиця 10

Визначення найбільш критичних складових ІТС

Складові ІТС / Складові ІТС	$\mathbf{O_1}$	$\mathbf{O}_2$	…	$\mathbf{O}_i$	Бал, «вага» критерію	Місце критерію в ранжуванні
$\mathbf{O_1}$	$r_{O_1O_1}^k$	$r_{O_2O_1}^k$	…	$r_{O_iO_1}^k$	WC_1	RC_1
$\mathbf{O}_2$	$r_{O_1O_2}^k$	$r_{O_2O_2}^k$	…	$r_{O_iO_2}^k$	WC_2	RC_2
…	…	…	…	…	…	…
$\mathbf{O}_j$	$r_{O_1O_j}^k$	$r_{O_2O_j}^k$	…	$r_{O_iO_j}^k$	WC_m	RC_n

Вихідними даними цього етапу є оцінка критичності складових ІТС.

Наприклад, при $i = j = 4$ (етап 5) експерти визначають значення $r^k_{O_1O_1} \dots r^k_{O_iO_j}$, заповнюючи табл. 11 визначаючи найбільш критичні складові ІТС.

Таблиця 11

Визначення найбільш критичних складових ІТС

Складові ІТС / Складові ІТС	SV	NC	NH	WS	Бал, «вага» критерію	Місце критерію в ранжуванні
SV		>	>	>	3	1
NC	<		>	>	5	2
NH	<	<		>	8	3
WS	<	<	<		9	4

Таким чином, маємо бал критерію згідно з яким визначаємо місце критерію в ранжуванні. Найбільш критичним у цьому випадку є складова ІТС Server, а найменш критичним WorkStation.

Етап 8 – Ранжування ступенів небезпеки кіберінцидентів. Вхідними даними цього етапу є оцінка критичності складових ІТС (етап 7, табл. 10) та оцінки впливу кіберінцидентів на складові ІТС (етап 6, 23).

Визначається порівняльна значущість можливого збитку, до якого може призвести кіберінцидент відповідно до значень кожного критерію (26) і їх «ваги» (табл. 10). Це важливо для диспетчеризації стратегій і оперативних впливів. Оцінка порівняльної значущості може бути підрахована за формулою:

$$Q_j = \sum_{i=1}^{i} a_i x_{ij}, j = \overline{1, j}, \quad (26)$$

де x_{ij} – значення i-го критерію j-го виду кіберінциденту в табл. 9; a_i – «вага» i-го критерію в табл. 11. При використанні значень критеріїв з табл. 11 чим менше значення Q_j, тим більшу небезпеку становить кіберінцидент.

Розрахунок нормованих оцінок (табл. 12) видів кіберінцидентів здійснюється за формулою:

$$\mathbf{IL}_j = \frac{Q_j}{\sum_j Q_j}. \quad (27)$$

Таблиця 12

Оцінка рівня небезпеки кіберінциденту

Рівень небезпеки	Кіберінцидент	Нормована оцінка
1	$\mathbf{I}_1$	$\mathbf{IL}_1$
2	$\mathbf{I}_2$	$\mathbf{IL}_2$
…	…	…
n	$\mathbf{I}_n$	$\mathbf{IL}_j$

У разі виникнення декількох кіберінцидентів паралельно (ймовірність цього є досить високою з огляду на наведену на рис. 4 статистику і дослідження [22]), та маючи оцінки рівнів небезпеки кіберінцидентів, можна провести пріоритезацію кіберінцидентів з метою адекватного реагування на них.

Вихідними даними цього етапу є оцінки рівня небезпеки (критичності) кіберінцидентів, які виникнуть в результаті реалізованої категорії атаки.

Наприклад, використовуючи значення з табл. 9 та табл. 11 за виразом (26) розраховуємо оцінку рівня небезпеки кіберінциденту (табл. 13).

Для кіберінциденту MW отримуємо:

$$Q_1 = 3\times2 + 5\times3 + 8\times3 + 9\times1 = 54,$$

UA: $Q_2 = 3\times2 + 5\times4 + 8\times3 + 9\times1 = 59,$

BN: $Q_3 = 3\times1 + 5\times2 + 8\times3 + 9\times1 = 46.$

Нормовані оцінки видів кіберінцидентів, розраховані за (27): $\mathbf{IL}_1 = 0.34$, $\mathbf{IL}_2 = 0.37$, $\mathbf{IL}_3 = 0.29$ та вносяться до табл. 13.

Таблиця 13

Оцінка рівня небезпеки кіберінцидента

Рівень небезпеки	Кіберінцидент	Нормована оцінка
1	BN	0,29
2	MW	0,34
3	UA	0,37

Таким чином, можна зробити висновок, що при реалізації кібератаки *buffer_overflow* найбільшу небезпеку несе (є найбільш критичним) кіберінцидент Botnet далі Malware, а потім Unauthorized Access.

Висновки. Таким чином, у цій роботі розроблено метод мережево-цетричного моніторингу кіберінцидентів, який за рахунок класифікації кібератак та порівняння їх параметрів з еталонними, формування множини базових правил і встановлення зв'язків між підкласом кібератаки та категорією кіберінцидентів на базі обробки їх статистики, ідентифікації об'єктів захисту та експертного оцінювання впливу на них кіберінцидентів, узгодження суджень експертів та ранжування ступенів небезпеки кіберінцидентів, дозволяє визначити найбільш важливі об'єкти захисту (складові ІТС чи кіберпростору), а також прогнозувати категорії кіберінцидентів, які виникнуть внаслідок реалізації кібератаки, та їх рівень небезпеки (критичності).

Цей метод та сформовані на його основі засоби будуть корисними для команд реагування на кіберінциденти типу CERT/CSIRT для ефективної обробки кіберінцидентів (зокрема диспетчеризації) та адекватного на них реагування, а також для підрозділів, на які покладаються обов'язки щодо захисту ІТС як в межах підприємства, так і в межах держави.

ЛІТЕРАТУРА

[1]. Гнатюк В.О. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі / В.О.Гнатюк // Безпека інформації. — №3 (19). — 2013. — С. 175-180.

[2]. ISO/IEC 27035:2011 — Information technology — Security techniques — Information security incident management, 2011. — 69 p.

[3]. Гнатюк В.О. Огляд систем виявлення вторгнень на основі honeypot-технологій / Гнатюк В.О., Волянська В.В., Гізун А.І. // Безпека інформації. — №2 (18). — 2012. — С. 75-79.

[4]. Гізун А.І. Аналіз сучасних систем управління кризовими ситуаціями / А.І. Гізун, А.О. Корченко, С.О. Скворцов // Безпека інформації. — №1 (21). — 2015. — С. 86-99.

[5]. Синявский В.К. Влияние содержания и принципов «сетецентрической войны» на процессы управления войсками (силами) / В.К. Синявский // Наука и военная безопасность. — 2010. — №4. — С. 36-45.

[6]. Парадигма сетецентрического управления и ее влияние на процессы управления войсками [Электронний ресурс]. — Режим доступа:: http://agat.by /pres/statia%20nayka-3.pdf.

[7]. Network centric warfare and wireless communications: [Электронний ресурс]. — Режим доступа: http://www.meshdynamics.com/military-mesh-networks.html

[8]. Затуливетер Ю.С. Компьютерный базис сетецентрического управления / Ю.С. Затуливетер // Труды российской конференции с международным участием «Технические и программные средства в системе управления, контроля и измерения» (18-20 октября 2010 г.). — М., 2010 — С. 17-37.

[9]. Трахтенгерц Э.А. Сетецентрические методы компьютерной поддержки управления ликвидацией последствий чрезвычайных ситуаций / Шершаков В.М., Трахтенгерц Э.А., Камаев Д.А. — М.: ЛЕНАНД, 2015. — 160 с.

[10]. Гнатюк С.О. Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки / Гнатюк С.О., Хохлачова Ю.Є., Охріменко А.О., Гребенькова А.К. // Захист інформації. — №1 (54). — 2012. — С. 121-126.

[11].Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.О. Гнатюк // Безпека інформації. — Т. 19, №2. — 2013. — С. 118-129.

[12].Грищук Р.В. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак / Р.В. Грищук, В.В. Охрімчук, В.С. Ахтирцева // Захист інформації. — 2016. — №1 (18). — С. 21-29.

[13].KDD CUP99 [Electronic resource]. — Access to resources: https://kdd.ics.uci.edu/databases/kddcup99/task.html

[14]. Official site Common Attack Pattern Enumeration and Classification [Electronic resource]. — Access to resources: https://capec.mitre.org

[15].CERT-UA. Базовий курс з інформаційної безпеки [Електронний ресурс]. — Режим доступу: http://cert.gov.ua

[16]. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»: № 80/94-ВР від 5 липня 1994 р. / Верховна Рада України // Відомості ВРУ. — 1994. — №31. — Ст. 286.

[17]. Карпинский Н. Метод формирования базовых детекционных правил для систем обнаружения вторжений / Н. Карпинский, А. Корченко, С. Ахметова // Захист інформації. — Т. 17, №4. — 2015. — С. 312-324.

[18]. Гізун А.І. Формалізована модель побудови евристичних правил для виявлення інцидентів /

А.І. Гізун, В.О. Гнатюк, О.М. Супрун // Вісник Інженерної академії України. — 2015. — №1. — С. 110-115.

[19]. Корченко А.О. Евристичні правила на основі логіко-лінвистичних зв'язок для виявлення та ідентифікації порушника інформаційної безпеки / А.О. Корченко, А.І. Гізун, В.В. Волянська, О.В. Гавриленко // Захист інформації. — 2013. — №3 (60). — С. 251-257.

[20]. Gizun A. Approaches to Improve the Activity of Computer Incident Response Teams / A. Gizun, V. Gnatyuk, N. Balyk, P. Falat // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. — Pp. 442-447.

[21]. Горніцька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В. Волянська, А.О. Корченко // Захист інформації — №1. — 2012. — С. 108-121.

[22].Герега О.М. Гіпотеза і формальна модель сингулярної динаміки інцидентів кібернетичної безпеки / О.М. Герега, С.О. Гнатюк, В.Г. Кононович, І.В. Кононович // Інформатика та математичні методи в моделюванні. — Т. 6, №1. — 2016. — С. 26-37.

REFERENCES

[1]. Gnatyuk V.O. Analysis of definitions «incident» and its interpretation in cyberspace / V.O. Gnatyuk //Ukrainian scientific journal of information security, №3 (19), 2013, P. 175-180.

[2]. ISO/IEC 27035:2011 — Information technology — Security techniques — Information security incident management, 2011. — 69 p.

[3]. Gnatyuk V.O. Review of intrusion detection systems based on honeypot-technologies / Gnatyuk V.O., Volyanskaya V.V., Gizun A.I. // Ukrainian scientific journal of information security, №2 (18), 2012, P. 75-79.

[4]. Gizun A.I. Analysis of current crisis management systems / Gizun A.I., A.O. Korchenko, S.O. Skvortsov // Ukrainian scientific journal of information security, №1 (21), 2015, P. 86-99.

[5]. Synyavskyy V.K. Effect of content and principals of «network-centric war» on prosses of command and control (forces) / V.K. Synyavskyy // Science and Military Safety, 2010, №4, P. 36-45.

[6]. The paradigm of network-centric management and its impact on the processes of command and control [Electronic resource]. — Access to resources: http://agat.by/pres/statia%20nayka-3.pdf.

[7]. Network centric warfare and wireless communications: [Electronic resource]. — Access to resources: http://www.meshdynamics.com/military-mesh-networks.html

[8]. Zatuliveter Yu.S. Computer basis of network-centric management/ Zatuliveter Yu.S.// Proceedings of Russian conference with international participation «Hardware and software in system of management, control and measurement » (October 18-20, 2010.). — M., 2010, P. 17-37.

[9]. Trahtengerts E.A. Network-centric methods for computer support of managing emergency response / V.M. Shershakov, EA Trahtengerts, D.A. Kamaev// M.: LENAND, 2015, 160 p.

[10]. Gnatyuk S.O. Theoretical basis for construction and functioning of information security incident management systems / Gnatyuk S., Khokhlacheva Yu., Ohrimenko A., Grebenkova A.// Ukrainian information security research journal, №1 (54), 2012, P. 121-126.

[11]. Gnatyuk S.O. Cyberterrorism: history, modern trends and countermeasures / Gnatyuk S.O. // Ukrainian scientific journal of information security, Issue. 19, №2, 2013, P. 118-129.

[12].Gryshchuk R. Sources of primary data for development of patterns of potentially dangerous cyberattacks / R.V. Gryshchuk, V.V. Okhrimchuk, V.S. Akhtyrtseva // Ukrainian information security research journal, 2016, №1 (18), P. 21-29.

[13].KDD CUP99 [Electronic resource]. — Access to resources: https://kdd.ics.uci.edu/databases/kddcup99/task.html

[14]. Official site Common Attack Pattern Enumeration and Classification [Electronic resource]. — Access to resources: https://capec.mitre.org

[15].CERT-UA. Basic course about information security [Electronic resource]. — Access to resources: http://cert.gov.ua

[16]. The law of Ukraine « About information security in information and telecommunication systems»: № 80/94-BP from July 5, 1994/ Verkhovna Rada of Ukraine // Information the Verkhovna Rada, 1994, №31, Art. 286.

[17]. Karpinskii N. The method of forming core detection rules for intrusion detection systems / N. Karpinskii, Korchenko A., S. Ahmetova // Ukrainian information security research journal, Issue 17, №4, 2015, P. 312-324.

[18]. Gizun A.I. Formalized model for construction heuristic rules to detect incidents / Gizun A.I, Gnatyuk V.O., Suprun O.M. // Journal of Engineering Academy of Ukraine, 2015, №1, P. 110-115.

[19]. Korchenko A.O. Heuristic rules based on logic-linvistic links for detection and identification information security intruder / Korchenko A.O., Gizun A.I, Volyanskaya V.V., Gavrylenko O.V. // Ukrainian information security research journal, 2013, №3 (60), P. 251-257.

[20]. Gizun A. Approaches to Improve the Activity of Computer Incident Response Teams / A. Gizun, V. Gnatyuk, N. Balyk, P. Falat // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems:

Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. — Pp. 442-447.

[21]. Gornitska D.A. Determining coefficients of importance for expert evaluation in the field of information security / Gornitska D.A., Volyanskaya V.V., Korchenko A.O.// Ukrainian information security research journal, №1, 2012, P. 108-121.

[22]. Gerega O.M. Hypothesis and formal model of singular dynamics for cybersecurity incidents / Gerega O.M., Gnatyuk S.O., V.G., Kononovich I.V. // Informatics and mathematical methods in modeling, Issue 6, №1, 2016, P. 26-37.

МЕТОД СЕТЕЦЕНТРИЧЕСКОГО МОНИТОРИНГА КИБЕРИНЦИДЕНТОВ В СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Процесс внедрения информационно-коммуникационных технологий в большинстве сфер сегодняшней общественной жизни направлен на повышение эффективности бизнес-процессов. Однако наличие уязвимостей и киберугроз порождает киберинциденты, для локализации и нейтрализации которых необходимы эффективные методы обнаружения, идентификации, обработки и расследования. Одним из подходов является применение сетецентрической концепции, ориентированной на противодействие возникновению и ликвидации последствий киберинцидентов с помощью средств, объединенных информационными сетями в единую систему. В работе, на базе этой концепции, предложен метод сетецентрического мониторинга киберинцидентов, который реализуется в 8 этапов: классификация кибератак, выявление типа кибератаки, категоризация киберинцидентов, формирование множества правил экстраполяции киберинцидентов, определение объектов защиты, определение влияния киберинцидентов на составляющие информационно-телекоммуникационных систем, определения наиболее критических составляющих информационно-телекоммуникационных систем, ранжирование степени опасности киберинцидентов. Этот метод позволяет определить наиболее важные объекты защиты, а также прогнозировать категории киберинцидентов, которые возникнут в результате реализации кибератаки, и их уровень опасности (критичности). Кроме того, этот метод и сформированные на его основе инструментальные средства будут полезными для команд реагирования на киберинциденты типа CERT / CSIRT для эффективной обработки киберинцидентов (в частности диспетчеризации) и адекватного на них реагирования, а также для подразделений, на которые возлагаются обязанности по защите информационно-телекоммуникационной системах как в пределах предприятия, так и в пределах государства.

Ключевые слова: киберинцидент, информационно-телекоммуникационная система, сетецентрическая концепция, мониторинг, критичность, база KDD 99, CERT/CSIRT.

METHOD FOR CYBERINCIDENTS NETWORK-CENTRIC MONITORING IN MODERN INFORMATION & COMMUNICATION SYSTEMS

Information and communication technologies implementation in many spheres of social live is directed on business processes efficiency improving. However vulnerabilities and cyberthreats generate cyberincidents. New effective methods of detection, identifying, processing and investigation are necessary for localization and counteraction. One of approaches is network-centric concept oriented on counteraction to cyberincidents beginning and emergency recovery by network combining unique system of measures. Based on this concept in the paper method for cyberincidents network-centric monitoring that realizes using 8 stages: cyberattack classification; cyberattack type detection; cyberincident categorization; forming of rules plurality for cyberincident extrapolation; security objects defining; cyberincident influence defining on information and communication systems components; most criticality components defining in information and communication systems; cyberincident danger level rating. This method allows to define most important security objects and also forecast cyberincidents categories resulted from cyberattacks and danger level (criticality). Besides this method and instrumentations based on it can be useful for cyberincidents response teams CERT / CSIRT to process cyberincidents (in particular dispatching) and response. As well as departments that assign functions to secure information and communication systems both in company and state.

Keywords: cyberincident, information and communication system, network-centric concept, monitoring, criticality, KDD 99 base, CERT/CSIRT.

Корченко Александр Григорьевич, доктор технических наук, профессор, лауреат Государственной премии Украины в области науки и техники, заведующий кафедрой безопасности информационных технологий Национального авиационного университета, старший научный сотрудник Национальной академии СБ Украины.

E-mail: agkorchenko@gmail.com

Корченко Олександр Григорович, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, старший науковий співробітник Національної академії СБ України.

Korchenko Oleksandr, Dr Eng (Information security), professor, laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University, Senior Researcher

Гнатюк Віктор Олександрович, асистент кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: viktorgnatyuk@ukr.net
Гнатюк Виктор Александрович, ассистент кафедры телекоммуникационных систем Национального авиационного университета.
Gnatyuk Viktor, Assistant Teacher of Telecommunication Systems Academic Dept in National Aviation University.

Іванченко Євгенія Вікторівна, кандидат технічних наук, доцент, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: icaocentre@nau.edu.ua
Иванченко Евгения Викторовна, кандидат технических наук, доцент, профессор кафедры безопасности информационных технологий Национального авиационного университета.
Ivanchenko Yevgeniya, PhD in Eng, Professor of IT-Security Academic Dept in National Aviation University.

Гнатюк Сергій Олександрович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: s.gnatyuk@nau.edu.ua
Гнатюк Сергей Александрович, кандитат технических наук, доцент, доцент кафедры информационных технологий Национального авиационного университета.
Gnatyuk Sergiy, PhD in Eng, Associate Professor of IT-security Academic Dept in National Aviation University.

Сейлова Нургуль Абадуллаєвна, кандидат технічних наук, доцент, завідувач кафедри інформаційної безпеки Казахського національного дослідницького технічного університету ім. К.І. Сатпаєва.
E-mail: seilova_na@mail.ru
Сейлова Нургуль Абадуллаевна, кандидат технических наук, доцент, заведующая кафедрой информационной безопасности Казахского национального исследовательского технического университета им. К.И. Сатпаева.
Seilova Nurgul, PhD in Eng, Chairman of Information Security Academic Dept in Kazakh National Research Technical University n.a. K.I. Satpayev.