УДК 004.4

Касаткін Дмитро Юрійович
кандидат педагогічних наук, доцент, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів та природокористування України
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

Волошин Семен Михайлович
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів та природокористування України
ORCID: https://orcid.org/0000-0002-4913-7003
E-mail: voloshyn@nubip.edu.ua

Гусєв Борис Семенович
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів та природокористування України
ORCID: https://orcid.org/0000-0003-1658-7822
E-mail: gusevbs@gmail.com

Матієвський Володимир Валерійович
старший виклад кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів та природокористування України
ORCID: https://orcid.org/0000-0002-1954-8493
E-mail: m_vv@outlook.com

АЛГОРИТМИ РОЗРОБКИ БАЗИ ЗНАНЬ ДЛЯ ВДОСКОНАЛЕННЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ВИРІШЕННІ ПРОБЛЕМ КІБЕРБЕЗПЕКИ

Анотація. *У статті представлено розробку модульної системи підтримки прийняття рішень (СППР) для кібербезпеки, спрямовану на підвищення захищеності критично важливих комп'ютерних систем (КВКС). В основі системи лежить модель підсистеми нечіткого виводу (НечВ), яка, використовуючи дані з датчиків та систем SIEM, здатна виявляти ознаки загроз, аномалій та атак шляхом фазифікації вхідних значень. Розроблений алгоритм формування бази знань про типові та аварійні ситуації дозволяє системі не тільки ефективно реагувати на відомі загрози, але й аналізувати непередбачувані ситуації. Застосування модуля НечВ дає змогу створити багатопараметричний образ уразливості КВКС, що забезпечує більш комплексну та точну оцінку їх захищеності.*

Ключові слова: *критично важливі комп'ютерні системи, кібербезпека, система підтримки прийняття рішень, багатопараметричний "образ", оцінка захищеності.*

Вступ. У процесі експлуатації критично важливих комп'ютерних систем (КВКС) одним із пріоритетних завдань опрацювання даних, що надходять від різних пристроїв, які входять до структури комплексних систем захисту інформації (далі – КСЗІ, для яких мається на увазі, перш за все, апаратно-програмні складові), є отримання відомостей про стан компонентів захисту. Ефективність і безпомилковість під час оперативного оцінювання ступеня захищеності КСЗІ може ускладнитися через вплив наведених нижче факторів. Перший – дані, що надходять (від датчиків SIEM, мультиагентних систем, сенсорів, що визначають наявність загроз, кібератак, аномалій, далі запроваджено абревіатуру датчикові підсистеми – ДатП), можуть бути різними за своїми параметрами. Другий – у процесі отримання даних можливий вплив зовнішніх впливів, що впливають на автентичність характеристик, що відстежуються.

Третє – реакція на деструктивні втручання обмежені часовими рамками, при цьому залишається мінімальний час для результатів аналізу. Четверте – можливі ситуації, коли комбінація оцінюваних параметрів у КВКС призводить до "нечіткості" під час ухвалення рішень з оцінки поточних станів захищеності КВКС (на відміну від типових). З огляду на перераховані причини, оперативні та ефективні рішення в процесі аналізу складних таргетованих кібератак на КВКС і відповідних процедур ухвалення рішень, вимагають застосування спеціальних аналітичних систем. Цілком очевидно, що подібні системи мають бути засновані на сучасних методах автентифікації станів КВКС і КСЗІ. Також доцільно залучити потенціал інтелектуалізованих адаптивних систем підтримки ухвалення рішень (СППР) у задачах кібербезпеки (КрБ), а також і розпізнавання загроз, аномалій та кібератак [1].

У період лавиноподібного зростання складності та кількості кібератак на КВКС [2], і зростання чисельності параметрів, що надходять від сенсорних ДатП КСЗІ, виникла необхідність впровадження в структури КСЗІ адаптивних експертних (АЕС) і СППР. Це необхідно для комплексного багатокритеріального аналізу даних від ДатП КСЗІ, які формують дані для оцінювання захищеності КВКС.

Зауважимо, що одним із найрезультативніших методів у розв'язанні цього класу завдань є метод, що передбачає побудову АЕС і СППР на базі теорії нечітких множин (ТНМ). Можливе також використання апарату нечіткої логіки (НЛ) [1, 3, 4].

Використання АЕС і СППР здатне мінімізувати вплив "людського фактора" на якість прийнятих рішень. Крім того, зростає швидкість ухвалення рішення. Скорочуються можливі ситуації, пов'язані з відволіканням персоналу служб інформаційної безпеки на рутинні роботи. Також зрештою, скорочується собівартість володіння подібними комплексами.

Огляд літератури та постановка проблеми останніми роками ускладнилися сценарії реалізації кібератак [2, 5]. Фіксується зростання кількості фіксованих у КВКС аномалій та інших спроб несанкціонованого втручання в роботу складних цифрових систем [2, 6]. У цих умовах виник напрямок досліджень з інтелектуалізації процедур підтримки прийняття рішень у процесі розпізнавання загроз, кібератак та аномалій. Аналіз наявного світового досвіду [2, 4-8] підтверджує, що екстенсивний підхід до розв'язання завдань кібербезпеки КВКС коштом нарощування засобів і заходів із захисту інформації (ЗІ), часто не приводять до очікуваного результату. Перспективним напрямком досліджень стали роботи, присвячені створенню інтелектуалізованих систем підтримки ухвалення рішень (СППР) [1, 4] та експертних систем (ЕС) [3, 8] у задачах оцінювання захищеності об'єктів інформатизації. Ці дослідження ще не завершені.

У [1, 3, 4, 8] проаналізовано досвід упровадження комерційних СППР та ЕС для задач аналізу загроз, атак і аномалій. Зазначено, що комерційні системи мають закритий характер, і їх придбання окремими компаніями або організаціями пов'язане зі значними фінансовими витратами.

Таким чином, з огляду на полеміку в роботах [1, 2, 8], видається релевантним завдання з розроблення нових і вдосконалення наявних моделей та алгоритмів для адаптивних СППР, що задіяні в процесах опрацювання даних від різноманітних ДатП підсистем кібербезпеки і (КрБ) захисту інформації (ЗІ) у КВКС.

Мета дослідження – розробити нові або вдосконалити наявні моделі та алгоритми для адаптивних СППР, що задіяні в процесах аналізу даних від ДатП підсистем кібербезпеки та захисту інформації в КВКС.

У рамках статті розглянуто завдання з розроблення:

модуля "нечіткого логічного висновку" для експертного вивчення даних від ДатП КВКС;

алгоритму, що формує базу знань (БЗ) про типові та непередбачувані ситуації (НепС) у КВКС (що забезпечує експертний аналіз ступеня захищеності КВКС).

Моделі та методи загальна структура розроблюваної модульної системи підтримки ухвалення рішень у задачах кібербезпеки наведена на рис. 1.

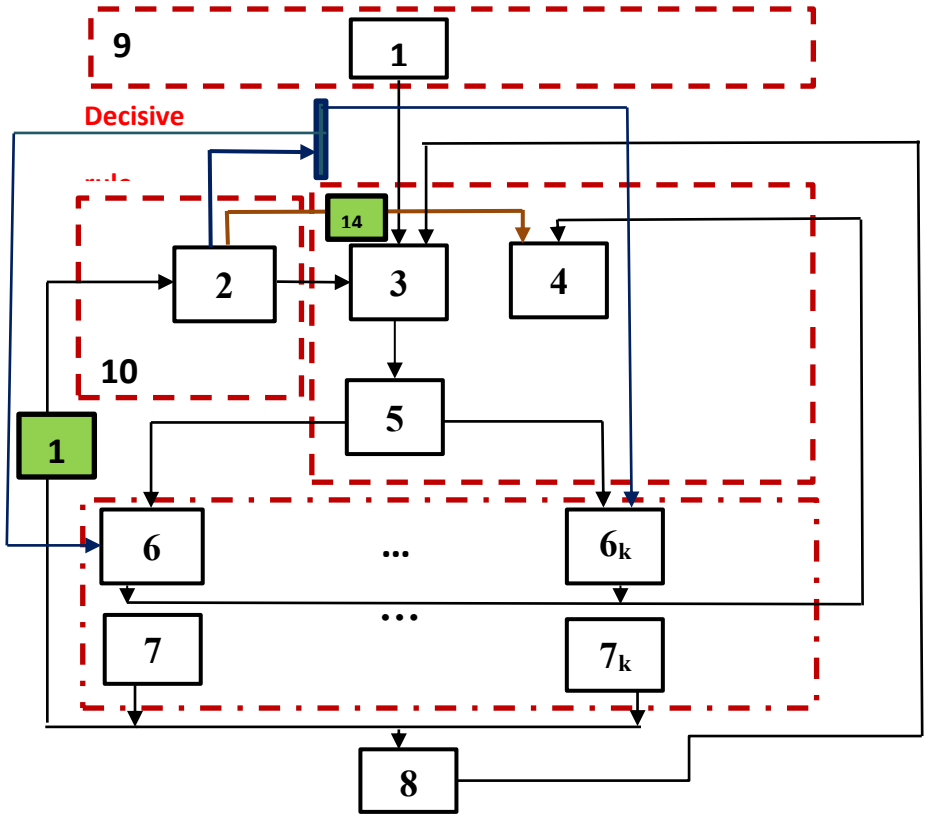


Рисунок 1 – Загальна структура модульної системи підтримки прийняття рішень у задачах кібербезпеки

Позначення, прийняті на схемі: 1 – пристрій введення; 2 – сервер; 3 – модуль візуалізації; 4 – модуль дефазифікації; 5 – модуль фазифікації; 6 (6_k) – модулі підсистеми нечіткого виведення; 7 (7_k) – пристрої виведення; 8 – модуль виведення результатів аналізу та рекомендацій щодо виходу з непередбачуваних ситуацій; 9 – модуль первинного опрацювання інформації, що надходить від датчиків, мультиагентних систем, сенсорів, які визначають наявність загроз, кібератак, аномалій; 10 – модуль сервера з базами знань (БЗ); 11 – модуль аналізу основних параметрів функціонування КВКС з інтегрованою оцінкою захищеності; 12 – модулі співробітників служб захисту інформації та кібербезпеки КВКС (за кількістю підсистем КВКС); 13 – нові правила (рекомендації), які додають до БЗ; 14 – рекомендації з виходу з непередбачуваних ситуацій, пов'язаних із КрБ КВКС.

Модуль нечіткого логічного виводу (НЛВ) та алгоритми, що формують БЗ типових (еталонні) та непередбачених ситуацій для СППР з аналізу захищеності КВКС описані нижче.

Модулі НЛВ призначені для реалізації системи нечіткого виводу (НечВ) на рис. 1 позначені як 6–6_k. Ґрунтуючись на правилах нечіткого виводу (НечВ), за вхідними значеннями ДатП $\left\{Rd\left(R_{i,n_i}(t)\right), m\left(R_{i,n_i}(t)\right)\right\}\left(i=\overline{1,k}; n_i=\overline{1,N_i}\right)$, визначаються вихідні значення

$$\left\{(Rdc\left(R^j_{i,n_i}(t)\right), m\left(Rdc^j_{i,n_i}(t)\right)\right\}\left(i=\overline{1,k}; n_i=\overline{1,N_i}; j=\overline{1,J}\right).$$

При цьому вважаємо, що вхідні значення були отримані як результат процедури фаифікації у відповідному модулі (модуль 5, рис. 1). Кожний елемент вихідних значень, своєю чергою, характеризує наявність (відсутність) ознаки НепС (далі введено позначення – *EmS*). Тоді конкретну ознаку непередбаченої ситуації (*j*), наприклад, що виникла як наслідок кібератаки на КВКС, можна описати за допомогою змінних, що описані нижче.

Вводяться такі змінні:

$Md^j_{i,n_i}(t)$ – характеристика дискретного стану n_i-го $Param$, наприклад, кількість байтів від джерела до адресату, кількість байтів відповіді клієнту, ознаки з'єднання, кількість "root" доступів, кількість операцій створення файлів, кількість запитів на надання оболонки,

кількість операцій на доступ до контролю файлів та ін. (приймаємо за KDD 99) [11 , 12]. Ця змінна може набувати одного з наступних значень, див. рис. 2:

«1» – відхилення від норми зверху;

«0» – типова ситуація (або норма);

«-1» – відхилення від норми знизу;

«2» – відхилення від норми знизу або зверху;

$m\left(Md_{i,n_i}^{j}(t)\right)$ – експериментальна оцінка ступеня експлікованості впливу n_i-ї величини (параметр – $Param$) (i) підсистеми КВКС на виникнення j-ї EmS (наприклад, аномалії в мережі КВКС), у кожний момент часу (t).

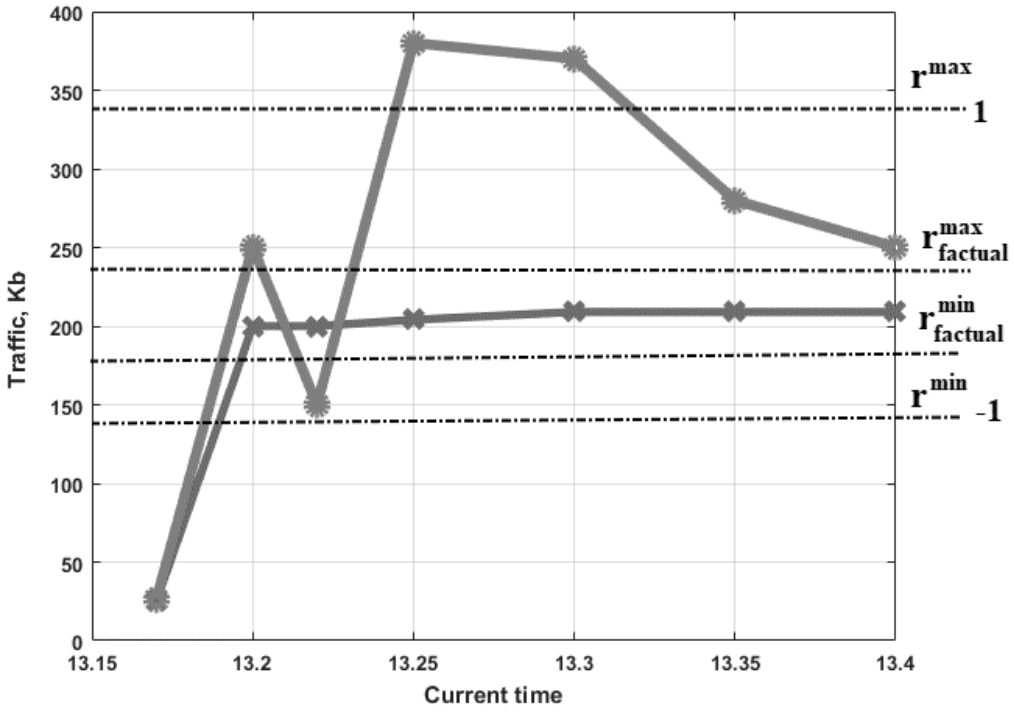


Рисунок 2 – Формування змінної для модуля підсистеми нечіткого виведення

Позначення: "0" – типова ситуація (або норма); "1" – відхилення від норми зверху; "-1" – відхилення від норми внизу; "2" – відхилення від норми внизу або вгорі

Правила виявлення j-ї EmS можна описати таким чином:

$$if\ RD\left(R_{i,n_i}(t)\right) \vee Md_{i,n_i}^{j}(t) = 1\ \ that\ is\ (j)$$
зі ступенем експлікованості $m\left(Md_{i,n_i}^{j}(t)\right)$; (1)

$$if\ RD\left(R_{i,n_i}(t)\right) \vee Md_{i,n_i}^{j}(t) = -1\ \ that\ is\ (j)$$
зі ступенем експлікованості $m\left(Md_{i,n_i}^{j}(t)\right)$; (2)

$$if\ \left(Rd\left(R_{i,n_i}(t)\right) = 1 \vee Md_{i,n_i}^{j}(t) = -1\right) \vee \left(Md_{i,n_i}^{j}(t)\right) = 2\ that\ is\ (j)$$
зі ступенем експлікованості $m\left(Md_{i,n_i}^{j}(t)\right)$; (3)

На рис. 2 показано приклад формування змінних для модуля підсистеми нечіткого виведення під час наповнення БЗ СППР даними щодо трафіку протоколу TCP (для конкретної

КВКС на прикладі атаки TCP-flood). На графіку, показаному лінією із двома штрихами, задано фактичне середнє порогове значення трафіку. Якщо протягом від 30 секунд буде зареєстровано відхилення від норми (червона лінія), до БЗ СППР заноситься відповідна інформація, яка описує аномалію або загрозу. Якщо протягом заданого проміжку середні значення метрик перевищать порогові значення, то аналітику буде виведено повідомлення про відхилення від норми зверху або знизу ("1" або "-1"). Інформація про відхилення також доступна для перегляду адміністратору мережі КВКС.

У кожен момент (t) для виявлення EmS за ознакою (j) може змінюватися тільки одне з перерахованих трьох правил (1) – (3).

Вважаємо, що кожне правило, описане в БЗ СППР з розпізнавання загроз, аномалій і кібератак в КВКС, тобто *j*-й EmS, може зіставити значення відхилень $R_{i,n_i}(t)$ в момент (t) для n_i-го *Param i*-ї підсистеми КВКС зі ступенем експлікованості впливу n_i-го параметра на EmS, яка дорівнює $m\left(Md_{i,n_i}^{j}(t)\right)$;

Як наслідок використання правил (1) – (3) для n_i-го *Param* та *i*-ї підсистеми КВКС можна сформувати (J) вихідних значень тобто .

$$\left\{\left(Rdc\left(R_{i,n_i}^{j}(t)\right),\ m\left(Rdc_{i,n_i}^{j}(t)\right)\right\}\left(i=\overline{1,k};n_i=\overline{1,N_i};j=\overline{1,J}\right).$$

Зауважимо, що для фіксованих (наприклад, критичних номерів *j*-х EmS) вважаємо, що:

- якщо є активне правило з (1) – (3) то можлива *j*-а EmS, тобто

$$Rdc_{i,n_i}^{j}(t)=m\left(R_{i,n_i}^{j}(t)\right)\vee m\left(Rdc_{i,n_i}^{j}(t)\right)=m\left(Md_{i,n_i}^{j}(t)\right);$$

- якщо немає активних правил з (1)-(3) то не можлива *j*-та EmS, тобто

$$Rdc_{i,n_i}^{j}(t)=0\vee m\left(Rdc_{i,n_i}^{j}(t)\right)=m\left(Md_{i,n_i}^{j}(t)\right).$$

У модулі дефазифікації (J) вихідним значенням

$$\left\{\left(Rdc\left(R_{i,n_i}^{j}(t)\right),\ m\left(Rdc_{i,n_i}^{j}(t)\right)\right\}\left(i=\overline{1,k};n_i=\overline{1,N_i};j=\overline{1,J}\right)$$

ставиться числове значення (нечітке). За даним значенням у подальшому за допомогою СППР визначаємо набір рекомендацій щодо виходу з непередбачених ситуацій (*EMS*).

Вагові коефіцієнти, наприклад, для *j*-ій *EMS*, визначені таким чином:

$$\xi_i^j=\frac{\sum_{n_i=1}^{N_i} m\left(Rdc_{i,n_i}^{j}(t)\right)\cdot Rdc_{i,n_i}^{j}(t)}{\sum_{n_i=1}^{N_i} m\left(Rdc_{i,n_i}^{j}(t)\right)}. \tag{4}$$

Вважаємо, що *EMS* (j^*) відбулася в *i*-ій підсистемі КВКС, якщо:

$$\xi_i^{j^*}(t)=\underset{j=\overline{1,J}}{max}\left(\xi_i^{j}(t)\right)\vee\xi_i^{j^*}(t)\geq thv_i, \tag{5}$$

де thv_i – порогове значення ступеня виявлення (наприклад, одноразово виявлено, частково виявлено, не виявлено) *EMS*. Вважаємо, що $thv_i \in [0,1]$.

Якщо $\xi_i^{j^*}(t) < thv_i$ то *EmS* в i-й підсистемі на даний момент (t) не ідентифіковано. У такій ситуації слід розпочати інтерактивний аналіз експерта з КрБ і СППР. При цьому можна задіяти алгоритм формування БЗ для системи НечВ, див. рис. 1.

Алгоритм, що формує БЗ для типових (еталонних) і непередбачуваних ситуацій для СППР описано далі.

Початкові дані для підсистеми нечіткого виводу включають:

- допустимі межі $\left[r_{i,n_i}^{\min}, r_{i,n_i}^{\max}\right]$, що визначають типові режими функціонування КВКС;
- функцію приналежності до непередбачених режимів у КВКС для параметрів, що відстежуються, для ситуацій відхилення їх від допустимих меж.

Персональне формування БЗ для типових режимів роботи КВКС наповнюється з урахуванням інструкцій для штатного поведінки КВКС.

За підсумками роботи програмної та апаратної складових КСЗІ відбувається заповнення БЗ СППР фактичними даними про штатні режими роботи системи.

Вважаємо: функція m $\left(R_{i,n_i}(t)\right)$ для фактичних допусків – це кусочно-лінійна функція, за допомогою якої встановлюють ступінь експлікованості (приналежності):

Якщо «0», то *Param* перебуває у фактичній зоні межі, що допускається;

Якщо «1», то *Param* перебуває поза розрахункової області межі, що допускається.

Порогові значення $tv_{q_{n_i}}(t), q_{n_i} = \overline{1, Q_{n_i}}$ розраховувалися при запиті до БЗ з використанням наступних формул:

$$tv_{q_{n_i}}(t) = tv_{Q_{n_i}} \cdot \frac{\left(q_{n_i} - 1\right)^{st_{n_i}}}{\left(Q_{n_i} - 1\right)^{st_{n_i}}}, \qquad (6)$$

$$st_{n_i} = u \cdot \frac{1}{su}$$

де $st-$ ступінь заповнення БЗ для конкретного параметра; $u-$ кількість тестів, які враховані в статистиці; $su-$ кількість тестів СППР, у яких БЗ вважається заповненою (фрагмент БЗ прототипу СППР «Аналізатор загроз» показано на рис.3 [11]).

Процедуру формування БЗ, що включає правила для модуля нечіткого виводу в процесі автоматизованої обробки показань від датчиків SIEM, мультиагентних систем, сенсорів, що визначають наявність загроз, кібератак, аномалій описано нижче.

Нове або існуюче правило виявлення непередбаченої ситуації в КВКС за значенням n_i-го параметра $n_i=\overline{1,N_i}$ для підсистеми ($i=\overline{1,k}$) КВКС формуємо на основі

$$Rd(R_{i,n_i}^j(t), Md_{i,n_i}^j(t)),$$

Далі слід визначити ступені експлікованості впливу $m\left(Md_{i,n_i}^j(t)\right)$ n_i-параметра на виникнення $j = \overline{1,J}$ *EMS*.

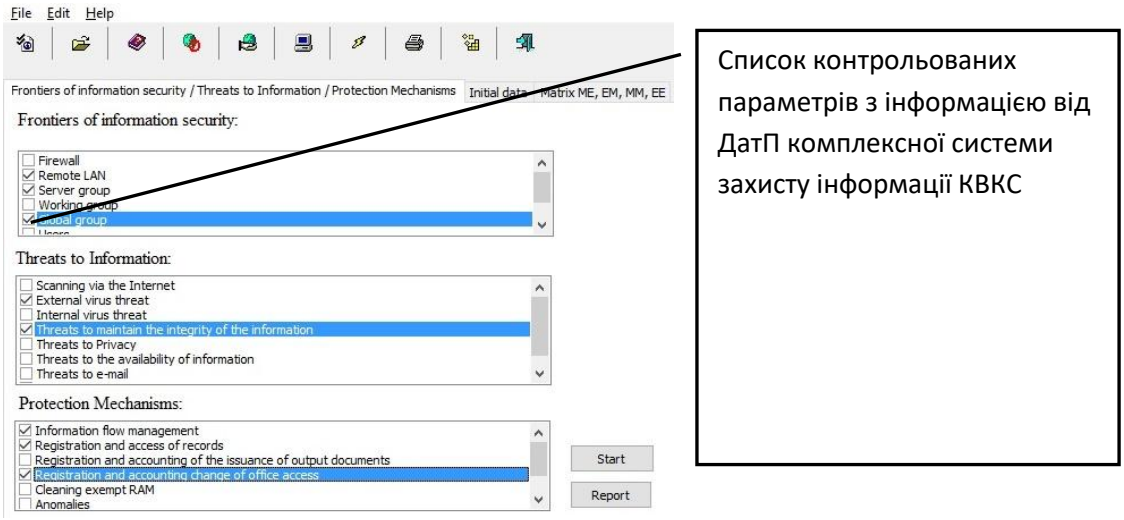
Використовуються правила, описані виразами (1)-(3).

Початкові величини для виявлення $j = \overline{1,J}$ *EMS*:

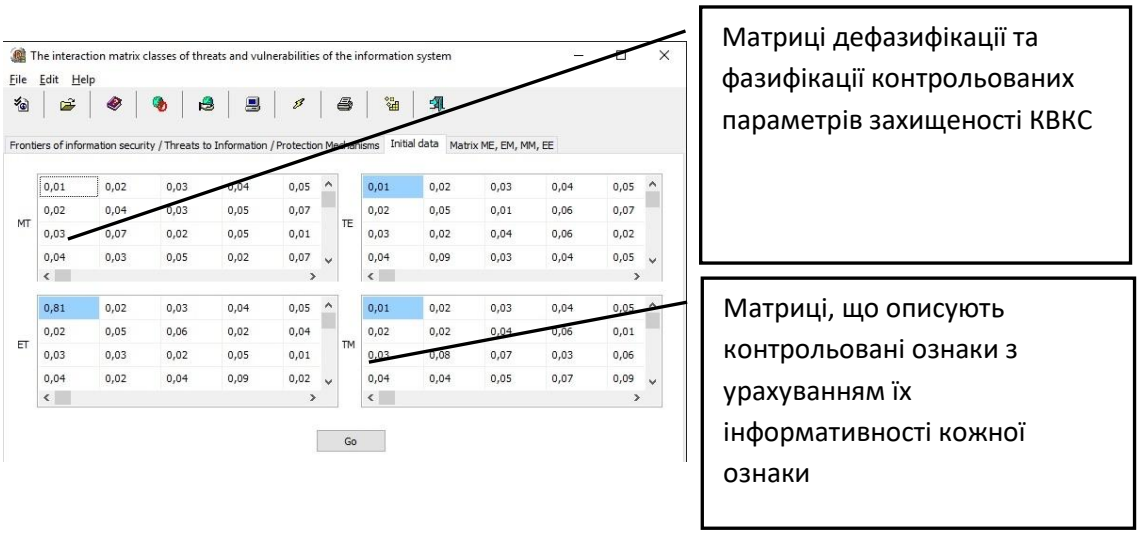
$Md_{i,n_i}^j(t)$ – параметри, що характеризують дискретні стани n_i –го параметра $(n_i = \overline{1, N_i})$; для підсистеми $\left(i = \overline{1,k}\right)$ КВКС, які впливають на виникнення $(j = \overline{1,J})$ *EmS* ;

$m\left(Md_{i,n_i}^j(t)\right)$ – параметри, які характеризують експертне оцінювання ступеня експліційованості впливу n_i-го параметра на появу $(j = \overline{1,J})$ *EmS* .

Отримані значення заносилися в БЗ СППР "Аналізатор загроз" [12] – рис. 3 – при первинному описі експертами. Також можливе занесення даних у БЗ під час автоматичного/автоматизованого збирання показань від датчиків SIEM, мультиагентних систем, сенсорів, що визначають наявність загроз, кібератак, аномалій.



а)



б)

Рисунок 3 – Інтерфейс СППР "Аналізатор загроз"

Якщо експерт виявив нову непередбачувану (позаштатну) ситуацію із захищеністю КВКС, він, має можливість відреагувати на повідомлення віконного інтерфейсу СППР. Після чого експерт робить запис у БЗ. Новий запис характеризує поточний стан підсистем, які ідентифікували нештатні ситуації.

При цьому оцінювання фахівцями виконано на підставі самостійного візуального відстеження показань від датчиків SIEM, мультиагентних систем, сенсорів, що визначають наявність загроз, кібератак, аномалій (червоний колір) і за допомогою СППР (синій колір), як показаено на рис. 4. Еталонне значення оцінюваного параметра захищеності прийнято рівним 1 [1, 11, 13]. Якщо оцінка параметра дорівнює 0 – захист відсутній. Аналогічне оцінювання виконано для показника захищеності серверів КВКС, що проілюстровано на рис. 5.

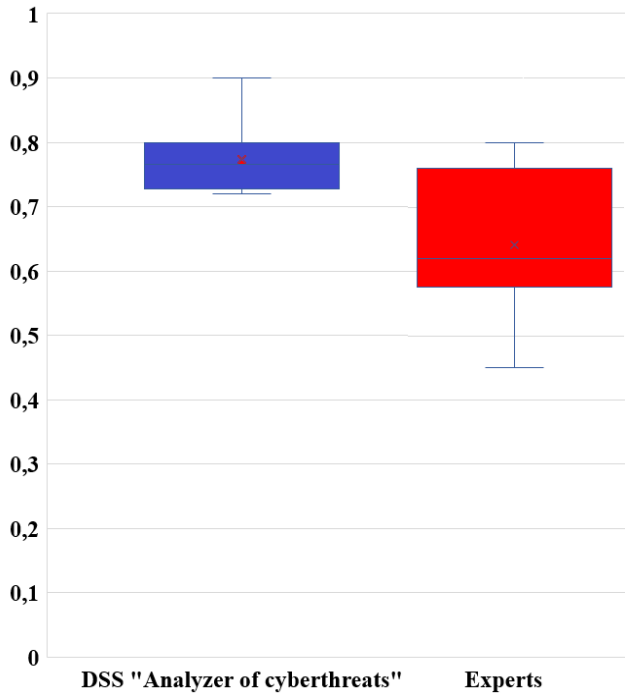


Рисунок 4 – Результати оцінювання експертами самостійно та за допомогою СППР "Аналізатор загроз" ступеня захищеності КВКС

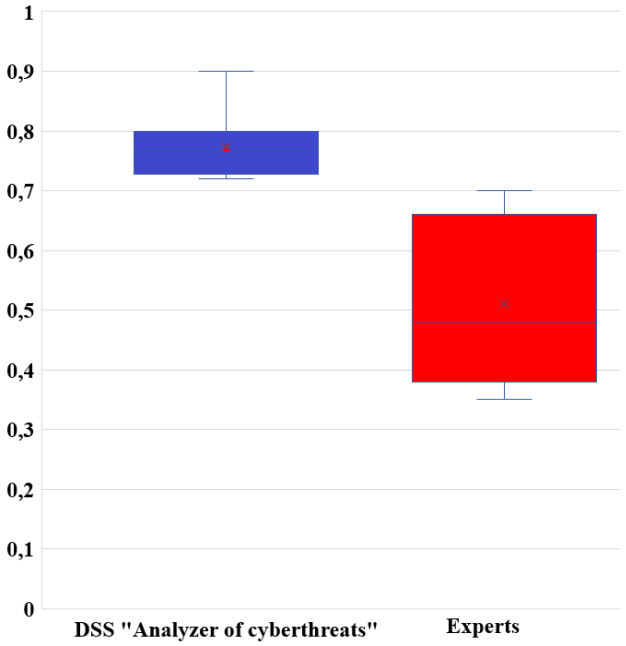


Рисунок 5 – Результати оцінювання експертами самостійно та за допомогою СППР "Аналізатор загроз" ступеня захищеності серверів КВКС

На рис. 4 і 5 видно, що розбіжність у думці експертів, які використовували СППР "Аналізатор загроз", приблизно на 14-18 % менша, ніж для варіанта оцінювання без використання СППР.

Під час тестування прототипу СППР також апробовано механізми взаємодії експертів і СППР "Аналізатор загроз" у процесі синтезу керівних правил у задачах оцінювання ступеня захищеності КВКС.

Висновки. У роботі вперше запропоновано: модель для модуля «нечіткого логічного виводу», який призначений для реалізації підсистеми нечіткого виводу (НечВ). На основі правил нечіткого виводу (НечВ) за вхідними значеннями ДатП визначаються вихідні значення для оцінювання за допомогою СППР ступеня захищеності КВКС. Модель заснована на припущенні, що вхідні значення для підсистеми НечВ були отримані як результат процедури фазифікації у відповідному модулі. Кожен елемент вихідних значень характеризує наявність (відсутність) ознаки непередбаченої ситуації, пов'язаної з аномаліями, атаками чи іншими спробами несанкціонованого втручання у роботу КВКС; алгоритм формування бази знань непередбачених та типових ситуацій у КВКС. Алгоритм відрізняється від відомих тим, що дозволив сформувати сукупність випадків типових варіантів реагування на загрози, аномалії та атаки у КВКС, а також правила виводу для автентифікації непередбачених ситуацій, які пов'язані з цілеспрямованим деструктивним впливом на КВКС.

Показано, що запропоновані моделі та алгоритми експертного вивчення даних від ДатП, відрізняються від відомих тим, що у них застосовуються елементи теорій експертних систем, нечітких множин, а також апарат нечіткої логіки. Використання для модуля «нечіткого логічного виводу» дозволяє забезпечити відображення стану найбільш уразливих компонентів КВКС як багатопараметричний образ (БПВ). Отриманий БПО використовується в СППР для якісної оцінки процесів, що протікають у КВКС. При цьому бралася до уваги можлива «нечіткість» в оцінюванні ситуації із захищеністю КВКС.

Список використаних джерел

1. Lakhno, V., Boiko, Y., Mishchenko, A., Kozlovskii, V., & Pupchenko, O. (2017). Development of the intelligent decision-making support system to manage cyber protection at the object of informatization. Eastern-European Journal of Enterprise Technologies, (2(9)), pp. 53–61.
2. Iasiello, E. (2013, June). Cyber attack: A dull tool to shape foreign policy. In Cyber Conflict (CyCon), 2013 5th International Conference on (pp. 1–18). IEEE.
3. Goztepe, K. (2012). Designing Fuzzy Rule Based Expert System for Cyber Security, International Journal of Information Security Science, 1(1), pp. 13–19.
4. Akhmetov, B., Lakhno, V., Boiko, Y., Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity, Eastern-European Journal of Enterprise Technologies, 1(2 (85)), pp. 4–15.
5. Hu, X., Xu, M., Xu, S., & Zhao, P. (2017). Multiple cyber attacks against a target with observation errors and dependent outcomes: Characterization and optimization. Reliability Engineering & System Safety, 159, pp. 119–133.
6. Yang, Y., Xu, H. Q., Gao, L., Yuan, Y. B., McLaughlin, K., & Sezer, S. (2017). Multidimensional intrusion detection system for IEC 61850-based SCADA networks. IEEE Transactions on Power Delivery, 32(2), pp. 1068–1078.
7. Wong, K., Dillabaugh, C., Seddigh, N., & Nandy, B. (2017). Enhancing Suricata intrusion detection system for cyber security in SCADA networks. In Electrical and Computer Engineering (CCECE), 2017 IEEE 30th Canadian Conference on (pp. 1–5). IEEE.
8. Elhag, S., Fernández, A., Bawakid, A., Alshomrani, S., & Herrera, F. (2015). On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems. Expert Systems with Applications, 42(1), pp. 193–202.
9. Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal: A Global Perspective, 25(1-3), pp. 18–31.
10. Villaluna, J. A., & Cruz, F. R. G. (2017). Information security technology for computer networks through classification of cyber-attacks using soft computing algorithms. In Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), 2017 IEEE 9th International Conference on (pp. 1–6). IEEE.
11. Lakhno, V., Kazmirchuk, S., Kovalenko, Y., Myrutenko, L., & Zhmurko, T. (2016). Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the

coverage matrices of features. Eastern-European Journal of Enterprise Technologies, (3 (9)), pp. 30–38. DOI: 10.15587/1729-4061.2016.71769.
12. Lakhno, V., Tkach, Y., Petrenko, T., Zaitsev, S., & Bazylevych, V. (2016). Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks. Eastern-European Journal of Enterprise Technologies, (6 (9)), pp. 32–44. DOI: 10.15587/1729-4061.2016.85600
13. Zhang, Y., Wang, L., Xiang, Y., & Ten, C. W. (2016). Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation. IEEE Transactions on Power Systems, 31(6), pp. 4379–4394.

Kasatkin Dmytro,
Candidate of Pedagogical Sciences, Head of the Department of Computer Systems, Networks and Cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

Voloshyn Semen,
Candidate of Engineering Sciences, Associate Professor of the Department of Computer Systems, Networks and Cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID https://orcid.org/0000-0002-4913-7003
E-mail: voloshyn@nubip.edu.ua

Gusev Borys,
Candidate of Engineering Sciences, Associate Professor of the Department of Computer Systems, Networks and Cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID https://orcid.org/0000-0003-1658-7822
E-mail: gusevbs@gmail.com

Matiievskyi Volodymyr,
Senior Lecturer of the Department of Computer Systems, Networks and Cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID https://orcid.org/0000-0002-1954-8493
E-mail: m_vv@outlook.com

ALGORITHMS FOR THE DEVELOPMENT OF A KNOWLEDGE BASE TO ENHANCE DECISION SUPPORT SYSTEMS IN ADDRESSING CYBERSECURITY CHALLENGES

Annotation. *This article presents the development of a modular decision support system (DSS) for cybersecurity, aimed at enhancing the protection of critical computer systems (CCS). The system is based on a fuzzy logic inference subsystem (FIS) model that utilizes data from sensors and SIEM systems to detect signs of threats, anomalies, and attacks through fuzzification of input values. A developed algorithm for forming a knowledge base of typical and emergency situations allows the system not only to effectively respond to known threats but also to analyze unforeseen situations. The application of the FIS module enables the creation of a multi-parameter image of CCS vulnerability, which ensures a more comprehensive and accurate assessment of their security.*

Keywords: *critical computer systems, cybersecurity, decision support system, security assessment.*