КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.20.174182
УДК 004.056.53

Добришин Юрій Євгенович
к.т.н., доцент
ORCID ID: 0000-0003-2473-9507
Національна академія Служби безпеки України, м. Київ
ydobryshyn@gmail.com

Сидоренко Сергій Миколайович
старший викладач
ORCID ID: 0009-0003-1185-1505
Національна академія Служби безпеки України, м. Київ
s.s.m.ukr@gmail.com

Ворохоб Максим Віталійович
аспірант кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5160-7134
m.vorokhob.asp@kubg.edu.ua

АВТОМАТИЗОВАНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ЩОДО ВІДНОВЛЕННЯ ПОШКОДЖЕНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВНАСЛІДОК ВПЛИВУ КІБЕРАТАК

Анотація. У роботі розглядаються технологічні питання вирішення актуальної задачі щодо розробки структурно-логічної схеми, яка є підставою для створення автоматизованої системи підтримки прийняття рішення, призначеної для відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак.

На підставі проведених досліджень процесів діагностування та відновлення програмного забезпечення, розгляду та аналізу наукових робіт у галузі проектування, розробки, впровадження спеціалізованих автоматизованих систем підтримки прийняття рішення запропонована структура автоматизованої системи підтримки прийняття рішення, яка призначена для відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак.

Зазначена система являє собою складну ієрархічну структуру з високим рівнем організації та складається з окремих підсистем, які забезпечують виконання задач діагностування пошкодженого програмного забезпечення, визначення способів його відновлення, призначення оптимальної послідовності технологічних операцій щодо забезпечення працездатності програмного забезпечення після впливу кібератак.

Програмні модулі зазначеної системи дозволяють проводити аналіз процесів виходу з ладу програмного забезпечення після навмисних дії, які здійснюються за допомогою засобів електронних комунікацій, а також застосовувати технології діагностування, на базі яких можливо використовувати формалізовані методики рішення окремих задач щодо призначення операцій з відновлення дефектів програмного забезпечення автоматизованих інформаційно-телекомунікаційних систем, а також визначити внутрішній зміст операцій та взаємозв'язки між ними.

Впровадження автоматизованої системи підтримки прийняття рішення, призначеної щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак, дозволяє забезпечити виконання автоматизованого проектування технологічних процесів відновлення пошкодженого програмного забезпечення враховуючі складність формалізації, неповноти і суперечливості інформації, а також застосування певної послідовності управлінських операцій і процедур.

Ключові слова: автоматизована інформаційно-телекомунікаційна система, діагностування, структурно-логічна схема, системи підтримки прийняття рішень, дефекти програмного забезпечення, способи відновлення.

ISSN 2663 - 4023

ПОСТАНОВКА ПРОБЛЕМИ

Суттєвою проблемою щодо визначення причин пошкодження компонентів програмного забезпечення та виявлення дефектів у його роботі внаслідок впливу кібератак, є неповнота і суперечливість інформації стосовно властивостей дефектів, способів їх відновлення, а також переліку технологічних операцій та послідовності їх призначення з метою забезпечення захисту електронних інформаційних ресурсів, що обробляються в автоматизованих інформаційно-телекомунікаційних системах та комплексах.

Технологію відновлення пошкодженого програмного забезпечення складно формалізувати за відсутності теорії і математичних моделей, що описують функціональні залежності між об'єктами, які приймають участь у процесі діагностування та відновлення пошкодженого програмного забезпечення.

Розв'язання вище описаної задачі потребує застосування спеціального математичного апарату, а також розробки методичних та технологічних засад щодо створення та впровадження спеціалізованих автоматизованих систем, призначених для підтримки прийняття рішення (далі - СППР) з метою відновлення пошкодженого програмного забезпечення, внаслідок впливу кібератак.

Це дозволить класифікувати та виявляти якісні зв'язки між технологічними операціями, а також формалізувати технологію їх призначення за допомогою прийняття рішень відносно розв'язання складних структурованих або неструктурованих завдань стосовно оптимального вибору способу відновлення дефектів та технологічних операцій щодо усунення дефектів.

Саме тому автори вважають питання розробки та застосування систем підтримки прийняття рішень, спрямованих на виявлення дефектів пошкодженого програмного забезпечення, актуальними і такими, що потребують вирішення.

Аналіз останніх досліджень і публікацій.

На теперішній час дослідженням та розробкою систем підтримки прийняття рішення активно займаються вітчизняні та закордонні науковці.

Проблеми формування методології проектування, класифікації, архітектури, розробки та застосування систем підтримки прийняття рішення, а також методів та моделей прийняття раціональних рішень на підставі системного аналізу висвітлюються у роботах багатьох вчених, таких як П.І. Бідюк, В.Л. Бурячок, А.Д Кожухівський, О.В Нестеренко, С.В. Цюцюра, А.В. Яцишин, О. Ф.Волошин, В.Ф. Ситник та інші.

Так у наукових працях [1-4] представлені методологія проектування інформаційних систем підтримки прийняття рішень та альтернативні підходи до застосування і супроводження СППР. Особливий інтерес у зазначених наукових роботах представляє запропонований метод розробки систем підтримки прийняття рішень на основі мережі Байєса, а також систем, обробка інформації в яких здійснюється шляхом використання експертних оцінок.

У роботах [5, 6] розглядаються теоретичні та практичні питання щодо технології прийняття рішень, яка передбачає застосування певної послідовності управлінських операцій і процедур, які необхідні під час використання СППР. Значна увага приділяється операціям присвяченим питанням діагностування виявлених проблем, визначення можливих способів їх розв'язання та оцінювання варіантів їх усунення.

Окремі дослідники [7, 8], спираючись на важливість забезпечення рівня інформаційної безпеки автоматизованих систем та комплексів під час накопичування та обробки даних, пропонують застосування СППР для практичної реалізації процесів обробки інформації евристичного походження, а також щодо підвищення рівня

інформаційної безпеки підприємств, на підставі індивідуального підбору методів та засобів, що належать до політики безпеки суб'єкта господарювання, з використанням експертних даних.

Інтерес представляє робота науковців [9], яка може бути взята за основу для розробки концептуальних підходів з проектування систем підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. У дослідженні, на підставі досвіду та наукових джерел надаються методичні матеріали щодо розробки систем управління екологічною безпекою. На думку фахівців у галузі екологічної безпеки, такі системи необхідні для виявлення негативних тенденцій в екологічних процесах, знаходження взаємозв'язків між параметрами і факторами, що впливають на екологічну безпеку, а також розробку пропозицій щодо покращення стану управління екологічною безпекою.

Питання безпеки систем підтримки прийняття рішень розглядається у роботі [10]. Автори стверджують , що внаслідок загроз інформаційній та кібербезпеці, питання захисту інформації в СППР набувають усе більшої актуальності та пропонують методичні, технологічні заходи, а також програмні засоби щодо побудови захищених СППР.

Мета дослідження.

Метою статті є надання методичних рекомендацій та пропозицій з питань розробки структурно-логічної схеми автоматизованої системи підтримки прийняття рішення, яка дозволяє визначати властивості дефектів програмного забезпечення, способи та послідовність їх відновлення після впливу кібератак

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак, являє собою складну ієрархічну структуру з високим рівнем організації. У відповідності до призначення зазначена система повинна забезпечити виконання наступних завдань:

$$Z=\{zi\},i=1....n \quad (1)$$

де:

z1 - введення завдання;

*z*2 - прийняття рішення;

*z*3 – програмна реалізація щодо прийняття рішення;

z4 – зберігання постійної інформації;

*z*5 – надання результатів рішення завдання у текстовій та графічній інформації;

*z*6– визначення спеціальних завдань;

*z*7 – оцінювання результатів;

Система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак включає ряд підсистем, а саме, з методичних, технічних, інформаційних, введення бази даних тощо (див-рисунок).

Структура СППР щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак

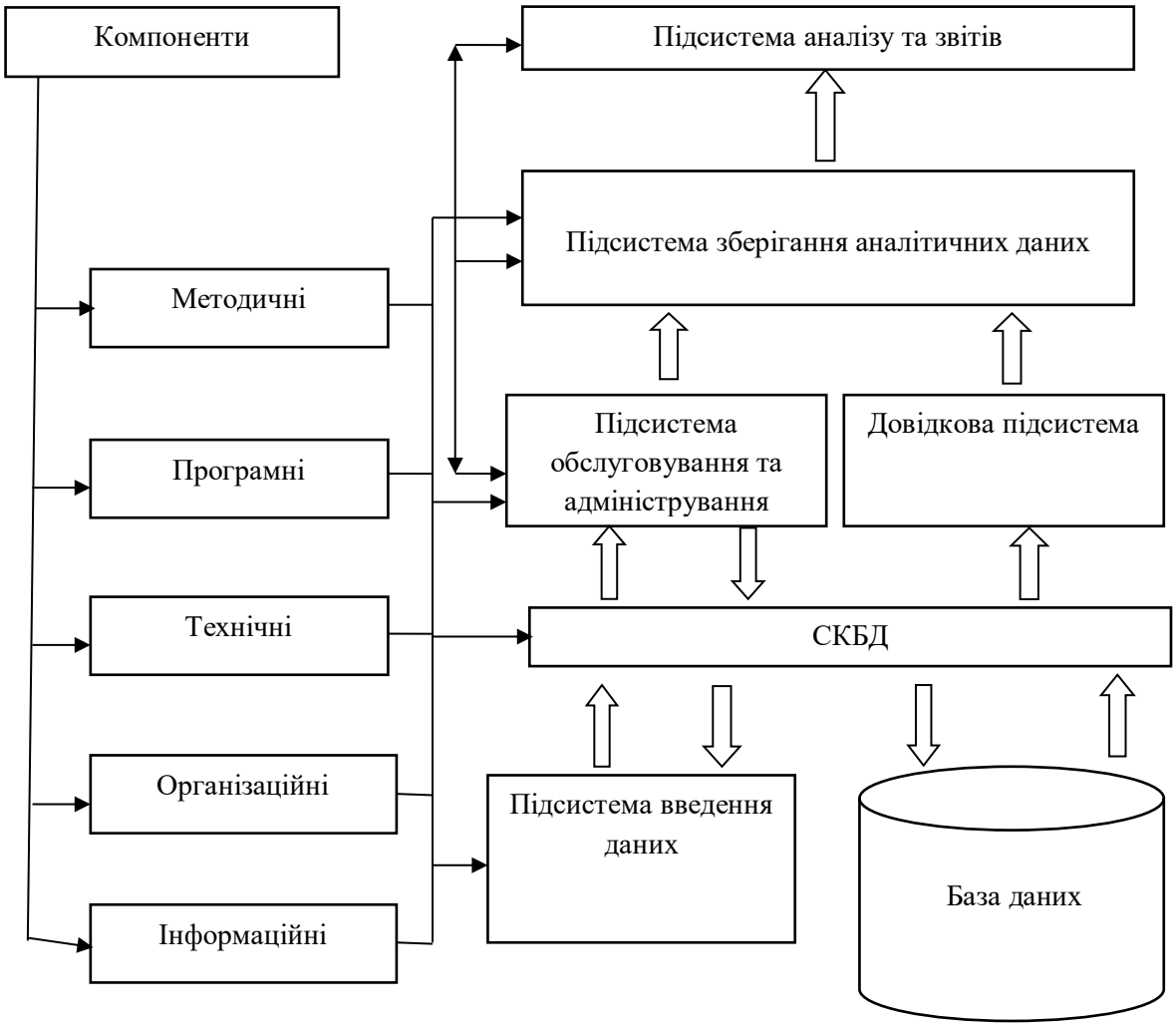

Рис.1 Структурна схема СППР щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак

Компонентами методичного забезпечення в СППР є документи, що регламентують технологію процесу прийняття рішення під час роботи з системою.

Метою документів є організація функціонування СППР з мінімальними витратами та високою якістю прийняття рішень. Така задача передбачає проведення робіт з формалізації процесу прийняття та підтримки рішень, яка визначає послідовність виконання кожної проектної задачі, з максимально структурованим описом прийняття рішення.

Робота СППР щодо відновлення пошкодженого програмного забезпечення внаслідок впливу передбачає наступне:

- надання відомостей, що стосується інформації о можливих комп'ютерних атаках, дефектів програмного забезпечення, прогнозованих ситуаціях та наслідків від прийняття рішення;

- визначення способів відновлення дефектів пошкодженого програмного забезпечення, їх аналіз та можливість корегування;

- оцінку прийнятих рішень, формування послідовності операцій та кращого маршруту відновлення програмного забезпечення.

Завдання СППР – автоматизація усіх процедур прийняття рішень, пошук інформації та її аналіз, попередню обробку інформації та прийняття самого рішення. Окремі процедури в СППР не підлягають формалізації, тому частина з них буде виконуватися у інтерактивному режимі.

Програмні компоненти СППР реалізують типові запити. Зазначені запити повинні включати опис структури даних, типові команди, складні лексеми. Під час застосування запитів, передбачається вивід результатів запиту у форматі мови XML.

Особливе значення у СППР приділяється інформаційно-довідкової підсистемі. Засоби зазначеної підсистеми, повинні реалізувати введення інформації, формування словників щодо опису ситуацій, виводу довідкової інформації, можливість підключення зовнішніх програмних компонентів.

У системі активно використовується реляційна база даних, програмні засоби якої повинні забезпечувати зберігання інформації та надання її користувачам системи у зручному форматі.

У якості програмного продукту, який підтримує структурні компоненти бази даних, може бути використовуватися програмне забезпечення сучасних систем керування базою даних (СКБД). Екземпляр СКБД повинен підтримувати роботу декілька баз та забезпечувати їх управління та адміністрування, використовуючи для цього простий та зручний інтерфейс. Основу структури бази даних складають таблиці, між якими забезпечується взаємозв’язок. Для забезпечення цілісності даних в таблицях застосовуються ключові поля.

Для зберігання інформації в СППР виконується створення резервної копії, а також передбачена можливість відновлення роботи системи в разі пошкодження файлів даних або інформаційних масивів бази.

Засоби програмного забезпечення СППР повинні забезпечувати:

- супроводження бази даних інформаційного забезпечення системи (введення, отримання нормативно-довідкової інформації, класифікаторів, довідників, картотек);

- кодування інформації;

- працездатність СППР у локальної мережі підприємства;

- застосування клієнт-серверної архітектури;

- застосування сучасних телекомунікаційних технологій та введення електронної пошти;

- багатокористувальний режим роботи користувачів;

- цілодобовому режимі.

Програмне забезпечення СППР відноситься до спеціального програмного забезпечення, яке може працювати під управлінням різних версій операційної системи Windows. Зазначене спеціальне програмне забезпечення СППР забезпечує рішення інформаційно-аналітичних, розрахункових та завдань щодо виконання технологічних операцій з визначення стану дефекту програмного забезпечення, призначення способу його відновлення та послідовності усунення дефектів програмного забезпечення. Крім того програмне забезпечення є уніфікованим засобом щодо організації інформаційної взаємодії між користувачами і окремими програмними компонентами (модулями).

Компонентами технічного забезпечення СППР щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак, є комплекс технічних засобів у складі серверного та мережного обладнання, клієнтські машини.

Інформаційне забезпечення СППР містіть інформацію про існуючі кібератаки, які можуть виникати під час експлуатації автоматизованих систем та комплексів, дефекти програмного забезпечення, способи їх відновлення, технологічні операції що застосовуються з метою забезпечення відновлення роботи програмних компонентів систем тощо.

Інформацію, яка обробляється в СППР, можливо позначити як *{І}*. Зазначена інформація включає множену інформації *{Ік},* що необхідна для керування системою, множену вхідній інформації *{Ів}*, множену термінальної інформації*{ІТ}*.

Множена інформації для керування СППР може бути описана, як:

$$Ік= \{Ік1,\ Ік2, Ік3\}, \quad (2)$$

де:

Ік1,- інформація що належить до програм;

Ік2 - інформація, що належить до проектних рішень;

Ік3 – відомості щодо оцінки прийняття рішень;

Вхідна інформація *{Ів}* включає:

$$Ів= \{Ів1,\ Ів2, Ів3\}, \quad (3)$$

Ів1 – інформацію, що містить вхідні данні щодо наявні дефекти програмного забезпечення;

Ів2 – інформацію, що є загальної для системи;

*Ів**3*** – інформацію**,** що містить нормативно-довідникові данні, необхідні для введення аналізу та прогнозування. Зазначена інформація представляє собою форми документів, які можуть бути первинними, вторинними та нормативними. Вторинні документи розподілені на групи: текстові, звіти, класифікатори, картотеки. Для організації інформаційного забезпечення у підсистемі СППР використовуються принципи удосконалення інформації.

Під час організації інформаційного забезпечення підтримуються власні принципи:

- виключення масових первинних документів;
- застосування єдиних потоків інформації;
- одноразове введення повідомлень в систему;
- використання інформації, яка має оптимальну цінність.

Форми усіх документів системи уніфіковані. Це дозволяє значно покращити трудомісткість налаштування програм, а також експлуатації підсистеми.

Під час роботи уся інформація, що використовується на ручних операціях, значна зменшена за рахунок того, що користувач здійснює роботу з системою у інтерактивному режимі, шляхом введення в систему запитань та отримання від машини відповіді.

Система класифікації та кодування побудована на локальних цифрових кодах, які використовуються в основному самою системою

Нормативна база підсистеми зберігається у масивах бази. Додатково у системі використовуються групи документи, які класифікуються на первинні, вторинні та нормативні документи.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШОГО ДОСЛІДЖЕННЯ

Аналіз впровадження та експлуатації у різних галузях виробництва автоматизованих СППР дозволяють розробити та запропонувати структурно-логічну схему автоматизованої системи прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Запропонована схема являє собою складну ієрархічну структуру з високим рівнем організації та складається з окремих підсистем, які забезпечують виконання задач з аналізу дефектів програмного забезпечення, вибору способів їх відновлення, оцінку та обрання найкращих альтернатив відновлення.

Дана технологія обробки інформації в СППР по відновленню пошкодженого програмного забезпечення внаслідок впливу кібератак, у подальшому дає можливість здійснювати прийняття рішень відносно розв’язання складних структурованих або неструктурованих задач з метою оптимального вибору способу відновлення дефектів та технологічних операцій по їх усуненню.

СПИСОК ВИКОРИТАНИХ ДЖЕРЕЛ

1 Бідюк, П.І., Кожухівський, А.Д., Кожухівська, О.А. (2013). Система підтримки прийняття рішень для аналізу і прогнозування стану підприємства. *Радіоелектроніка, інформатика, управління*, 1, 128-136.

2 Бідюк, П.І,. Терентьєв, О.М,. Коновалюк, М.М. (2010). Байєсівські мережі в технологіях інтелектуального аналізу даних. *Штучний інтелект*, 2, 104-113.

3 Нестеренко, О.В,. Савенков, О.І,. Фаловський, О.О. (2016). *Інтелектуальна система підтримки прийняття рішень: навч. посібн.* Національна академія управління.

4 Ситник, В.Ф., Дубровіна, А.В. (2002). Проблеми моделювання рішень у групових СППР. *Моделювання та інформаційні системи в економіці*, 68, 9-14.

5 Цюцюра, С.В,. Криворучко, О.В,. Цюцюра, М.І. (2012). Теоретичні основи та сутність управлінських рішень. Моделі прийняття управлінських рішень. *Управління розвитком складних систем*, *9*, 50-58.

6 Волошин, О.Ф. Мащенко, С.О. (2010). Моделі та методи прийняття рішень: навч. посіб. Видавничо-поліграфічний центр "Київський університет".

7 Бурячок, В.Л., Толюпа, С.В., Аносов, А.О., Козачок, В.А., Лукова-Чуйко, Н.В. (2015). Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. ДУТ.

8 Азарова, А.О, Дьогтєва, І.О, Шиян, А.А. (2022). Система підтримки прийняття рішень щодо підвищення рівня інформаційної безпеки підприємства. *Інформаційні технології та комп’ютерна інженерія*, *1*, 12-18.

9 Яцишин, А. В., Попов, О.О., Артемчук, В.О., Ковач, В.О., Зінов’єва, І.С. (2019). Автоматизовані інформаційні системи підтримки прийняття управлінських рішень у галузі екологічної безпеки. *Інформаційні технології і засоби навчання*, 4, 286-300.

10 Ковтунець, В.В., Нестеренко, О.В., Савенков, О.І. (2016). Безпека систем підтримки прийняття рішень: навч. посіб. Київ: Національна академія управління.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023

Dobryshyn Yurii
Ph.D., associate professor
ORCID ID: 0000-0003-2473-9507
National Academy of the Security Service of Ukraine, Kyiv
ydobryshyn@gmail.com

Sydorenko Serhii
Senior Lecturer
ORCID ID: 0009-0003-1185-1505
National Academy of the Security Service of Ukraine, Kyiv
s.s.m.ukr@gmail.com

Vorokhob Maksym
postgraduate student
Volodymyr Buriachok Department of Information and Cybersecurity
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0001-5160-7134
m.vorokhob.asp@kubg.edu.ua

AUTOMATED DECISION SUPPORT SYSTEM FOR RESTORING DAMAGED SOFTWARE AS A RESULT OF CYBERATTACKS

Abstract. The paper examines the technological issues of solving the current problem of developing a structural and logical scheme, which is the basis for creating an automated decision support system designed to restore damaged software as a result of cyberattacks.
On the basis of research into the processes of software diagnosis and recovery, review and analysis of scientific works in the field of design, development, implementation of specialized automated decision support systems, the structure of an automated decision support system designed to restore damaged software due to the impact of cyberattacks is proposed.
The specified system is a complex hierarchical structure with a high level of organization and consists of separate subsystems that ensure the performance of the tasks of diagnosing damaged software, determining methods of its recovery, and determining the optimal sequence of technological operations to ensure the functionality of the software after the impact of cyber attacks.
The software modules of the specified system make it possible to analyze the processes of software failure after intentional actions, which are carried out with the help of electronic communications, as well as to apply diagnostic technologies, on the basis of which it is possible to use formalized methods of solving individual problems regarding the assignment of operations to repair software defects of automated information and telecommunication systems, as well as to determine the internal content of operations and the relationships between them.
The implementation of an automated decision support system designed to restore damaged software as a result of cyberattacks allows for automated design of technological processes for restoring damaged software, taking into account the complexity of formalization, incompleteness and inconsistency of information, as well as the application of a certain sequence of management operations and procedures.

Keywords: automated information and telecommunication system, diagnostics, structural and logical scheme, decision support systems, software defects, recovery methods.

REFERENCES

1 Bidiuk, P.I., Kozhukhivskyi, A.D., Kozhukhivska, O.A. (2013). Systema pidtrymky pryiniattia rishen dlia analizu i prohnozuvannia stanu pidpryiemstva. Radioelektronika, informatyka, upravlinnia, 1, 128-136.
2 Bidiuk, P.I,. Terentiev, O.M,. Konovaliuk, M.M. (2010). Baŷiesivski merezhi v tekhnolohiiakh intelektualnoho analizu danykh. Shtuchnyi intelekt, 2, 104-113.
3 Nesterenko, O.V,. Savenkov, O.I,. Falovskyi, O.O. (2016). Intelektualna systema pidtrymky pryiniattia rishen: navch. posibn. Natsionalna akademiia upravlinnia.

4 Sytnyk, V.F., Dubrovina, A.V. (2002). Problemy modeliuvannia rishen u hrupovykh SPPR. Modeliuvannia ta informatsiini systemy v ekonomitsi, 68, 9-14.
5 Tsiutsiura, S.V,. Kryvoruchko, O.V,. Tsiutsiura, M.I. (2012). Teoretychni osnovy ta sutnist upravlinskykh rishen. Modeli pryiniattia upravlinskykh rishen. Upravlinnia rozvytkom skladnykh system, 9, 50-58.
6 Voloshyn, O.F. Mashchenko, S.O. (2010). Modeli ta metody pryiniattia rishen: navch. posib. Vydavnycho-polihrafichnyi tsentr "Kyivskyi universytet".
7 Buriachok, V.L., Toliupa, S.V., Anosov, A.O., Kozachok, V.A., Lukova-Chuiko, N.V. (2015). Systemnyi analiz ta pryiniattia rishen v informatsiinii bezpetsi: pidruchnyk. DUT.
8 Azarova, A.O, Dohtieva, I.O, Shyian, A.A. (2022). Systema pidtrymky pryiniattia rishen shchodo pidvyshchennia rivnia informatsiinoi bezpeky pidpryiemstva. Informatsiini tekhnolohii ta kompiuterna inzheneriia, 1, 12-18.
9 Iatsyshyn, A. V., Popov, O.O., Artemchuk, V.O., Kovach, V.O., Zinovieva, I.S. (2019). Avtomatyzovani informatsiini systemy pidtrymky pryiniattia upravlinskykh rishen u haluzi ekolohichnoi bezpeky. Informatsiini tekhnolohii i zasoby navchannia, 4, 286-300.
10 Kovtunets, V.V., Nesterenko, O.V., Savenkov, O.I. (2016). Bezpeka system pidtrymky pryiniattia rishen: navch. posib. Kyiv: Natsionalna akademiia upravlinnia.