DOI: https://doi.org/10.36910/6775-2524-0560-2024-55-11
УДК 519.816(004.056)
Добришин Юрій Євгенович, к.т.н., доцент
https://orcid.org/0000-0003-2473-9507
Національна академія Служби безпеки України, м. Київ

ФОРМАЛІЗАЦІЯ ПРОЦЕСУ ПРОЕКТУВАННЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ПІДВИЩЕННЯ РІВНЯ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Добришин Ю.Є. Формалізація процесу проектування систем підтримки прийняття рішень щодо підвищення рівня захисту програмного забезпечення. В роботі представлені дослідження можливості формалізації процесу проектування систем підтримки прийняття рішень щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Проблема проектування вказаних систем пов'язана з тим, що внаслідок дії кібератак складно однозначно визначити їх тип, стан та характер пошкодженого програмного забезпечення автоматизованих систем та комплексів, суперечливість відомостей про дефекти, способи їх виявлення та усунення, а також призначити оптимальний перелік технологічних операцій з відновлення програмних компонентів, що експлуатуються. Рішення описаної задачі потребує розробки та застосування формалізованих методів щодо проектування компонентів систем підтримки прийняття рішень, призначених для відновлення пошкодженого програмного забезпечення внаслідок дії кібератак, та адаптування спеціального математичного апарату щодо класифікації інформації та технологій відновлення дефектів пошкодженого програмного забезпечення шляхом прийняття рішень відносно завдань, які складно формалізуються. Процеси проектування повинні включати аналіз проектної діяльності у галузі захисту інформації; оцінку інформації, що використовується протягом експлуатації різних автоматизованих систем; характеристику та можливості засобів захисту інформації, що здійснюють виявлення загроз та кібератак; аналіз дефектів програмного забезпечення; розробку алгоритмів та методичних матеріалів, що функціонують та використовуються у системах підтримки прийняття рішень.
Ключові слова: системи підтримки прийняття рішень, процес проектування, формалізація, кібератака, дефект програмного забезпечення, автоматизовані системи та комплекси, кіберзагроза, кібербезпека

Dobryshyn Yu. Formalization of the design process of decision-making support systems for increasing of the level of software protection. The work presents research opportunities formalization of the design process of decision-making support systems for the restoration of damaged software due to the impact of cyber attacks. The problem of designing the specified systems is related to the fact that due to cyberattacks it is difficult to unambiguously determine their type, state and nature of damaged software of automated systems and complexes, inconsistency of information about defects, methods of their detection and elimination, as well as to assign an optimal list of technological operations with recovery of software components that are in use. The solution to the described problem requires the development and application of formalized methods for the design of components of decision-making support systems intended for the restoration of damaged software as a result of cyber-attacks, and the adaptation of a special mathematical apparatus for the classification of information and technologies for repairing defects in damaged software by making decisions regarding tasks that are difficult are formalized. Design processes should include analysis of design activities in the field of information protection; evaluation of information used during operation of various automated systems; characteristics and capabilities of information protection tools that detect threats and cyberattacks; analysis of software defects; development of algorithms and methodical materials that function and are used in decision support systems.
Keywords: decision support systems, design process, formalization, cyber attack, software defect, automated systems and complexes, cyber threat, cyber security

Постановка наукової проблеми. Останнім часом серйозна увага приділяється питанням проектування та створення систем підтримки прийняття рішень, що застосовуються в підрозділах для виявлення, попередження та усунення вторгнень в комп'ютерні системи та мережі (далі-СППР). На думку фахівців, на теперішній час відсутній формалізований математичний опис багатьох процесів, що відбуваються під час та застосування сучасних кібератак, способів їх усунення, призначення оптимальних маршрутів відновлення програмного забезпечення автоматизованих систем та комплексів. Все це заважає здійснювати достовірно процес проектування компонентів та програмних модулів СППР щодо підвищення рівня захисту програмного забезпечення.

На теперішній час існує проблема, коли значна вартість та трудомісткість проектування систем підтримки прийняття рішень затримують впровадження компонентів, що належать до їх складу. Це призводить до погіршення використання засобів обчислювальної техніки та малої ефективності СППР.

Усунення зазначеної диспропорції можливе тільки за рахунок удосконалення технології проектування, яка має декілька суттєвих принципових відмінностей, внаслідок того, що СППР розробляється для автоматизованих систем та комплексів, які отримують пошкодження або збій у роботі програмного забезпечення, після дії різних кібератак, появи дефектів, для яких необхідно

прийняти рішення щодо характеру їх впливу на працездатність програмного забезпечення автоматизованих систем та комплексів, відповідно до чого призначити оптимальні способи відновлення їх працездатності.

Виникає задача, яка дозволяє здійснювати розробку СППР з використанням вже раніше існуючих типових частин програмного забезпечення, що достатньо якісно зарекомендували себе в роботі під час прийняття різних складних рішень, з додатковим доопрацюванням окремих пакетів прикладних програм СППР та з урахуванням захисту інформації в наслідок впливу кібератак. Не виключається можливість здійснювати розробку проектів СППР щодо захисту інформації з повторним використанням відомих проектів вже існуючих СППР.

Таким чином, за рахунок використання вказаних підходів, час розробки СППР зменшується, але збільшуються помилки проектування внаслідок неможливості вдосконалення технології проектування СППР, призначених щодо захисту інформації, враховуючи особливості технологій виявлення кібератак, оцінювання дефектів та визначення способів відновлення пошкодженого програмного забезпечення.

Виникає унікальна задача, яка передбачає проведення робіт з формалізації процесу проектування СППР, шляхом аналізу проектної діяльності у галузі захисту інформації, визначення відомостей, необхідних для проектування, розробки алгоритмів, що функціонують в СППР та створення необхідних методичних матеріалів.

Аналіз досліджень. Проблеми створення та застосування методології проектування систем підтримки прийняття рішень, останнім часом активно розглядаються у роботах багатьох вітчизняних та закордонних фахівців. Це пов'язано з тим, що для застосування політики безпеки під час обробки інформації та забезпечення безперервності бізнесу, компаніям необхідно впроваджувати системи управління ризиками в сфері інформаційної безпеки [1, 2].

На думку фахівців протистояти постійному збільшенню та складності кібератакам можна, зокрема, за допомогою програмних компонентів, що здійснюють розпізнавання кібератак та забезпечені модулями системи підтримки прийняття рішень, які поєднують знання та досвід прийняття рішень з питань відновлення пошкодженого програмного забезпечення.

Аналізуючи роботи багатьох авторів, необхідно зазначити, що у статтях окремим напрямком представлені дослідження у галузі проектування та застосування СППР, а також описуються методи розробки їх моделей та програмного забезпечення [3], включаючи розробку експертних систем [4, 5].

Суттєвим недоліком окремих статей [6, 7] є відсутність архітектурної реалізації СППР, адекватної до реального процесу обробки інформації. Це пов'язане з тим, що процеси, які виникають під час впливу кіберзагроз важно формалізувати. Тому, за висновком авторів, більшість СППР та експертних систем значну частину часу знаходяться у стадії тестування.

Інтерес представляє робота авторів [8], де розглядаються недоліки існуючих СППР та експертних систем, що застосовуються у галузі інформаційної безпеки. До таких недоліків належать необхідність присутності висококваліфікованих фахівців при складанні бази знань, труднощі алгоритмізації складних процесів відновлення програмного забезпечення тощо.

У науковій роботі представлена система підтримки прийняття рішень, заснована на аналітичному ієрархічному процесі та методах змішаного цілісного програмування для оптимального вибору дій щодо забезпечення інформаційної безпеки підприємства.

Запропонований підхід дозволяє максимізувати величину ризику при фіксованій сумі бюджету за рахунок визначення оптимального набору запобіжних заходів. СППР також допомагає особам, які ухвалюють рішення на підприємстві, визначити мінімальний бюджет інформаційної безпеки підприємства для заданого рівня ризику.

Продовження зазначеного підходу щодо проектування СППР досліджується у наукових працях [9 - 12], де автори розглядають теоретичні та практичні питання з технології підтримки прийняття рішень та пропонують ряд цікавих методів для розробки СППР, які базуються на аналізі та обробці інформації, шляхом використання експертних оцінок, певної послідовності управлінських операцій та процедур.

В зазначених наукових роботах питання розробки та застосування СППР вирішуються на підставі індивідуального аналізу політики безпеки суб'єкта господарювання з використанням індивідуальних методів та засобів проектування програмних компонентів СППР. Автори вважають,

що в основу розробки СППР повинен покладений системний підхід та моделювання процесами виявлення дефектів програмного забезпечення та їх усунення за рахунок взаємозв'язку між атаками та організаційними та технологічними заходами політики інформаційної безпеки. На думку фахівців такий підхід суттєво забезпечити рівень інформаційної безпеки на підприємстві.

Аналізуючи матеріали декілька робіт з питань розробки СППР [13 - 15], необхідно зазначити, що автори у своїх наукових працях пропонують шляхи щодо розробки моделі підтримки прийняття рішень у галузі кібербезпеки, яка базується на аналізі ризиків, враховуючи тільки фінансові фактори загроз. Такий підхід може бути ефективним для підтримки економічно-орієнтованих рішень, але не враховує структуру кібербезпеки підприємства.

Інша група авторів [16] пропонує підходи щодо проектування системи підтримки прийняття рішень, враховуючи аналіз ризиків та структури кібербезпеки, відповідно до існуючих стандартів. На думку авторів така модель забезпечує належний захист інформації та практично без помилок визначає загрози та кібератаки. У роботі, також надаються результати рекомендацій щодо проектування СППР у вигляді статистичної оцінки захисту інформації автоматизованої системи, які отримані шляхом практичного проведення атак на її програмне забезпечення.

Таким чином, огляд та систематизація матеріалу розглянутих наукових праць вказує на необхідність продовження робіт щодо формалізації процесів проектування СППР щодо підвищення рівня захисту програмного забезпечення. Такі дослідження повинні бути направлені на розробку методів проектування складних нетипових задач, які виникають під час виявлення та дії кібератак, враховуючи вимоги та обмеження, що визначають порядок обробки інформації на підприємстві під час її експлуатації, а також супроводження та адміністрування програмного забезпечення автоматизованих систем та комплексів.

Мета роботи. Метою статті є дослідження можливості формалізації процесу проектування систем підтримки прийняття рішень, призначених для відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак та надання пропозицій щодо розробки структурно-логічної схеми вказаних систем.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Проектування компонентів СППР щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак, представляє собою складну задачу. Складність проектування визначається тім, що сам процес розробки компонентів вказаної системи ще недостатньо формалізований.

У процесі проектування вирішуються наступні проектні задачі B_j із застосування та допомогою різних формалізованих методик проектування

$$A = \{A_1, A_2\ A_3 \ldots\ldots A_{11}\}, \quad (1)$$

де: A_1 – дослідження інформаційного об'єкту ;

A_2 – аналіз потоків інформації щодо появи кібератаки;

A_2 - аналіз характеристик кібератаки;

A_3 – попередня оцінка рівня загрози програмного забезпечення;

A_4 – надання пропозицій щодо можливих дефектів програмного забезпечення, які виникають у наслідок дії кібератаки;

A_5 – аналіз інформації, отриманої за результатами дефектації пошкодженого програмного забезпечення у наслідок дії кібератаки;

A_6 – оцінка дефектів пошкодженого програмного забезпечення після дії кібератаки;

A_7 – вибір переліку та способів відновлення пошкодженого програмного забезпечення у наслідок дії кібератаки;

A_8 – надання пропозицій щодо вибору необхідного переліку програмного та технічного забезпечення для відновлення пошкодженого програмного забезпечення;

A_9 – остаточний вибір способу усунення дефектів програмного забезпечення,

A_{10} розробка послідовності технологічних операцій щодо відновлення пошкодженого програмного забезпечення;

A_{11} – оцінка економічної ефективності щодо відновлення пошкодженого програмного забезпечення;

З метою здійснення робіт з проектування, технологія розробки СППР, передбачає використання двох основних етапів, а саме, по перше розробка технологічного проекту СППР, а по друге виконання його техніко-економічне обґрунтування. На теперішній час основним критерієм проектування СППР є його економічна ефективність. У зв'язку з чим, на початку проектування розробляється частина проектних матеріалів E_p, необхідних для розрахунку проектного коефіцієнту ефективності капітальних затрат E_{kf} щодо створення СППР, після чого здійснюється перевірка наступної умови:

$$E_p \gg E_{kf} \quad (2)$$

де, E_{kf} коефіцієнт ефективності капітальних затрат, який визначається під час створення СППР.

Аналізуючи стан проектування СППР, необхідно зазначити, що процес проектування має безліч особливостей. Особливість проектування пов'язана перш за все з неоднозначними явищами, що виникають під час впливу кібератак, фактами появи дефектів, способів їх виявлення та усунення, а також визначення оптимальних маршрутів з метою забезпечення відновлення програмного забезпечення автоматизованих систем та комплексів.

Визначено, що для розробки проекту СППР щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак, головним є аналіз та використання інформації, яка приймає участь у проектуванні, яка складається з керуючої, вихідний та термінальної, а саме:

-керівна інформація $J_{\text{у}}$ регламентує технологічний процес проектування на підставі вимог керівних та методичних матеріалів з проектування СППР;

-вихідна J_o складається з нормативної інформації та інформації щодо об'єкту проектування, який є об'єктом впливу кібератак;

-у свою чергу термінальна інформація J_t є результатом безпосереднього проектування і містить відомості щодо текстових, табличних, графічних матеріалах, які, як правило, зберігаються носіях інформації.

Враховуючи зміст термінальної інформації, представимо її компоненти у вигляді певних складових, об'єднаних між собою:

$$J_t = \{J_1 \cup J_2 \cup J_3\} \quad (3)$$

де: J_1 – складові інформації, які раніше використовувалися для розробки СППР та застосовується для проектування без змін;

J_2 – складові інформації, отримані за результатами об'єднання елементів вихідної інформації;

J_3 – складові інформації, отримані за результатами попередньої обробки елементів вихідної інформації.

Процес проектування характеризується у функціональному відношенні як процес якісних та кількісних змін інформації, а у відношенні її структури – як сукупність взаємопов'язаних операцій. На підставі цього функцію (F_p) технологічного проектування СППР можна формалізувати у вигляді:

$$F_p = J_{\text{у}} \times J_{\text{о}} \rightarrow J_t \quad (4)$$

де, термінальна інформація J_t є відображенням вихідної $J_{\text{о}}$ та керівної інформації $J_{\text{у}}$.

Структурні компоненти проектування $\{CK\}$ можна представити у вигляді наступного рівняння $CK = \{B_i\}$, де B_i є певної задачею, для якої виконується проектні процедури, наприклад, пошук інформації, попередня обробка інформації, класифікація кібератаки, оцінювання стану загроз, підготовка варіантів рішень щодо усунення кібератак.

Таким чином, проектування включає сукупність проектних процедур, які виконуються для кожної задачі. Функції кожної процедури f_i передбачають перетворення інформації з одного проміжного стану в інший.

У свою чергу структура кожної проектної задачі B_i визначається за результатами

застосування операції об'єднання графів - функцій процедур, а саме:

$$B_i = f_1 \cup f_2 \cup f_3 \ldots \cup f_n \quad (5)$$

Остаточно структуру технологічного процесу проектування СППР можна описати графом, який представляє об'єднання графів-функцій проектних задач:

$$G\,(J,Q) = B_1 \cup B_2 \cup B_3 \ldots\ldots \cup B_n \ldots \quad (6)$$

Зазначимо окремі особливості, що характеризують процес проектування СППР:

$$Q = \{Qi\}, \quad i = \overline{1_1 k}\,, \quad (7)$$

де: Q_i – замкнутість процесу проектування;

Q_2 – можливість удосконалення технології проектування;

Q_3 – старіння результатів проектування.

Особистістю проектної діяльності є старіння проектних матеріалів. Істинність проекту під час розробки U_0 та під час реалізації $U_\text{р}$ знаходиться у залежності

$$U_0 > U_\text{р} \quad (8)$$

Ця причина пояснюється тем, що об'єктивна реальність працездатності автоматизованих систем та комплексів постійно змінюється в наслідок імовірності появи та остаточного виявлення кібератак, дефектів програмного та апаратного забезпечення, способів їх відновлення, в внаслідок чого змінюється адекватність програмного забезпечення для компонентів СППР, які раніше були розроблені.

Тобто можна зазначити, що інтервал часу T_i, протягом якого може бути отриманий економічний ефект від реалізації проекту, є величина, що функціонально залежить від багатьох факторів

$$T_i = f\{PR_1, PR_2 \ldots\ldots PR_n\} \quad (9)$$

де: PR_1 – проектні рішення, що використовують нові технології та їх економічність;

PR_2 – проектне рішення, яке враховує зовнішні впливи;

PR_3 – інші проектні рішення.

Вибір рішення залежить від різних варіантів проектів $V_\text{в} = \{Vk\}, \quad k = \overline{1_1 n}$, та передбачає вибір такого варіанту V_0, де $V_0 \in V_\text{в}$, який відповідає завданню на проектування.

Загальний об'єм проектування суттєво зменшується, якщо вибір здійснюється не на множині варіантів проектів $V_\text{в}$, а множині варіантів проекту, які задовольняють умови

$$V_\text{у} = V_\text{в} \setminus V_n \quad (10)$$

де: V_n - множина незадовільних варіантів проекту.

За рахунок такого підходу, значно зменшується кількість варіантів проектів $V_\text{в}$, які потребують подальшої переробки, а сам процес проектування представляється у вигляді ієрархічної структури рівнів розробки, які характеризуються ступеню деталізації елементів.

На певному рівні здійснюється пошук умовного варіанту V_{yi} з деталізацією відомостей. На наступному рівні обрані варіанти переробляються більш детально на підставі певних критеріїв. Таким чином, у процесі проектування використовуються два напрямки – генерування різноманіття варіантів $V_{\text{в}i}$, їх аналіз та обмеження.

Послідовність проектування необхідно розподілити на дві паралельні задачі. Перша – це розробка системи збору інформації, її передавання та первинної обробки. Друга – розробка системи обробки даних. За часом вказані задачі можуть виконуватися паралельно або послідовно, в залежності від кількості осіб, які здійснюють розробку проекту.

Проектування передбачає ітераційний підхід щодо вирішення задач. Це пов'язано з тим, що на етапах розробки результати проектування необхідно порівнювати з нормативними показниками. Якщо терміни розробки не відповідають нормативним показникам, то здійснюється корегування

завдання і процес проектування продовжується. Необхідно зазначити що напрямком проектування є формалізація уніфікованих процедур розробки СППР, які відповідають сучасним технологія створення проекту. Послідовність проектування передбачає використання окремих процедур, пов'язаних між собою певними правилами.

Як було раніше зазначено, головними проектними процедурами під час проектування буде пошук інформації або її генерування, з подальшим вибором найкращого варіанту. У разі відсутності інформації, що необхідна для проектування, здійснюється корегування завдання на проектування. Якщо завдання неможливо скорегувати, то процес проектування або закінчується, або корегується для продовження проектування. Окрім цього виконується етап перевірки необхідності обробки інформації, яка аналізувалась раніше, якщо це необхідно, то для проектування застосовується процедура попередньої обробки інформації.

Важливим елементом є те, що процедури пошуку інформації та прийняття рішення виконуються на всіх рівнях проектування. Після чого застосовуються процедури, які здійснюють оцінку відповідності проектного рішення проектної задачі. У разі, якщо проектне рішення відповідає нормативними показникам, то оформлюється текстова та графічна документація проекту, якщо ні, то перевіряється можливість коректування завдання.

На проектування, впровадження та експлуатацію СППР впливають багато обмежень:

$$M = \{M_1, M_2, M_3, M_4\} \tag{11}$$

де: M_1 – грошеві ресурси на придбання технічного обладнання та математичного забезпечення; M_2 - трудові ресурси проектувальників; M_3 - трудові ресурси кваліфікованих спеціалістів з експлуатації СППР; M_4 – капітальні вкладення тощо. Обмеження М також впливають на кількість підсистем та задач, відповідно і на множину алгоритмів. Тому склад першочергових задач СППР залежить від суб'єктивних факторів та не є оптимальним з економічної точки зору.

Дослідження розрахованих економічних показників ефективності СППР показують, що ступень впливу однакових факторів для різних проектів СППР суттєво відрізняється. Тому для кожної СППР включають тільки ті задачі, які забезпечують вплив факторів, що дають економію.

Висновки. Таким чином, для ефективності проектування СППР щодо підвищення рівня захисту програмного забезпечення, необхідно мати певний математичний апарат, за допомогою якого можна розробити оптимальну технологію проектування зазначених систем. Такий математичний апарат, повинен враховувати особливості процесів виявлення, оцінювання кібератак, а також обмежень на проектування підсистем та множину алгоритмів.

Розробка СППР щодо підвищення рівня захисту програмного забезпечення можлива тільки за рахунок удосконалення технології проектування, пов'язаної з формалізацією процесів, що приймають участь у технологічних операціях виявлення кібератак, оцінювання дефектів пошкодженого програмного забезпечення та призначення оптимального способу їх відновлення з метою забезпечення надійної працездатності автоматизованих систем та комплексів, для яких застосовуються зазначені системи.

Список бібліографічного опису

1. Delgado, F., Esenarro, D., Juбrez, R., Reбtegui, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *Cuadernos dedesarrollo aplicados a las TIC,* 10(2), 123–141.
2. Kure, HI., Islam, S., Razzaque, MA. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Appl. Sci. Switzerland*, 8(6), 1–29.
3. Fielder, A. (2016) Decision support approaches for cyber security investment. *Decision Support Systems*, 86, 13–23.
4. Atymtayeva, L. (2014) Building a Knowledge Base for Expert System in Information Security. *Chapter Soft Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing,* 270, 57–76.
5. Gamal, M.M. (2011) Security Analysis Framework Powered by an Expert System. *International Journal of Computer Science and Security (IJCSS)*, 4(6), 505–527.
6. Lee, K., C. Wei, J., Mao, C.-H., Dai, J.-H., Kuang, Y.-T. (2016). Cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation. *Soft Computing,* 1–14.
7. Pan, S., Morris, T., Adhikari, U. (2015). Developing a Hybrid Intrusion Detection System Using Data Mining or Power. *Systems*, 6(6), 3104–3113.
8. Ferda, Ö., Banu, G. (2021). A Decision Support System for Optimal Selection of Enterprise Information Security Preventative Actions. *IEEE Transactions on Network and Service Management*, 18(3), 3260-3279

9. 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.
10. Волошин, О.Ф. Мащенко, С.О. (2010). *Моделі та методи прийняття рішень*: *навч. посіб.* Київ: Видавничополіграфічний центр "Київський університет".
11. 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*. Київ: ДУТ.
12. 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.
13. Diesch, R., Pfaff, M., Krcmar, H. (2020). *A comprehensive model of information security factors for decision-makers. Comput. Secur*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404820300341.
14. Roldán-Molina G., Almache-Cueva M., Silva-Rabadão C., Yevseyeva I., Basto-Fernandes V. (2017). A Decision Support System for Corporations Cybersecurity Management. In Proceedings of IEEE 12th Iberian Conference on Information Systems and Technologies, CISTI'2017, 21-24 June 2017, Lisbon, Portugal. IEEE.
15. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. (2016). *Decision support approaches for cyber security investment. Decis. Support.* Retrieved from: https://www.sciencedirect.com/science/article/pii/S0167923616300239.
16. Khairur, R., Benfano, S. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Indonesia gyptian Informatics Journal*, 23, 383–404.

References

1. Delgado, F., Esenarro, D., Juбrez, R., Reбtegui, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *Cuadernos dedesarrollo aplicados a las TIC,* 10(2), 123–141.
2. Kure, HI., Islam, S., Razzaque, MA. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Appl. Sci. Switzerland*, 8(6), 1–29.
3. Fielder, A. (2016) Decision support approaches for cyber security investment. *Decision Support Systems*, 86, 13–23.
4. Atymtayeva, L. (2014) Building a Knowledge Base for Expert System in Information Security. *Chapter Soft Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing,* 270, 57–76.
5. Gamal, M.M. (2011) Security Analysis Framework Powered by an Expert System. *International Journal of Computer Science and Security (IJCSS)*, 4(6), 505–527.
6. Lee, K., C. Wei, J., Mao, C.-H., Dai, J.-H., Kuang, Y.-T. (2016). Cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation. *Soft Computing,* 1–14.
7. Pan, S., Morris, T., Adhikari, U. (2015). Developing a Hybrid Intrusion Detection System Using Data Mining or Power. *Systems,* 6(6), 3104–3113.
8. Ferda, Ö., Banu, G. (2021). A Decision Support System for Optimal Selection of Enterprise Information Security Preventative Actions. *IEEE Transactions on Network and Service Management*, 18(3), 3260-3279
9. Bidyuk, P.I., Kozhukhivskyi, A.D., Kozhukhivska, O.A. (2013). Decision support system for analyzing and forecasting the state of the enterprise. Radio electronics, informatics, management, 1, 128-136.
10. Voloshyn, O.F. Mashchenko, S.O. (2010). Decision-making models and methods: teaching. manual Kyiv: Kyiv University Publishing and Printing Center.
11. Buryachok, V.L., Tolyupa, S.V., Anosov, A.O., Kozachok, V.A., Lukova-Chuiko, N.V. (2015). System analysis and decision-making in information security: a textbook. Kyiv: DUT.
12. Azarova, A.O., Dyogteva, I.O., Shiyan, A.A. (2022). Decision support system for increasing the level of information security of the enterprise. Information technologies and computer engineering, 1, 12-18.
13. Diesch, R., Pfaff, M., Krcmar, H. (2020). *A comprehensive model of information security factors for decision-makers. Comput. Secur*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404820300341.
14. Roldán-Molina G., Almache-Cueva M., Silva-Rabadão C., Yevseyeva I., Basto-Fernandes V. (2017). A Decision Support System for Corporations Cybersecurity Management. In Proceedings of IEEE 12th Iberian Conference on Information Systems and Technologies, CISTI'2017, 21-24 June 2017, Lisbon, Portugal. IEEE.
15. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. (2016). *Decision support approaches for cyber security investment. Decis. Support.* Retrieved from: https://www.sciencedirect.com/science/article/pii/S0167923616300239.
16. Khairur, R., Benfano, S. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Indonesia gyptian Informatics Journal*, 23, 383–404.