Міністерство освіти і науки України

Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Наукова робота
представлена на здобуття премії Президента України для молодих учених

Методи та технології розроблення та впровадження ґарантоздатних систем на основі Інтернету речей

Автори:

1. **ІЛЛЯШЕНКО Олег Олександрович** – кандидат технічних наук, доцент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

2. **КОЛІСНИК Марина Олександрівна** – докторантка, кандидат технічних наук, доцент, доцент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

3. **СТРЄЛКІНА Анастасія Андріївна** – аспірантка, асистент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

4. **КОЦЮБА Ігор Васильович** – кандидат технічних наук, головний інженер проекту Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України.

Харків – 2020

Мета роботи

Забезпечення відповідності вимогам до надійності та безпеки, підвищення гарантоздатності інформаційно-аналітичних та інформаційно-керуючих систем критичного застосування на основі Інтернету речей (ІСКІР) шляхом розроблення й впровадження методів і технологій оцінювання, створення й забезпечення цих вимог при використанні.

Науково-прикладна задача

Розроблення методів, засобів і технологій створення та впровадження ґарантоздатних ІСКІР

Задачі дослідження

1. Запропонувати концепцію, принципи забезпечення ґарантоздатності ІСКІР.

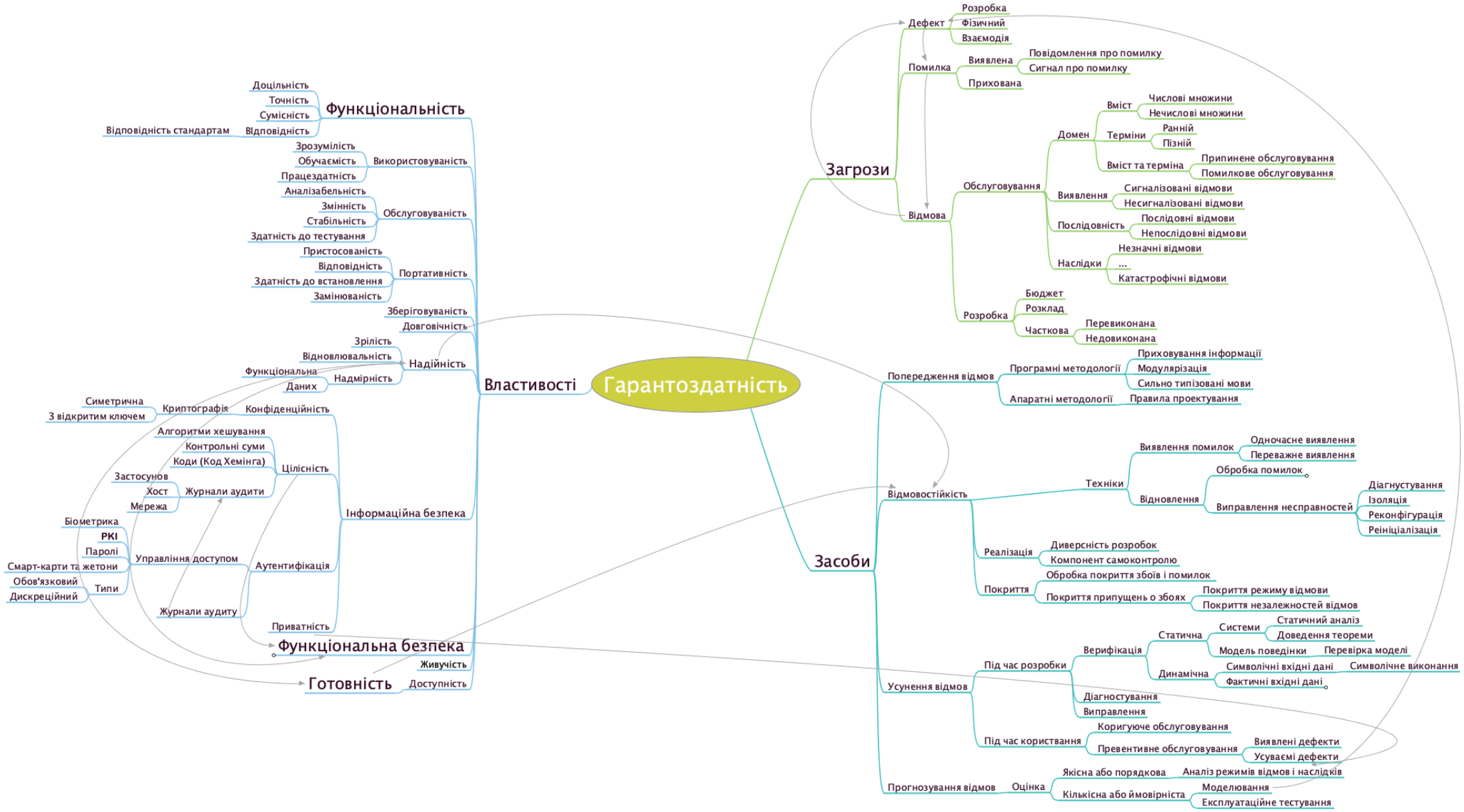
2. Розробити нормативний профіль ІСКІР, який враховує та гармонізує перелік і зміст вимог міжнародних і національних стандартів до безвідмовності, готовності, функційної та кібербезпеки, а також ураховувати їх при розробленні й модернізації.

3. Розробити і дослідити математичні моделі й методи оцінювання продуктивності, готовності, функціональної та кібербезпеки ІСКІР, які враховують різні види відмов і кібератак на системи, дозволяють проаналізувати їх функціональну поведінку і сформулювати рекомендації щодо вибору апаратних і програмних компонентів, архітектури, протоколів взаємодії тощо.

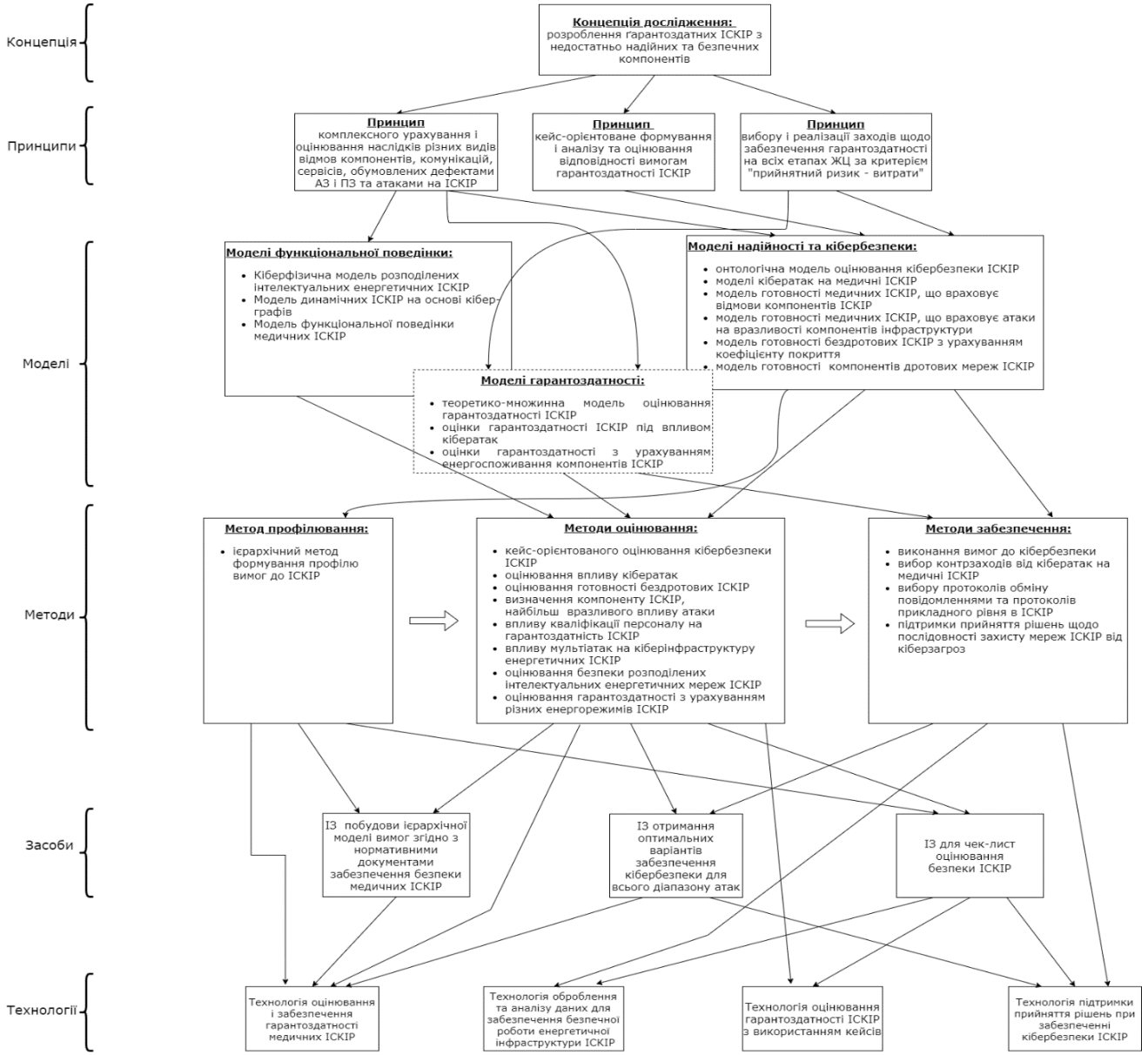
4. Запропонувати методи розроблення ґарантоздатних ІСКІР для різних комплексів (медичних, енергетичних, індустріальних, комунікаційних тощо) та забезпечення їх надійності та безпечності при створенні, модернізації та використанні.

5. Розробити й впровадити інформаційні технології підтримки прийняття рішень при створенні, модернізації та забезпеченні ґарантоздатності ІСКІР.

Актуалізована таксономія поняття ґарантоздатності для ІСКІР



Методологія створення ґарантоздатних ІСКІР



Теоретико-множинна модель оцінювання ґарантоздатності ІСКІР

M_{00}^{10}			M_{00}^{F0}		
$M_{R_I 0}^{10}$	$M_{0 R_D}^{10}$	$M_{R_I R_D}^{10}$	$M_{R_I 0}^{F0}$	$M_{0 R_D}^{F0}$	$M_{R_I R_D}^{F0}$
M_{00}^{1V}			M_{00}^{FV}		
$M_{R_I 0}^{1V}$	$M_{0 R_D}^{1V}$	$M_{R_I R_D}^{1V}$	$M_{R_I 0}^{FV}$	$M_{0 R_D}^{FV}$	$M_{R_I R_D}^{FV}$

Рис. 5.1. Модельний діапазон для ІСКІР

F – потужність множини функціональних станів $F = \left\{ S_{F_0}, S_{F_1}, \ldots, S_{F_m} \right\}$;

V – потужність множини вразливостей безпеки $V = \left\{ S_{V_0}, S_{V_1}, \ldots, S_{V_p} \right\}$;

R_I – потужність множини рівнів деградування інфраструктури ІСКІР $R_I = \left\{ S_{R_{I_0}}, S_{R_{I_1}}, \ldots, S_{R_{I_k}} \right\}$;

R_D –потужність множини відмов пристрою $R_D = \left\{ S_{R_{D_0}}, S_{R_{D_1}}, \ldots, S_{R_{D_l}} \right\}$.

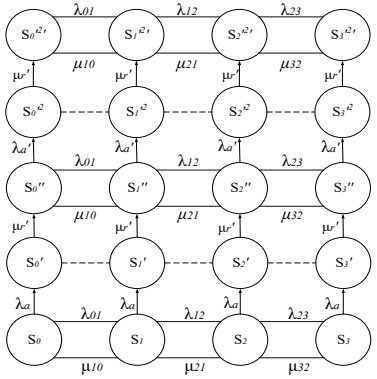


Рис. 5.2. Модель, що враховує успішні атаки на стадії обробки запиту на обслуговування (без зупинок і усуненням двох вразливостей)

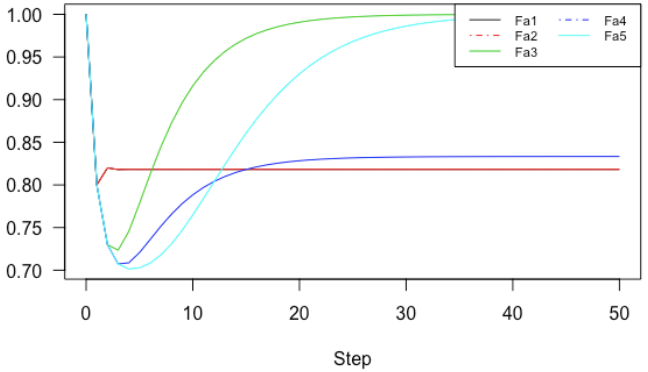


Рис. 5.3. Зміна функції готовності при успішній атаці

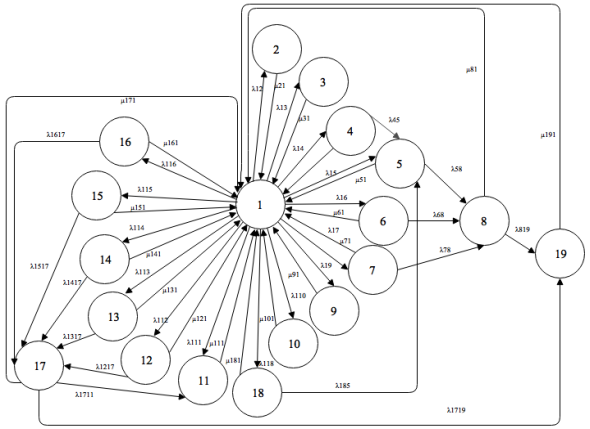


Рис. 5.4. Марковський граф відмов медичної ІСКІР інфраструктури

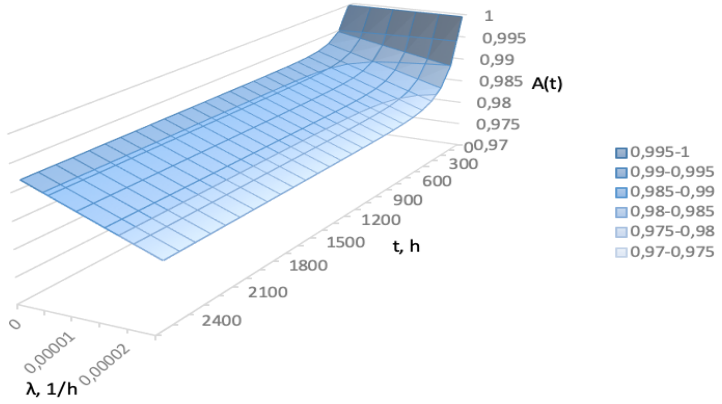


Рис. 5.5. Зміна функції готовності в залежності від різних причин відмов медичного пристрою

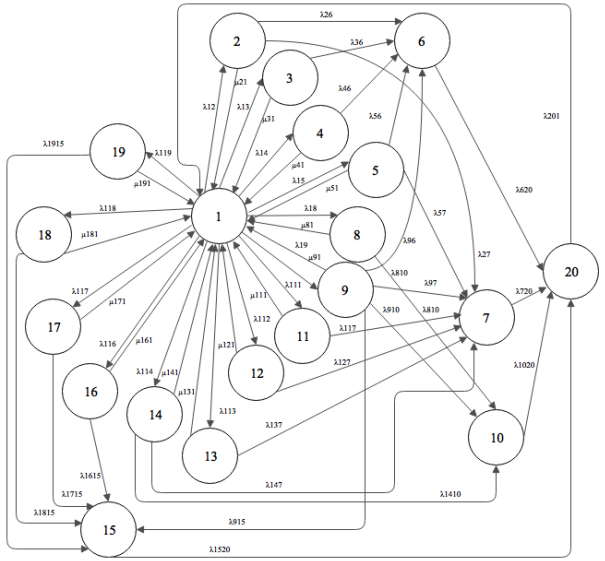


Рис. 5.6. Марковський граф атак на вразливості компонент медичної ІСКІР

Метод профілювання вимог до ґарантоздатності ІСКІР

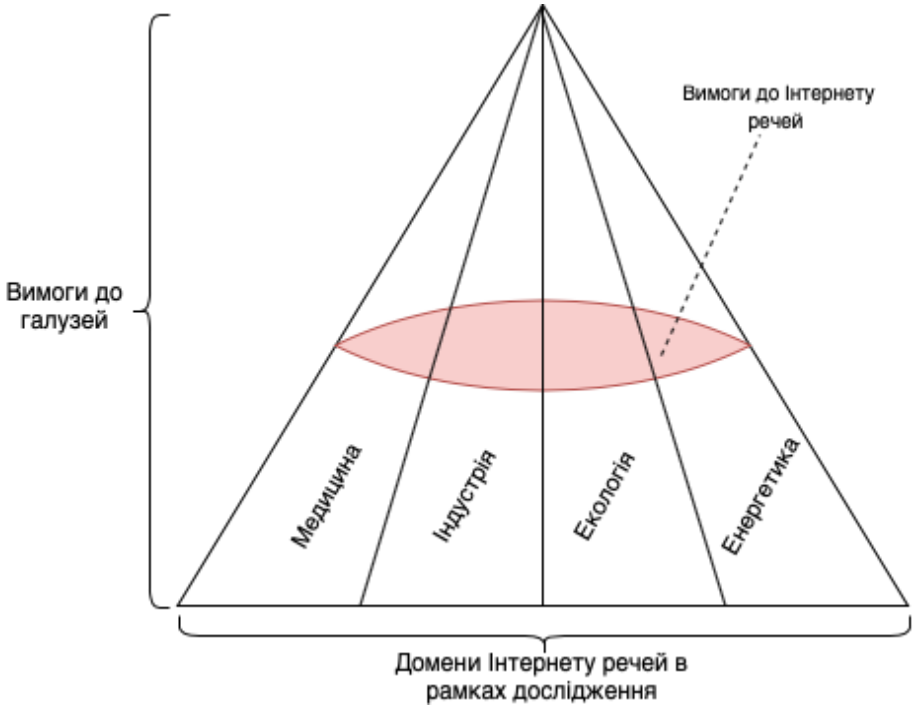


Рис 6.1. Концептуальне представлення методу профілювання вимог до ґарантоздатності ІСКІР

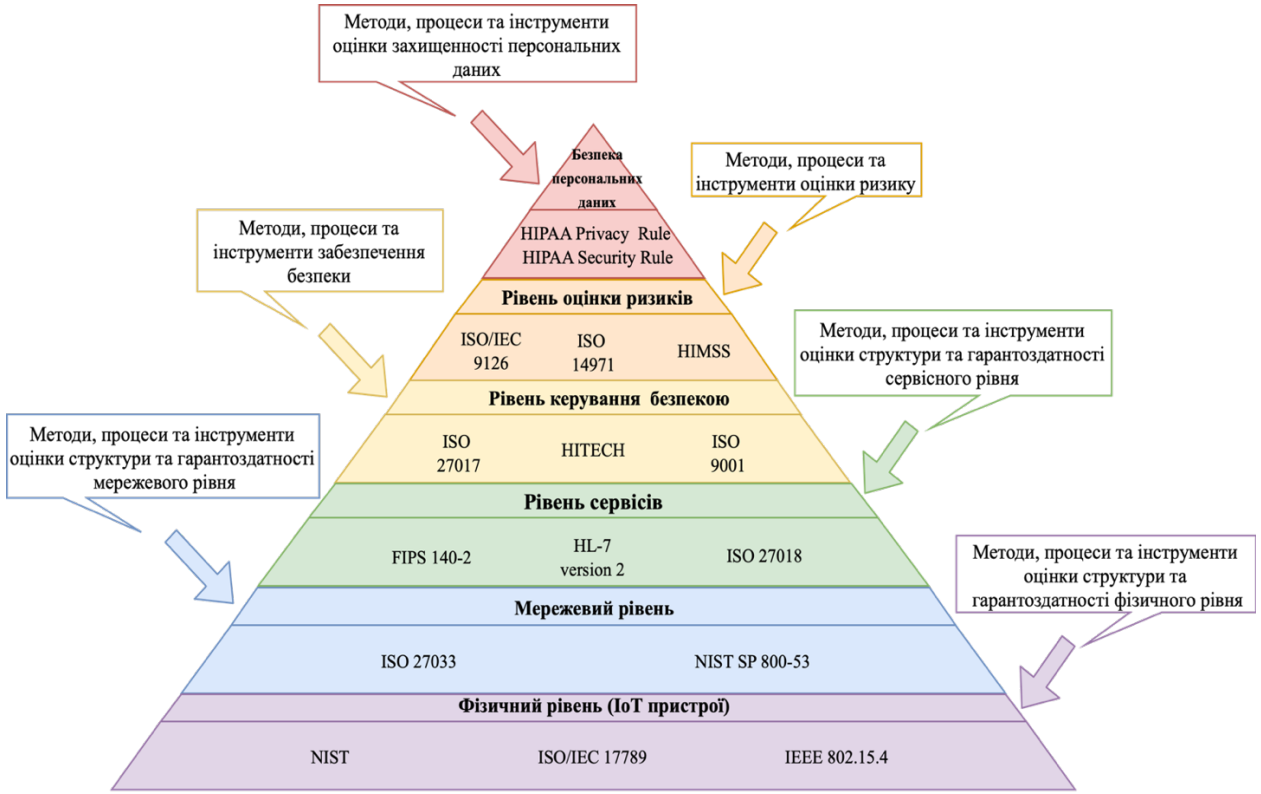


Рис 7.2. Профільоутворююча нормативна база вимог до медичних ІСКІР

Онтологічна модель для оцінювання кібербезпеки ІСКІР

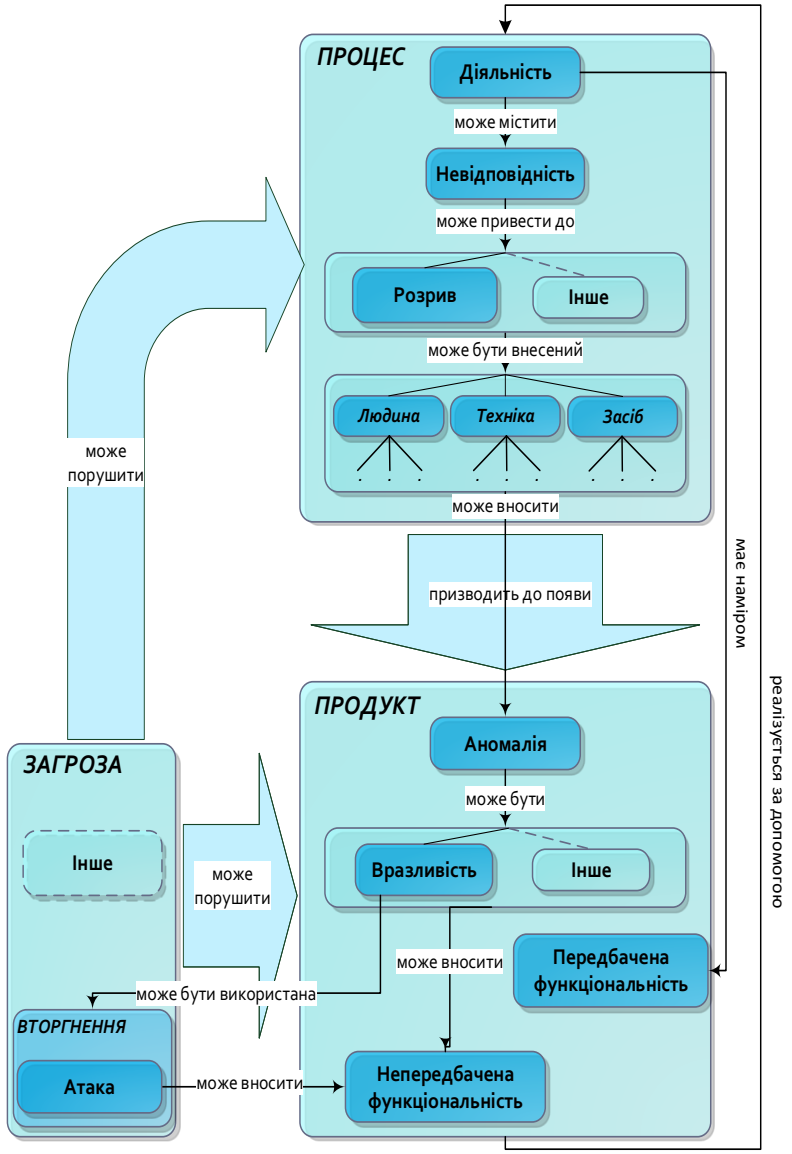


Рис. 7.1. Таксономія оцінювання безпеки ІСКІР за процесно-продуктним підходом

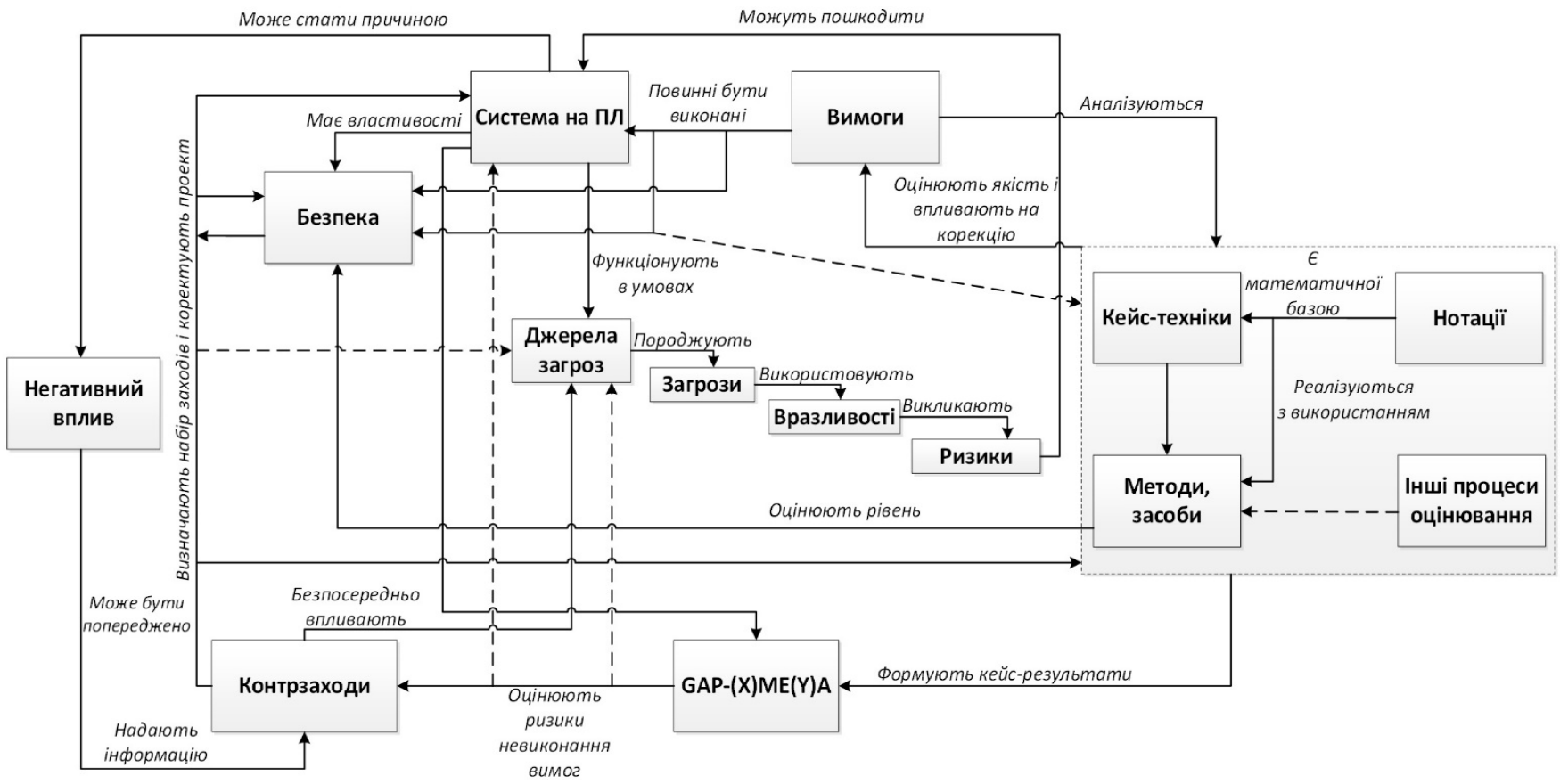


Рис. 7.2. Онтологічна модель безпеки систем ІСКІР з використанням кейсів

Метод кейс-орієнтованого оцінювання безпеки ІСКІР

Властивість $P_i^{\{j\}}$	Опис властивості
P_0	Resistancy of the TOE to attacks performed by an attacker possessing Basic attack potential
P_1^0	Readiness of the TOE for testing
$P_1^{0,1}$	Consistency of the TOE with ST
$P_1^{0,1,1}$	Conformity of the TOE reference with the CM capabilities (ALC_CMC) sub-activities and ST introduction
$P_2^{0,1,1}$	Consistency of the all TOE configurations with ST
$P_3^{0,1,1}$	Conformity of the testing environment to the security objectives for the operational environment described in the ST
$P_2^{0,1}$	Accuracy of the TOE installing
$P_1^{0,1,2}$	Successful completion of the AGD_PRE.1

Свідоцтво $E_i^{\{j\}}$	Опис свідоцтва
E_1^0	TOE is suitable for testing
E_2^0	Security Target is available
E_3^0	Guidance documentation is available
E_4^0	Information is publicly available to support the identification of potential vulnerabilities
E_5^0	Current information regarding potential vulnerabilities is available (e.g. from an evaluation authority)

Вимога Requirement 15.2.3.4.3 AVA_VAN.1.3E (*The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential*) до забезпечення компоненту запевнення AVA VAN.1 (Vulnerability survey) з класу AVA (Vulnerability assessment) зі стандарту ISO/IEC 15408-3 (2008) Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.

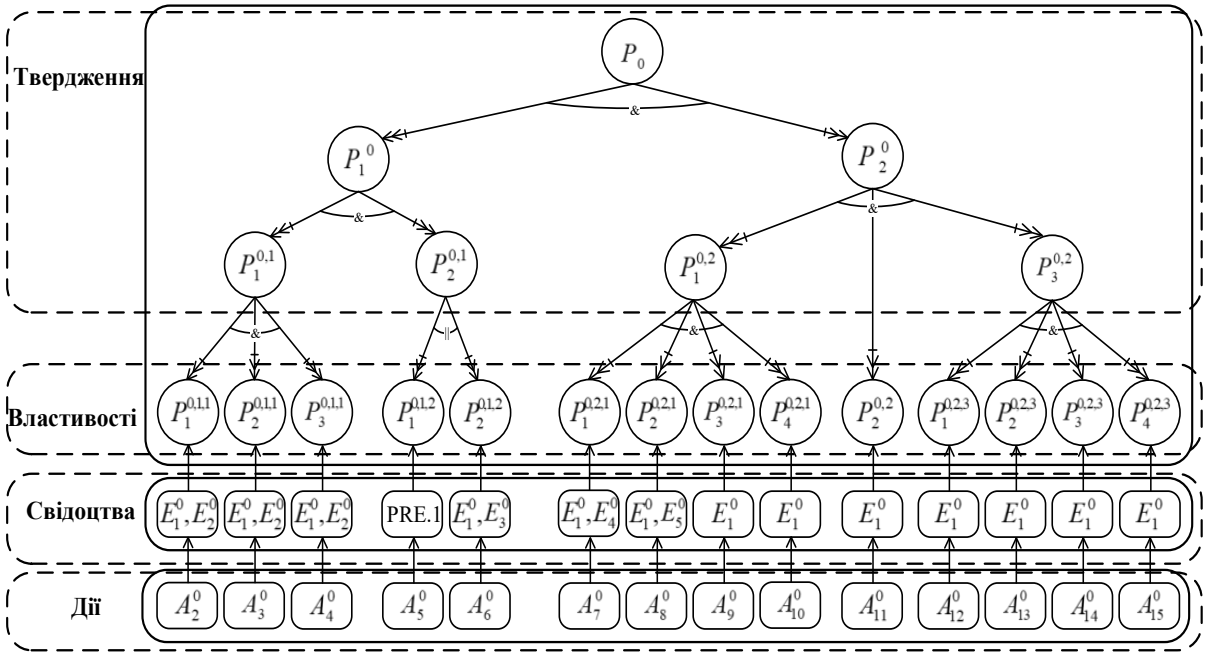


Рис. 8.1. Модель кейсу запевнення ASAC у графовій формі

Дія $A_i^{\{j\}}$	Опис дії
A_1^0	Obtain the evidences
A_2^0	Check the conformity of the TOE reference with the CM capabilities (ALC_CMC) sub-activities and ST introduction
A_3^0	Check the consistency of all configurations of the TOE with ST
A_4^0	Check the conformity of the testing environment to the security objectives for the operational environment described in the ST

Метод забезпечення виконання вимог до кібербезпеки ІСКІР

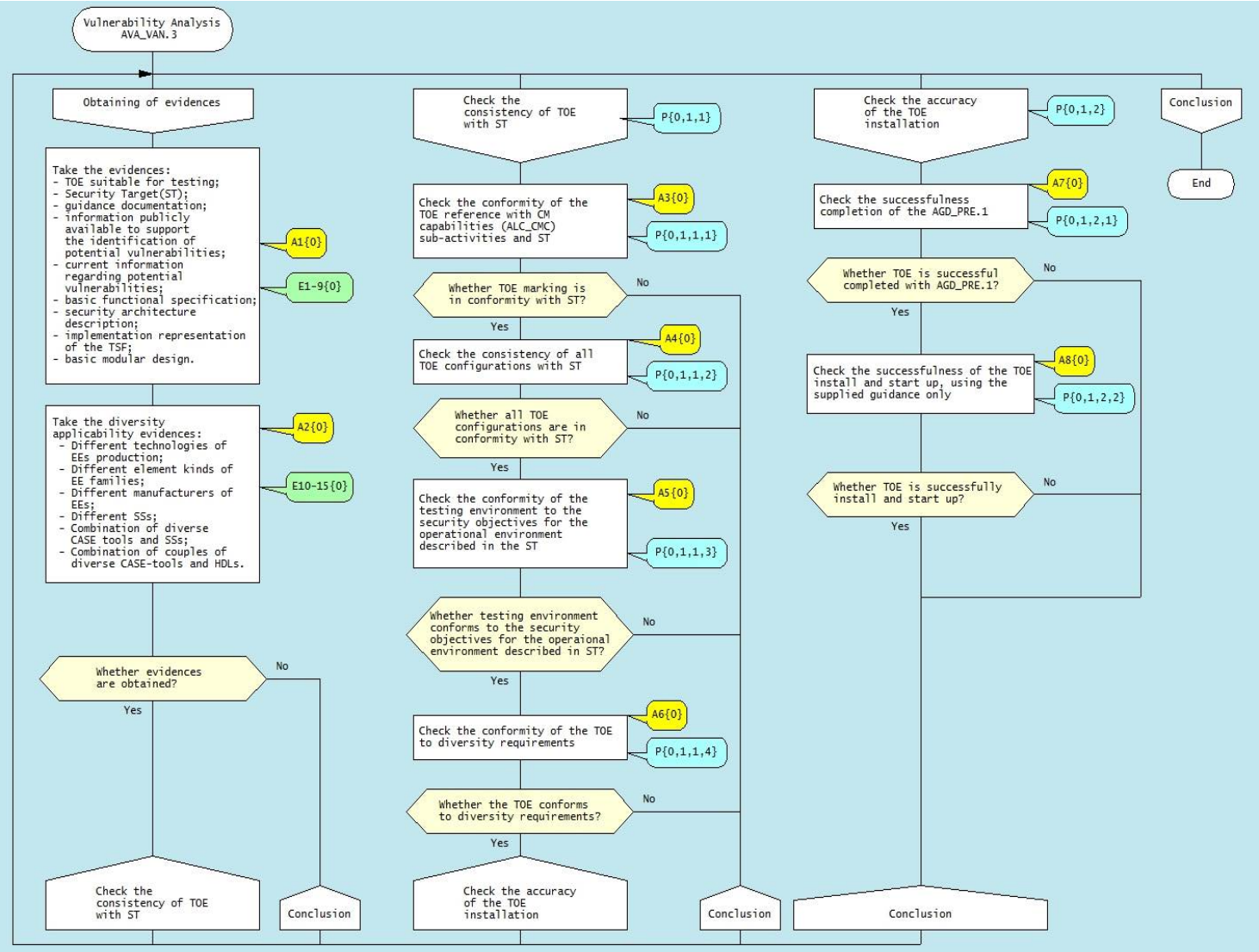


Рис. 9.1. Діаграма кейсу ASAC на мові ДРАКОН

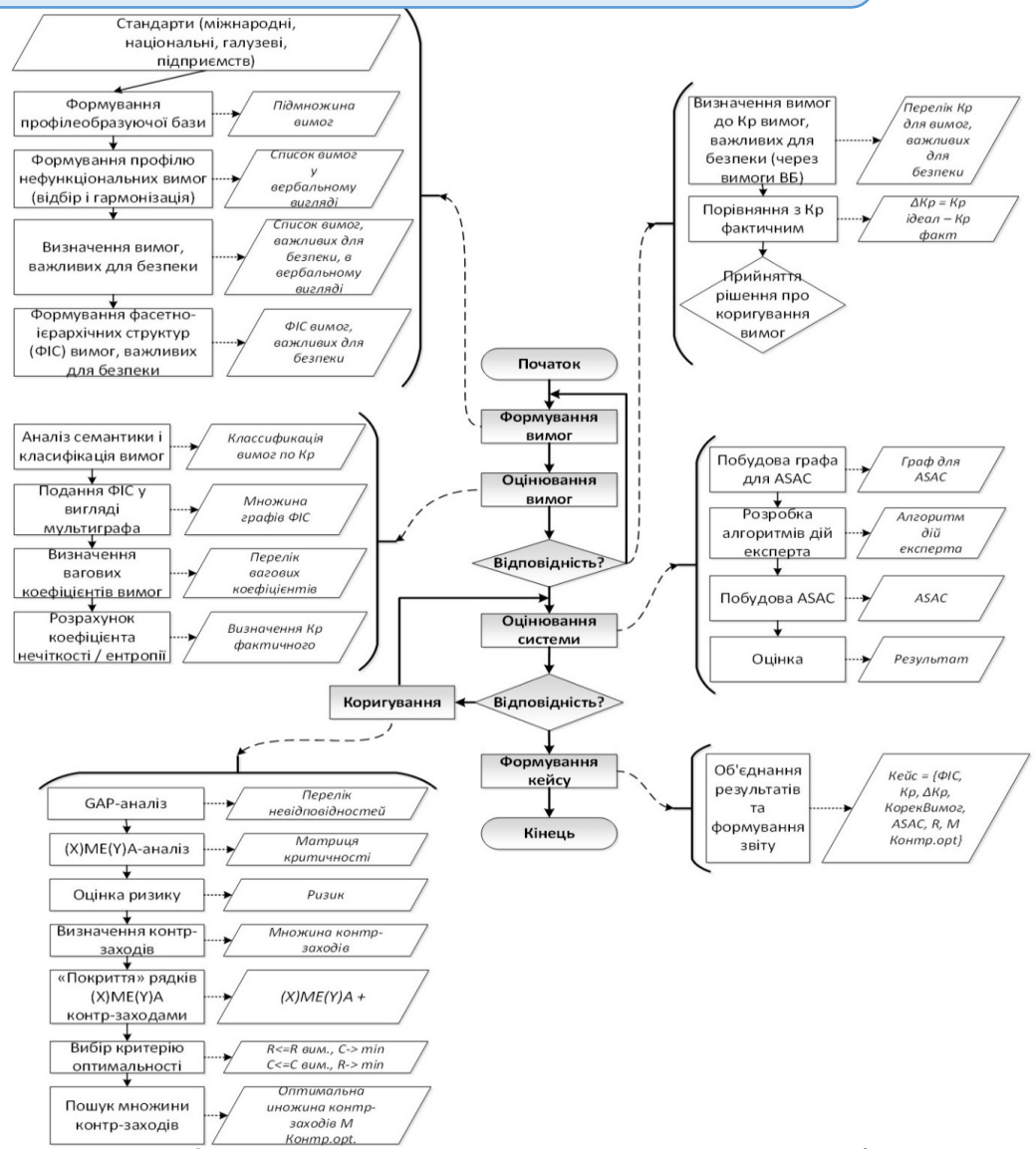


Рис. 9.2. Загальний алгоритм застосування методу забезпечення виконання вимог до кібербезпеки ІСКІР із використанням кейсів

Метод вибору контрзаходів від кібератак на медичні ІСКІР

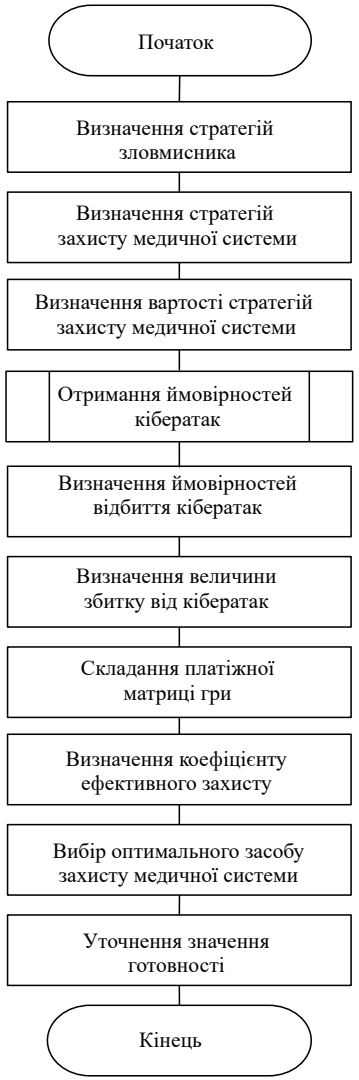


Рис. 10.1. Алгоритм методу вибору контрзаходів від кібератак

Таблиця 11.1

Приклад платіжної матриці

Засіб захисту \ Атака	Ймовірність атаки	Засоби захисту			
		IDS	Firewall	Аутентифікація	Криптографія
		Ймовірність захисту від кібератаки			
Аналіз трафіку	5,74e-05	0,7	0,85	0,001	0,3
Спуфінг	4,29e-05	0,7	0,8	0,1	0,001
Клонування	0,000169642	0,01	0,9	0,5	0,001
Несанкціонований доступ	0,01081887	0,01	0,9	0,9	0,6
Людина-по-середині	4,89e-05	0,01	0,6	0,5	0,4
DoS/DDoS	0,000100901	0,4	0,8	0,001	0,001

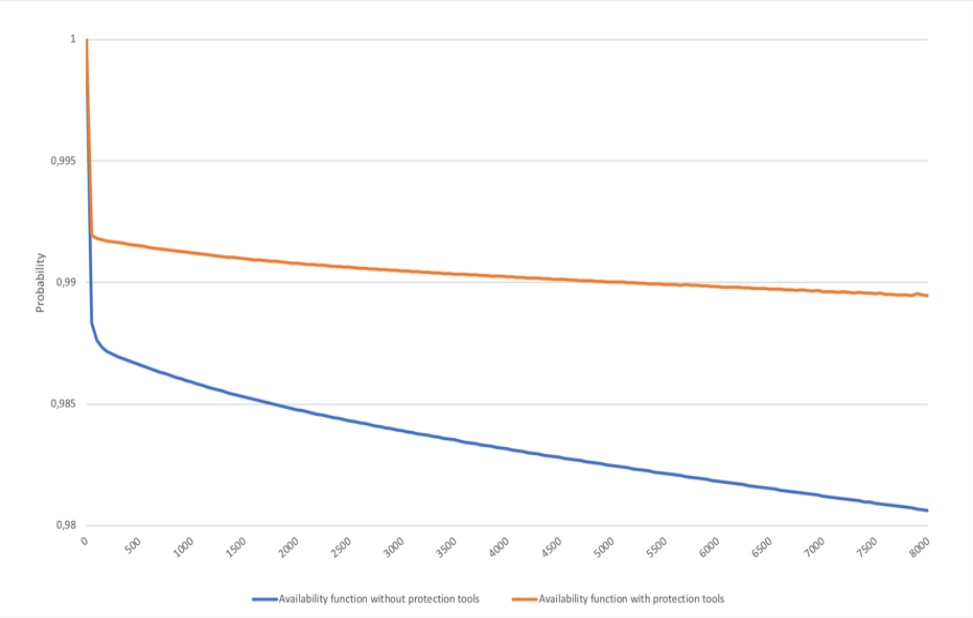


Рис. 10.2. Зміна функції готовності після використання методу (модель на рис. 5.6)

Отже, готовність може бути збільшена до 4%. З іншого боку, якщо мова йде про неготовність медичної ІСКІР системи, яка становила близько 8%, а після уточнення 4%, тобто, можна зробити висновок, що існує потенціал для зменшення неготовності медичної ІСКІР на 200% або в 2 рази.

Метод оцінювання впливу мультиатак на кіберінфраструктуру енергетичних ІСКІР

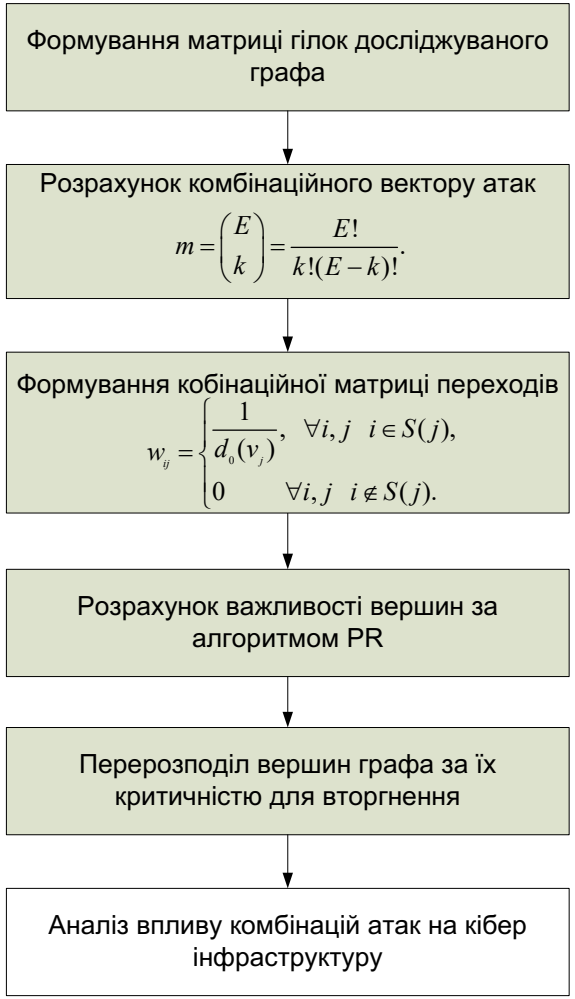


Рис. 11.1. Алгоритм методу мультиатак на кіберінфраструктуру енергетичних ІСКІР

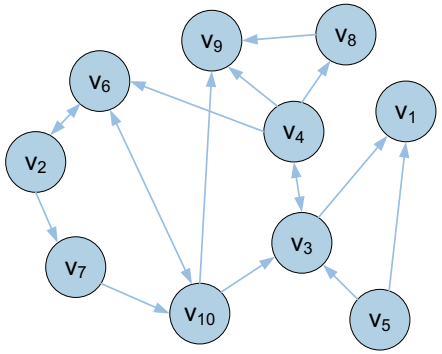


Рис. 12.2. Граф досліджуваної системи (приклад)

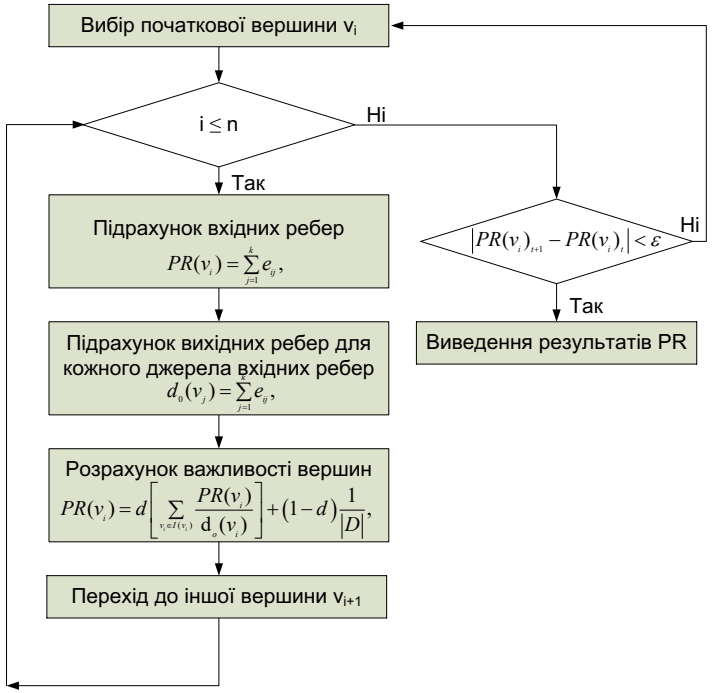


Рис. 11.3. Схема розрахунку показника PR

Технологія оцінювання і забезпечення ґарантоздатності медичних ІСКІР

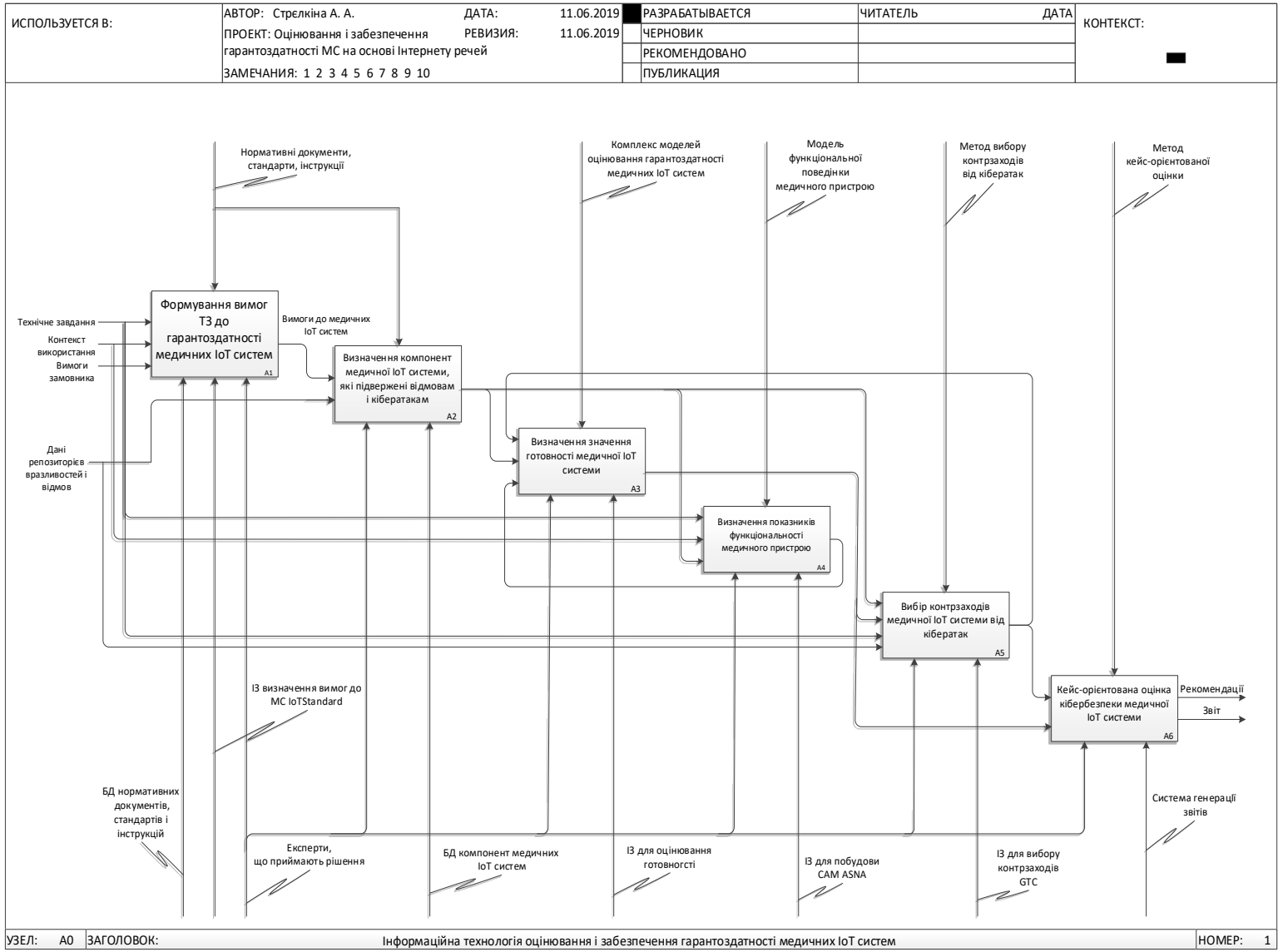


Рис. 12.1. IDEF0-діаграма інформаційної технології оцінювання та забезпечення ґарантоздатності медичних ІСКІР

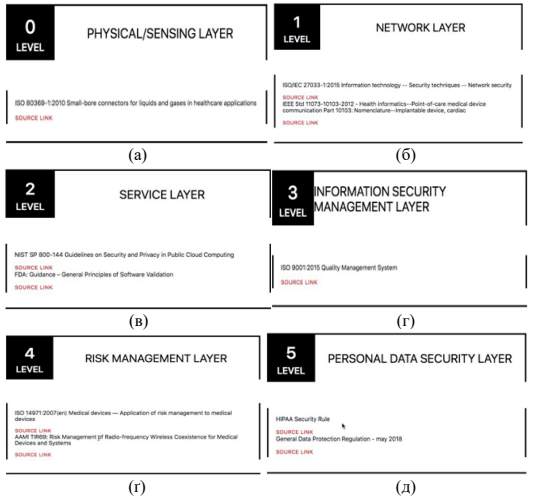


Рис. 12.2 ІЗ побудови ієрархічної моделі нормативних документів забезпечення безпеки медичних ІСКІР (метод профілювання вимог до ґарантоздатності ІСКІР)

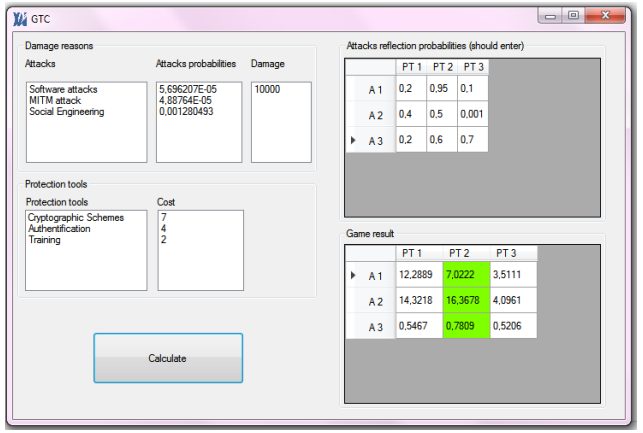


Рис. 12.3 ІЗ отримання оптимальних варіантів забезпечення кібербезпеки для різних атак (метод вибору контрзаходів від кібератак на медичні ІСКІР)

Технологія оброблення та аналізу даних для забезпечення безпечної роботи енергетичної інфраструктури ІСКІР

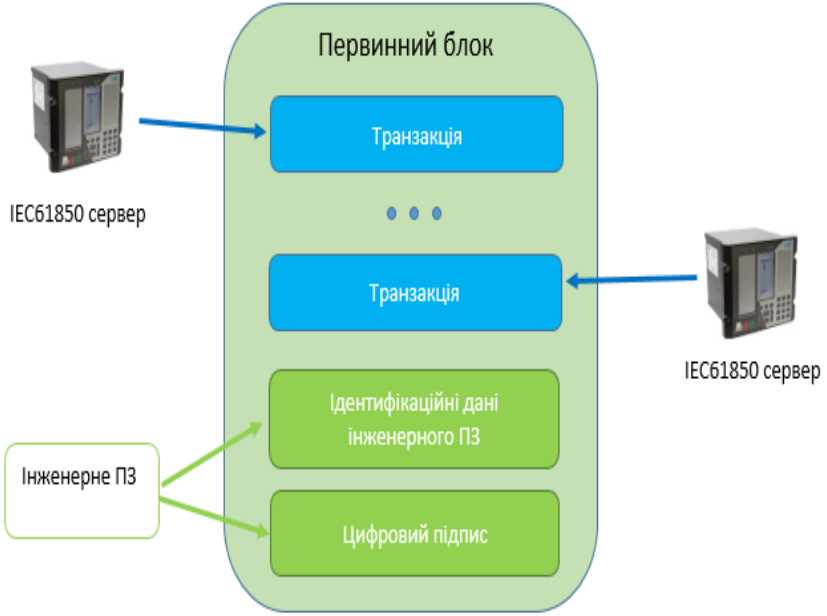
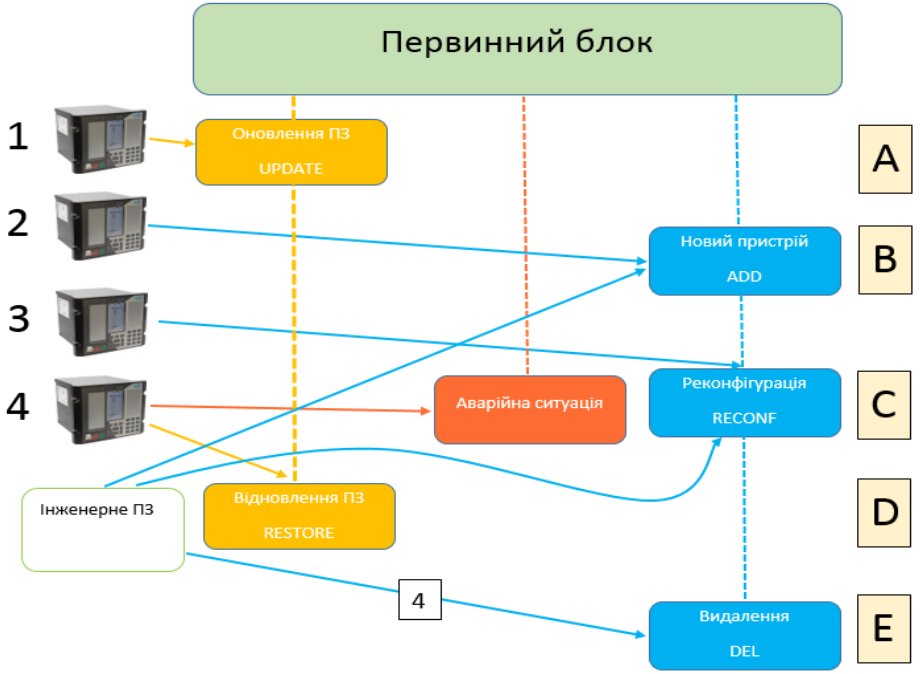


Рис. 13.1. Структура первинного блоку



- - - - - - - - Ланцюг блоків зміни стану ПЗ

- - - - - - - - Ланцюг блоків з аварійними даними

----------Ланцюг блоків операцій зміни конфігурації

Рис.13.2. Схема обміну даними між ланцюгами

Технологія оцінювання ґарантоздатності ІСКІР з використанням кейсів

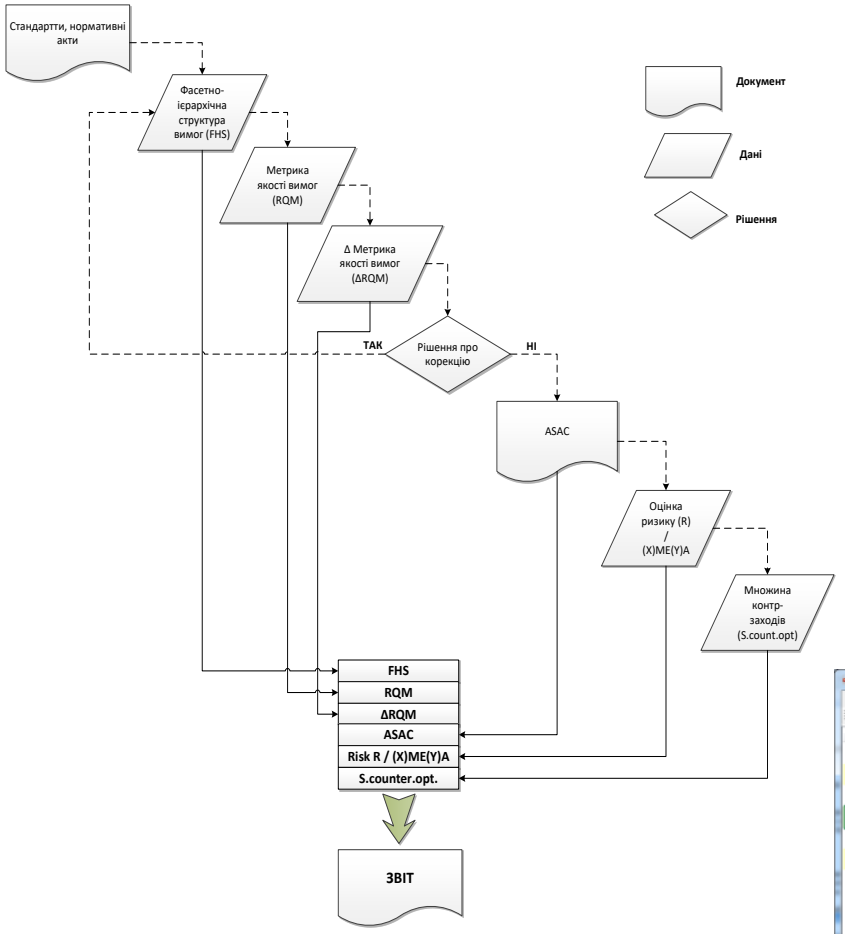


Рис. 14.1. Технологія кейс-орієнтовного оцінювання ґарантоздатності ІСКІР

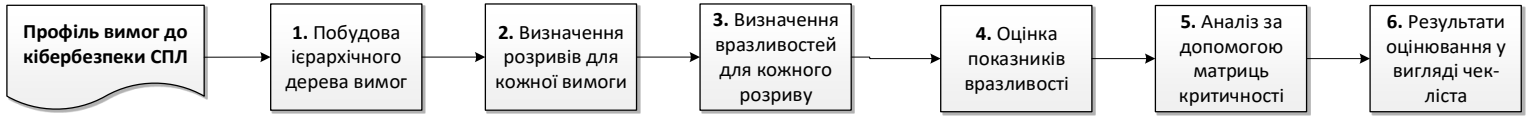


Рис. 14.2. Основні етапи роботи програми CLASICS

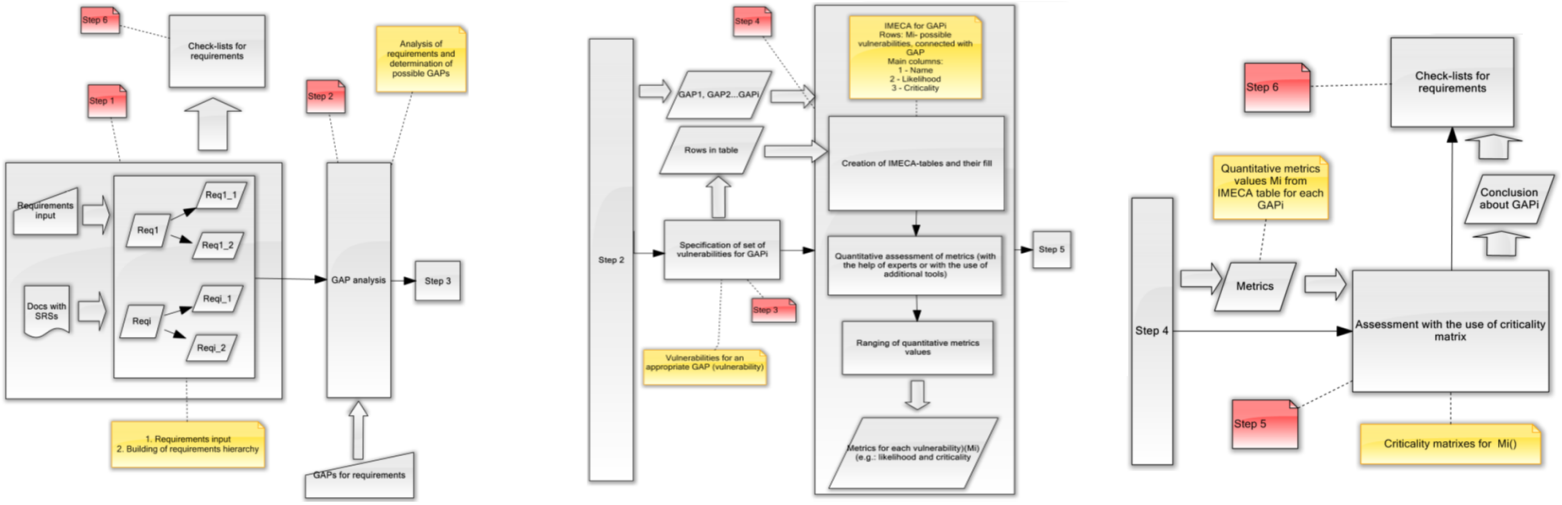


Рис. 14.3. Загальний процесс роботи утиліти “CLASICS”

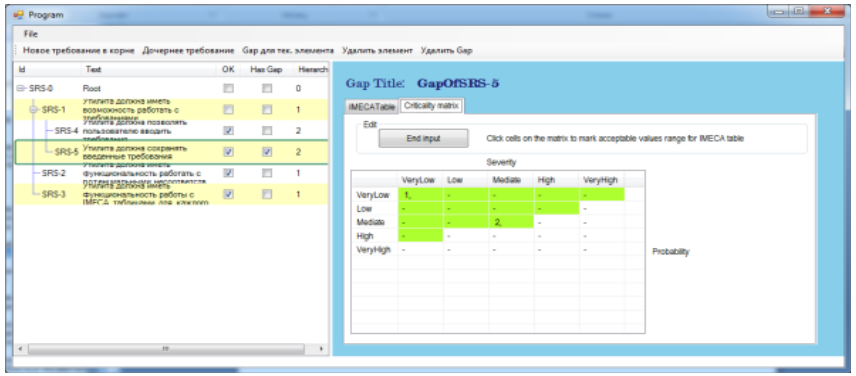


Рис. 14.4. Інтерфейс програми CLASICS

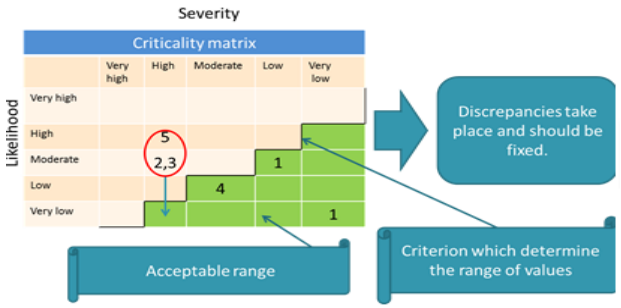


Рис. 14.5. Побудова матриці критичності для оцінювання ризику

Технологія підтримки прийняття рішень при забезпеченні кібербезпеки ІСКІР

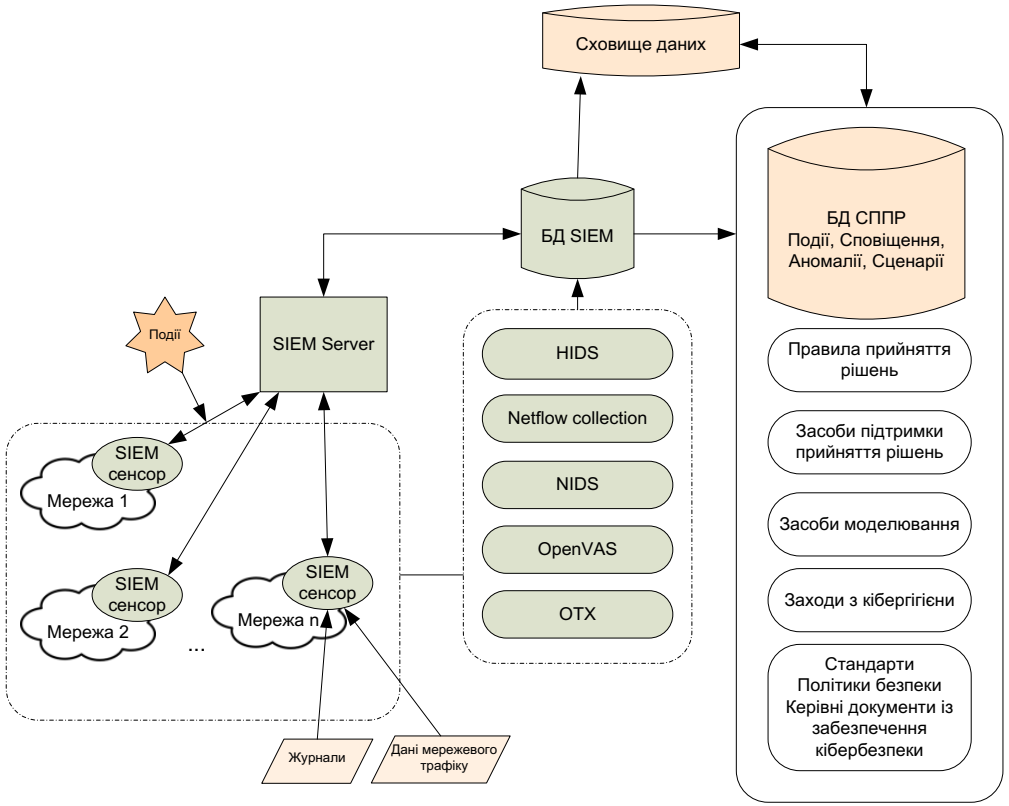


Рис. 15.1.Основні компоненти OSSIM AlientVault та СППР

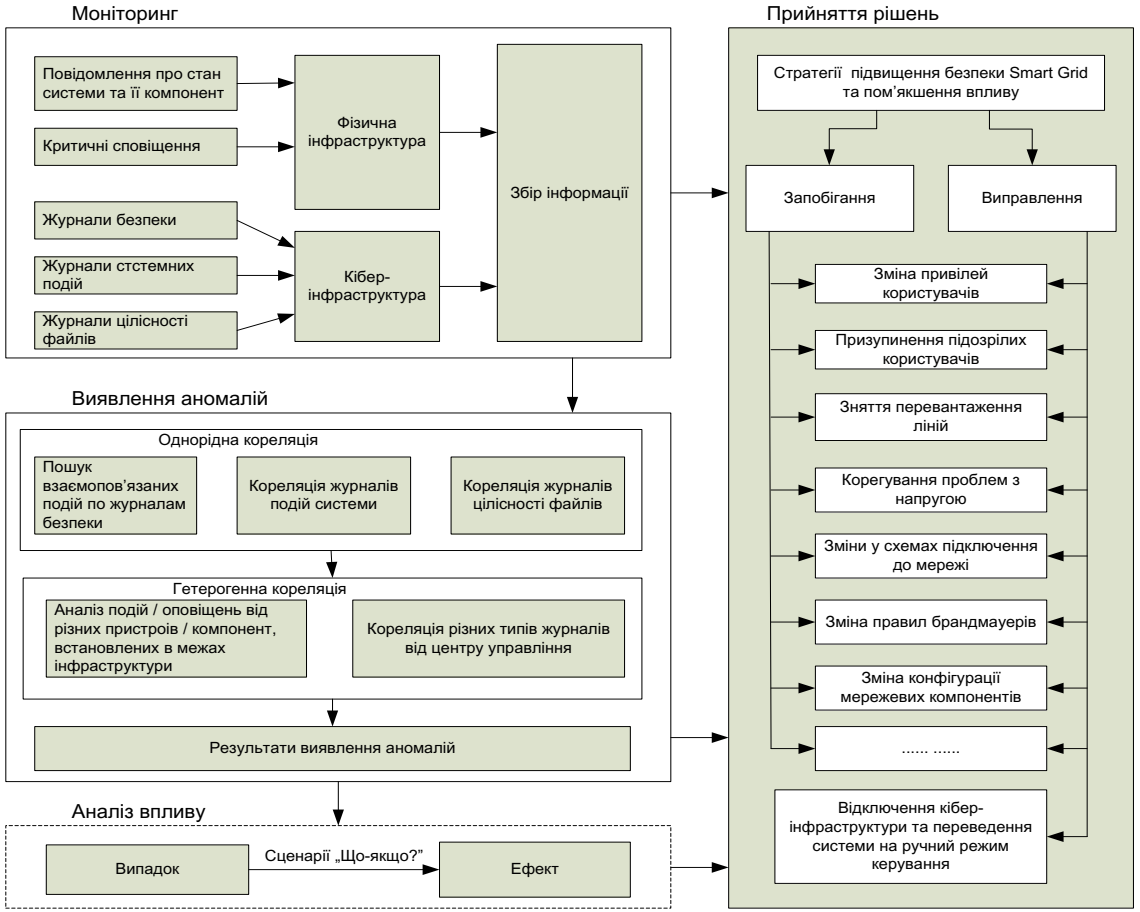


Рис. 15.2. Базові компоненти інформаційної технології

Архітектура інтелектуальної енергетичної інфраструктури ІСКІР

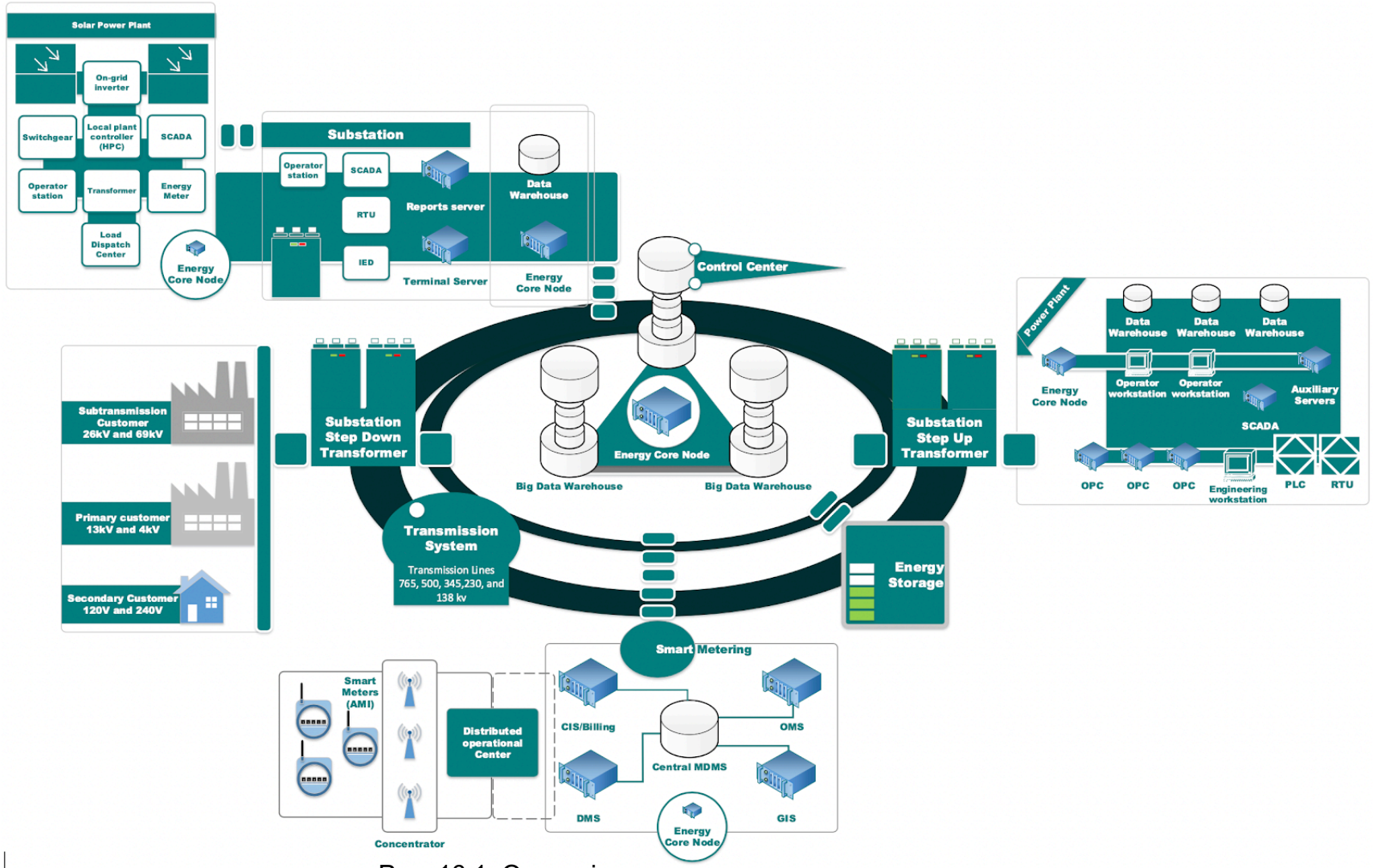


Рис. 16.1. Основні компоненти
та архітектура інтелектуальною енергетичної інфраструктури ІСКІР

Впровадження результатів досліджень і розробок

Галузі, підприємства (організації), системи			Результати досліджень і розробок							
			Моделі			Методи			Технології	
			Моделі гарантоздатності	Моделі функціональної поведінки	Моделі надійності та кібербезпеки	Метод профілювання вимог	Методи оцінювання	Методи забезпечення	Інструментальні засоби	Інформаційні технології
Енергетика	ТОВ «НВП «Радікс»	Компоненти ІСКІР			+	+			+	
		Нормативні документи			+	+				
	ПрАТ «Сєвєродонецьке НВО «Імпульс»	Компоненти ІСКІР		+	+		+	+		
		ПЗ								+
Медицина	ТОВ «ХАІ-МЕДИКА»	Системи телемедицини		+		+			+	
Транспортні системи	ТОВ «НВП «Залізничавтоматика»	Мікропроцесорні системи					+			
Машинобудування	ПрАТ «ФЕД»	ІСКІР					+	+		
Аерокосмічні системи	НТ СКБ «Полісвіт» ДНВП «Об’єднання «Комунар»	Вбудовані системи				+	+	+		
Державні нормативні документи	Державна служба спеціального зв’язку та захисту інформації	ОКІ		+			+	+		+
	ПАТ «Інститут Інформаційних Технологій»	ОКІ				+	+	+	+	
Вища освіта	НАКУ «ХАІ», ІПМ ім. Глухова, СНУ ім. Даля, ТТУ, ІІТ «Алессандро Фаедо»	Учбовий процес	+	+	+	+	+	+	+	+
Міжнародні проекти	Освітні проекти TEMPUS	MASTAC, SAFEGUARD, GREENCO, SEREIN, CABRIOLET	+	+	+	+	+	+	+	+
	Освітній проект ERASMUS+	ALIOT	+	+	+	+	+	+	+	+
	Науковий проект FP7	KhAI-ERA	+	+	+	+	+	+	+	+
	Наукові проекти Horizon 2020	ECHO, COST Action DigForAsp, SPEAR	+	+	+	+	+	+	+	+

Публікації претендентів

Кількість публікацій претендентів за роботою: **89**, а саме:

- **8** монографій (у т.ч. 6 - видавництвах Springer, River Publishers);
- **2** навчальних посібника;
- **36** статей (34 наукових статті у збірниках, що включені до переліку наукових фахових видань України, 2 статті в збірниках, що входять до наукометричних баз даних);
- **41** публікації матеріалів міжнародних конференцій та тези доповідей (**30** публікації в матеріалах конференцій, що входять до наукометричних баз даних, **11** публікацій у матеріалах конференцій, тезах доповідей та виданнях, що не включені до переліку наукових фахових видань України);
- **1** патент України на корисну модель, **1** свідоцтво на авторський твір.

Цитування публікацій претендентів

	Кількість посилань згідно бази даних		
	Web of Science	Scopus	Google Scholar
Загальна кількість цитувань	48	128	253
h-індекс робіт	3	6	8
h-індекс авторів			
О. О. Ілляшенко	2	4	7
М. О. Колісник	1	2	4
А. А. Стрєлкіна	1	3	4
І. В. Коцюба	1	2	2
Загальний h-індекс авторів	5	11	17

Висновки

Комплекс науково-прикладних задач розроблення методів, засобів і технологій створення та впровадження ґарантоздатних ІСКІР

ВИРІШЕНО

1. Розроблено концепцію, принципи забезпечення ґарантоздатності ІСКІР, які базуються на розвитку парадигми фон Неймана створення надійних і безпечних систем на основі недостатньо надійних і безпечних компонентів.

2. Розроблено нормативний профіль ІСКІР, який враховує та гармонізує перелік і зміст вимог міжнародних і національних стандартів, що надає змогу приймати рішення щодо відповідності таких систем вимогам.

3. Розроблено і досліджено математичні моделі й методи оцінювання продуктивності, готовності, функціональної та кібербезпеки ІСКІР, які враховують різні види відмов і кібератак на системи.

4. Розроблено методи створення ґарантоздатних ІСКІР для різних комплексів та забезпечення їх надійності та безпечності при розробленні, модернізації та використанні.

5. Розроблено і впроваджено інструментальні засоби та інформаційні технології підтримки прийняття рішень при створенні, модернізації та забезпеченні ґарантоздатності ІСКІР.

ДОЗВОЛИЛО

Зменшити ризики порушення показників ґарантоздатності та зменшити час оцінювання, а також автоматизувати процес і підвищити достовірності оцінювання при розробленні та впровадженні ІСКІР, а також підвищити компетенції персоналу з забезпечення ґарантоздатності компонентів від кіберзагроз. Повнота забезпечення кібербезпеки зростає на 20-30%.