Методика дослідження кібербезпеки розумного будинку. Частина 2. Алгоритми тестування

Виконала:

студентка

групи 1БС-17 м

Савченко К.В.

Керівник:

к.т.н, доц. каф. ЗІ

Войтович О.П.

Актуальність комплексної магістерської кваліфікаційної роботи:

Інтернет речей (IoT) став невід’ємною частиною нашого життя і мільярдів людей по всьому світу. Однак зростання кількості підключених пристроїв веде до збільшення ризиків безпеки: від заподіяння фізичної шкоди людям, перехоплення чутливих даних до атак на відмову в обслуговуванні на критичні інформаційні системи. Оскільки ряд таких об'єктів і систем IoT вже піддавалися нападу і було завдано значний збиток, забезпечення їх захисту виходить на перший план.

Мета комплексної магістерської кваліфікаційної роботи:

Підвищення рівня кібербезпеки системи розумного будинку шляхом розробки методики тестування на проникнення

Об’єкт дослідження:

Методика дослідження кібербезпеки розумного будинку

Предмет дослідження:

Алгоритм тестування на проникнення системи розумного будинку

Постановка задачі:

- виконати огляд літературних джерел;
- виконати аналіз існуючих підходів та засобів тестування;
- вивчити міжнародні стандарти тестування безпеки;
- розробити методику тестування безпеки;
- розробити супровідну документацію;
- обґрунтувати економічну доцільність.

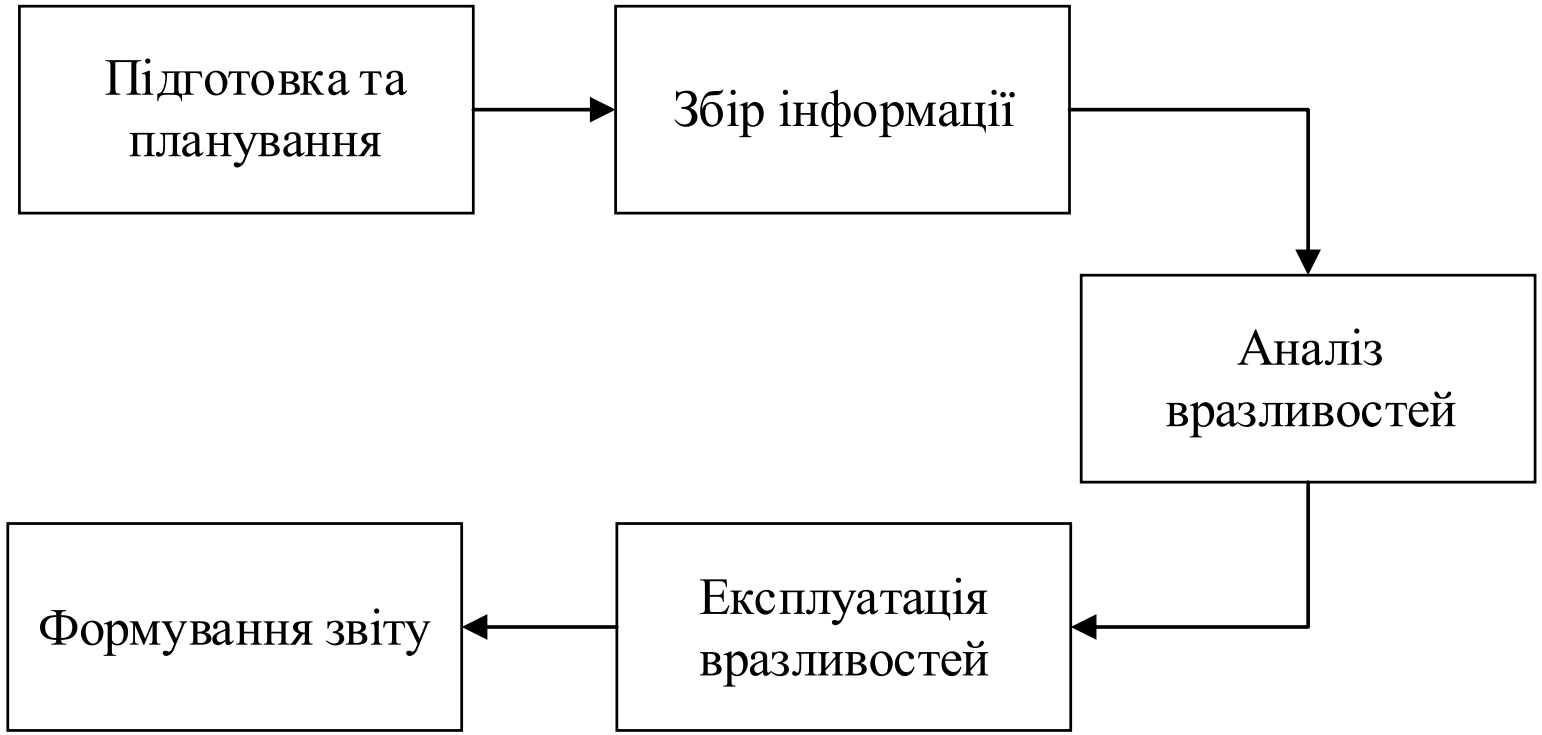
Результати порівняння сценаріїв «Чорної скриньки», «Білої скриньки» та «Сірої скриньки»:

Критерій	«Чорна скринька»	«Біла скринька»	«Сіра скринька»
Визначення	Тестування, як функціональне, так і не функціональне, без знання внутрішньої будови компонента чи системи	Тестування, яке базується на знанні внутрішньої будови компонента чи системи	Тестування, при якому лише частково відома внутрішня будова компонента чи системи
Рівні, до яких можливе застосування техніки	В основному: – Приймальне тестування – Системне тестування	В основному: – Юніт-тестування – Інтеграційне тестування	В основному: – Інтеграційне тестування
Хто виконує	Як правило, тестувальники	Як правило, розробники	Як правило, тестувальники
Знання програмування	Не потрібні	Необхідні	Не потрібні
Знання реалізації	Не потрібні	Необхідні	Не потрібні
Основа для тест-кейсів	Специфікація, вимоги	Проектна документація	Специфікація, вимоги

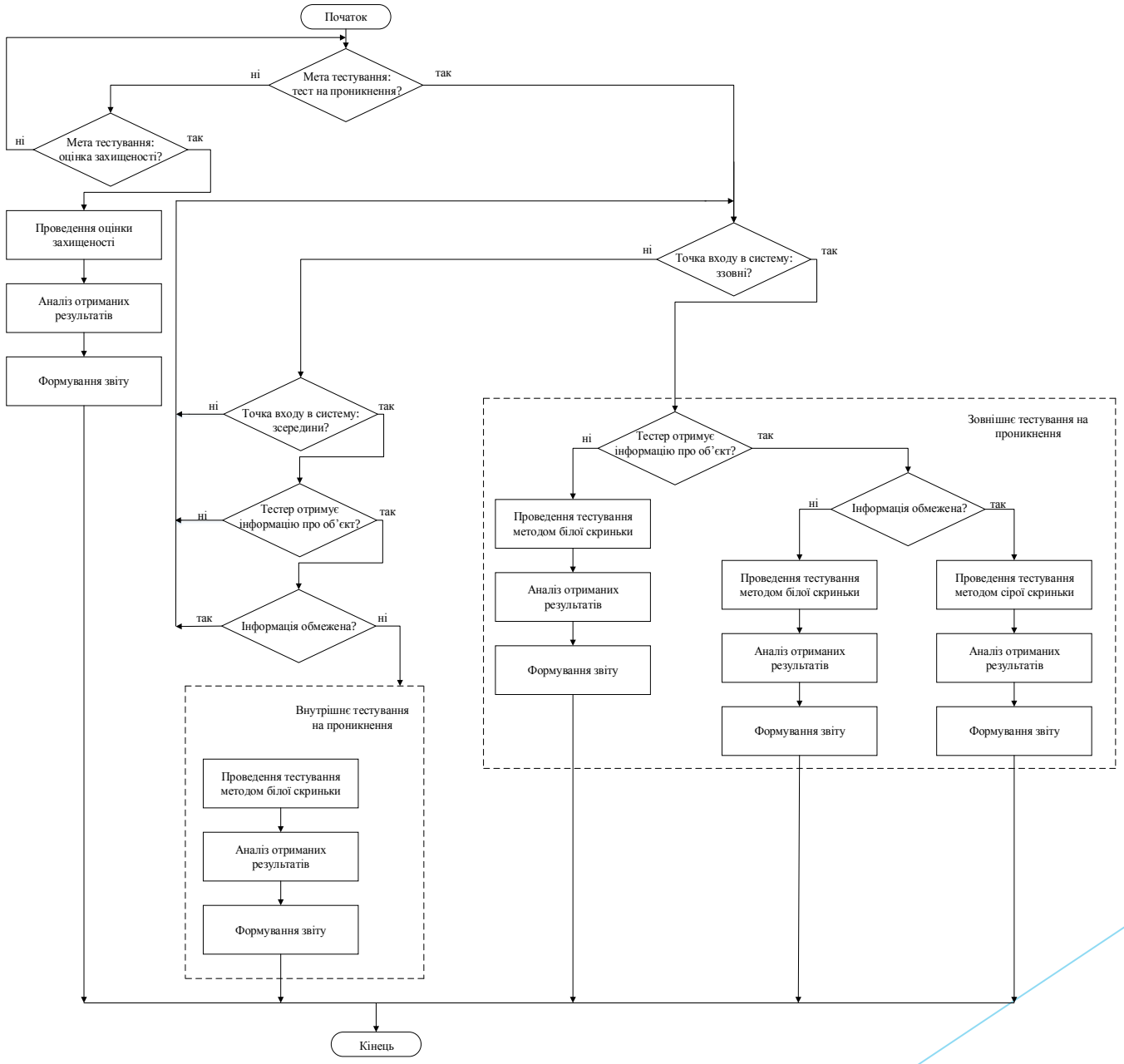
Результати порівняння міжнародних методик проведення тестування на проникнення:

Методика	Фази		
OSSTMM	Тести, необхідні для підтвердження відповідності засобів захисту методиці		
	Список очікуваної інформації при вдалій атаці		
BSI	Підготовка	Підготовка	
		Розвідка	
		Аналіз інформації та ризиків	
	Виконання тестів	Спроби активного втручання	
	Створення звіту	Кінцевий аналіз	
PTEST	Підготовка	Попередня взаємодія	
		Збір інформації	
		Моделювання загроз	
	Виконання тестів	Аналіз вразливостей	
		Експлуатація вразливостей	
		Пост-експлуатація	
	Створення звіту	Звіт	
ISSAF	Підготовка	Планування і підготовка	
		Оцінка	Збір інформації
			Мережевий маппінг
			Ідентифікація вразливостей
	Виконання тестів	Оцінка	Проникнення
			Отримання доступу та розширення привілеїв
			Компрометація віддалених користувачів
			Підтримка доступу
			Приховування слідів
			Аудит
	Створення звіту	Звітність, зачищення та знищення артефактів	

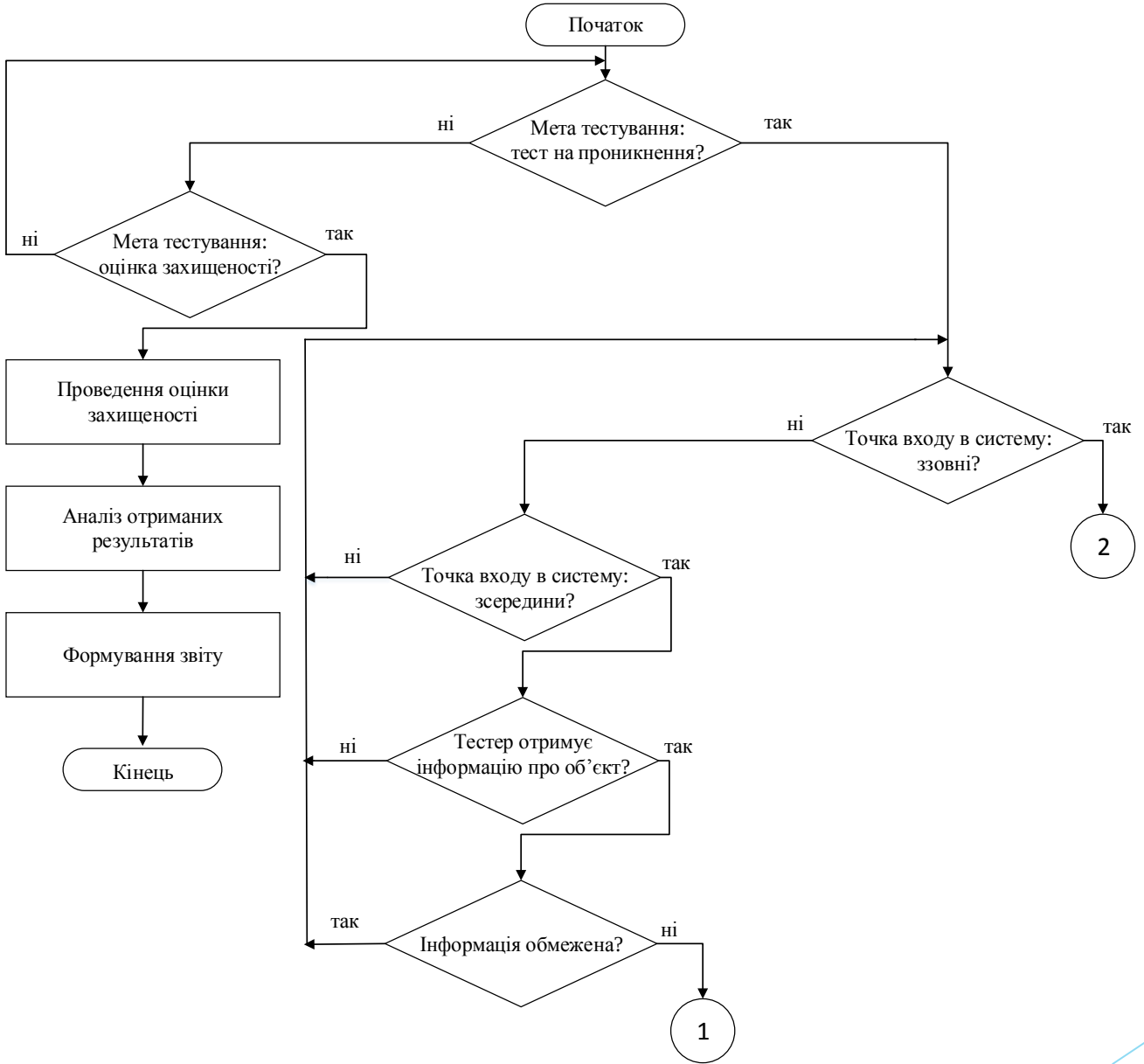
Життєвий цикл тесту на проникнення:



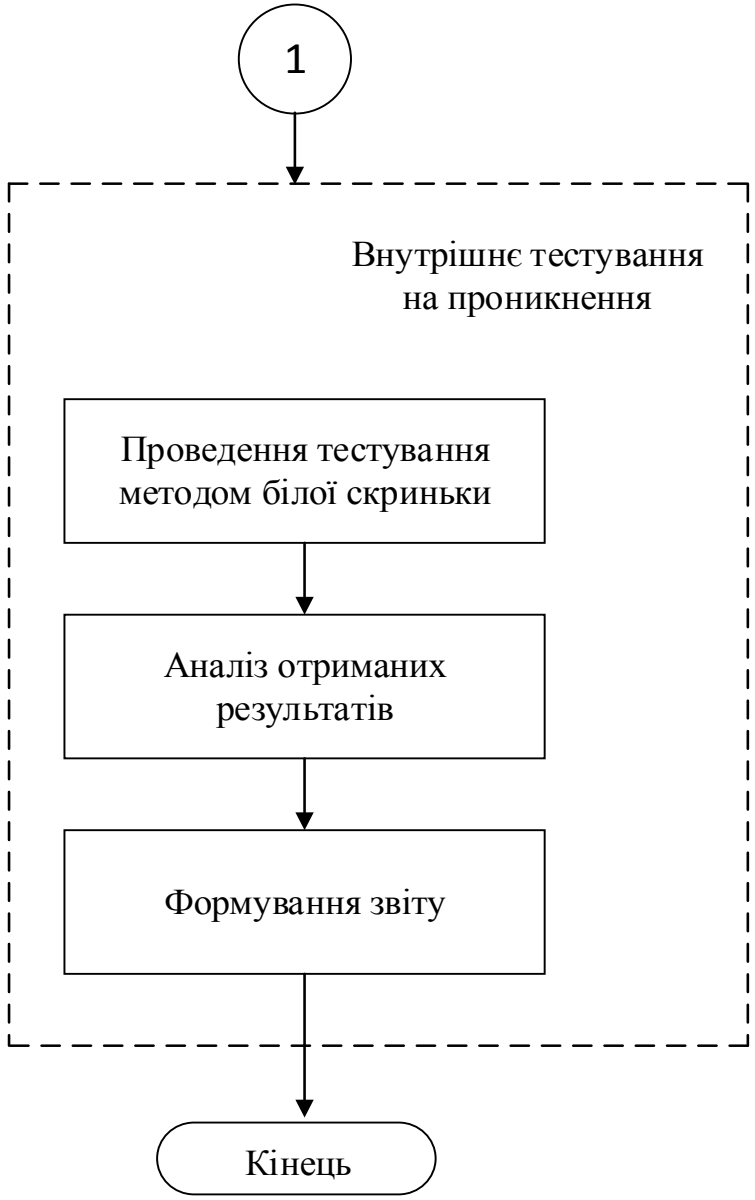
Алгоритм вибору необхідного тесту:



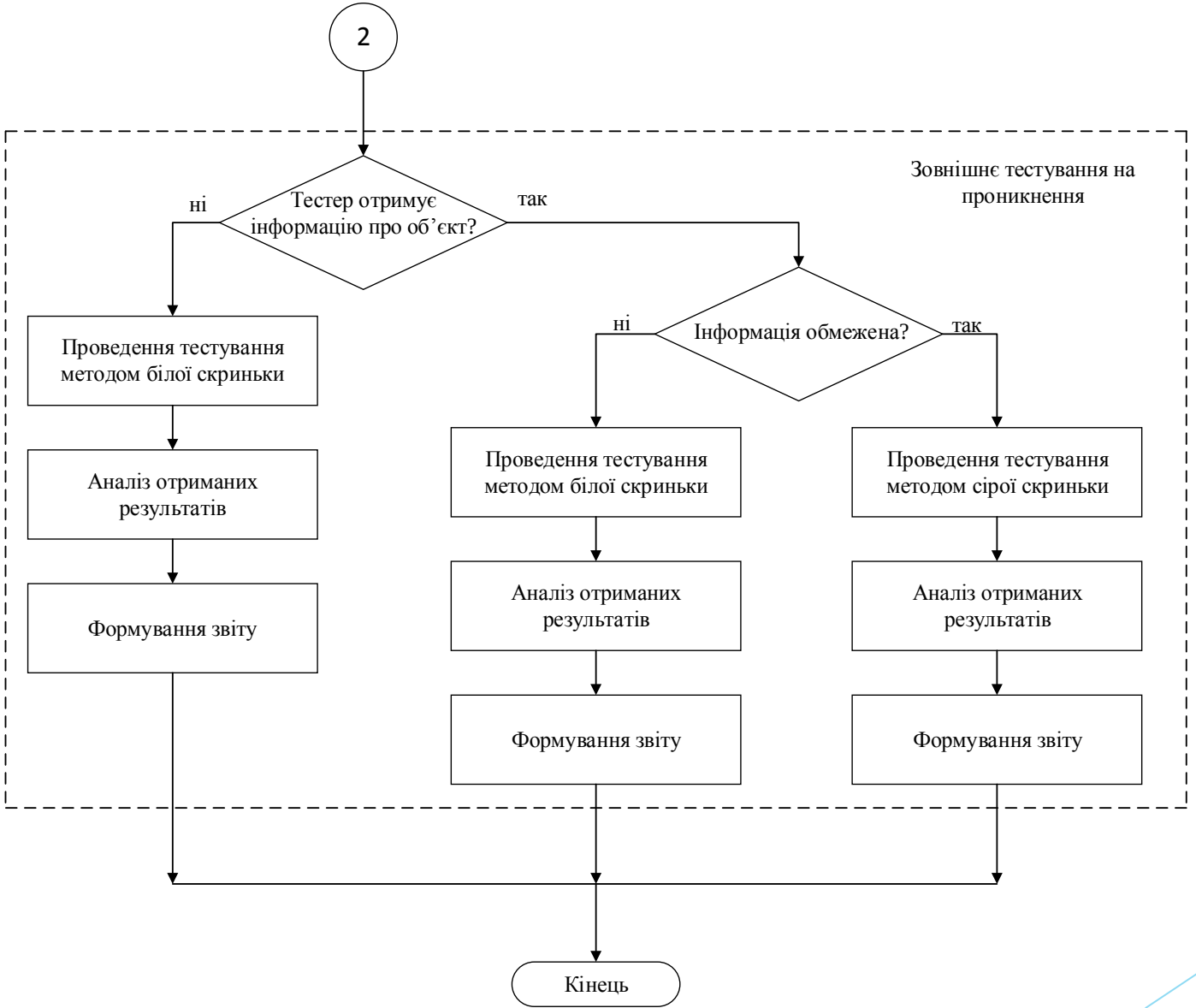
Алгоритм вибору необхідного тесту: вибір типу тестування



Алгоритм вибору необхідного тесту: внутрішнє тестування на проникнення



Алгоритм вибору необхідного тесту: зовнішнє тестування на проникнення



Типові атаки на мобільні пристрої:

- системні уразливості (архітектурних рішень мобільної платформи);
- небезпечне зберігання даних;
- недостатня захищеність протоколів передачі даних;
- вразливості системи авторизації та автентифікації;
- низький рівень криптостійкості;
- вразливості коду програми;
- прихований функціонал додатків;
- неналежний контроль за клієнтськими додатками.

Типові атаки на веб-сайти:

- XSS;
- SQL-injection;
- HTML-bug;
- Brute Force;
- Insufficient Session Expiration;
- Buffer Overflow;
- Content Spoofing;
- Denial of Service тощо.

Типові атаки на апаратну складову: ***Bluetooth-модуль***

- Злом PIN-коду
- Атака з підміною пристрою
- Атака на piconet-мережу ;
- Атака зі скиданням ключа зв'язку;
- Атака підробки точки доступу;
- Атака з переповненням буфера;
- тощо.

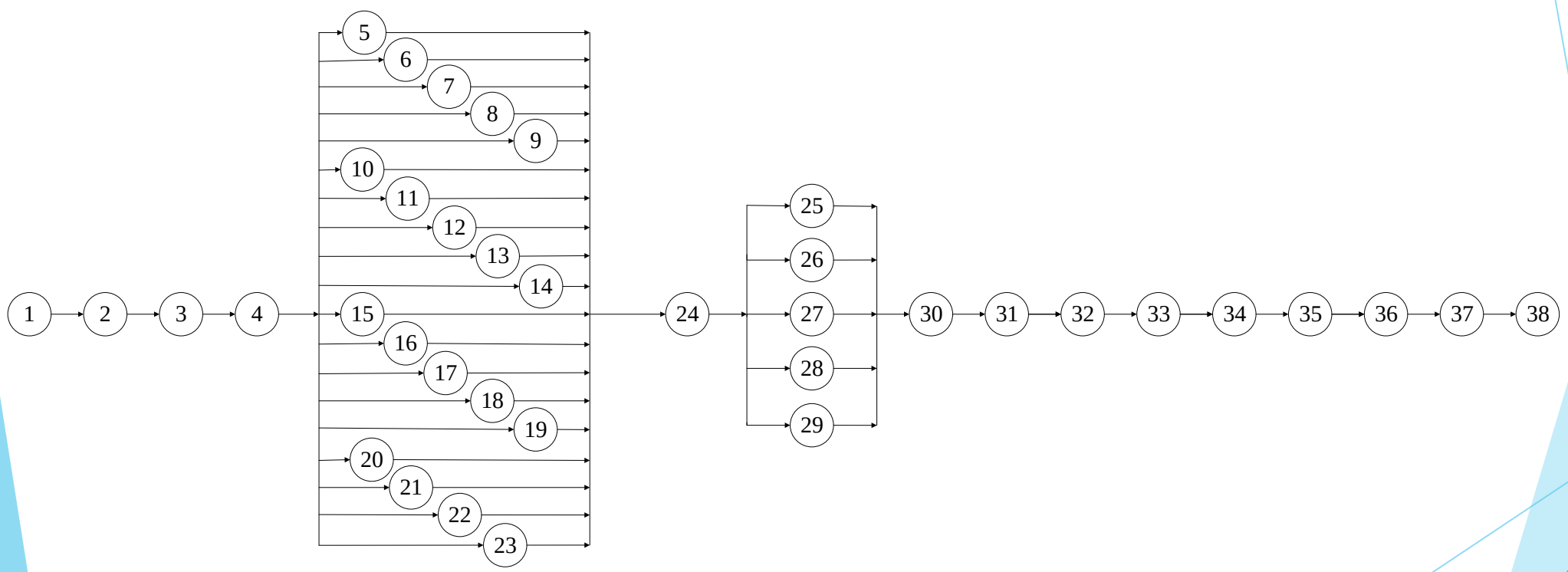
Типові атаки на апаратну складову: Wi-Fi-модуль

- Атака на налаштування параметрів канального рівня;
- DoS атаки;
  - Атака на фізичний рівень (глушіння) ;
  - Затоплення сеансу зв'язку підробленими фреймами ;
  - Атака за допомогою неправильно сформованих кадрів аутентифікації;
  - Заповнення буфера точки доступу;
  - Атака шляхом видалення кадрів;
  - DoS-атака, заснована на циклічному переборі ідентифікаторів EAP;
- Атаки на систему аутентифікації;
- тощо.

Перелік виконуваних тестів:

№	Складова частина системи			Кроки перевірки			
1	Мобільний додаток			1.1	Системні вразливості		
				1.2	Hardcoded and Forgotten		
				1.3	Протоколи передачі даних		
				1.4	Авторизація/автентифікація		
				1.5	Декомпіляція		
2	Веб-сайт			2.1	DoS		
				2.2	XSS		
				2.3	Sql		
				2.4	HTML		
				2.5	BruteForce		
				2.6	Підміна вмісту		
				2.7	Недостатня автентифікація		
				2.8	Недостатня авторизація		
				2.9	Передбачуване розташування каталогів		
				2.10	Виконання команд ОС		
				2.11	Відсутність таймаута сесії		
				2.12	Індексування директорій		
				2.13	Небезпечне відновлення паролів		
				2.14	Переповнення буфера		
				2.15	Передбачуване значення ідентифікатора сесії		
3	Апаратна частина	3.1	Bluetooth	3.1.1	Атака на піконет мережу		
				3.1.2	Переповнення буфера		
				3.1.3	Злом pin-коду		
				3.1.4	Атака з підміною пристрою		
				3.1.5	Атака зі скиданням ключа зв'язку		
				3.1.6	Підробка точки доступу		
		3.2	Wi-Fi	3.2.1	Атака на канальний рівень		
				3.2.2	Атака на систему автентифікації		
				3.2.3	DoS	3.2.3.1	Атака на фізичний рівень
						3.2.3.2	Затоплення сеансу зв'язку
						3.2.3.3	Неправильно сформовані кадри
						3.2.3.4	Переповнення буфера точки доступу
						3.2.3.5	Циклічний перебір EAP

Мережевий графік паралельного тестування усіх складових системи розумного будинку:



Перелік робіт по паралельному тестуванню усіх складових системи розумного будинку в MS Project:

Диаграмма Ганта

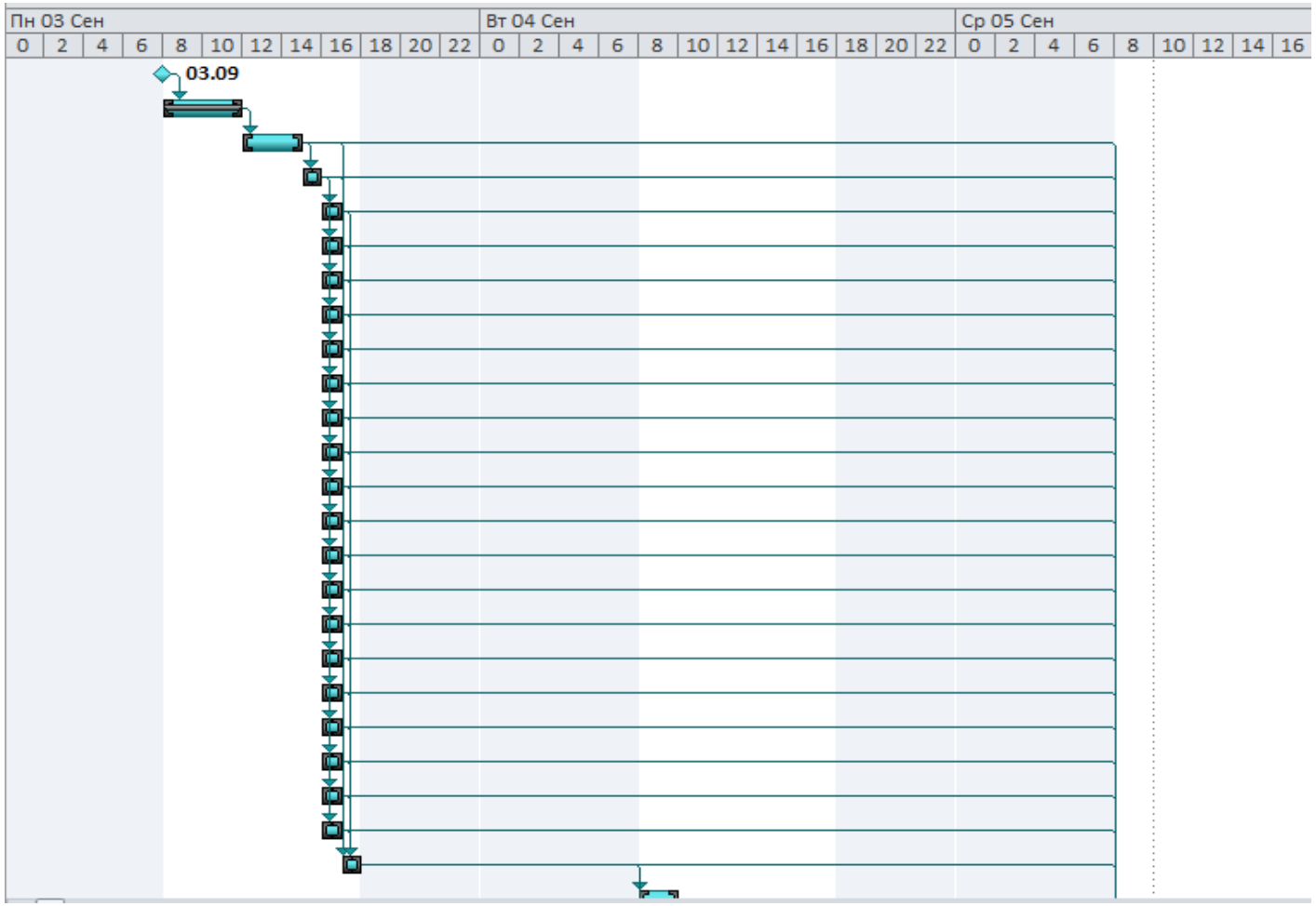
	Режим задачи	Название задачи	Длительно	Начало	Окончание	Предшественники
1		Початок	0 часов	Пн 03.09.18	Пн 03.09.18	
2		Підготовчий етап	3 часов	Пн 03.09.18	Пн 03.09.18	1
3		Аналіз вразливостей	2 часов	Пн 03.09.18	Пн 03.09.18	2
4		2.1	1 час	Пн 03.09.18	Пн 03.09.18	3
5		2.2	1 час	Пн 03.09.18	Пн 03.09.18	4
6		2.3	1 час	Пн 03.09.18	Пн 03.09.18	4
7		2.4	1 час	Пн 03.09.18	Пн 03.09.18	4
8		2.5	1 час	Пн 03.09.18	Пн 03.09.18	4
9		2.6	1 час	Пн 03.09.18	Пн 03.09.18	4
10		2.7	1 час	Пн 03.09.18	Пн 03.09.18	4
11		2.8	1 час	Пн 03.09.18	Пн 03.09.18	4
12		2.9	1 час	Пн 03.09.18	Пн 03.09.18	4
13		2.10	1 час	Пн 03.09.18	Пн 03.09.18	4
14		2.11	1 час	Пн 03.09.18	Пн 03.09.18	4
15		2.12	1 час	Пн 03.09.18	Пн 03.09.18	4
16		2.13	1 час	Пн 03.09.18	Пн 03.09.18	4
17		2.14	1 час	Пн 03.09.18	Пн 03.09.18	4
18		2.15	1 час	Пн 03.09.18	Пн 03.09.18	4
19		1.1	1 час	Пн 03.09.18	Пн 03.09.18	4
20		1.2	1 час	Пн 03.09.18	Пн 03.09.18	4
21		1.3	1 час	Пн 03.09.18	Пн 03.09.18	4
22		1.4	1 час	Пн 03.09.18	Пн 03.09.18	4
23		1.5	1 час	Пн 03.09.18	Пн 03.09.18	4
24		3.1.1	1 час	Пн 03.09.18	Пн 03.09.18	3;19;20;21;22;23;4;5;6;7;8;9;10;11;12;13;14;15;16;17;18

Продовження переліку робіт по паралельному тестуванню усіх складових системи розумного будинку в MS Project:

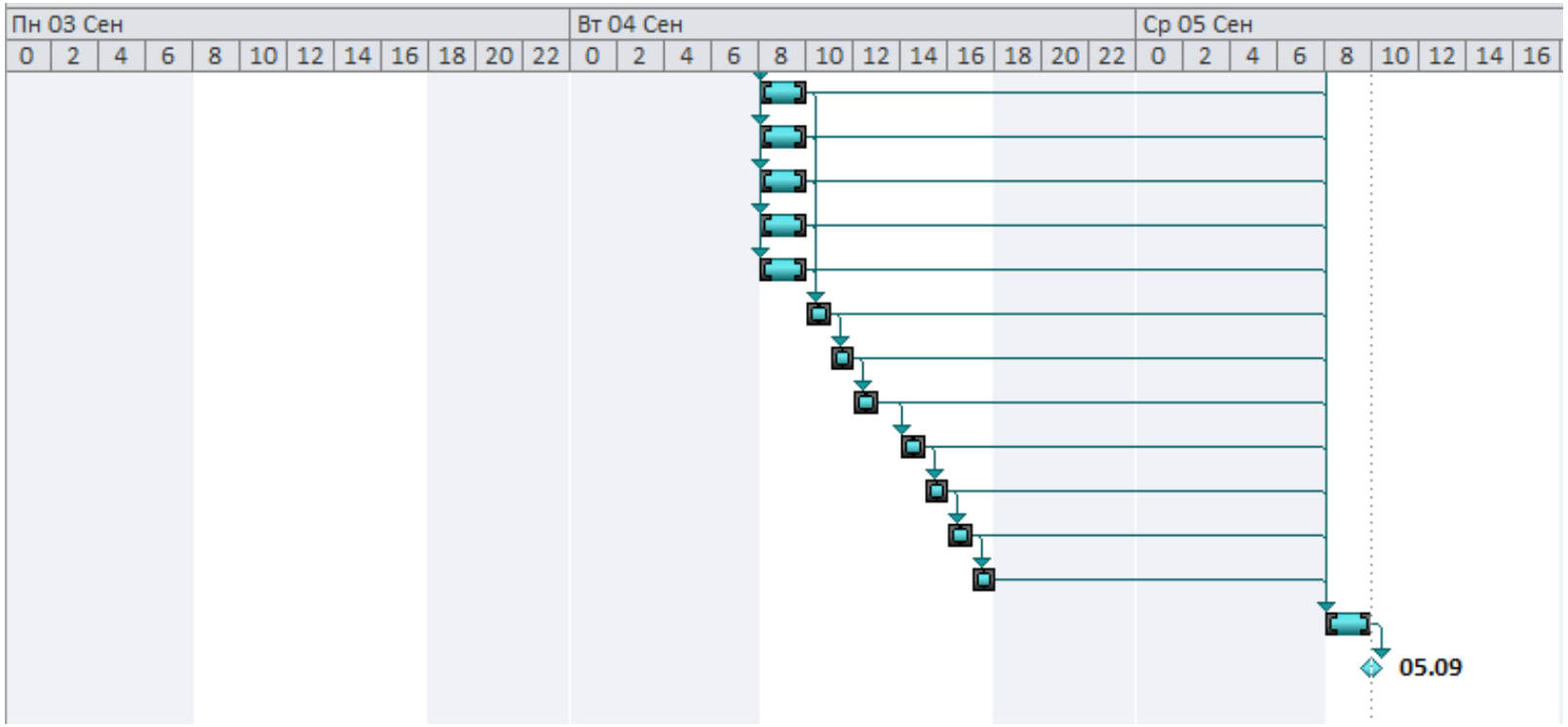
Диаграмма Ганта

25			3.1.2	1 час	Вт 04.09.18	Вт 04.09.18	24
26			3.1.3	1 час	Вт 04.09.18	Вт 04.09.18	24
27			3.1.4	1 час	Вт 04.09.18	Вт 04.09.18	24
28			3.1.5	1 час	Вт 04.09.18	Вт 04.09.18	24
29			3.1.6	1 час	Вт 04.09.18	Вт 04.09.18	24
30			3.2.1	1 час	Вт 04.09.18	Вт 04.09.18	25;26;27;28;29
31			3.2.2	1 час	Вт 04.09.18	Вт 04.09.18	30
32			3.2.3.1	1 час	Вт 04.09.18	Вт 04.09.18	31
33			3.2.3.2	1 час	Вт 04.09.18	Вт 04.09.18	32
34			3.2.3.3	1 час	Вт 04.09.18	Вт 04.09.18	33
35			3.2.3.4	1 час	Вт 04.09.18	Вт 04.09.18	34
36			3.2.3.5	1 час	Вт 04.09.18	Вт 04.09.18	35
37			Формування звіту	1 час	Ср 05.09.18	Ср 05.09.18	3;19;20;21;22;23;4;5;6;7;8;9;10;11;12;13;14;15;16;17;18;24;25;26;27;28;29;30;31;32;33;34;35;36
38			Кінець	0 часов	Ср 05.09.18	Ср 05.09.18	37

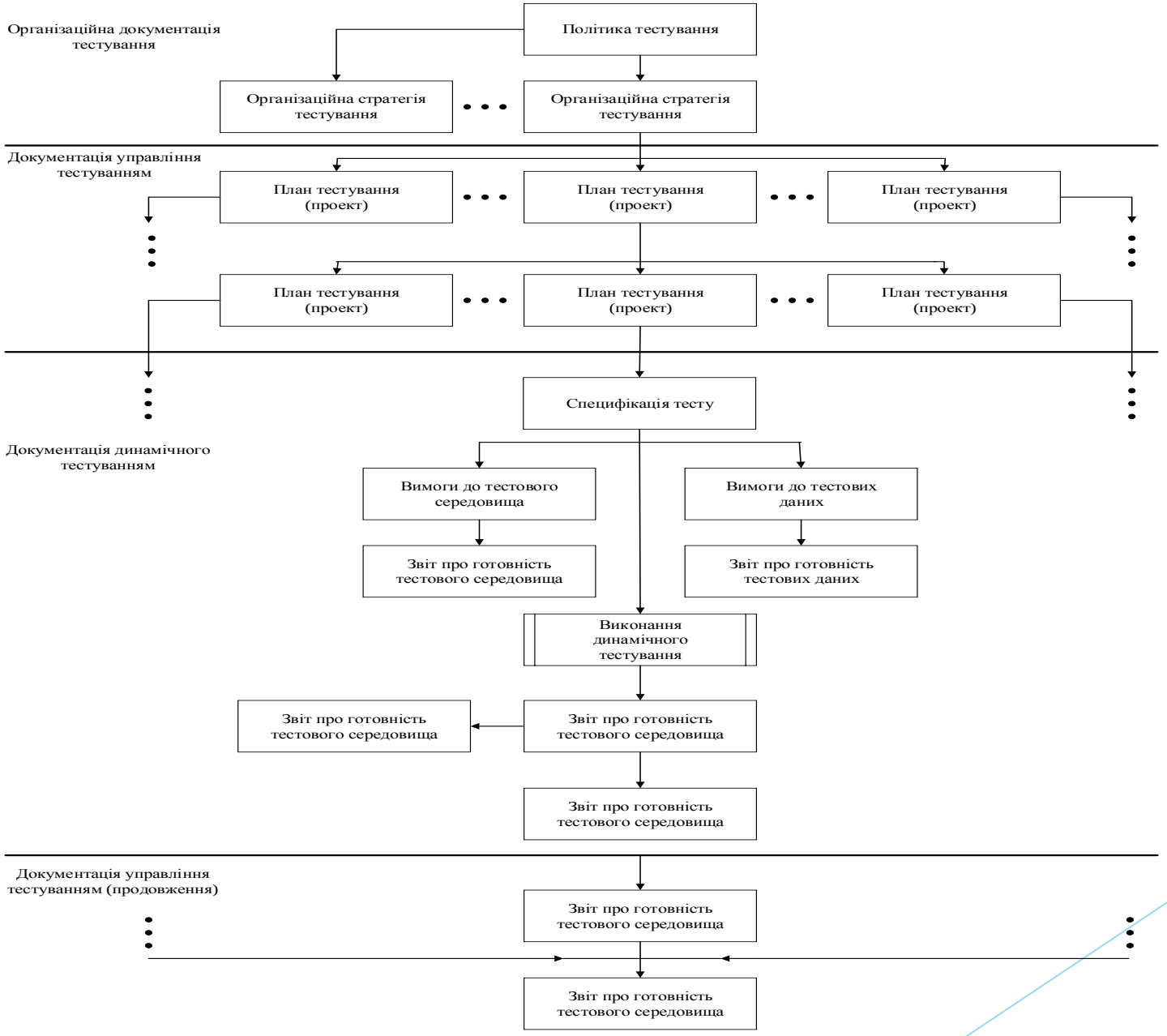
Діаграма Ганта паралельного тестування усіх складових системи розумного будинку:



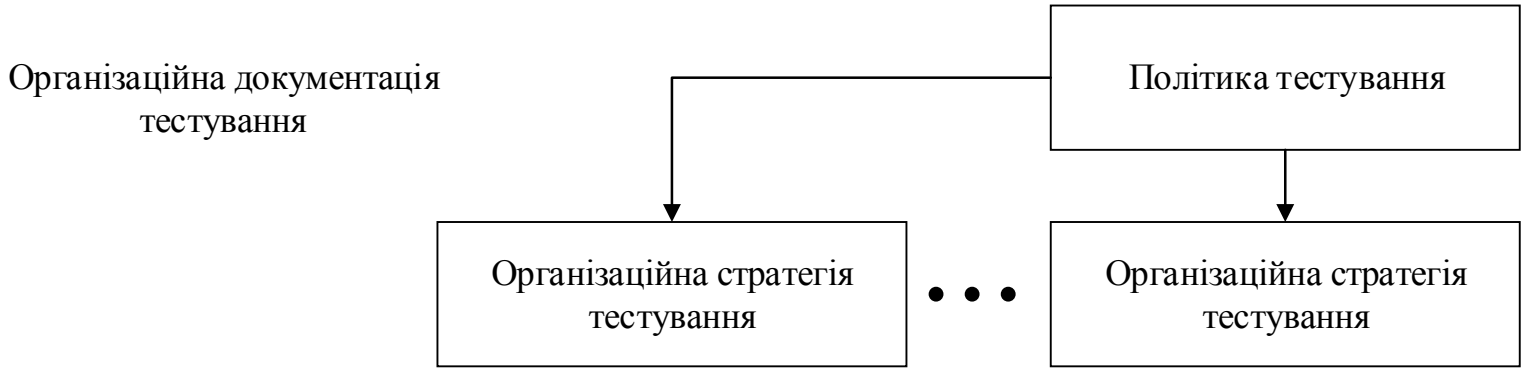
Продовження діаграми Ганта паралельного тестування усіх складових системи розумного будинку:



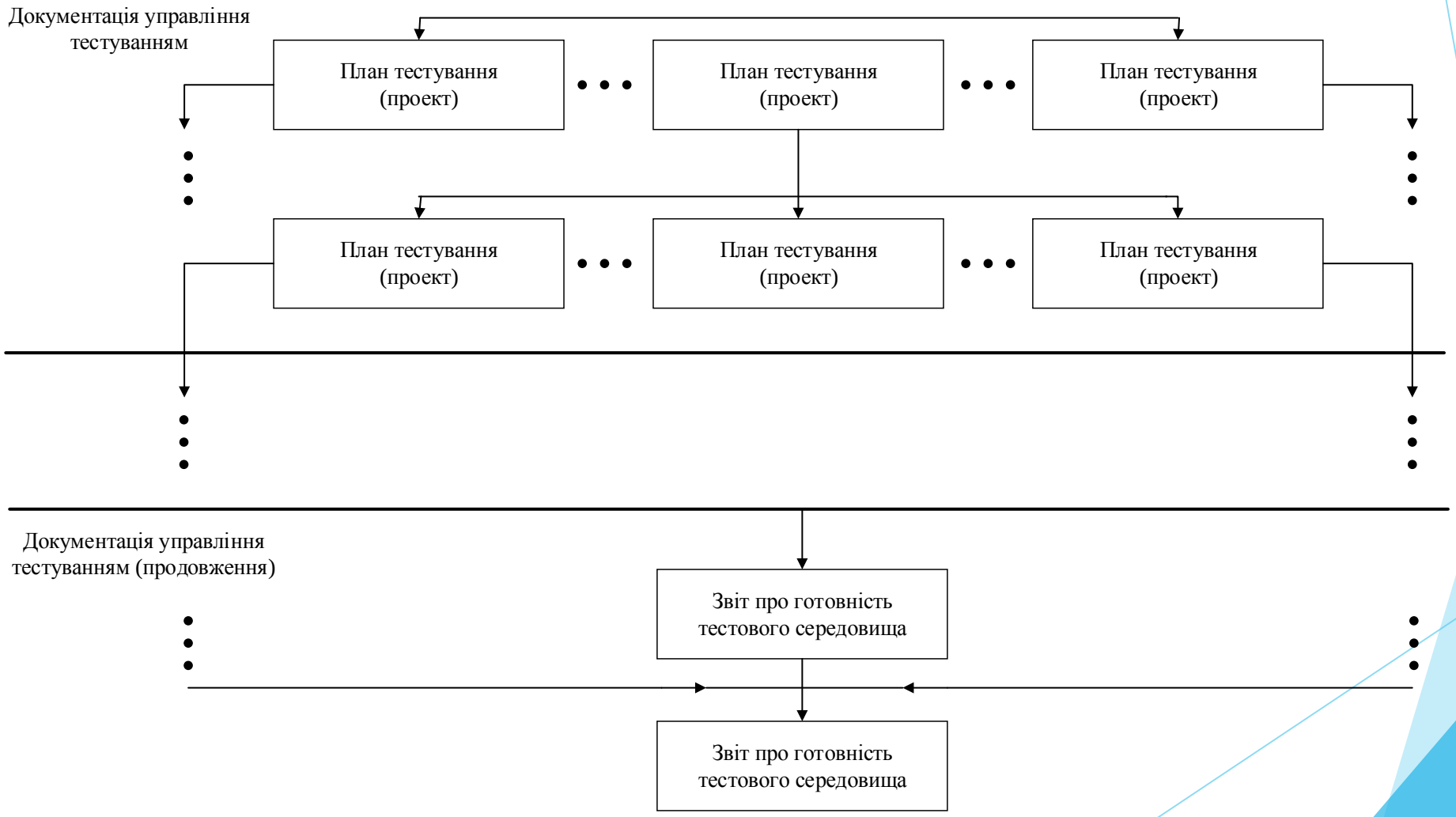
Ієрархія документації тестування:



Ієрархія документації тестування:
Організаційна документація тестування

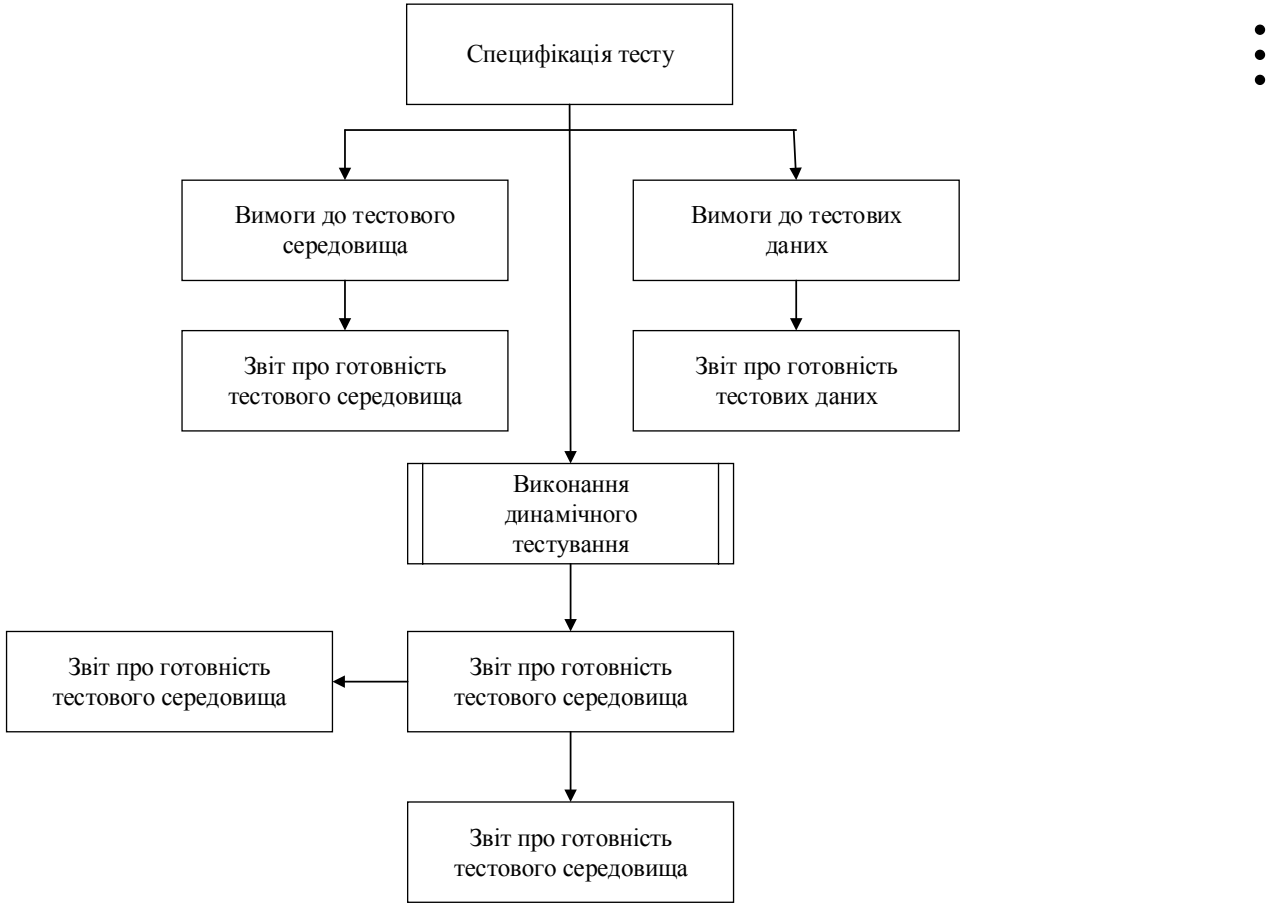


Ієрархія документації тестування:
Документація управління тестування



Ієрархія документації тестування:
Документація динамічного тестування

Документація динамічного тестуванням



Обґрунтування економічної доцільності:

- Проведено оцінку комерційного потенціалу розробки;
- Спрогнозовано витрати на виконання наукової роботи – 65667,37 грн.;
- Спрогнозовано чистий прибуток від впровадження результатів розробки – за 3 роки 200402,9 грн.;
- Термін окупності – 1,1 року.

Представлення Результатів комплексної магістерської кваліфікаційної роботи:

Конференції:

- XLVI науково-технічна конференція факультету інформаційних технологій та комп’ютерної інженерії Вінницького національного технічного університету. Доповідь визнана найкращою.
- 54 студентська наукова конференція Науково-Технологічного Університету AGH в Кракові (Польща).
- Шоста Міжнародна науково-практична конференція «Методи та засоби кодування, захисту й ущільнення інформації»
- XLVII Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії.

А також опубліковані тези доповідей.

Дякую за увагу!