Принципи побудови та структурна схема автоматизованої системи для аналізу бінарних вразливостей програмного забезпечення

Карко В.В.
ФТІ ФБ-41м

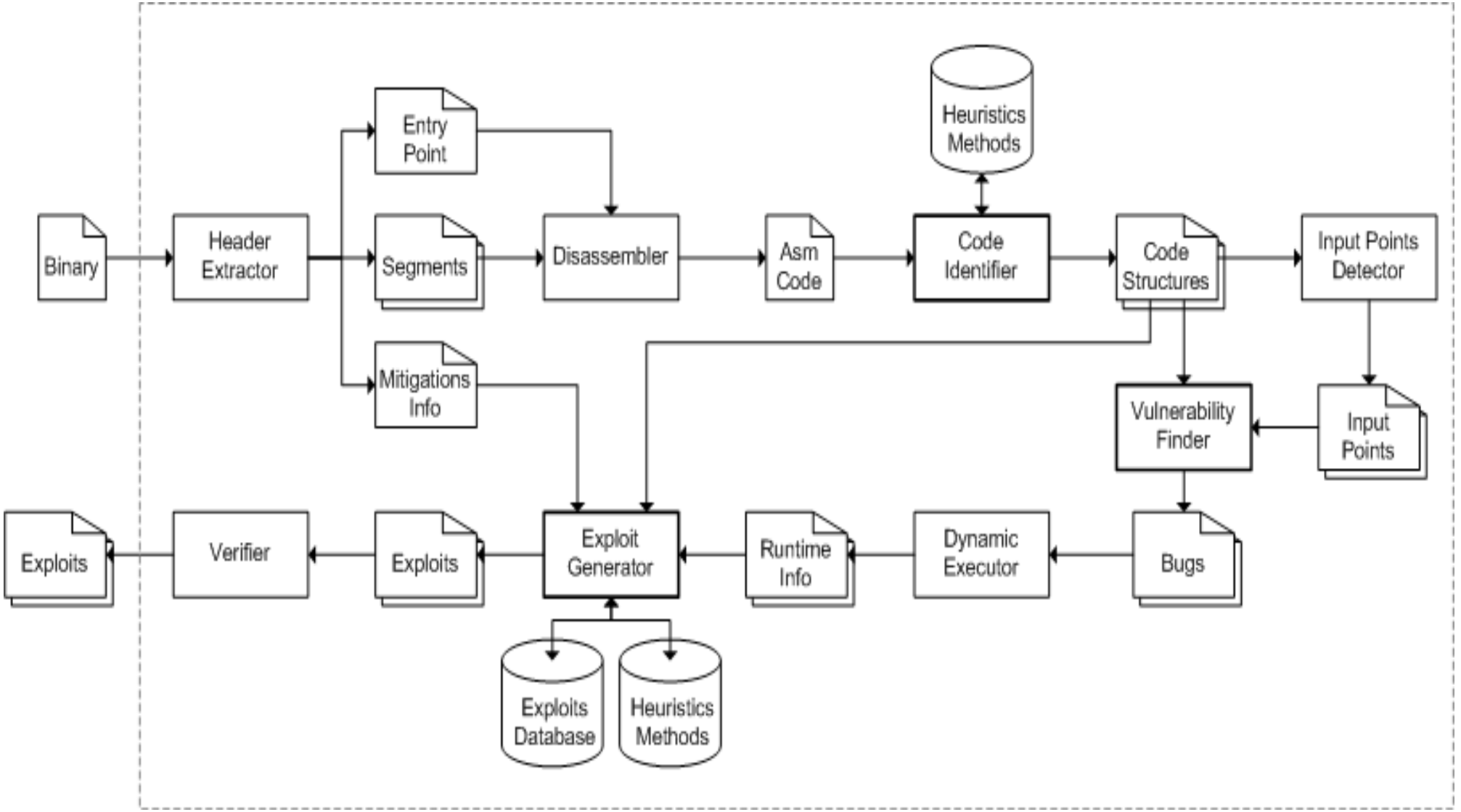
Завдання автоматизованої системи

- знаходження вразливостей у заданому бінарному файлі
- побудова відповідних експлойтів
- формування висновку щодо можливості експлуатації вразливостей
- представлення детальної інформації про пройдені системою етапи

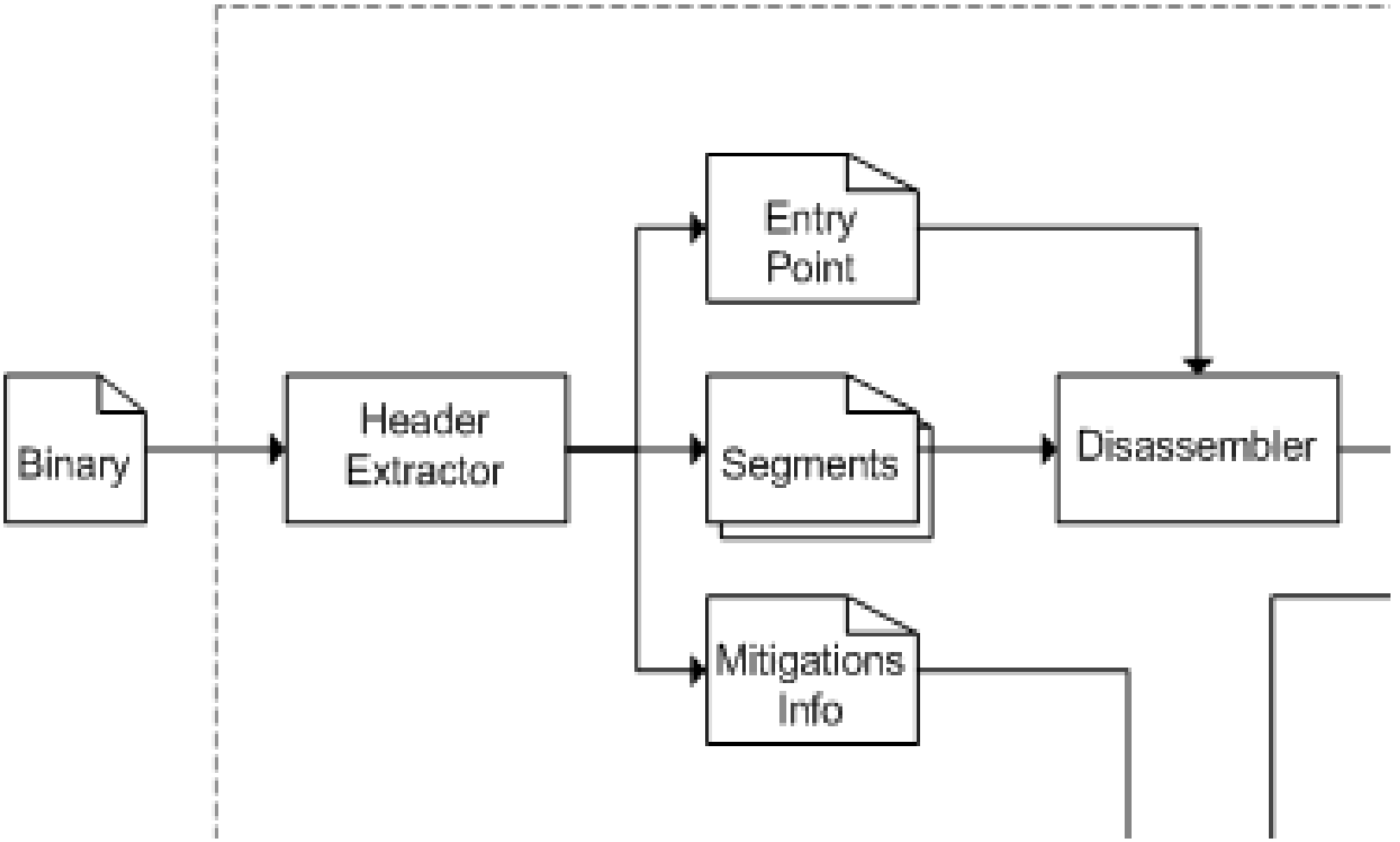
Вимоги до системи

- Можливість роботи системи без вихідного коду
- Робота з певною архітектурою
- Робота системи в автоматичному та автоматизованому режимі
- Підвищенні вимоги до використання ресурсів системою
- Зниження інтерференції системи та програми

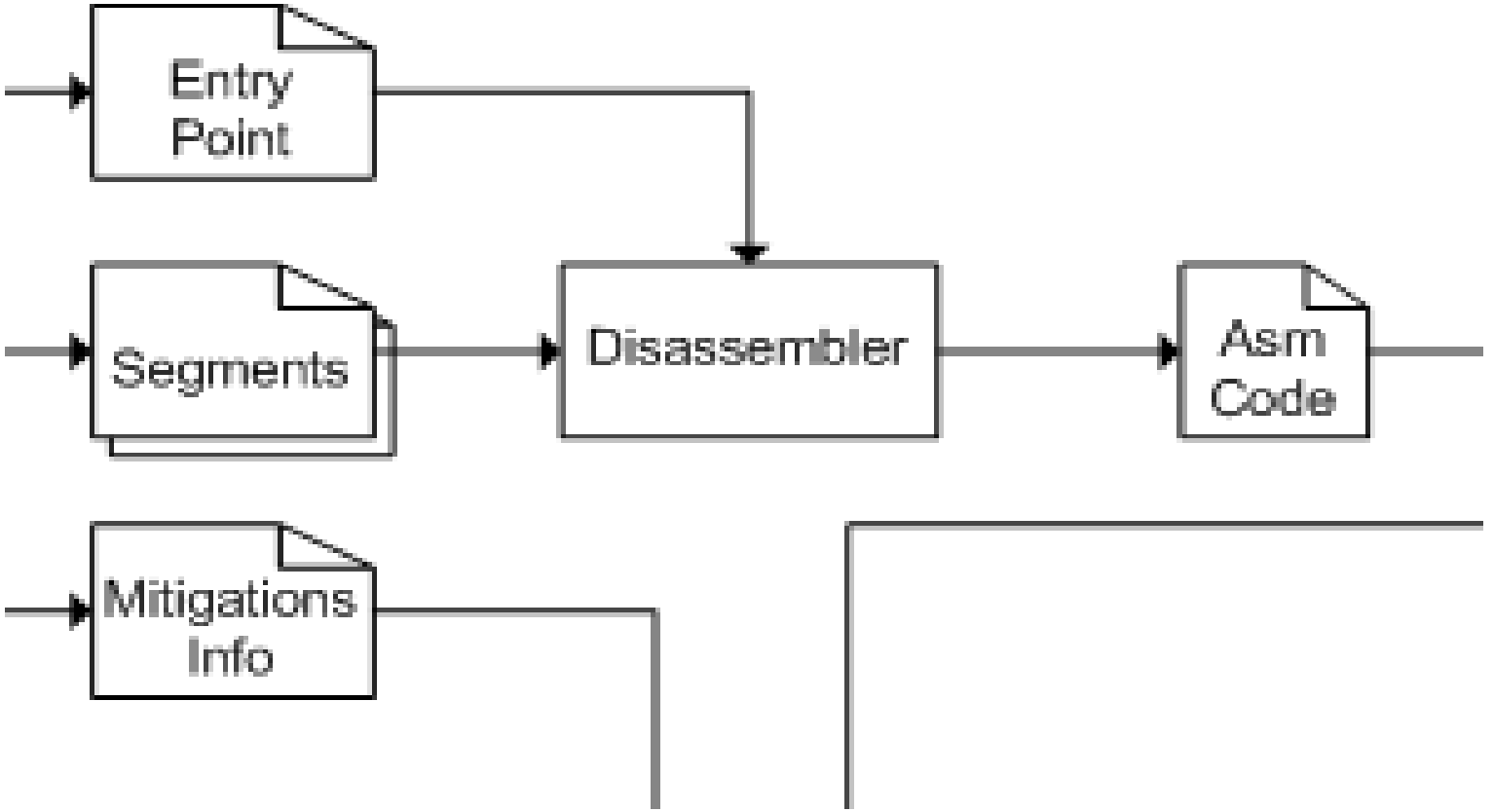
Структурна схема системи



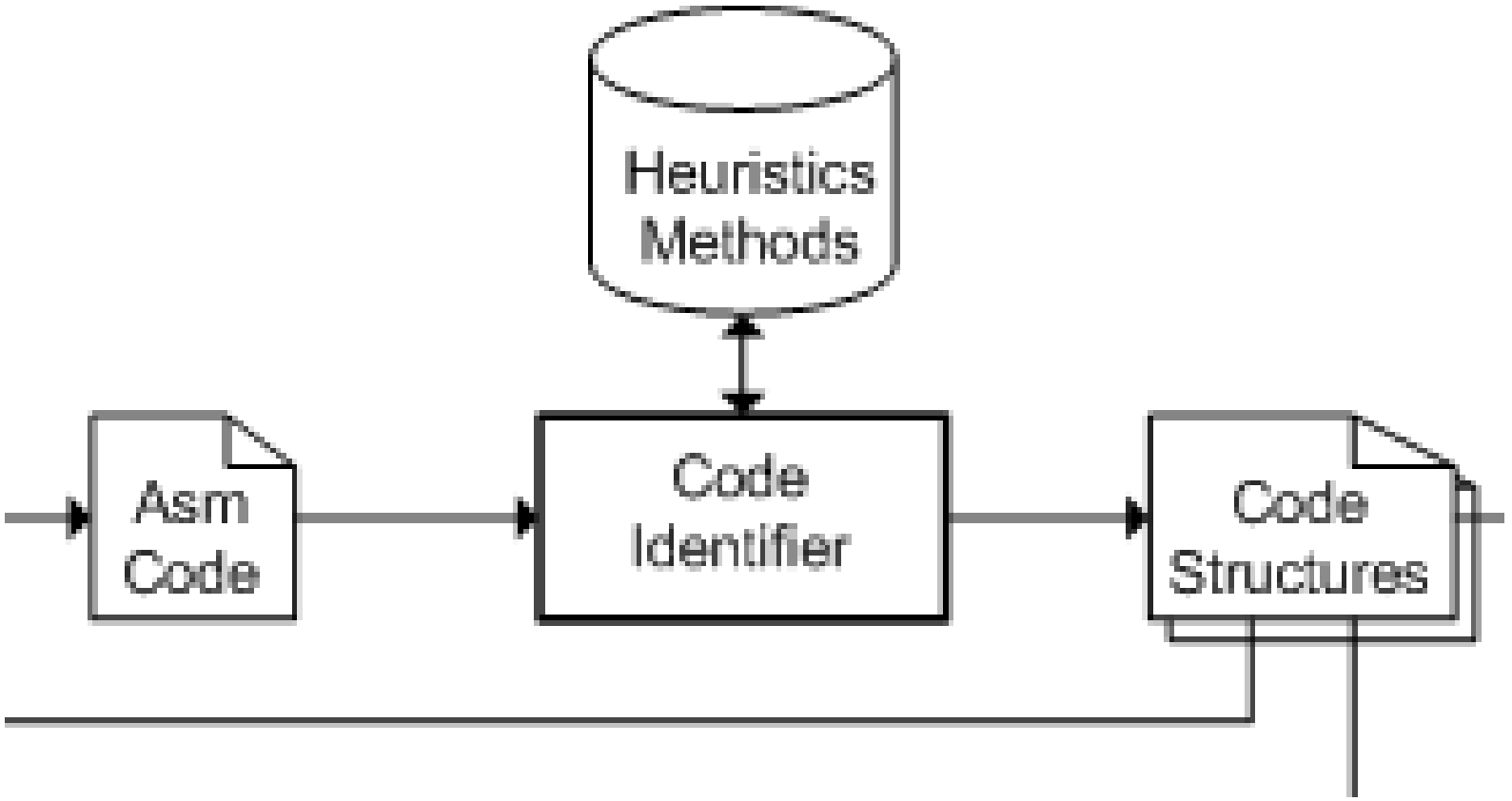
Header Extractor



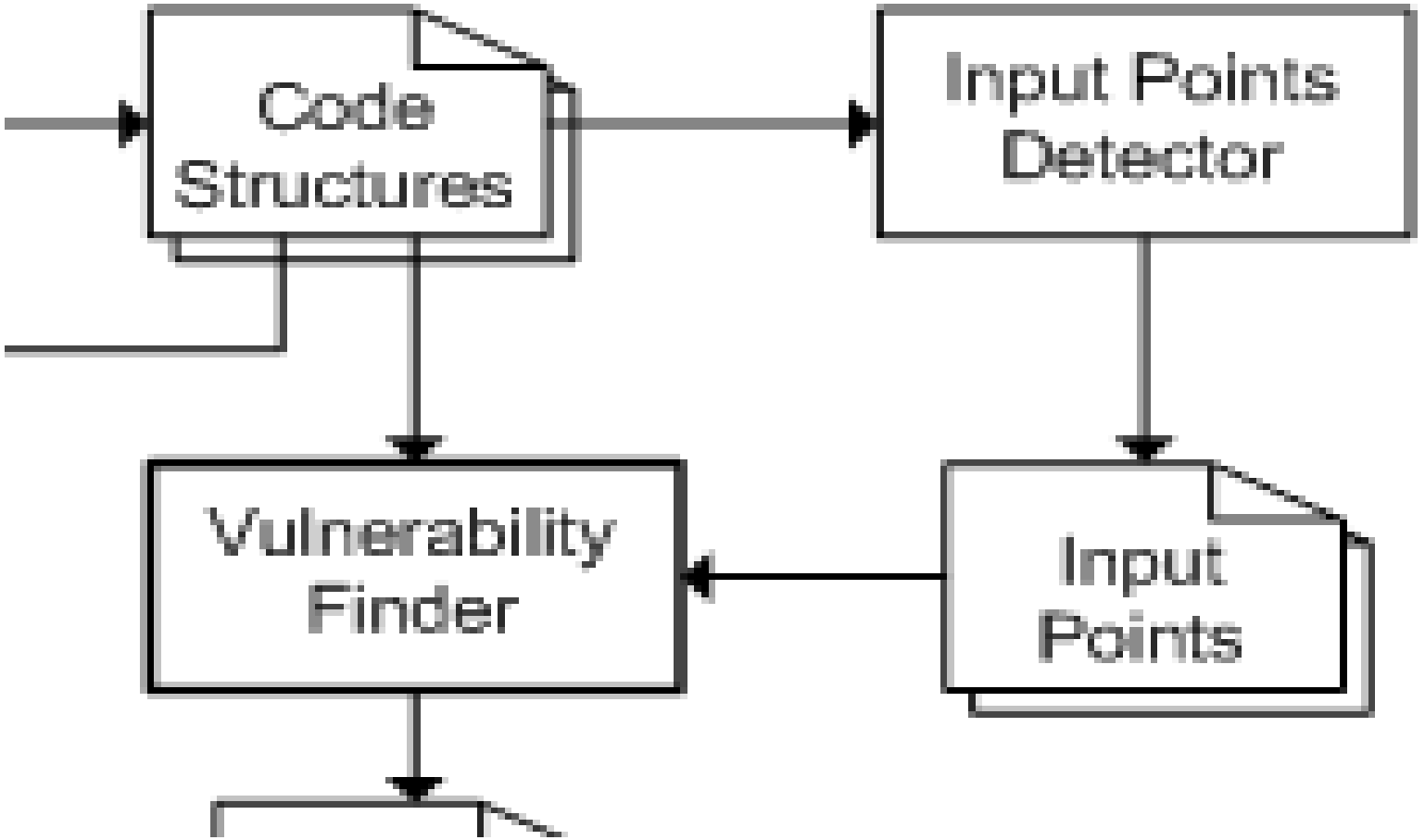
Disassembler



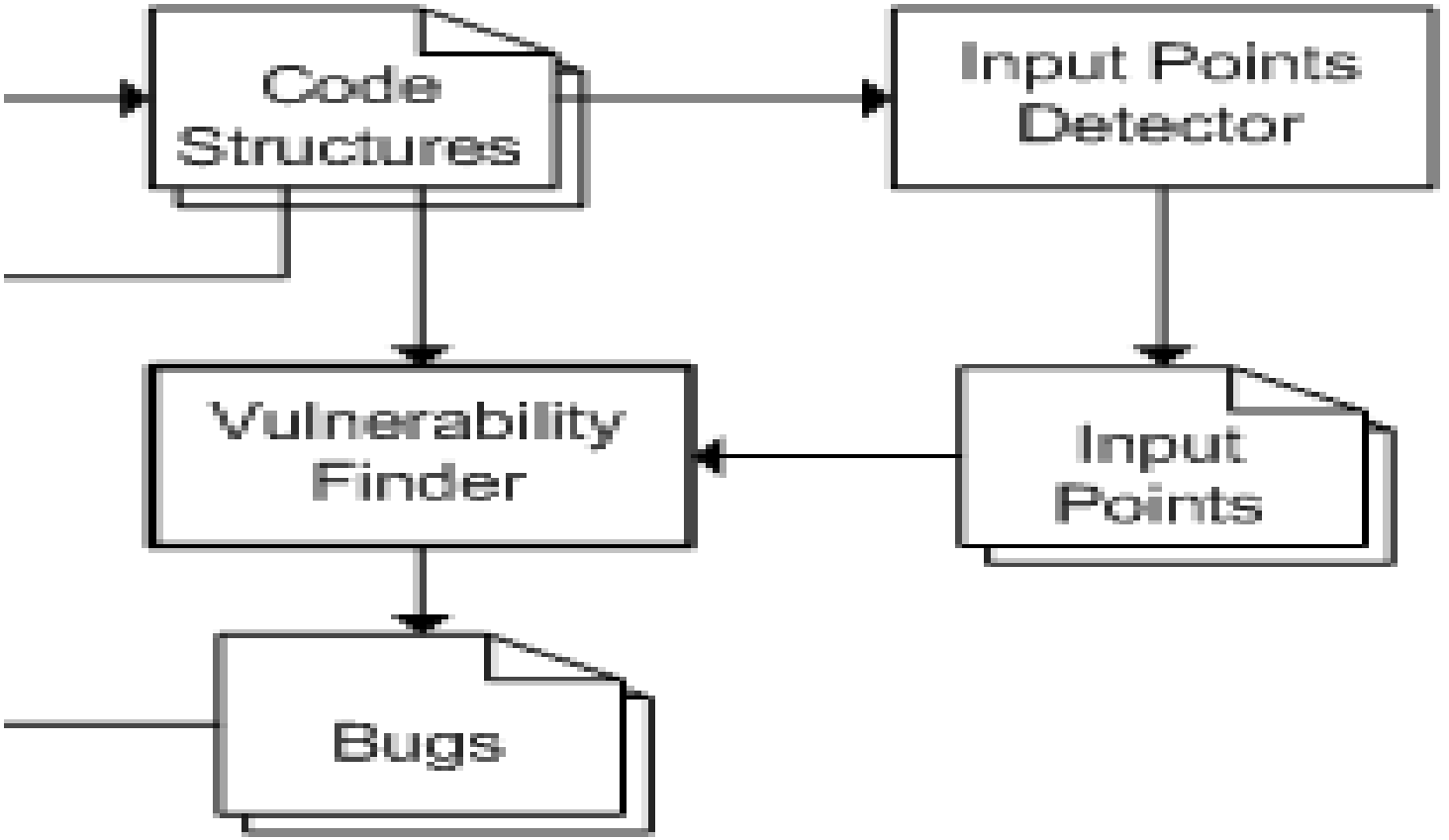
Code Identifier



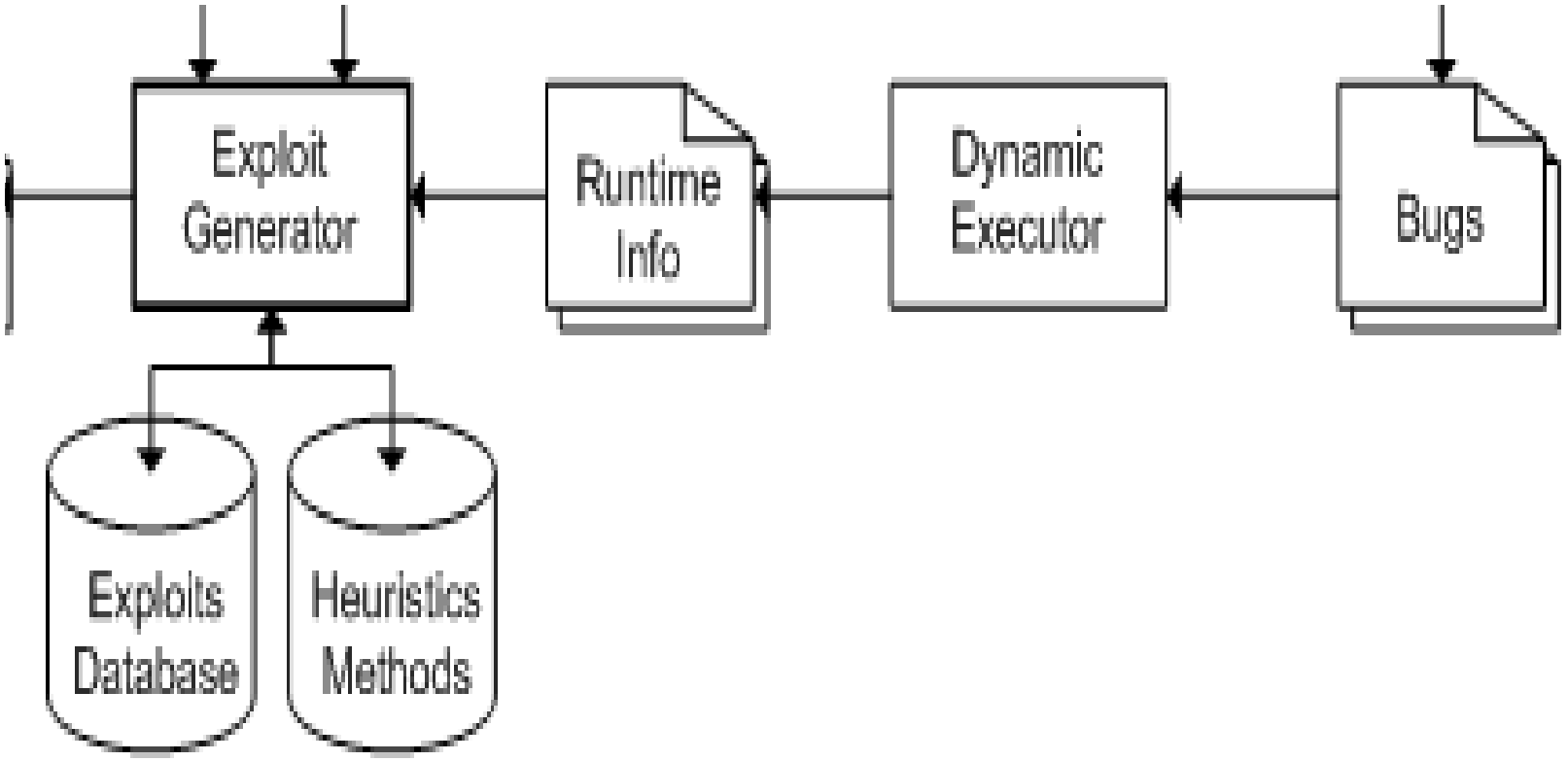
Input points Detector



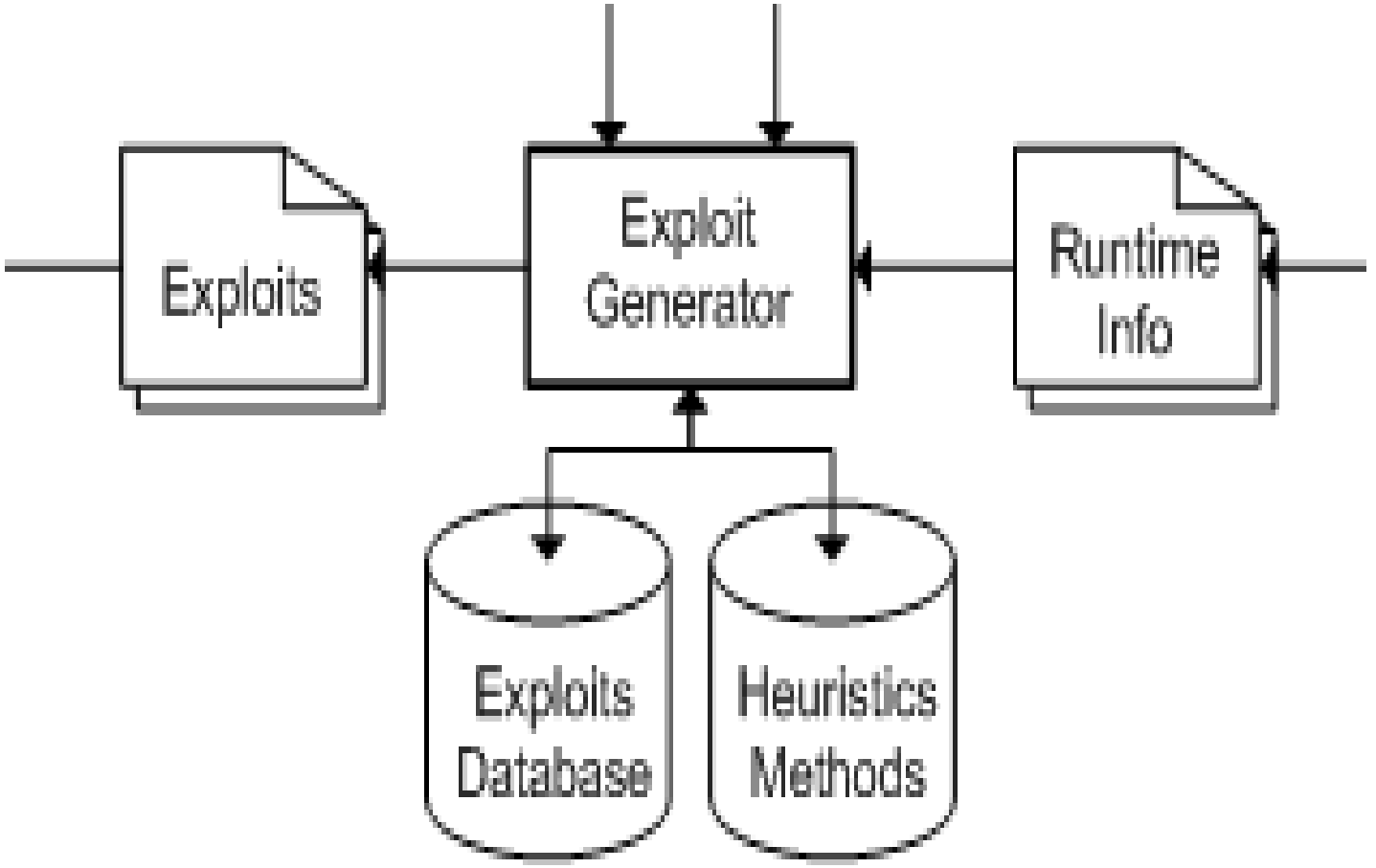
Vulnerability Finder



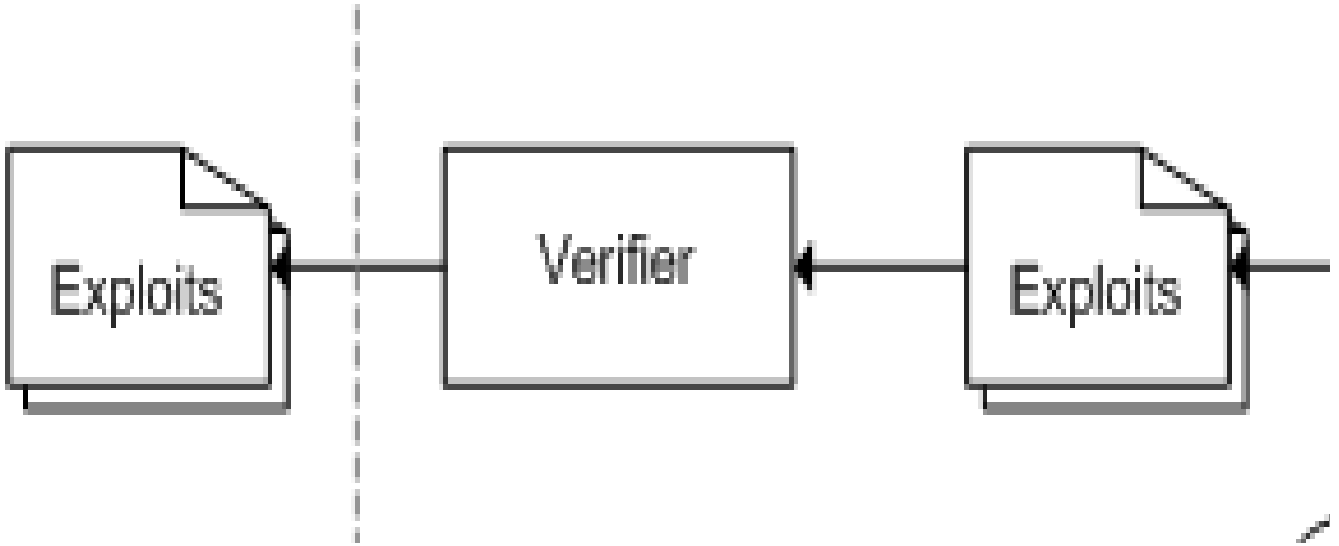
Dynamic Executor



Exploit Generator



Verifier



Висновки

- Основні вимоги до автоматизованої системи для аналізу бінарних вразливостей програмного забезпечення
- Детальна структурна схема системи
- Найбільш складними для реалізації є блоки виявлення вразливостей та генерації експлойту
- Не існує єдиного, ефективного рішення цих задач

Дякую за увагу