SPIIRAS

Применение онтологического подхода и логического вывода для управления информацией и событиями безопасности

Ольга Полубелова, Игорь Саенко

Лаборатория проблем компьютерной безопасности
Санкт-Петербургского Института Информатики и Автоматизации РАН

Санкт-Петербург, Россия

Содержание

- **SIEM-системы**
- **Стандарты представления данных в системах информационной безопасности (SCAP, IDMEF, CBE, CIM)**
- **Онтологический подход для построения модели данных**
- **Построение репозитория на основе гибридного подхода**
- **Заключение**

Главные задачи теоретических исследований и реализации

1. **Предложить более выразительный, гибкий, масштабируемый способ к представлению данных в программных продуктах в области информационной безопасности**

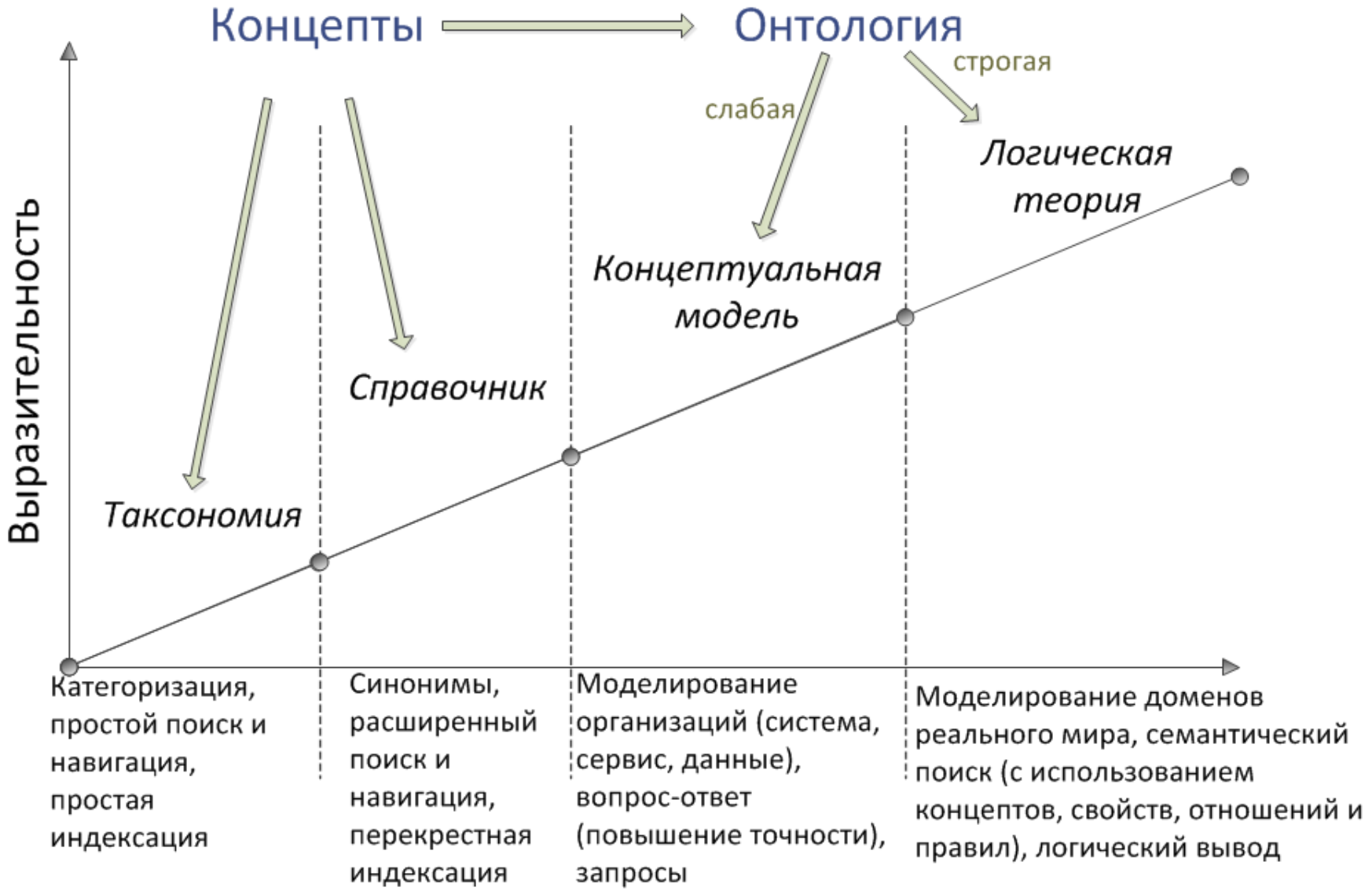
2. **Обеспечить возможность применения в различных сферах (критические инфраструктуры, мобильные услуги, сетевая инфраструктура)**

3. **Предложить открытую и легко расширяемую архитектуру репозитория на основе предложенного подхода к представлению данных**

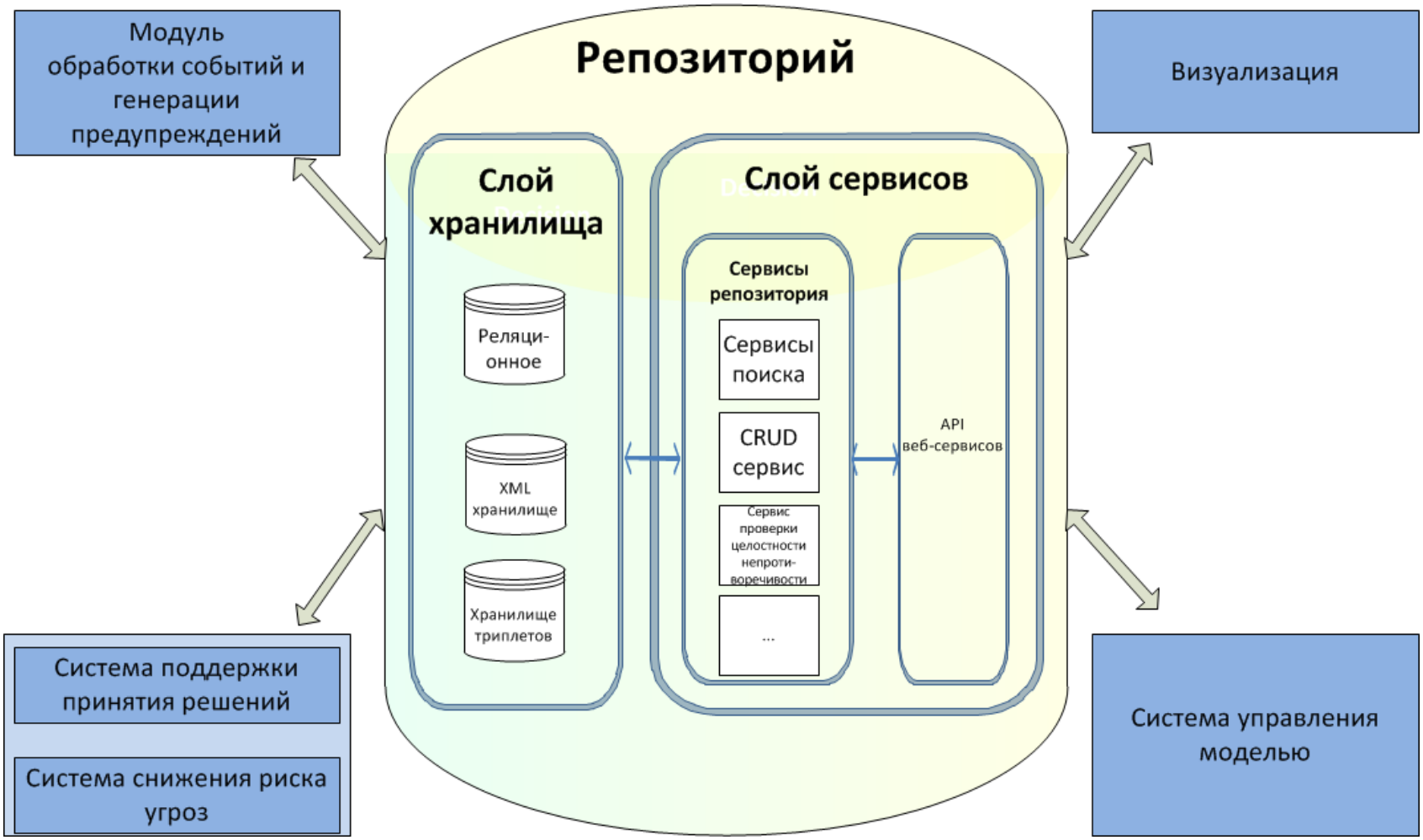
Стандарты представления данных в области информационной безопасности

- Common Event Expression (CEE, MITRE)
- Common Base Event (CBE, IBM)
- Common Event Format (CEF)
- The Common Intrusion Specification Language (CISL)
- The Intrusion Detection Message Exchange Format (IDMEF)
- Distributed Audit Service (XDAS)
- The Incident Object Description Exchange Format (IODEF)
- Common Information model (CIM)

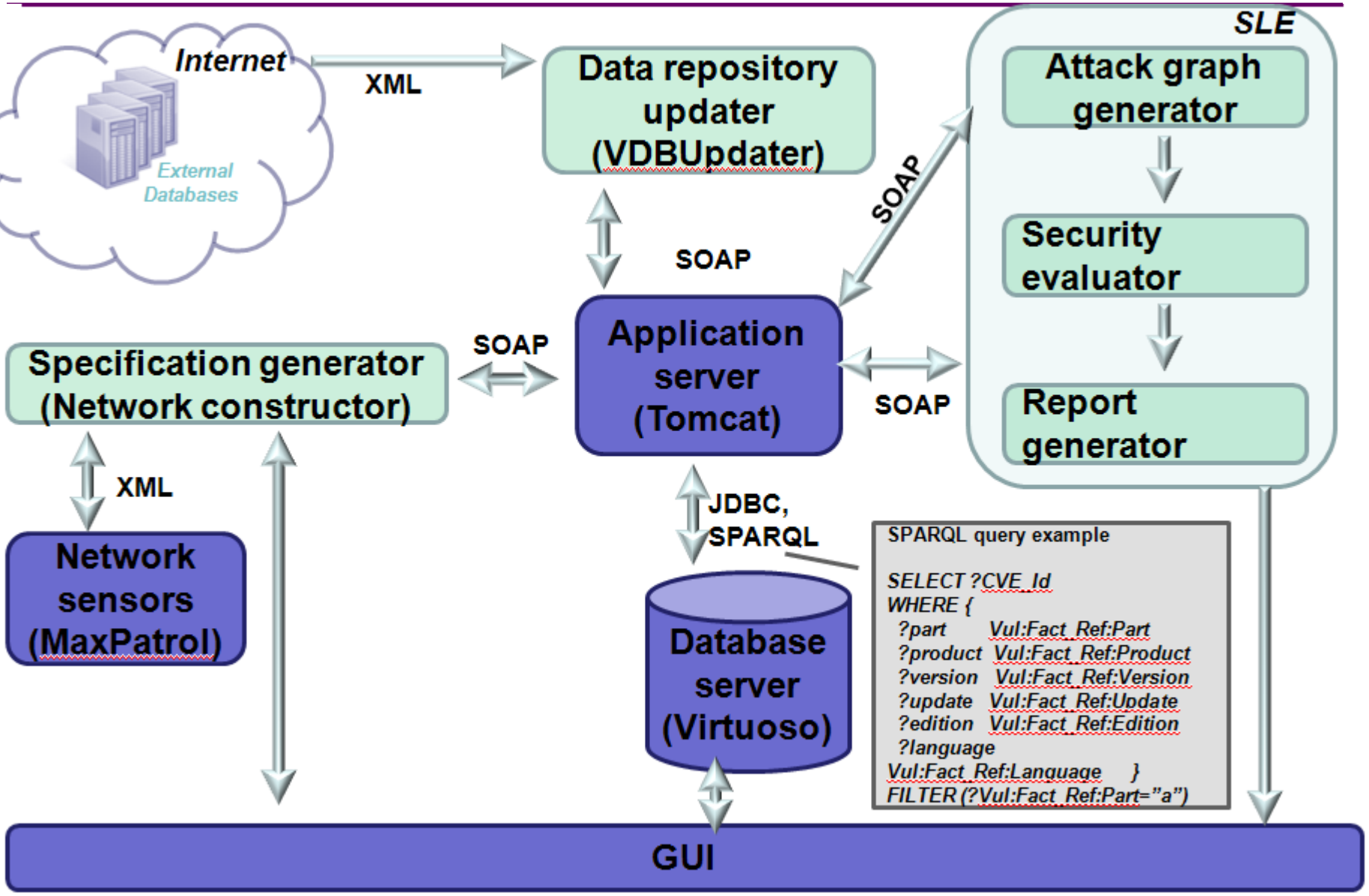
Применение онтологий



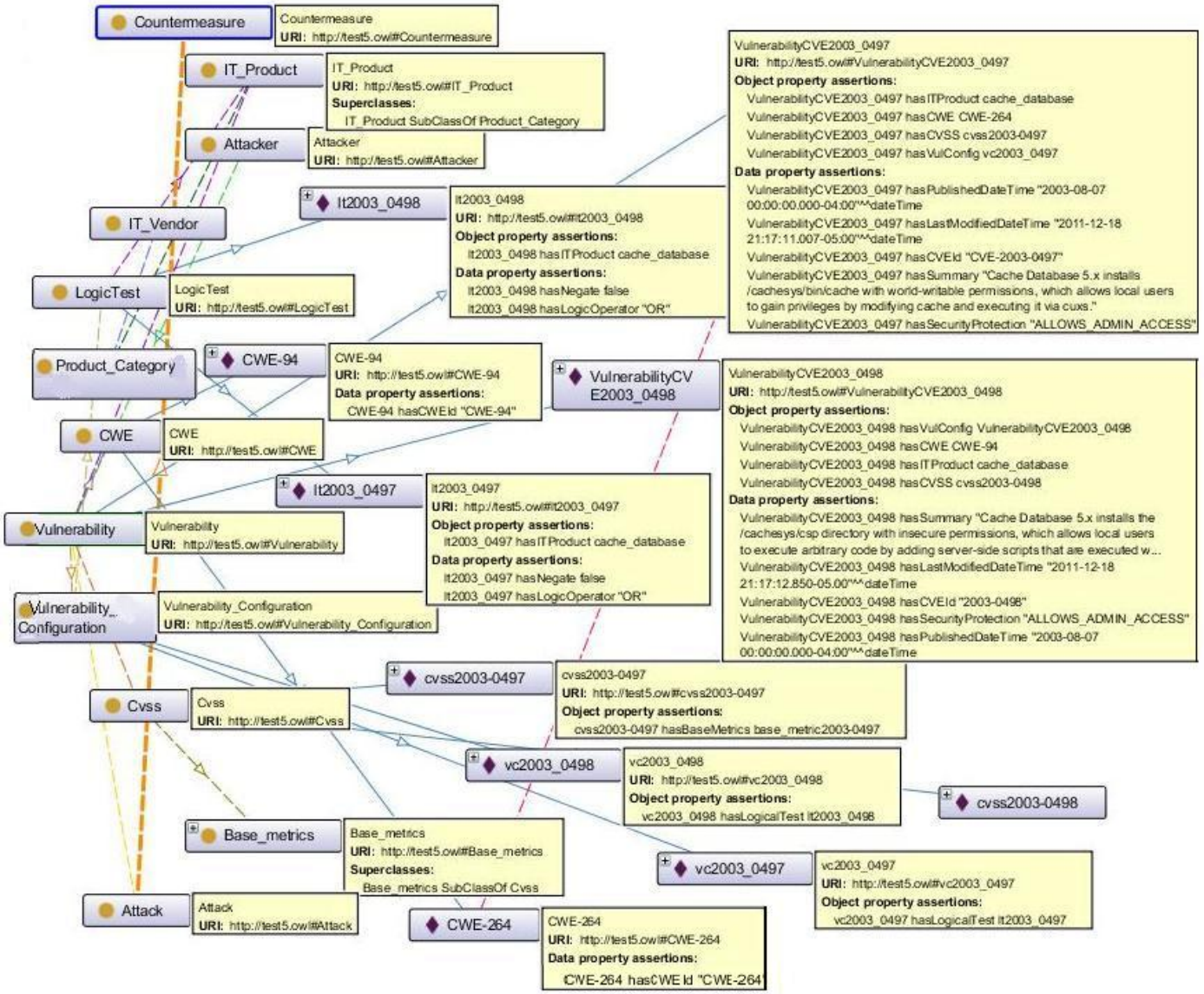
Место репозитория в проекте MASSIF



Применение в задаче моделирования атак



Онтологическая модель для представления сущности «уязвимость»



Отображение схем данных NIST стандартов в уровень модели данных

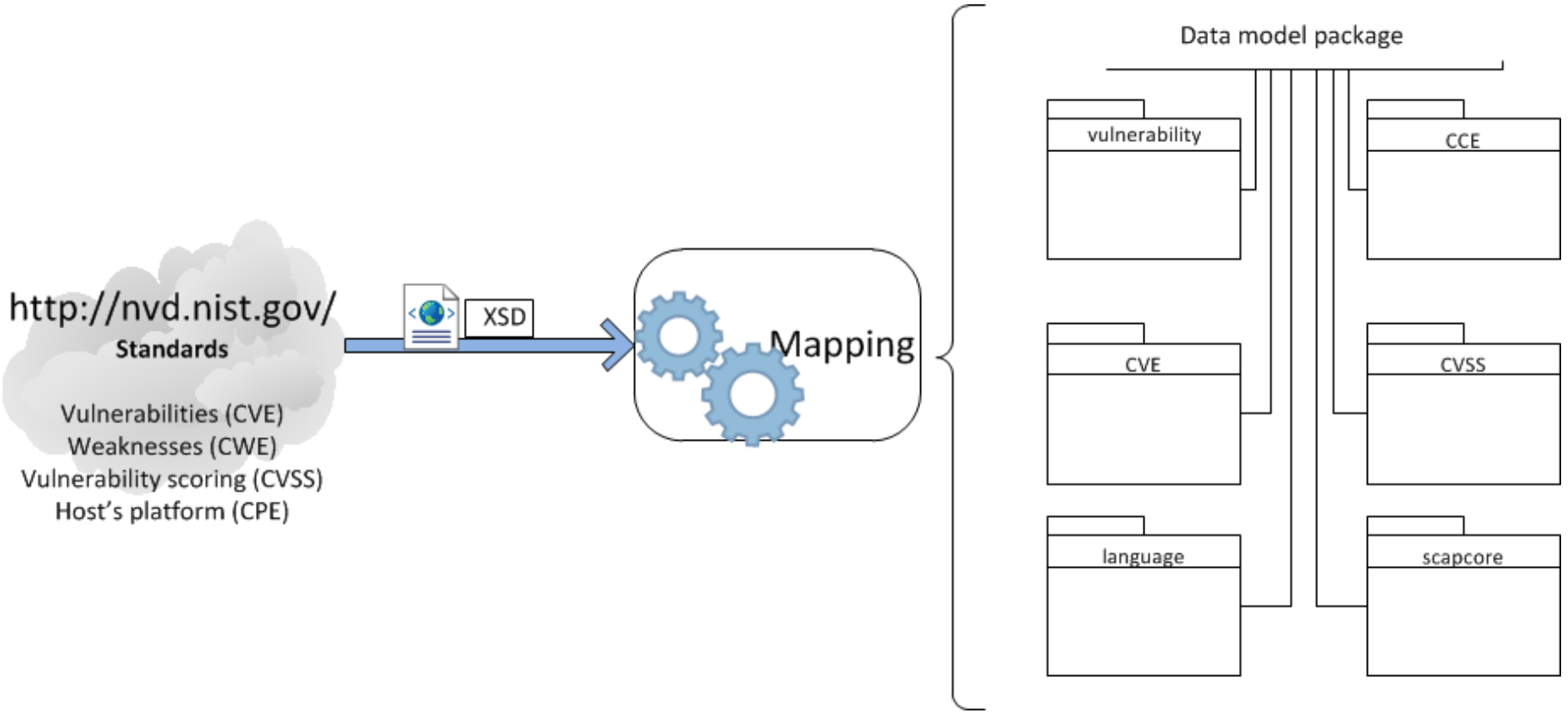
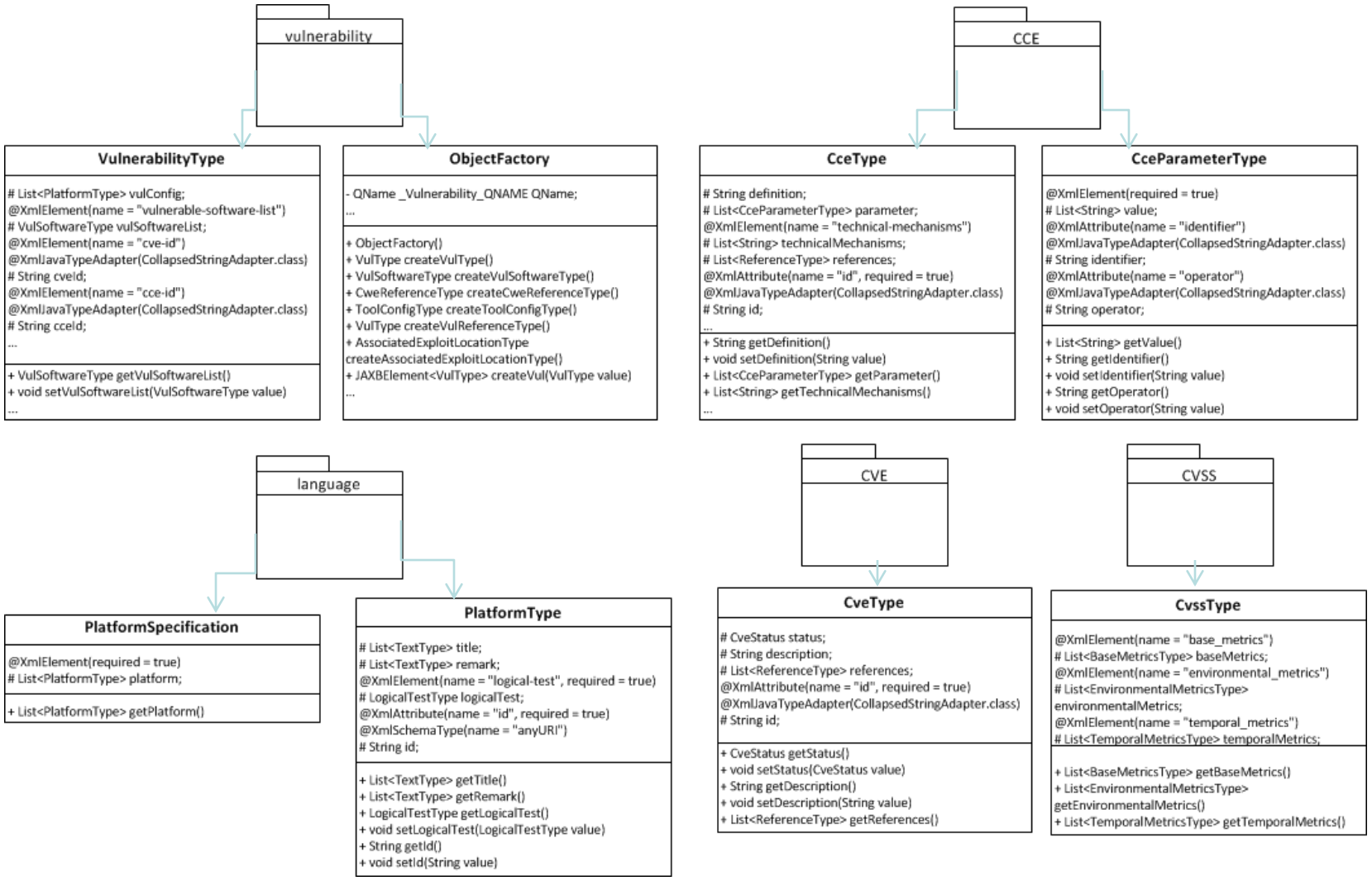


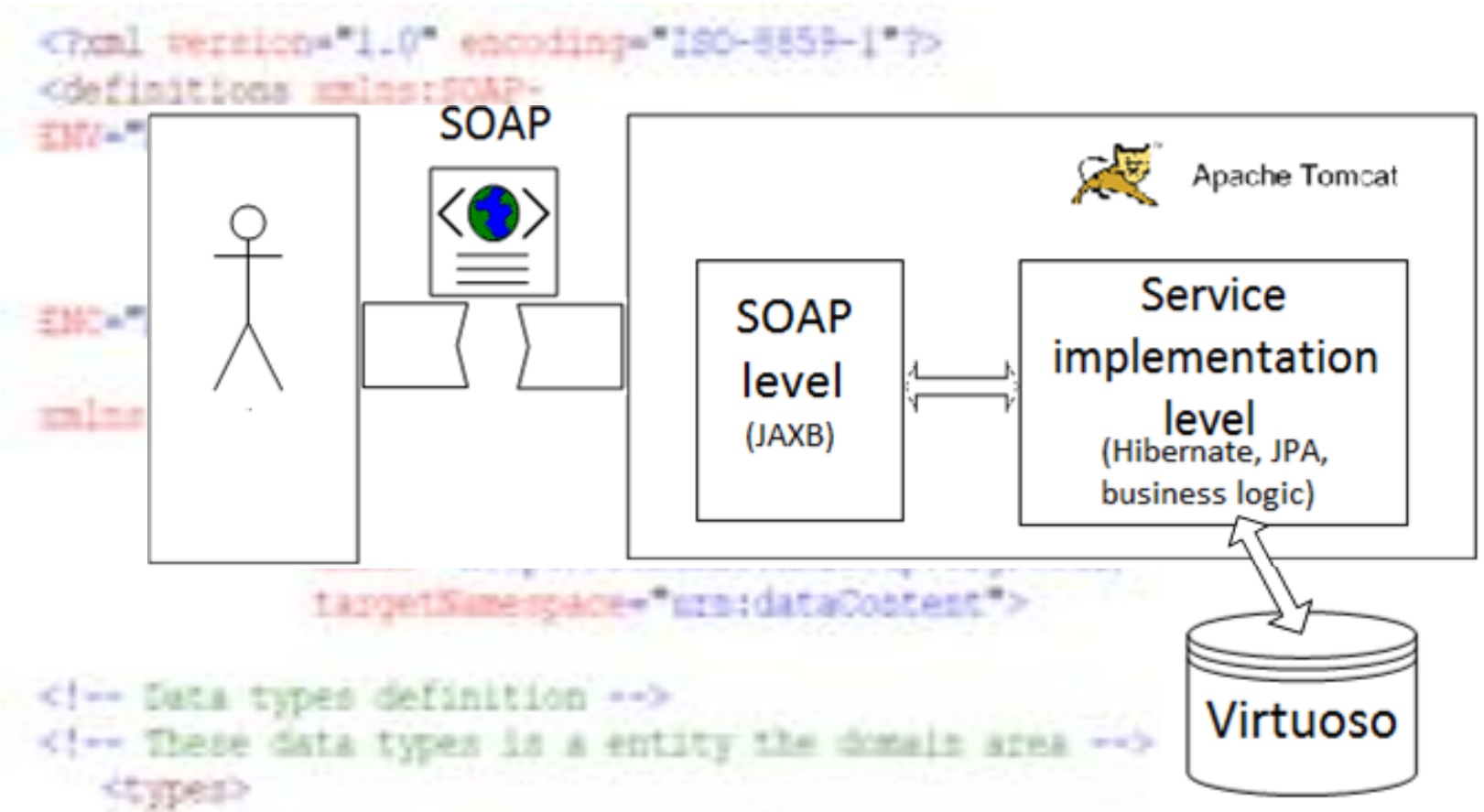
Диаграмма классов уровня модели данных



Архитектура репозитория

- **SOA архитектура**
- **Взаимодействие с модулями через SOAP**
- **Гибридное хранилище**

Аспекты технической реализации



Заключение

Полученные результаты:

- Онтологический подход для построения моделей данных в SIEM-системах
- Онтология для компонента моделирования атак
- Предложена архитектура репозитория с учетом онтологического подхода к представлению данных
- Реализация репозитория

Дальнейшие исследование

- Расширение представленной онтологической модели
- Продолжение работы по реализации репозитория
- Использование систем логического вывода
- Реализация механизмов верфикации политик безопасности

Контакты

Полубелова Ольга Витальевна

ovp@comsec.spb.ru

http://www.comsec.spb.ru/polubelova/

Саенко Игорь Борисович

ibsaenko@comsec.spb.ru

http://comsec.spb.ru/saenko/