Лекция «Состязательные модели в задачах информационной безопасности»

Инструкции для преподавателей.

**Слайд 1 (Программа модуля).**

В модуле рассматриваются систему управления знаниями в информационной безопасности: онтологии, таксономии, словари и другие виды баз знаний. В настоящее время уже разработаны сообществом базы данныхm, например MITRE, CVE, STIX и другие. Подход с использованием баз знаний хорошо зарекомендовал себя в поиске (пример Knowledge Graph). Для описания онтологий используются графы и специальные средства из описания и работы с ними.

<https://www.ontotext.com/knowledgehub/fundamentals/what-is-a-knowledge-graph/>

**Слайд 2 (Актуальность).**

В различных видах обеспечения безопасности (информационная безопасность, кибербезопасность, киберфизическая безопасность) существует множество актуальных на сегодняшний день задач: сетевой мониторинг, повышение осведомленности о киберобстановке, выявление аномалий, оценка уязвимости, противодействие атакам. Эффективное решение этих задач становится невозможным без специальных средств автоматизации, поскольку увеличивается количество и тип атак и ручного труда даже самых высококвалифицированных специалистов недостаточно для противодействия атакам. Один из способов повысить эффективность автоматизированных систем является использование накопленных экспертных знаний в машиночитаемом виде. Различные системы организации знаний являются хорошим инструментом для решения этой задачи. Для использования накопленных экспертных знаний в автоматизации необходимо формализованное представление знаний Формализованное представление знаний это область искусственного интеллекта, которая создает структурированную информацию на основе выявленной семантики (смысла) концепций, свойств, связей, отдельных объектов из какой-то предметной области (например, медицина, финансы, информационная безопасность, промышленное производство).

**Слайд 3 (Системы организации знаний)**

Для хранения знаний используются следующие структуры:

* Контролируемые словари: обеспечивают способ организации знаний для последующего поиска, используются в схемах предметной индексации, предметных рубриках, тезаурусах, таксономиях и других системах организации знаний
* Тезаурусы: объединяют термины в группы по определенному признаку, например, с учетом похожести (синонимы)
* Таксономии: категорированные слова, упорядоченные по иерархическому признаку
* Онтологии: формальное описание знаний из какого-то домена (предметной области) с учетом имеющихся сложных правил и связей между элементами, позволяющим сделать автоматическое извлечение знаний
* Датасеты: наборы машиночитаемых данных

Также существует множество других видов представления формальных знаний, более подробно см., например, здесь:

https://www.researchgate.net/publication/324993820\_Improving\_semantic\_interoperability\_in\_the\_obstetric\_and\_neonatal\_domain\_through\_an\_approach\_based\_on\_ontological\_realism

**Слайд 4 (Понятие онтологии)**

Онтология является самым популярным представлением знаний о предметной области (домена), позволяющем описать объекты этого домена, их свойства и связи между объектами. Онтология опирается на «гипотезу открытого мира», это означает, что если искомый объект не найден в онтологии, то он не обязательно не существует. В противоположность этому базы данных работают в соответствии с гипотезой «закрытого мира»: если запрос к базе данных не нашел объект, то система считает, что такого объекта нет. Например

**:Alice :knows :Bob .**

не означает, что только Алиса знает Боба. Поэтому базы данных хорошо подходят для хранения и поиска конкретной информации, а онтологии большое подходят для выявления новых знаний, например для создания экспертных систем.

Мощь онтологии заключается в том, что она основана на дескриптивной логике предикатов первого порядка, что позволяет выявлять различные логические заключения. В подобных системах всегда ищется баланс между наглядностью и сложностью извлечения фактов (ризонинг). Для эффективной работы ризонинга в онтологии необходимо максимально подробно определить свойства сущностей и связей между ними.

Онтологии бывают разного вида, например онтология верхнего уровня (общая отнология, применимая ко многим различным областям) или доменная (онтология для конкретной области знаний). Для области информационной безопасности доменные онтологии могут описывать семантику работы сети и устройств, уязвимости, информационные потоки и многое другое.

**Слайд 5 (Примеры использования онтологий)**

Системы организации знаний на основе онтологий уже очень распространены и используются во многих отраслях. Самый яркий пример это knowledge graph для поиска информации в Интернет, благодаря этой технологии качество поиска стало очень высоким. Другие примеры использования онтологий на практике:

* банки используют графы знаний для анализа транзакций (fraud detection)
* в консалтинге используются графы на основе юридических документов
* в здравоохранении используются накопленные сведения на основе данных о здоровье пациентов, Health Electronic Record (HER).
* в промышленной индустрии графы знаний используются для анализа цепочек поставщиков (supply-chain management), в целом для Индустрии 4.0 характерно взаимодействие киберфизических систем между собой, что приводит к автоматизации и необходимости управлять знаниями
* во многих отраслях базы знаний используются для организации работы чат-ботов, в том числе и для обработки сложных запросов на естественном языке (например, сервис asknow).
* онтологии могут применяться для широкого круга задач обработки естественного языка, например: аннотирование текстов с помощью онтологий, извлечение знаний, NER, Named Entity Linking, Relation Linking, автоматический вывод новых знаний, ризонинг.

В целом направление SemTech переживает в настоящее время бурное развитие. Но информации на русском языке по данной тематики по-прежнему очень мало.

При этом важно осознавать, что далеко не всегда онтологии оказываются действенным инструментом для решения задачи, необходимо подходить к выбору способа решения с учетом особенностей предметной области.

**Слайд 6 (Дескрипционная логика)**

Дескрипционная логика это язык представления знаний, позволяющий описывать понятия [предметной области](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BC%D0%B5%D1%82%D0%BD%D0%B0%D1%8F_%D0%BE%D0%B1%D0%BB%D0%B0%D1%81%D1%82%D1%8C) в однозначном формализованном виде. Обеспечивает наглядность описываемой информации (см. пример на слайде), при этом, благодаря близости к математической логике, сохраняется возможность вычислений для извлечения сведений с использованием логических конструкций. Благодаря этим свойствам дескрипционная логика активно применяется на практике, обеспечивая компромисс между выразительностью и разрешимостью.

Дескрипционные логики были выбраны в качестве логической основы для языка веб-онтологий OWL. Имеющиеся в дескрипционных логиках понятия «концепт», «роль», «индивид» и «база знаний» в OWL соответствуют понятиям «класс», «свойство», «объект» и «онтология» соответственно.

**Слайд 7 (Средства описания онтологий)**

Основные инструменты для хранения онтологий (графов знаний)

* RDF (Resource Description Framework)
* OWL (Ontology Web Language)

RDF часто хранятся в xml в виде троек (субъект, предикат, объект)

* Форматы: RDF/XML, Turtle, N-Triples, JSON-LD, RDFa, HTML5 Microdata
* Примеры RDF хранилищ – Virtuoso, 4store (4store.org), stardog.

RDFS (RDF Schema): для описания словарей, таксономий, тезаурусов, простых онтологий

OWL позволяет дополнительно описывать логические правила над данными (ограничения), используется для сложных онтологий.

Язык веб-онтологий [OWL](https://ru.wikipedia.org/wiki/Web_Ontology_Language) разрабатывается как язык, на котором можно формулировать и публиковать в веб так называемые [сетевые онтологии](https://ru.wikipedia.org/wiki/%D0%9E%D0%BD%D1%82%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)) — формально записанные утверждения о понятиях и объектах некоторой предметной области. Одним из требований к таким онтологиям заключается в том, чтобы содержащиеся в них знания были «доступны» для машинной обработки, в частности, для автоматизированного логического вывода новых знаний из уже имеющихся. Для этого требуется, чтобы язык, на котором формулируются онтологии, имел точную семантику, а соответствующие логические проблемы были разрешимы (и имели практически допустимую вычислительную сложность). Кроме того, желательно, чтобы такой язык имел довольно большую выразительную силу, пригодную для формулировки на нём практически значимых фактов.

Последний является языком, имеющим [XML](https://ru.wikipedia.org/wiki/XML)-формат, поэтому можно сказать, что OWL является переформулировкой некоторых ДЛ с использованием синтаксиса XML. Поскольку существует много ДЛ, различающихся как по выразительной силе, так и по вычислительной сложности, это привело к тому, что в языке OWL имеется несколько вариантов.

**Слайд 8 (RDF)**

Триплет RDF состоит из объекта и субъекта (вершины графа), связанных предикатом.

**Слайд 9 (Примеры баз знаний)**

DBPedia (<https://www.dbpedia.org/>), с 2007 года, более 6 миллиардов фактов, получена парсингом информации в текстовом виде в Wikipedia (разные языки). <https://www.wikipedia.org/> один из первых успешных применений семантических технологий.

Yago (<https://yago-knowledge.org/>), обработка WikiPedia и семантического тезауруса (словаря) WordNet (wordnet.princeton.edu), более 120 миллионов фактов

NELL, Never Ending Language Learner (<http://rtw.ml.cmu.edu/rtw/>), читает web страницы и выделяет в граф знаний, более 14,4 миллиардов фактов

WikiData (<https://www.wikidata.org/wiki/Wikidata:Main_Page>), поставщик данных для WikiPedia, 7 миллиардов знаний о 90 миллионов сущностей, сюда загружают данные крупные компании, например Facebook и Google.

Google Knowledge Graph (https://developers.google.com/knowledge-graph), развитие графа Freebase, который изначально был большой онтологической базой, собранной Интернет сообществом.

Кроме того: открытые графы знаний, специализированные графы знаний, например, для медицины: BioPortal – репозиторий биомед-графов (более 140 миллионов фактов), PubMed – аннотации медицинский статей

В настоящее время созданно и поддерживается сообществами или коммерческими компаниями огромное множество баз знаний, они связанны между собой, актуальную картину можно увидеть на <https://lod-cloud.net/>

**Слайд (Хранение информации в графах)**

Существуют различные виды графовых баз знаний.

Одним из популярных инструментов создания запросов к базам знаний является SPARQL.

**Слайд (Редактор Protege)**

Программа Protege для создания, редактирования и использования онтологий разработана в Стэнфордском университете, распространяется бесплатно, ее можно скачать себе на компьютер по ссылке <https://protege.stanford.edu/products.php>, либо воспользоваться web-версией <https://webprotege.stanford.edu/> На официальной странице можно скачать архив для использования на локальном компьютере.

Сейчас это популярный open-source продукт для создания онтологий в любых областях

**Слайд (Онтологии кибербезопасности)**

Описательные онтологии для кибербезопасности структурируют информацию из предметной области и объединяют сведения из различных связанных предметных областей с точки зрения кибербезопасности.

К таким глобальным широко используемым стандартам относятся

* ISO/IEC, https://www.iso.org
* OASIS, https://www.oasis-open.org
* NIST, https://www.nist.gov
* ITU-T, https://www.itu.int
* MITRE, https://www.mitre.org
* the Open Grid Forum, https://www.ogf.org
* IEEE, <https://www.ieee.org>

Использование информации из существующих баз знаний

* об угрозах (Common Vulnerabilities Enumeration, CVE, https://cve.mitre.org/), National Vulnerability Database, https://nvd.nist.gov
* об уязвимостях (Common Weakness Enumeration, CWE, https://cwe.mitre.org/)
* о паттернах атак (Common Attack Pattern Enumeration and Classification, CAPEC, [https://capec.mitre.org](https://capec.mitre.org/))

позволяет получать более полную информацию и происходящем инциденте и предпринимать наиболее правильные и эффективные действия.

**Слайд (матрица MITRE)**

Матрица MITRE ATT&CK описывает тактики и техники, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру.

Матрица MITRE D3Fend описывает методы защиты от атак.

**Слайд (матрица MITRE на русском языке)**

Компания Positive Technologies выяснила, 37% специалистов по ИБ (https://www.ptsecurity.com/ru-ru/research/analytics/kak-rossijskie-kompanii-zashchishchayutsya-ot-celevyh-atak/) планируют начать использовать матрицу ATT&CK для мониторинга и расследования атак. Эксперты компании перевели её на русский язык и опубликовали

https://mitre.ptsecurity.com/ru-RU/techniques?utm\_source=telegram&utm\_medium=seclab

в интерактивном формате. В адаптированной версии видно, какие угрозы из международной базы знаний можно выявить с помощью системы анализа трафика PT Network Attack Discovery и как она это делает.

**Слайд (CVE)**

<https://cve.mitre.org/>

База знаний об угрозах.

**Слайд (CWE)**

<https://cwe.mitre.org/>

База знаний об уязвимостях.

**Слайд (CAPEC)**

<https://capec.mitre.org/>

База знаний о паттернах атак.

**Слайд (Графы знаний в машинном обучении)**

* Графы являются полуструктурированными
* Восстановление ребер по паттернам
* Эмбеддинги на графах
* Определение семантической близости
* Факт чекинг