

**Примеры запросов DL для семантической модели CAPEC&CWE**  
**Examples of the DL queries for the CAPEC&CWE semantic model**  
<https://github.com/nets4geeks>

1	2	3	4
#	Вопрос	Question	DL examples
	<u>Об атаках:</u>	<u>Attacks:</u>	
1	Какие типы атак позволяют достичь данного технического эффекта (например, “нарушение логики выполнения”)?	Which attack patterns might impact a particular impact, i.e. “Alter execution logic”?	CAPEC and impactsTechnicalImpact value Alter_execution_logic
2	Какие типы атак используют определенный метод атаки (например, “Brute Force”)?	Which attack patterns might use a particular attack method (i.e. “Brute Force”)?	CAPEC and usesMethod value Brute_Force
3	Какие типы атак могут использовать данный дефект программного обеспечения (например, CWE 120)?	Which attack patterns might use a particular software weakness (i.e. CWE 120)?	CAPEC and targetsCWE value iCWE_120
4	Какие типы атак нацелены на данное свойство информационной безопасности, например, доступность?	Which attack patterns might target a particular scope (security property), i.e. availability?	CAPEC and scopes value Availability
5	Какие типы атак, нацеленные на данное свойство информационной безопасности (доступность), имеют заданную вероятность осуществления (>5)?	Which attacks patterns, that target a particular scope (i.e. availability), might have a particular likelihood (i.e. >5)?	CAPEC and scopes value Availability and (scoresLikelihood some xsd:integer[> 5])
6	Какие типы атак, нацеленные на данное свойство информационной безопасности (доступность), имеют заданную “тяжесть”?	Which attacks patterns, that target a particular scope (i.e. availability), might have a particular severity (i.e. >5)?	CAPEC and scopes value Availability and (scoresSeverity some xsd:integer[> 5])
7	Какие типы атак, нацеленные на данное свойство информационной безопасности (доступность), требуют заданного уровня подготовки злоумышленника?	Which attacks patterns, that target a particular scope (availability), might require a particular skill level of adversary (i.e. >5)?	CAPEC and scopes value Availability and (scoresRequiredSkill some xsd:integer[> 5])
	<u>О дефектах:</u>	<u>Weaknesses:</u>	
8	Какие дефекты программного обеспечения позволяют достичь данного технического эффекта (например, “нарушение логики	Which weaknesses might impact a particular impact, i.e. “Alter execution logic”?	CWE and impactsTechnicalImpact value Alter_execution_logic

	выполнения»)?		
9	Какие дефекты программного обеспечения используются данным типом атаки (например, CAPEC 100)?	Which weaknesses might be used by a particular attack pattern (i.e. CAPEC 100)?	CWE and isTargetedBy value iCAPEC_100
10	Какие дефекты программного обеспечения нацелены на данное свойство информационной безопасности, например, доступность?	Which weaknesses might target a particular scope (security property), i.e. availability?	CWE and scopes value Availability
11	Какие дефекты программного обеспечения, нацеленные на данное свойство информационной безопасности (доступность), имеют заданную вероятность создания эксплоита (>5)?	Which weaknesses that target a particular scope (i.e. availability), might have a particular exploit likelihood (i.e. >5)?	CWE and scopes value Availability and (scoresExploitLikelihood some xsd:integer[> 5])
12	Какие дефекты программного обеспечения, нацеленные на данное свойство информационной безопасности (доступность), возникают на данном этапе жизненного цикла («Архитектура и проектирование»)?	Which weaknesses that target a particular scope (i.e. availability), might be appeared on a particular stage of life cycle (Architecture and Design)?	CWE and scopes value Availability and appearedAtPhase value Architecture_and_Design
13	Какие дефекты программного обеспечения, нацеленные на данное свойство информационной безопасности (доступность), могут быть обнаружены данным методом («Black box»)?	Which weaknesses that target a particular scope (i.e. availability), might be detected by a particular method (Black box)?	CWE and scopes value Availability and isDetectedBy value Black_Box
14	Какие дефекты программного обеспечения, нацеленные на данное свойство информационной безопасности (доступность), могут быть смягчены данным методом («Firewall»)?	Which weaknesses that target a particular scope (i.e. availability), might be mitigated by a particular method (Firewal)?	CWE and scopes value Availability and isMitigatedBy value Firewall