

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1570

(09/2011)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Обмен информацией, касающейся
кибербезопасности – Идентификация и обнаружение

Механизмы обнаружения, используемые при обмене информацией о кибербезопасности

Рекомендация МСЭ-Т X.1570

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

**Механизмы обнаружения, используемые при обмене
информацией о кибербезопасности**

Резюме

В Рекомендации МСЭ-Т X.1570 приводятся система обнаружения информации о кибербезопасности, а также механизм, обеспечивающий возможность такого обнаружения. Обнаружение может рассматриваться как этап жизненного цикла информации о кибербезопасности, смежный с этапами опубликования и получения информации, которые важны и необходимы для обнаружения. Таким образом, в рамках этой системы рассматриваются вопросы опубликования информации о кибербезопасности, приобретения возможного списка и получения необходимой информации. Схема обнаружения может быть реализована за счет произвольно выбираемых механизмов при условии, что она согласуется со структурой. В число этих механизмов входит обнаружение на основе идентификатора объекта (OID) и обнаружение на основе структуры описания ресурсов (RDF), которые также представлены в данной Рекомендации.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1570	02.09.2011 г.	17-я

Ключевые слова

Информация о кибербезопасности, обнаружение информации, обнаружение источника.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: <http://www.itu.int/ITU-T/ipr/>.

© ITU 2012

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1 Сфера применения	1
2 Справочные документы	1
3 Определения	1
3.1 Термины, определенные в других документах	1
3.2 Термины, определенные в настоящей Рекомендации	1
4 Сокращения и акронимы	2
5 Условные обозначения	2
6 Механизм идентификации и определения местонахождения источника информации о кибербезопасности	3
7 Типы и уровень детализации обнаруженной информации о кибербезопасности	3
8 Идентификатор информации о кибербезопасности	4
9 Типы механизмов обнаружения	5
9.1 Механизмы обнаружения на основе OID в обмене информацией о кибербезопасности	5
9.2 Механизмы обнаружения на основе RDF в обмене информацией о кибербезопасности	6
10 Методы доступа к обнаруженной информации	7
Дополнение I – Онтология оперативной информации о кибербезопасности	8
I.1 Домены операций кибербезопасности	8
I.2 Роли	8
I.3 Информация о кибербезопасности	9
Дополнение II – Спецификации, описывающие базы данных и базы знаний	12
Дополнение III – Наглядная реализация обнаружения на основе RDF	13
III.1 Пример реализации обнаружения на основе RDF	13
III.2 Иерархия классов информации о кибербезопасности	13
Библиография	15

Введение

В настоящее время обмену информацией о кибербезопасности придается все большее значение. Особое внимание привлекает международный стандарт, касающийся обмена информацией о кибербезопасности, под названием CYBEX. Обнаружение на основе стандарта CYBEX, обеспечивающее схему поиска источника информации о кибербезопасности, относится к числу различных технических спецификаций CYBEX. В настоящей Рекомендации поясняются его структура и методы.

Механизмы обнаружения, используемые при обмене информацией о кибербезопасности

1 Сфера применения

В данной Рекомендации приводятся система обнаружения информации о кибербезопасности, а также механизм, обеспечивающий возможность такого обнаружения. Обнаружение может рассматриваться как этап жизненного цикла информации о кибербезопасности, смежный с этапами опубликования и получения информации, которые важны и необходимы для обнаружения. Таким образом, в рамках этой системы рассматриваются вопросы опубликования информации о кибербезопасности, приобретения возможного списка и получения необходимой информации. Схема обнаружения может быть реализована за счет произвольно выбираемых механизмов при условии, что она согласуется со структурой. В число этих механизмов входит обнаружение на основе идентификатора объекта (OID) и обнаружение на основе системы описания ресурсов (RDF), которые также представлены в данной Рекомендации.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.660] Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*.

[W3C RDF] W3C Recommendation (2004), *Resource Description Framework (RDF): Concepts and Abstract Syntax*.
<<http://www.w3.org/TR/rdf-concepts/>>

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 идентификатор объекта (object identifier) [ITU-T X.660]: Упорядоченная последовательность первичных целых значений от корня дерева международных идентификаторов объектов к тому или иному узлу, однозначно идентифицирующая данный узел.

3.1.2 онтология (ontology) [b-Gruber]: Эксплицитная спецификация концептуализации.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 информация о кибербезопасности (cybersecurity information): Структурированная информация или знания относительно:

- 1 "состояния" оборудования, программного обеспечения или сетевых систем с точки зрения кибербезопасности, особенно уязвимостей;
- 2 экспертно-технического анализа инцидентов или событий;
- 3 эвристике и сигнатур, полученных на основе имевших место событий;

- 4 сторон, внедряющих средства обмена информацией о кибербезопасности в пределах этой структуры;
- 5 спецификаций обмена информацией о кибербезопасности, в том числе модулей, схем, правил и присвоенных номеров;
- 6 атрибутов идентичности и доверия в отношении всего вышеупомянутого;
- 7 требований, руководящих указаний и практики в отношении реализации.

ПРИМЕЧАНИЕ. – Настоящее определение основано на описании информации о кибербезопасности в [b-ITU-T X.1500].

3.2.2 обмен (информацией о кибербезопасности) (exchange (cybersecurity information)): Передача информации о кибербезопасности между двумя или несколькими объектами кибербезопасности. Такая передача может осуществляться в одном, двух или нескольких направлениях, т. е. многих со многими.

3.2.3 обнаружение (discovery): Действие или процесс обнаружения цели, т. е. получение знаний о цели впервые.

3.2.4 устройство поиска (retriever): Объект, осуществляющий поиск информации о кибербезопасности.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

CCE	Common Configuration Enumeration	Перечень общеизвестных конфигураций
CERT	Computer Emergency Response Teams	Группы реагирования на нарушения компьютерной защиты
CIRT	Computer Incident Response Team	Группа реагирования на компьютерные инциденты
CPE	Common Platform Enumeration	Перечень общеизвестных платформ
CVE	Common Vulnerabilities and Exposures	Общеизвестные уязвимости и незащищенность
CVSS	Common Vulnerability Scoring System	Система оценки общеизвестных уязвимостей
CWE	Common Weakness Enumeration	Перечень общеизвестных слабых мест
CWSS	Common Weakness Scoring System	Система оценки общеизвестных слабых мест
CYBEX	CYBersecurity information EXchange	Обмен информацией о кибербезопасности
HTTP	Hypertext Transfer Protocol	Протокол передачи гипертекста
IODEF	Incident Object Description Exchange Format	Формат обмена описаниями инцидентов как объектов
MAEC	Malware Attribute Enumeration and Characterization	Перечень и характеристики атрибутов вредоносного программного обеспечения
OID	Object Identifier	Идентификатор объекта
OVAL	Open Vulnerability and Assessment Language	Открытый язык описания уязвимости и оценки
RDF	Resource Description Framework	Структура описания ресурса
SCAP	Security Content Automation Protocol	Протокол автоматизации управления данными безопасности
SNMP	Simple Network Management Protocol	Простой протокол управления сетью
XCCDF	eXtensible Configuration Checklist Description Format	Расширяемый формат описания списка проверки конфигурации

5 Условные обозначения

Отсутствуют.

6 Механизм идентификации и определения местонахождения источника информации о кибербезопасности

Различные организации кибербезопасности реализуют общие протоколы кибербезопасности в целях получения информации о состоянии системы, уязвимости, экспертно-техническом анализе инцидента и эвристике инцидента в действующих приложениях, а также в целях обмена этой информацией. В связи с тем что такая информация становится доступной из разных источников, осуществляющим реализацию лицам следует согласовать вопрос о том, каким образом они будут идентифицировать организации кибербезопасности, принципы политики в отношении доверия и обмена информацией, а также саму информацию, которая подлежит обмену или распространению. Для этого в настоящем пункте вводится механизм идентификации и определения местонахождения источника информации о кибербезопасности – механизм обнаружения информации о кибербезопасности.

В поиске информации о кибербезопасности участвуют три объекта: устройство поиска, источник и каталог. Устройство поиска осуществляет поиск информации путем направления запросов, источник предоставляет запрошенную информацию, а каталог регистрирует метаданные информации источника и помогает устройству поиска в поиске соответствующего источника.

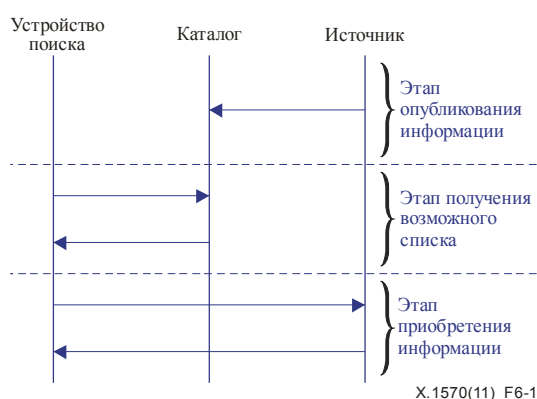
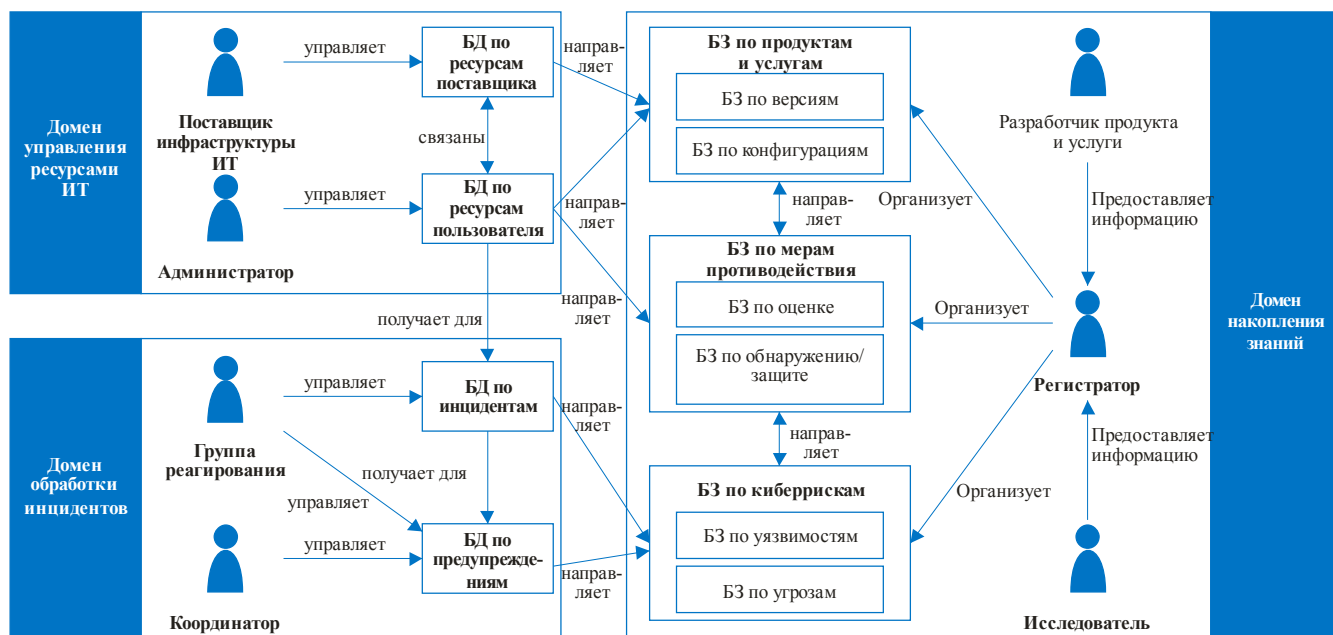


Рисунок 6-1 – Три этапа обнаружения

Процесс обнаружения – это процесс взаимодействия между тремя объектами, как показано на рисунке 6-1. Он состоит из трех этапов – опубликование информации, получение возможного списка и приобретение информации. Источник публикует свою информацию для киберсообщества, регистрируя ее в каталоге на этапе опубликования информации. На этапе получения возможного списка устройство поиска запрашивает в каталоге регистратора список возможных источников. Затем на этапе выбора источника оно выбирает из списка источник, который представляется наиболее подходящим, и получает информацию источника.

7 Типы и уровень детализации обнаруженной информации о кибербезопасности

Механизмы обнаружения способны обнаруживать информацию о кибербезопасности. Эти механизмы предназначены для обнаружения семи следующих типов информации: базы данных о ресурсах пользователей, базы данных о ресурсах операторов, базы данных об инцидентах, базы данных о предупреждениях, базы знаний о продуктах и услугах, базы знаний о киберрисках и базы знаний о мерах противодействия. На рисунке 7-1 представлена модель онтологии, используемая в настоящей Рекомендации, и показаны взаимосвязи между типами информации, используемыми в данной модели.



X.1570(11)_F7-1

БД: база данных БЗ: база знаний

Рисунок 7-1 – Онтология оперативной информации о кибербезопасности

Данная онтология представляет собой модель для описания получения, накопления и использования знаний об информации о кибербезопасности, состоящую из набора доменов операций, ролей и типов информации. Роли, обозначаемые на рисунке пиктограммами с изображением человека, являются типовыми, а объекты, такие как CIRT, могут выполнять одну или несколько из этих функций. Эта модель используется для определения доменов операций кибербезопасности и далее применяется для идентификации требуемых объектов кибербезопасности, поддерживающих операции в каждом домене. Подробное описание онтологии содержится в Дополнении I.

В таблице II.1 представлены спецификации по кибербезопасности, которые согласуются с семью типами информации, описанными в данной модели онтологии. Уровень детализации обнаруженной информации о кибербезопасности будет соответствовать уровню детализации стандартов. При использовании этого подхода уровень детализации гибкий, и поэтому для конкретных целей могут создаваться разные стандарты.

8 Идентификатор информации о кибербезопасности

Для идентификации информации о кибербезопасности требуется уникальный идентификатор. Любой глобально уникальный идентификатор, используемый для обмена информацией о кибербезопасности, должен обладать следующими характеристиками:

- простота, практичность, гибкость, расширяемость, масштабируемость и возможность развертывания;
- распределенное управление различными схемами идентификаторов;
- долговременная надежность центров регистрации идентификаторов, а также наличие высококачественных инструментальных средств обнаружения информации, относящейся к любому конкретному идентификатору.

Этим требованиям удовлетворяют два возможных уникальных идентификатора: идентификатор объекта (OID) и структура описания ресурса (RDF). Они представляют собой две основные парадигмы для общего обслуживания и обнаружения информации, рассматриваемые в пункте 9.

9 Типы механизмов обнаружения

Механизмы обнаружения могут внедряться с произвольно выбираемыми механизмами при условии, что они соответствуют данной структуре. Они подразделяются на два типа – централизованные и децентрализованные – в зависимости от того, как они регистрируют информацию о кибербезопасности и управляют ею.

В случае централизованных механизмов каталоги управляют одним или несколькими "центральными" регистрами, которые позволяют легко установить местонахождение целевой информации и быстро обнаружить ее (в некоторых случаях этап получения возможного списка может быть опущен). Однако сторона, осуществляющая поиск, должна сначала узнать о существовании данного регистра, прежде чем она сможет использовать его. Различия в ресурсах и затратах, связанных с ведением центрального репозитория, могут оказаться слишком большими, чтобы это могли позволить себе те, кто обладает ограниченными ресурсами. Обнаружение на основе OID является в данном случае одним из типичных механизмов.

В случае децентрализованных механизмов каталоги управляют несколькими "распределенными" регистрами. Это требует минимальных ресурсов и затрат, связанных с обеспечением доступности информации, а тем, кто предоставляет и ищет информацию, нет необходимости заранее знать о существовании друг друга. Между тем, чтобы найти информацию, не имея о ней никаких знаний, тому, кто ее ищет, требуется в буквальном смысле "перерывать" весь интернет. Обнаружение на основе RDF является в данном случае одним из типичных механизмов.

9.1 Механизмы обнаружения на основе OID в обмене информацией о кибербезопасности

Механизмы обнаружения на основе OID идентифицируют источники информации о кибербезопасности и определяют их местонахождение, используя OID, в иерархической древовидной структуре, листья которой идентифицируют объекты. OID обеспечивают иерархическое наименование, то есть конкатенацию значений дуг от корня дерева до одного из его листьев. До зарегистрированной информации о кибербезопасности можно добраться посредством перемещения по дереву от корня до одного из его листьев. Следует отметить, что информация о кибербезопасности регистрируется ниже дуги идентификатора объекта обмена информацией о кибербезопасности {joint-iso-itu-t(2) cybersecurity(48)} [b-ITU-T X.1500.1].

Этапы обнаружения, представленные в пункте 6, подробно рассматриваются в пунктах 9.1.1–9.1.3.

9.1.1 Этап опубликования информации

Регистрируя информацию, источник предоставляет много видов информации о метаданных, среди которых основными категориями являются: страна/регион, ID организации, тип информации и формат описания информации. Страна/регион указывает на страну соответствующей организации или регион организации, если источником является межнациональная организация, такая как МСЭ. ID организации указывает, о какой организации идет речь, и может быть описан, например, путем использования биржевого номера или уникального наименования корпорации. Тип информации указывает вид информации, описание которой приводится в пункте 7. Формат описания информации указывает соответствующий формат, например совместимый с CVE [b-ITU-T X.1520] или с ARF [b-ARF].

По получении запроса о регистрации от источника каталог регистрирует и хранит информацию, основанную на метаданных, и строит поддеревья OID. Хотя в настоящей Рекомендации не уточняется нормативная структура для дерева, описание некоторых возможных вариантов приводится в Дополнениях I и II.

9.1.2 Этап получения возможного списка

Устройство поиска не обязательно направляет запрос каталогу, который имеет единый согласованный регистр дерева OID. Оно может заблаговременно знать структуру дерева и, следуя этой структуре, определить необходимую информацию без направления запроса.

Каталог может принять произвольный запрос (включая запрос о поиске текста) и ответить возможным списком.

9.1.3 Этап приобретения информации

На основе возможного списка или посредством перемещения по дереву OID от корня до одного из листьев устройство поиска выбирает один источник и затем направляет запрос соответствующему источнику, который в ответ предоставляет информацию о кибербезопасности.

При обнаружении на основе OID этапы получения возможного списка и приобретения информации могут квалифицироваться как неразрывные, поскольку сужение возможного списка путем перемещения по дереву приводит к выбору одного источника.

9.2 Механизмы обнаружения на основе RDF в обмене информацией о кибербезопасности

Механизм обнаружения на основе RDF идентифицирует источники информации о кибербезопасности и определяет их местонахождение на основе RDF. На рисунке 9-1 показан принцип действия этого механизма. Источник может зарегистрироваться в одном или нескольких каталогах (содержащих регистры), что облегчает задачу устройств поиска, с тем чтобы они могли получать информацию. В процессе обнаружения между объектами производится обмен информацией об идентификациях и возможностях объектов кибербезопасности. Объекты кибербезопасности направляют запросы об обнаружении каталогам, каждый из которых имеет разные источники, которые образуют соответствующий диапазон поиска для поисковой системы.

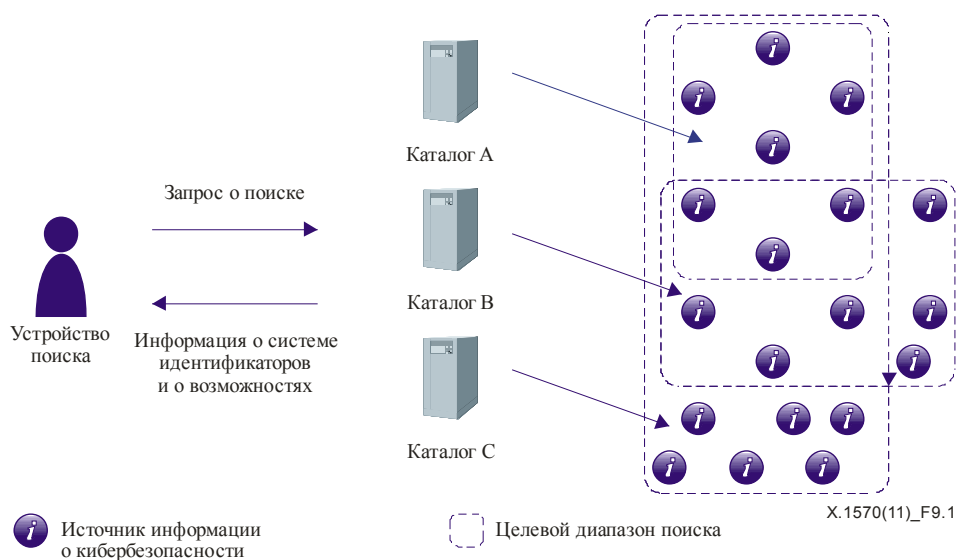


Рисунок 9-1 – Принцип обнаружения на основе RDF

В отличие от обнаружения на основе OID, обнаружение на основе RDF имеет каталоги, состоящие из многих объектов, см. рисунок 9-2. С функциональной точки зрения каталог состоит из агента обнаружения и агента регистра. Агент обнаружения связывается с устройством поиска (интерфейс для получателя), а агент регистра – с источником (интерфейс для источника). Агент обнаружения и агент регистра в некоторых случаях могут находиться внутри одного и того же компьютера. Обмен информацией о возможностях и об идентификаторе производится между этими четырьмя объектами.

Этапы обнаружения, представленные в пункте 6, подробно рассматриваются в пунктах 9.2.1–9.2.3.

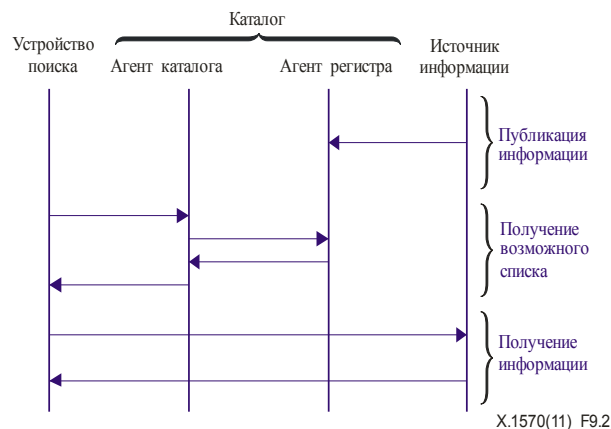


Рисунок 9-2 – Диаграмма последовательности обнаружения на основе RDF

9.2.1 Этап опубликования информации

Источник регистрирует свою информацию в агенте регистра, который генерирует и обеспечивает подходящие метаданные для данных на этапе опубликования информации. Как и в случае обнаружения на основе OID, при регистрации информации о кибербезопасности источник предоставляет много видов информации о метаданных, среди которых основными категориями являются страна/регион, ID организации, тип информации и формат описания информации. Страна/регион указывает на страну соответствующей организации или регион организации, если источником является межнациональная организация, такая как МСЭ. ID организации указывает, о какой организации идет речь, и может быть описан, например, путем использования биржевого номера или уникального наименования корпорации. Тип информации указывает вид информации, описание которой приводится в пункте 7. Формат описания информации указывает соответствующий формат, например совместимый с CVE или с ARF.

По получении запроса о регистрации от источника каталог регистрирует и хранит информацию, основанную на метаданных, и обновляет базу данных RDF. Поскольку агенты регистра зачастую используют иерархически распределенные регистры, агенту регистра необходимо определить, в каком регистре следует хранить данные.

Хотя в настоящей Рекомендации не уточняется нормативная структура для формата метаданных RDF, описание некоторых возможных вариантов приводится в Дополнениях I и II.

9.2.2 Этап получения возможного списка

Устройство поиска направляет запросы агенту обнаружения, который перенаправляет их одному или нескольким подходящим агентам регистра, которые осуществляют поиск своих баз данных, содержащих метаданные, и отвечают списком возможных источников на этапе получения возможного списка. Агент обнаружения агрегирует информацию, полученную от многих агентов регистра, и направляет ее устройству поиска.

9.2.3 Этап приобретения информации

Устройство поиска выбирает наиболее подходящий источник из полученного списка на этапе приобретения информации.

10 Методы доступа к обнаруженной информации

Для обмена информацией о кибербезопасности могут использоваться различные протоколы связи, в том числе HTTP (который использует RDF) и SNMP (который использует OID).

Некоторые стороны могут ограничить число сторон, которые могут иметь доступ к обнаруженной информации, путем установления правил управления доступом. Основные критерии этих правил включают IP-адрес, домен, протокол связи, ID и пароль, а также идентификационный сертификат.

Любая сторона, ищущая информацию о кибербезопасности, обменивается различными сообщениями, в том числе сообщениями запроса. Эти методы будут определены в Рекомендациях семейства МСЭ-Т X.1500.

Дополнение I

Онтология оперативной информации о кибербезопасности

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В пункте 7 настоящей Рекомендации используется онтология оперативной информации о кибербезопасности, показанная на рисунке 7-1. В данном дополнении дается подробное описание онтологии.

Она состоит из доменов операций кибербезопасности, ролей, необходимых для осуществления операций в доменах, и информации о кибербезопасности, связанной с ролями. Они подробно рассматриваются ниже.

I.1 Домены операций кибербезопасности

Термин "операция кибербезопасности" охватывает ряд операций безопасности в киберобществе, однако настоящая онтология касается в основном операций кибербезопасности, обеспечивающих информационную безопасность в киберобществах. Информационная безопасность представляет собой обеспечение конфиденциальности, целостности и доступности информации, а иногда она охватывает также контролируемость, подлинность и надежность информации.

Для описания домена таких операций онтологией предусматриваются три домена операций кибербезопасности: управления ресурсами ИТ, обработки инцидентов и накопления знаний.

Управление ресурсами ИТ: Этот домен выполняет операции кибербезопасности в организациях-пользователях, такие как установка и настройка ресурсов ИТ, а также управление ими, и охватывает как операции по предотвращению инцидентов, так и операции по контролю ущерба. Ресурсы ИТ включают не только собственные ресурсы ИТ-пользователя, но и сетевые соединения, облачные услуги и услуги определения идентичности, предоставляемые пользователю внешними объектами.

Обработка инцидентов: Этот домен обнаруживает инциденты, происходящие в киберобществах, путем мониторинга компьютерных событий, инцидентов, состоящих из нескольких компьютерных событий, и режимов атак, ставших причиной инцидентов, и обеспечивает реагирование на них. Точнее говоря, он осуществляет мониторинг компьютерных событий и при обнаружении аномалии формирует отчет по инциденту. На основе отчета он детально расследует инцидент, с тем чтобы выяснить схему атаки и меры противодействия. На основе анализа инцидента он может выдавать оповещения и инструкции, например, ранние предупреждения о возможных угрозах, организациям-пользователям.

Накопление знаний: Этот домен собирает и формирует информацию о кибербезопасности и извлекает повторно используемые знания для других организаций. В целях облегчения повторного использования он обеспечивает единые наименования и таксономию, с помощью которых упорядочивает и накапливает знания. Этот домен служит основой глобального взаимодействия за пределами границ организации.

I.2 Роли

С учетом определенных выше доменов операций кибербезопасности в данном разделе определяются роли, необходимые для выполнения операций кибербезопасности в каждом домене. В домене управления ресурсами ИТ имеются администратор и поставщик инфраструктуры ИТ, в домене обработки инцидентов – группа реагирования и координатор, а в домене накопления знаний – исследователь, разработчик продукта и услуги и регистратор их операций соответственно. Следует отметить, что роли определены с точки зрения функций, поэтому в зависимости от обстоятельств один объект может брать на себя несколько ролей.

Администратор: Эта роль предполагает административное управление системой своей организации и поддержание ее работоспособности. С этой целью при исполнении данной роли осуществляется мониторинг использования системы, проводится диагноз системы посредством проверок целостности, сканирования уязвимостей и тестирования на проникновение, а затем оценивается уровень безопасности системы. Типичным экземпляром является системный администратор в каждой организации. В качестве администратора выступает также поставщик услуг управления информационной безопасностью (MSSP), если та или иная организация поручает ему выполнение некоторых из вышеуказанных операций.

Поставщик инфраструктуры ИТ: Эта роль предполагает обеспечение инфраструктуры ИТ для той или иной организации. Инфраструктура включает сетевые соединения и облачные услуги, такие как программное обеспечение как услугу (SaaS), платформу как услугу (PaaS) и инфраструктуру как услугу (IaaS). Поставщик инфраструктуры ИТ обладает информацией о межорганизационных сетях, например, информацией о топологии сети и спецификациями облачных услуг. Типичными экземплярами являются поставщик услуг интернета (ISP), поставщик прикладных услуг (ASP) и поставщик облачных услуг (CSP).

Группа реагирования: Эта роль предполагает мониторинг и анализ различных инцидентов в киберобществах, например, несанкционированного доступа, атак типа распределенный отказ в обслуживании (DDoS) и фишинга, а также накопление информации об инцидентах. На основе информации в рамках этой роли могут осуществляться меры противодействия, например, блокирование трафика и занесение адресов фишинговых сайтов в черные списки. Типичным экземпляром является группа реагирования на инциденты в MSSP.

Координатор: Эта роль предполагает координацию деятельности с другими ролями и решение проблем потенциальных угроз, исходя из известной информации, имеющей отношение к инцидентам. При исполнении этой роли направляются предупреждения другим организациям и иногда иницируются совместные меры по ослаблению влияния разрушительных и крупномасштабных атак, таких как DDoS-атаки. Типичным экземпляром является Координационный центр CERT (CERT/CC), будь то коммерческий или некоммерческий.

Исследователь: Эта роль предполагает выполнение исследования по вопросам кибербезопасности, включая уязвимости и атаки, извлечение знаний из результатов исследований и их накопление. При исполнении этой роли через регистратора публикуется значительная часть повторно используемой информации, с тем чтобы отдельные организации могли осуществлять необходимые меры противодействия. Типичными экземплярами являются группа X-force корпорации International Business Machines (IBM), Risk Research Institute of Cyber Space (RRICS) корпорации Little eArth Corporation (LAC) и лаборатория McAfee Lab компании McAfee Inc.

Разработчик продукта и услуги: Эта роль предполагает разработку продуктов и услуг и накопление информации о них, например, об их версиях, конфигурациях, уязвимостях и корректировках. При исполнении этой роли через регистратора публикуется значительная часть повторно используемой информации, с тем чтобы, как и в случае исследователя, отдельные организации могли осуществлять необходимые меры противодействия. Типичными экземплярами являются поставщик программного обеспечения и самостоятельный частный разработчик программного обеспечения.

Регистратор: Эта роль предполагает классификацию, упорядочение и накопление знаний о кибербезопасности, предоставляемых исследователем и разработчиком продукта и услуги, с тем чтобы эти знания могли повторно использоваться другими организациями. Типичными экземплярами являются NIST и Агентство по содействию развитию информационных технологий в Японии. В некоторых случаях выступать в качестве регистратора и публиковать информацию может также объект, выступающий в качестве исследователя или разработчика продукта и услуги.

1.3 Информация о кибербезопасности

С учетом доменов операций и ролей в данном разделе определяется необходимая для операций информация о кибербезопасности. С учетом информации, с которой связана каждая из ролей, в настоящей онтологии определяются четыре базы данных – по ресурсам пользователя, ресурсам поставщика, инцидентам и предупреждениям – и три базы знаний – по продуктам и услугам, мерам противодействия и киберрискам.

1.3.1 База данных по ресурсам пользователя

В базе данных по ресурсам пользователя накапливается информация о ресурсах в рамках отдельных организаций и содержится такая информация, как списки программного/аппаратного обеспечения, их конфигурации, статус использования ресурсов, политика безопасности, в том числе политика управления доступом, результаты оценки уровня безопасности, а также топология интранета. В ней также содержится информация о внешних ресурсах, используемых отдельными организациями-пользователями, такая как списки абонированных облачных услуг (например, центры данных и SaaS) и сведения об их использовании. Такой информацией управляет администратор. Для описания результатов оценки ресурсов ИТ могут использоваться ARF и CRF, а для оценки уровня безопасности ресурса ИТ могут использоваться оценки CVSS и CWSS. Эти оценки полезны администраторам при установлении приоритетов срочности операций безопасности в отношении ресурсов ИТ.

1.3.2 База данных по ресурсам поставщика

В базе данных по ресурсам поставщика накапливается информация о ресурсах, расположенных за пределами отдельных организаций. В целях выполнения действенных и эффективных операций кибербезопасности эта база данных нуждается в увязке с той или иной базой данных по ресурсам пользователя, поскольку граница между внутренними и внешними ресурсами ИТ становится все более размытой, особенно при облачных вычислениях. Такой информацией управляет поставщик инфраструктуры ИТ. В этой базе данных содержится главным образом информация о сетях поставщика и облачных услугах. Информация о сетях поставщика относится к сетям, посредством которых каждая организация соединена с другими организациями, например информация о топологии, маршрутизации, политике управления доступом, статусе трафика и уровнях безопасности. Информация об облачных услугах включает спецификации услуг, информацию о загруженности и информацию о политике безопасности по каждой облачной услуге. Следует отметить, что информация, относящаяся к организациям-пользователям, такая как местная конфигурация каждой облачной услуги, хранится в базе данных по ресурсам пользователя.

1.3.3 База данных по инцидентам

В базе данных по инцидентам содержится информация об инцидентах, которая формируется на основе анализа информации в базе данных по ресурсам пользователя. Данной информацией управляет группа реагирования. В этой базе данных содержатся три вида записей: записи о событиях, записи об инцидентах и записи об атаках.

Запись о событиях содержит информацию о компьютерных событиях, в том числе о пакетах, файлах и относящихся к ним транзакциях. Как правило, компьютеры автоматически обеспечивают большинство записей в виде компьютерных журналов, таких как журналы регистрации времени и даты входа в систему, а также информацию о терминале при входе в систему привилегированных пользователей. Экземплярами этой записи являются журналы. Для описания записи может использоваться CEE.

Запись об инцидентах содержит информацию об инцидентах, связанных с безопасностью, и обеспечивает такую информацию, как текущее состояние систем пользователя и дальнейшие риски. Она образуется на основе анализа нескольких записей о событиях и их гипотез, которые создаются автоматически или вручную. Например, при обнаружении избыточного доступа к одному из компьютеров в записи об инцидентах должны быть отражены состояние данного компьютера (избыточный доступ к одному из компьютеров) и его предполагаемые последствия (отказ в обслуживании). На основе этой записи можно судить об опасности инцидента, а также о необходимости мер противодействия. Следует отметить, что запись об инцидентах может отражать ложные инциденты, то есть возможные инциденты, которые после расследования не будут сочтены инцидентами. Для описания записи может использоваться формат обмена описаниями инцидентов как объектов (IODEF).

Запись об атаках содержит информацию об атаках, сформированную на основе анализа записей об инцидентах. Она описывает последовательность развития атаки, например, как была начата атака, на какую часть ресурсов ИТ была направлена и как распространялся ущерб от атаки. Следует отметить, что эта запись нуждается в увязке с записью об инцидентах.

1.3.4 База данных по предупреждениям

В базе данных по предупреждениям содержится информация о предупреждениях кибербезопасности. Данная информация предназначается либо для неограниченного круга лиц, либо для конкретной организации. Информация для неограниченного круга лиц обычно содержит статистические данные и оповещения, а информация для конкретной организации – инструкции по безопасности специально для данной организации. Информация формируется на основе информации, содержащейся в базе данных по инцидентам и в базе знаний по киберрискам. Такой информацией управляют координатор и группа реагирования. На основе предупреждений организации-пользователи могут реализовать меры противодействия рискам кибербезопасности, о которых они предупреждены.

1.3.5 База знаний по киберрискам

В базе знаний по киберрискам накапливается информация о рисках кибербезопасности. Она предоставляется исследователем и разработчиком продукта и услуги, а затем упорядочивается и классифицируется регистратором. Данная база знаний включает в себя базы знаний по уязвимостям и по угрозам.

База знаний по уязвимостям: В этой базе знаний накапливается информация об известных уязвимостях, в которую входят наименования, таксономия и перечень известных уязвимостей программного обеспечения и системы. В нее также входит информация об уязвимостях, обусловленных человеческим фактором, каковыми являются уязвимости, которым подвержены люди как пользователи ИТ. Практическими экземплярами этой базы данных являются Национальная база данных об уязвимостях (NVD) и База данных уязвимостей при открытом исходном коде (OSVDB), а для описания содержания данной базы знаний могут использоваться CVE и CWE.

База знаний по угрозам: В этой базе знаний накапливается информация об известных угрозах кибербезопасности. Она включает базы знаний по атакам и по ненадлежащему использованию. В базе знаний по атакам накапливается информация об атаках, такая как информация о схемах атак, инструментальных средствах атак (например, вредоносном программном обеспечении) и их тенденциях. Информация о тенденциях включает, например, информацию о тенденциях имевших место ранее атак с точки зрения их географии и целей, а также статистическую информацию о имевших место ранее атаках. Для описания содержания данной базы знаний могут использоваться CAPEC и MAEC.

В базе знаний по ненадлежащему использованию накапливается информация о видах ненадлежащего использования, обусловленных неправильными действиями пользователей, совершенными будь то без злого умысла или со злым умыслом. Неправильные действия, совершенные без злого умысла, включают ошибки при вводе с клавиатуры, неправильное распознавание вследствие невнимательности, неправильное понимание и случаи попадания в фишинговую ловушку. Неправильные действия, совершенные со злым умыслом, включают случаи нарушения требований, такие как несанкционированное пользование услугой и доступ к ненадлежащим материалам. Следует отметить, что ради простоты базы знаний по атакам и по ненадлежащему использованию на рисунке 7-1 не показаны.

1.3.6 База знаний по мерам противодействия

В базе знаний по мерам противодействия накапливается информация о мерах противодействия рискам кибербезопасности. Она предоставляется исследователем и разработчиком продукта и услуги, а затем упорядочивается и классифицируется регистратором. Данная база знаний содержит базы знаний по оценке и по обнаружению/защите.

База знаний по оценке: В этой базе знаний накапливаются известные правила и критерии оценки уровня безопасности ресурсов ИТ, списки проверки конфигураций и эвристика, включая передовые методы. Формулы CVSS/CWSS являются двумя из лучших методов оценки уровней безопасности и накапливаются в этой базе знаний. Кроме того, для описания правил и обеспечения списков проверки могут использоваться XCCDF и OVAL.

База знаний по обнаружению/защите: В этой базе знаний накапливаются известные правила и критерии обнаружения угроз безопасности и защиты от них. В ней также накапливается эвристика, включая передовые методы.

1.3.7 База знаний по продуктам и услугам

В базе знаний по продуктам и услугам накапливается информация о продуктах и услугах. Она предоставляется исследователем и разработчиком продукта и услуги, а затем упорядочивается и классифицируется регистратором. Данная база знаний включает базы знаний по версиям и по конфигурациям.

База знаний по версиям: В этой базе знаний накапливается информация о версиях продуктов и услуг, включая названия и перечень их версий. В том, что касается продукта, сюда также включаются корректировки безопасности. Для перечня общеизвестных платформ может использоваться CPE.

База знаний по конфигурациям: В этой базе знаний накапливается информация о конфигурациях продуктов и услуг. Она включает названия, таксономию и перечень известных конфигураций продуктов и услуг. В том, что касается конфигурации услуги, в нее также входят руководящие указания в отношении видов использования услуги. Для перечня общеизвестных конфигураций продуктов может использоваться CCE.

Некоторая дополнительная информация по этой онтологии приводится в [b-Ontology] и в Дополнении II к [b-ITU-T X.1500].

Дополнение II

Спецификации, описывающие базы данных и базы знаний

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Семь типов информации, представленных в пункте 7, описываются целым рядом спецификаций по кибербезопасности, включая спецификации, совместимые с Рекомендацией МСЭ-Т X.1500 (например, CVE и IODEF), как явствует из таблицы II.1. Таким образом, уровень детализации обнаруженной информации о кибербезопасности будет соответствовать уровню детализации спецификаций. При использовании данного подхода уровень детализации является гибким, и поэтому для конкретных целей могут создаваться разные спецификации.

Таблица II.1 – Спецификации, поддерживающие онтологию

Домены	БЗ/БД		Спецификации
Управление ресурсами ИТ	БД по ресурсам пользователя		Оценки ARF, AI, CVSS/CWSS
	БД по ресурсам оператора		---
Обработка инцидентов	БД по инцидентам		CEE, IODEF
	БД по предупреждениям		IODEF
Накопление знаний	БЗ по киберрискам	БЗ по уязвимостям	CVE, CWE, CVRF
		БЗ по угрозам	CAPEC, MAEC
	БЗ по мерам противодействия	БЗ по оценке	Формула CVSS/CWSS
		БЗ по обнаружению/защите	OVAL, XCCDF
	БЗ по продуктам и услугам	БЗ по версиям	CPE
		БЗ по конфигурациям	CCE
ПРИМЕЧАНИЕ. – БД (база данных); БЗ (база знаний).			

Дополнение III

Наглядная реализация обнаружения на основе RDF

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

III.1 Пример реализации обнаружения на основе RDF

Принцип, представленный на рисунке 9-1, мог бы быть реализован посредством совместного размещения агентов обнаружения и агентов регистра внутри поисковой системы RDF. Объекты кибербезопасности направляют запрос об обнаружении поисковой системе RDF, которая возвращает список идентификаторов и их возможностей. Следует иметь в виду, что каждая поисковая система имеет различные источники, которые образуют ее диапазон поиска.

На практике для обеспечения масштабируемости источник может быть зарегистрирован и управляться на основе иерархии, как показано на рисунке III.1. Уровнем 1 может быть отдельная поисковая система RDF, работающая фактически как агент обнаружения, а уровнем 2 мог бы быть объект, зарегистрированный по правилам работы одного из региональных регистров, например Американского регистра номеров интернета (ARIN), Европейских IP сетей (RIPE) или Азиатско-Тихоокеанского центра сетевой информации (APNIC), и может быть введена дополнительная иерархия, в зависимости от реализации. Источником может быть CERT или какой-либо другой объект кибербезопасности.

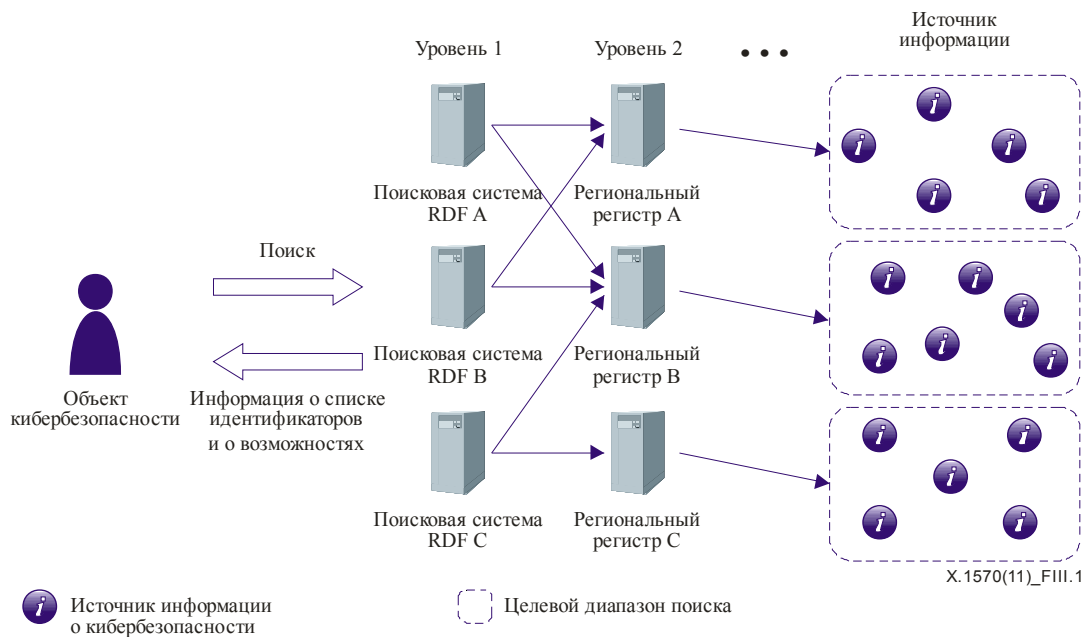


Рисунок III.1 – Иерархия регистра источника

III.2 Иерархия классов информации о кибербезопасности

На рисунке III.2 показана иерархия классов механизма обнаружения. Каждый класс представляет собой категорию, включенную в Дополнение II к [b-ITU-T X.1500]. Подробную информацию по каждой категории см. в указанной Рекомендации. Следует отметить, что использовано пространство имен XML, определенное МСЭ-Т [b-ITU-T X.1500].

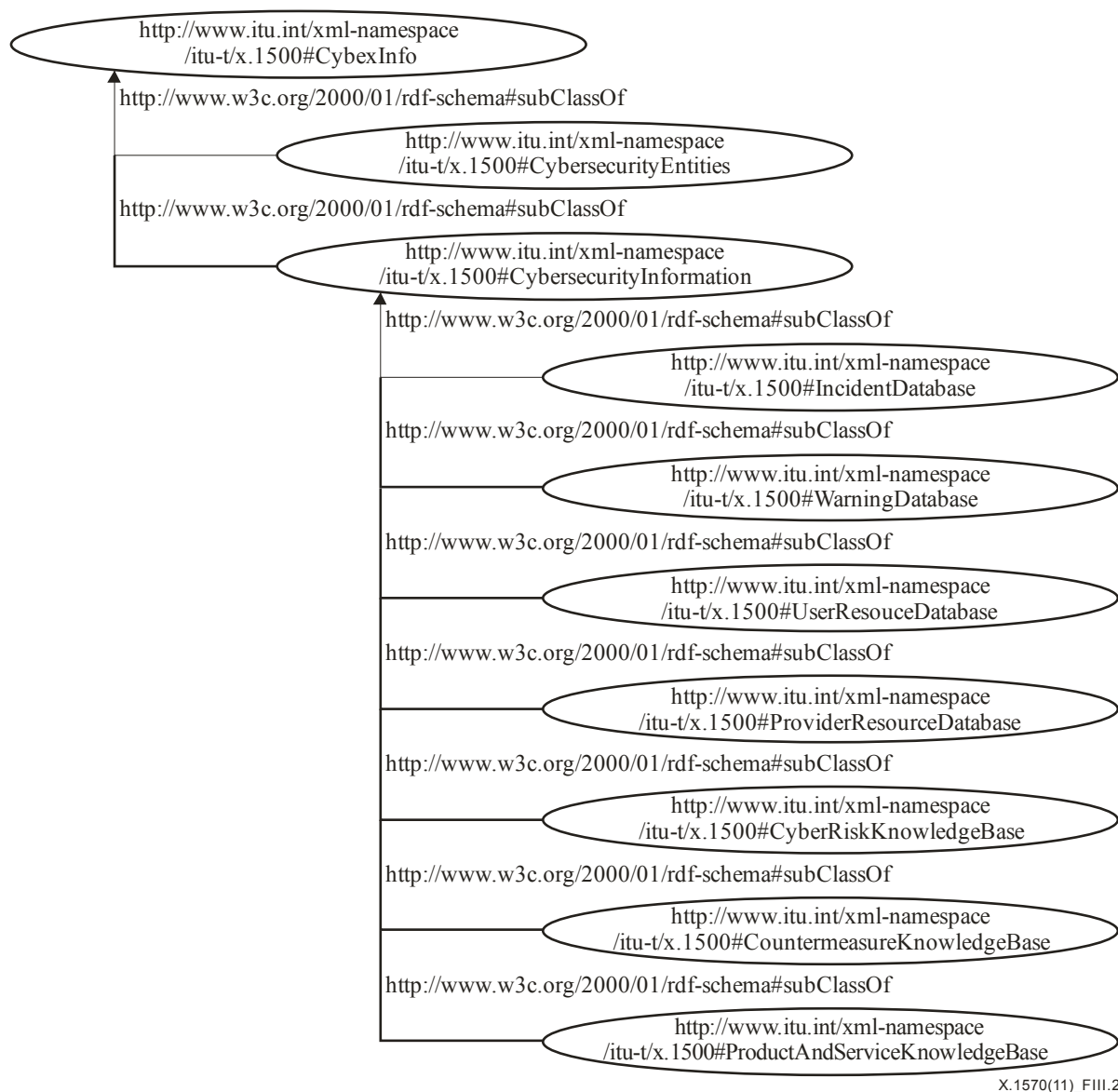


Рисунок III.2 – Иерархия классов информации о кибербезопасности

ПРИМЕЧАНИЕ. – Использование **.int** в наименовании домена верхнего уровня показано на рисунке III.2 в качестве примера и не предназначено для использования в работе.

Атрибуты каждого класса кибербезопасности обычно включают следующие атрибуты:

- **entry_date**: хранит дату ввода/изменения данных;
- **issuer_name**: хранит название автора (автором может быть частное лицо либо компания);
- **contact_email**: хранит адрес электронной почты контактной стороны;
- **resources**: хранит идентификаторы, например веб-адреса, для дополнительных ресурсов;
- **Info_type**: хранит тип информации, например CVE, CWSS [b-CWSS], CVSS [b-ITU-T X.1521], OVAL [b-OVAL], SCAP [b-SCAP], XCCDF [b-XCCDF], CPE [b-CPE], CCE [b-CCE] и ARF.

Любая сторона, ищущая информацию о кибербезопасности, может запросить данные в каком-либо компоненте того или иного конкретного класса. Поиск информации может осуществляться по критериям, включающим название класса, атрибут класса, а также дату и время внесения последнего изменения.

Пробная реализация схемы обнаружения доступна в сети по адресу: <http://cybiet.sourceforge.net/>.

ПРИМЕЧАНИЕ. – Эта реализация позволяет обнаружить информацию о кибербезопасности, которая систематизирована в соответствии с онтологией, описание которой представлено на рисунке 7-1.

Библиография

- [b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.
- [b-ITU-T X.1500.1] Recommendation ITU-T X.1500.1 (2012), *Procedures for the registration of arcs under the object identifier (OID) arc for cybersecurity information exchange*.
- [b-ITU-T X.1520] Рекомендация МСЭ-Т X.1520 (2011 г.), *Общезвестные уязвимости и незащищенность*.
- [b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system*.
- [b-AI] NIST, *The Asset Identification*.
<<http://scap.nist.gov/specifications/ai/>>
- [b-ARF] *Assessment Results Format*
<<https://measurablesecurity.mitre.org/incubator/arf/>>
- [b-CCE] *Common Configuration Enumeration*.
<<https://cce.mitre.org/>>
- [b-CPE] *Common Platform Enumeration*.
<<https://cpe.mitre.org/>>
- [b-CWSS] *Common Weakness Scoring System*.
<<https://cwe.mitre.org/cwss/>>
- [b-Gruber] Gruber T.R. (1993), *Toward principles for the design of ontologies used for knowledge sharing*. International Journal of Human-Computer Studies, Vol. 43, Issues 4-5, November 1995, pp. 907-928.
- [b-Ontology] Takahashi T., Kadobayashi Y., Fujiwara H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks (SIN), September 2010.
- [b-OVAL] *Oval – Open Vulnerability and Assessment Language*.
<<https://oval.mitre.org/>>
- [b-SCAP] *Security Content Automation Protocol (SCAP)*.
<<http://scap.nist.gov/>>
- [b-XCCDF] *XCCDF – The Extensible Configuration Checklist Description Format*
<<http://scap.nist.gov/specifications/xccdf/>>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи