Международный союз электросвязи

МСЭ-Т X.1500

(04/2011)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Обмен информацией, касающейся кибербезопасности – Обзор кибербезопасности

Методы обмена информацией о кибербезопасности

Рекомендация МСЭ-Т X.1500

ITU-T

Международный союз электросвязи

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.

Рекомендация МСЭ-Т X.1500

Методы обмена информацией о кибербезопасности

Резюме

В Рекомендации МСЭ-Т X.1500 описаны методы обмена информацией о кибербезопасности. Эти методы могут использоваться по отдельности или в том или ином сочетании, в зависимости от требования или случая, для того чтобы повысить уровень кибербезопасности путем согласованного, комплексного, глобального, своевременного и гарантированного обмена информацией. В них не накладываются обязательства по обмену информацией, а также не рассматриваются средства получения и конечное использование информации. Обмен информацией о кибербезопасности (CYBEX) является одним из элементов обеспечения уверенности и безопасности при использовании ИКТ.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1500	20.04.2011 г.	17-я

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/.

СОДЕРЖАНИЕ

Введение

Настоящая Рекомендация предусматривает возможность адаптации и расширения и не носит предписывающего характера, с тем чтобы обеспечить возможность применения в различных конкретизациях широкого спектра методов, часть из которых постоянно развивается и находится на разных этапах, в целях совершенствования обмена информацией о кибербезопасности, относящейся к инфраструктурам электросвязи/ИКТ, устройствам и услугам. Рекомендация подлежит периодическому пересмотру, обусловленному развитием этих методов, и те из них, которые сочтут целесообразными, опубликуют в качестве Рекомендаций МСЭ-Т серии X.1500.

Что касается методов, включенных в настоящую Рекомендацию, ожидается, что организации электросвязи/ИКТ, в том числе группы реагирования на компьютерные инциденты (CIRT), которые находятся в их непосредственном или совместном ведении:

a) получат информацию, которая позволит им принимать решения и меры, направленные на существенное повышение уровня конфиденциальности, целостности и доступности глобальных средств и услуг электросвязи/ИКТ;

b) получат информацию, способствующую безопасному процессу сотрудничества и безопасному управлению, благодаря которым повышается уровень гарантии при обмене информацией между организациями;

c) обеспечат согласованный подход к управлению и обмену информацией о кибербезопасности на глобальной основе;

d) повысят осведомленность о кибербезопасности и улучшат сотрудничество в целях снижения влияния киберугроз, кибератак и вредоносного программного обеспечения.

Эти методы включают:

- структурирование информации о кибербезопасности для целей обмена;
- идентификацию и обнаружение информации о кибербезопасности и объектов кибербезопасности;
- заключение соглашения о доверии и политике между объектами, осуществляющими обмен;
- запрашивание и предоставление информации о кибербезопасности;
- гарантирование целостности обмена информацией о кибербезопасности.

Они сгруппированы по следующим блокам:

- слабые места, уязвимость и состояние;
- событие, инцидент и эвристика;
- политика обмена информацией;
- идентификация, обнаружение и запрос;
- гарантия идентичности;
- протоколы обмена.

Рекомендация МСЭ-Т X.1500

Методы обмена информацией о кибербезопасности

1 Сфера применения

В настоящей Рекомендации представлена модель обмена информацией о кибербезопасности (CYBEX) и обсуждаются методы, которые могут использоваться для облегчения обмена информацией о кибербезопасности. Эти методы могут использоваться по отдельности или вместе, в зависимости от требования или случая, для того чтобы повысить уровень кибербезопасности путем согласованного, комплексного, глобального, своевременного и гарантированного обмена информацией. В них не накладываются обязательства по обмену информаций, а также не рассматриваются средства получения и конечное использование информации. Эти методы включают структурированное глобальное обнаружение и функциональную совместимость информации о кибербезопасности, при которых обеспечивается возможность непрерывного развития, учитывающего существенные виды деятельности и создание спецификаций в рамках многочисленных форумов по кибербезопасности. CYBEX является одним из элементов обеспечения уверенности и безопасности при использовании ИКТ.

Настоящая Рекомендация предназначена для выполнения следующих основных функций, которые, в зависимости от случая, могут использоваться по отдельности или вместе:

- структурирование информации о кибербезопасности для целей обмена;
- идентификация и обнаружение информации о кибербезопасности и объектов кибербезопасности;
- заключение соглашения о доверии и политике между объектами, осуществляющими обмен;
- запрашивание и предоставление информации о кибербезопасности;
- гарантирование целостности обмена информацией о кибербезопасности.

В соответствии с согласованными принципами политики и применимыми законодательными и нормативными актами средства получения и виды использования информации не входят конкретным образом в сферу применения настоящей Рекомендации и не рассматриваются в ней. В ряде национальных и региональных нормативных и законодательных актов может потребоваться реализация механизмов защиты информации, позволяющей установить личность. Настоящая Рекомендация не санкционирует применение методов, описанных в настоящей Рекомендации, и обмен информацией о кибербезопасности, относящейся к этим методам.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 кибербезопасность (cybersecurity) [b-ITU-T X.1205]: Набор инструментальных средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают доступность, целостность (которая может включать аутентичность и неотказуемость) и конфиденциальность.

ПРИМЕЧАНИЕ. – В ряде национальных и региональных нормативных и законодательных актов может потребоваться реализация механизмов защиты информации, позволяющей установить личность.

3.1.2 инцидент безопасности (security incident) [b-ITU-T E.409]: Любое неблагоприятное событие, в результате которого некий аспект безопасности может подвергнуться угрозе.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 гарантия (assurance): Степень уверенности в том, что процесс или конечный результат соответствуют определенным характеристикам или требованиям.

3.2.2 протокол обмена (exchange protocol): Набор технических правил и формат, которые регулируют обмен информацией между двумя или несколькими объектами.

3.2.3 политика обмена информацией (information exchange policy): Условия, относящиеся к использованию информации о кибербезопасности и к обмену этой информацией.

3.2.4 состояние системы (system state): Существующее состояние системы или объекта, включающее, например, информацию о конфигурации системы или объекта, использовании памяти или другие данные, касающиеся кибербезопасности.

3.2.5 уязвимость (vulnerability) (соответствует [b-ITU-T X.800]): Любое слабое место, которое может быть использовано для нарушения системы или информации, которая в ней содержится.

3.2.6 слабое место (weakness): Недостаток или дефект, который, хотя и не признается сам по себе в качестве уязвимости, мог бы в какой-то момент стать уязвимостью или мог бы способствовать привнесению других уязвимостей.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ARF	Assessment Results Format or Asset Reporting Format (depending on the context)	Формат обмена результатами оценки или формат представления сведений о ресурсах (в зависимости от контекста)
BEEP	Blocks Extensible Exchange Protocol	Протокол для расширяемого обмена блоками информации
CA	Certification Authority	Сертификационный орган
CAPEC	Common Attack Pattern Enumeration and Classification	Перечень и классификация общеизвестных схем атак
CCE	Common Configuration Enumeration	Перечень общеизвестных конфигураций
CEE	Common Event Expression	Описание общеизвестных событий
CEEE	Common Event Expression Exchange	Обмен описаниями общеизвестных событий
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
CYIQL	Cybersecurity Information Query Language	Язык запросов информации о кибербезопасности
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
EVC	Extended Validation Certificates	Сертификаты с расширенной валидацией

EVCERT	Extended Validation Certificate		Сертификат с расширенной валидацией
HTTP	HyperText Transfer Protocol		Протокол передачи гипертекста
IC	Integrated Circuit	ИС	Интегральная схема
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
IDS	Intrusion Detection System		Система обнаружения проникновений
IODEF	Incident Object Description Exchange Format		Формат обмена описаниями инцидентов как объектов
IPS	Intrusion Prevention System		Системы предотвращения проникновений
IT	Information Technology	ИТ	Информационные технологии
MAEC	Malware Attribute Enumeration and Characterization		Перечень и характеристики атрибутов вредоносного программного обеспечения
OID	Object Identifier		Идентификатор объекта
OS	Operating System	ОС	Операционная система
OVAL	Open Vulnerability and Assessment Language		Открытый язык описания уязвимости и оценки
RID	Real-time Inter-network Defense		Межсетевая защита в реальном времени
SCAP	Security Content Automation Protocol		Протокол автоматизации управления данными безопасности
SOAP	Simple Object Access Protocol		Простой протокол доступа к объектам
TLP	Traffic Light Protocol		Протокол маркировки информации
TLS	Transport Layer Security		Безопасность транспортного уровня
TNC	Trusted Network Connect		Доверенное подключение к сети
TPM	Trusted Platform Module		Модуль доверенной платформы
XCCDF	eXtensible Configuration Checklist Description Format		Расширяемый формат описания списка проверки конфигурации

5 Условные обозначения

При использовании в настоящей Рекомендации термина "стандарт" или "стандарты" в общем смысле его следует толковать как включающий стандарты, спецификации и Рекомендации.

6 Обмен информацией о кибербезопасности (CYBEX) – основной принцип

Настоящая Рекомендация, касающаяся обмена информацией о кибербезопасности (CYBEX), призвана выполнить простую конкретную задачу – описать методы, с помощью которых объекты кибербезопасности могут обмениваться информацией о кибербезопасности с использованием методов, обеспечивающих достаточный уровень гарантии. К числу таких объектов, как правило, относятся организации, физические лица, устройства или процессы, которые обладают информацией о кибербезопасности или пытаются ее получить. Наиболее часто этими объектами являются группы CIRT, а также операторы или разработчики оборудования, программного обеспечения или сетевых систем.

Обмен информацией о кибербезопасности полезен с точки зрения достижения более высокого уровня кибербезопасности и защиты инфраструктуры, а также содействия CIRT в выполнении их главных функций.

Обмен информацией о кибербезопасности может осуществляться в рамках узкоспециализированных доверительных сообществ, при соблюдении принципов доступа к специальной информации на основе ранее согласованных принципов политики, а также в рамках использования общедоступной информации. Типичными примерами видов информации, которой обмениваются между собой объекты, являются знания в отношении угроз, уязвимостей, инцидентов, рисков, способов уменьшения их влияния и связанных с этими способами средств устранения. Соответствующие методы, включенные в настоящую Рекомендацию, предназначены для облегчения обмена этой информацией и, таким образом, для повышения уровня кибербезопасности.

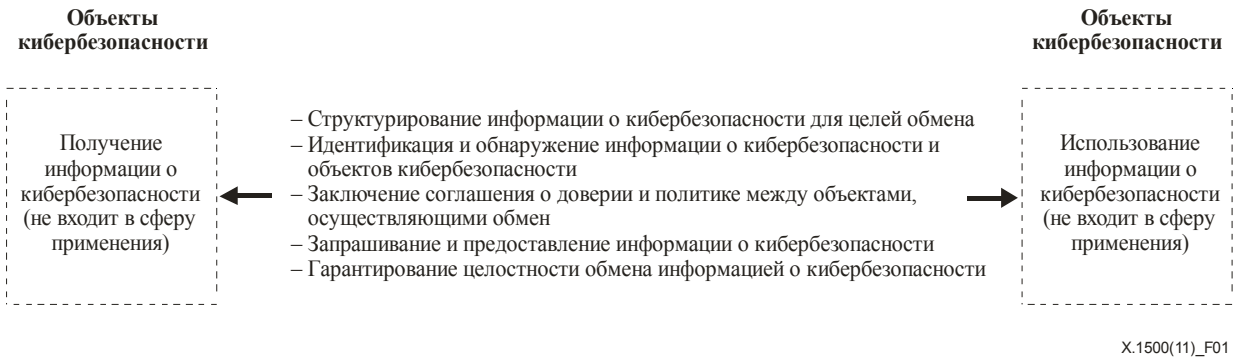

Рисунок 1 – Модель CYBEX

Как показано на рисунке 1, использованная в настоящей Рекомендации общая модель обмена информацией о кибербезопасности содержит основные функции, которые, в зависимости от случая, могут использоваться по отдельности или вместе, а также при необходимости могут быть расширены с целью более эффективного обеспечения гарантированного обмена информацией о кибербезопасности:

- структурирование информации о кибербезопасности для целей обмена;
- идентификация и обнаружение информации о кибербезопасности и объектов кибербезопасности;
- заключение соглашения о доверии и политике между объектами, осуществляющими обмен;
- запрашивание и предоставление информации о кибербезопасности;
- гарантирование целостности обмена информацией о кибербезопасности.

В пункте 7 описаны методы выполнения этих функций.

Обмен информацией о кибербезопасности может выполняться в двух направлениях. Это свойство позволяет с помощью проверенных информационных запросов и ответов обеспечивать требуемые уровни гарантии между сторонами или осуществлять сертификацию доставки.

В соответствии с согласованными принципами политики и применимыми законодательными и нормативными актами средства получения и виды использования информации не входят конкретно в сферу применения настоящей Рекомендации и не рассматриваются в ней. Например, в некоторых специализированных реализациях обмена информацией о кибербезопасности, таких как обратная трассировка источника атаки, могут потребоваться механизмы, связанные с конкретными приложениями, которые позволяют осуществлять рекурсивную серию запросов и ответов для получения необходимой информации. В то же время другие реализации, такие как обеспечение измеримости и управляемости кибербезопасности путем использования средств автоматизированного управления безопасностью, относятся к сфере применения. Эти и другие сценарии использования могут обеспечиваться методами, включенными в настоящую Рекомендацию. Настоящая Рекомендация не санкционирует применение включенных в нее методов и обмен информацией о кибербезопасности, относящейся к этим методам. Также могут быть уместными и другие методы.

7 Методы обмена структурированной информацией о кибербезопасности

Для осуществления обмена информацией о безопасности между двумя объектами обмен должен быть структурирован и описан согласованным образом, который понятен обоим объектам. Целью CYBEX является облегчение обмена информацией о кибербезопасности, которая включает "общие перечни", то есть упорядоченные списки значений общепринятой информации для одинаковых типов данных. Общий перечень позволяет взаимно увязывать распределенные базы данных и другие средства, а также упрощает проведение сравнений, касающихся кибербезопасности.

Для целей осуществления этого обмена в информацию о кибербезопасности включены структурированная информация или знания относительно:

- "состояния" оборудования, программного обеспечения или сетевых систем с точки зрения кибербезопасности, в особенности уязвимостей;

- экспертно-технического анализа инцидентов или событий;
- эвристики и сигнатур, которые получены на основе имевших место событий;
- участвующих объектов кибербезопасности;
- спецификаций обмена информацией о кибербезопасности, в том числе модулей, схем, условий и присвоенных номеров;
- атрибутов идентичности и гарантии всей информации о кибербезопасности;
- требований, руководящих указаний и практики в отношении реализации.

С тем чтобы описать на общем уровне желательные атрибуты обмена информацией о кибербезопасности, средства структурированной информации сгруппированы по следующим шести блокам методов, относящихся к отдельным группам обмена информацией о кибербезопасности:

- слабые места, уязвимость и состояние;
- событие, инцидент и эвристика;
- политика обмена информацией;
- идентификация, обнаружение и запрос;
- гарантия идентичности;
- протокол обмена.

Классификация этих блоков широкая, и средства, относящиеся к одному блоку, могут в реальности использоваться в одном или в нескольких других блоках, в зависимости от приложения.

Каждый из указанных выше блоков подробно описан в следующих ниже подпунктах. В описании каждого блока приводится анализ его роли в рамках CYBEX, а также перечисляются методы его реализации. Ни один из определенных методов не носит предписывающего характера; они лишь являются примерами методов, которые считают согласующимися с целями соответствующего блока. Выбор процедуры обусловлен, главным образом, степенью специализации сообщества пользователей, к которому она относится, а также глобальными преимуществами, полученными в результате заимствования.

В указанных в данной Рекомендации методах CYBEX определен набор дополнительных методов, которые обеспечивают возможность и облегчают выполнение этих и других конкретизаций.

В оставшейся части данного пункта и в связанном с ним Дополнении I описывается каждый блок, в том числе приводится обзор роли каждого блока в рамках CYBEX, а также перечисляются методы реализации каждого блока. Справочные документы не являются нормативными, и их подробное описание приведено в разделе "Библиография".

Лица, осуществляющие реализацию и использование этих блочных методов, должны соблюдать все применимые национальные и региональные законодательные и нормативные акты, а также принципы политики.

7.1 Блок обмена: слабые места, уязвимость и состояние

Средства, необходимые для блока обмена, касающегося слабых мест, уязвимости и состояния, обеспечивают обмен информацией о слабых местах и уязвимости, а также оценку состояния систем и приложений.

В таблице I.1 приводится перечень необходимых средств, соответствующих типам методов, которые могут способствовать обеспечению обмена информацией о слабых местах, уязвимости и состоянии.

7.2 Блок обмена: событие, инцидент и эвристика

Средства, необходимые для блока обмена, касающегося события, инцидента и эвристики, обеспечивают обмен информацией о наблюдаемых событиях, инцидентах и эвристике.

В таблице I.2 приводится перечень необходимых средств, соответствующих типам методов, которые могут способствовать обеспечению обмена структурированной информацией о событии, инциденте или эвристике между группами CIRT и другими сторонами. Эта обмениваемая информация может использоваться в целях создания комплексных средств реагирования на атаки, а также сокращения существующих слабых мест и уязвимостей.

7.3 Блок обмена: политика обмена информацией

Средства, необходимые для блока обмена, касающегося политики обмена информацией, обеспечивают обмен между объектами информацией о кибербезопасности, которая связана с условиями, касающимися обмениваемой информации, а также обеспечивают использование этой информации. Такое понимание можно отнести к конкретной обмениваемой информации или к широкому классу информации, к которому она принадлежит, либо его можно отнести к объектам, участвующим в обмене. Насколько это необходимо при данных обстоятельствах, целесообразно обеспечить уведомление участвующих объектов об этих принципах политики. Данное уведомление может осуществляться в разных формах и может передаваться вместе с информацией или предоставляться независимо – посредством механизма запроса-ответа.

В таблице I.3 приводится перечень необходимых средств, соответствующих типам методов, которые могут способствовать обеспечению обмена информацией о политике между объектами кибербезопасности. Отметим, что в рамках форумов по обмену информацией о безопасности продолжают появляться требования и протоколы, касающиеся обмена информацией о политике, и следует принять меры для обеспечения их надлежащей реализации.

7.4 Блок идентификации, обнаружения и запроса

Средства, необходимые для блока идентификации, обнаружения и запроса, обеспечивают процессы идентификации, обнаружения и запроса.

В рамках сообществ кибербезопасности существуют общие интересы, касающиеся идентификаторов кибербезопасности, а также их создания, администрирования, обнаружения, проверки и использования. К числу этих интересов относится:

- повышение ценности информации о кибербезопасности путем обеспечения возможности широкого обмена соответствующей информацией о событии и результатами анализа событий в течение длительного времени;
- повышение безопасности обмена информацией о кибербезопасности путем предоставления возможности получать информацию об идентификаторе для осуществления проверки, а также узнавать соответствующие принципы политики;
- повышение гибкости обмена информацией о кибербезопасности путем предоставления возможности получать новую или дополнительную информацию, относящуюся к сообщению, например статус информации.

Различным организациям кибербезопасности может потребоваться реализация общих протоколов 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. Возможность существования идентификатора, являющегося уникальным в глобальном масштабе и используемого для глобального обмена информацией о кибербезопасности, неизбежно подразумевает наличие у него таких характеристик, как:

- 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.

В таблице I.4 приводится перечень необходимых средств, соответствующих типам методов, которые могут способствовать идентификации организаций кибербезопасности, а также процессам обнаружения и запрашивания информации о кибербезопасности.

7.5 Блок гарантии идентичности

Средства, необходимые для блока гарантии идентичности, обеспечивают гарантию идентичности.

В рамках CYBEX реальный обмен структурированной информацией может осуществляться множеством различных способов: по сети или путем физической транспортировки. Ключевым элементом данного обмена является доверие – доверие к идентичности сторон, а также к передаваемой информации.

В таблице I.5 приводится перечень необходимых средств, соответствующих типам методов, которые могут обеспечивать гарантию идентичности.

7.6 Блок протокола обмена

В число необходимых средств в рамках блока протокола обмена входят протоколы обмена, которые могут использоваться в различных контекстах обмена информацией о кибербезопасности. Для безопасного обмена информацией необходимо то или иное сочетание протоколов, перечисленных ниже. Межсетевая защита в реальном времени (RID) обеспечивает систему передачи сообщений для обмена информацией об инцидентах и соответствующую политику в отношении указанной информации. Транспортный протокол для сообщений RID, инкапсулирующих документы об инцидентах в формате IODEF (а также любых расширений IODEF), включает перечисленные транспортные протоколы BEEP, SOAP и HTTPS. Транспортный протокол для сообщений RID (первоначальный протокол, разработанный для передачи сообщений RID) может быть заменен протоколами SOAP, BEEP или будущими протоколами по мере их разработки. В рамках RID учитываются параметры безопасности и конфиденциальности, с тем чтобы обеспечить возможность отделения передачи сообщений от транспортного протокола.

В таблице I.6 приводится перечень необходимых средств, соответствующих типам протоколов обмена, которые могут использоваться для обмена информацией.

Дополнение I

Методы обмена структурированной информацией о кибербезопасности

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Таблица I.1 – Методы блока обмена, касающегося слабых мест, уязвимости и состояния

Метод	Описание	Справочные документы
Общеизвестные уязвимости и незащищенность (CVE)	Метод общеизвестных уязвимостей и незащищенности является методом идентификации информации и обмена информацией об уязвимостях и незащищенности в системе безопасности и обеспечивает общие идентификаторы широко известных проблем. Цель метода CVE состоит в упрощении обмена данными между отдельными средствами управления уязвимостями (инструментальными средствами, хранилищами и услугами) с помощью данного "общего перечня". Метод CVE призван обеспечить возможность увязки баз данных по уязвимостям и других ресурсов, а также упростить сравнение инструментальных средств и услуг безопасности. Фактически в CVE не содержится информации, например, о рисках, воздействии, исправлении или подробной технической информации, а содержится только номер стандартного идентификатора с индикатором состояния, краткое описание и ссылки на соответствующие сообщения и инструкции относительно уязвимостей. Предполагается, что в CVE должен содержаться полный объем информации обо всех широко известных уязвимостях и незащищенности. Цель состоит в том, чтобы в CVE содержалась тщательно проверенная информация; вместе с тем главный упор делается на идентификацию уязвимостей и незащищенности, которые обнаруживаются с помощью инструментальных средств безопасности, а также на выявление любых новых проблем, которые становятся общими, и затем на решение любых более старых проблем безопасности, которые требуется проверить.	[b-ITU-T X.1520]
Система оценки общеизвестных уязвимостей (CVSS)	Система оценки общеизвестных уязвимостей обеспечивает открытую структуру представления информации о характеристиках и воздействии уязвимостей ИКТ. Система CVSS состоит из трех групп: базовой, временно́й и группы среды. По каждой из них формируется балльная оценка, находящаяся в пределах от 0 до 10, а также вектор – сжатое текстовое представление значений, использованных для получения оценки. Базовая группа отражает внутренние качества, присущие той или иной уязвимости. Временная группа отражает характеристики уязвимости, которые изменяются во времени. В группе внешних факторов представлены характеристики уязвимости, присущие только внешней среде пользователя. Система CVSS позволяет администраторам средств ИКТ, поставщикам бюллетеней с описанием уязвимостей, разработчикам средств безопасности, разработчикам приложений и исследователям воспользоваться принятием общего языка оценки уязвимостей ИКТ.	[b-ITU-T X.1521]

Таблица I.1 – Методы блока обмена, касающегося слабых мест, уязвимости и состояния

Метод	Описание	Справочные документы
Перечень общеизвестных слабых мест (CWE)	Перечень общеизвестных слабых мест – это результат процесса определения и обмена унифицированными и измеримыми наборами данных о слабых местах в программном обеспечении. С помощью CWE обеспечивается возможность более эффективного обсуждения, описания, отбора и использования инструментальных средств и услуг безопасности программного обеспечения, способных обнаруживать слабые места в исходном коде и операционных системах. Также обеспечивается возможность лучшего понимания слабых мест, связанных с архитектурой и проектным решением, и управления их устранением. Реализации CWE составляются и обновляются различными международными группами экспертов из коммерческих структур, академических организаций и правительственных учреждений, что обеспечивает широту и глубину содержания. В CWE предусматривается использование стандартной терминологии, что позволяет поставщикам услуг информировать пользователей о конкретных возможных слабых местах и предлагать пути их устранения. А это также позволяет покупателям программного обеспечения сравнивать похожие продукты, предлагаемые различными разработчиками.	[b-CWE]
Система оценки общеизвестных слабых мест (CWSS)	Система оценки общеизвестных слабых мест обеспечивает открытую структуру представления информации о характеристиках и воздействии слабых мест в программном обеспечении.	[b-CWSS]
Открытый язык описания уязвимостей и оценки (OVAL)	Открытый язык описания уязвимостей и оценки является результатом международных усилий в области спецификации, направленных на создание открытых и общедоступных данных безопасности, а также на стандартизацию передачи этой информации между всеми существующими инструментальными средствами и услугами безопасности. OVAL включает язык, используемый для кодирования подробных данных о системе, а также ряд хранилищ контента, которые ведутся во всем сообществе. Этот язык стандартизует три основных этапа процесса оценки: представление информации о конфигурации системы для проверки; анализ системы на наличие определенного машинного состояния (уязвимости, конфигурации, состояния корректировки и т. д.); и представление отчета о результатах данной оценки. Хранилища являются сборниками общедоступного и открытого контента, в котором используется этот язык. Разрабатываются схемы OVAL, написанные на XML, которые служат в качестве структуры и словаря для языка OVAL. Эти схемы соответствуют трем этапам процесса оценки: схема OVAL "Характеристики системы", предназначенная для представления информации о системе; схема OVAL "Определение", предназначенная для описания того или иного конкретного машинного состояния; а также схема OVAL "Результаты" – для представления сообщений о результатах оценки.	[b-OVAL]

Таблица I.1 – Методы блока обмена, касающегося слабых мест, уязвимости и состояния

Метод	Описание	Справочные документы
Расширяемый формат описания списка проверки конфигурации (XCCDF)	Расширяемый формат описания списка проверки конфигурации является языком спецификации, предназначенным для написания списков проверки по безопасности, контрольных показателей и связанных с ними документов. Документ XCCDF представляет собой структурированную совокупность правил, касающихся конфигурации безопасности, для некоторого набора целевых систем. Эта спецификация предназначена для обеспечения взаимного обмена информацией, создания документов, организационной и ситуационной адаптации, автоматизированной проверки на соответствие и оценки соответствия. Кроме того, в спецификации определена модель и формат данных для хранения результатов проверки на соответствие контрольным показателям. XCCDF призван обеспечить единую основу для составления списков проверки по безопасности, контрольных показателей и других руководств по конфигурации и тем самым содействовать более широкому применению передового опыта обеспечения безопасности. Документы XCCDF составляются на языке XML.	[b-XCCDF]
Перечень общеизвестных платформ (CPE)	Перечень общеизвестных платформ (CPE) представляет собой стандартный метод определения и описания программных систем и аппаратных устройств, имеющихся в перечне ресурсов вычислительной техники предприятия. CPE обеспечивает: спецификацию наименования, включая логическую структуру имен CPE в правильном формате, а также процедуры увязывания этих имен и устранения увязки между ними путем кодирования в машинно-читаемом виде; спецификацию совмещения, которая определяет процедуры сравнения имен CPE для определения того, относятся ли они к некоторым одинаковым продуктам или платформам или к ним всем; а также спецификацию словаря, которая определяет концепцию словаря идентификаторов и предписывает высокоуровневые правила для кураторов словаря.	[b-CPE]
Перечень общеизвестных конфигураций (CCE)	Перечень общеизвестных конфигураций обеспечивает уникальные идентификаторы задач, связанных с конфигурацией системы, с тем чтобы облегчить быстрое и точное сопоставление данных конфигурации для многих источников информации и инструментальных средств. Например, идентификаторы CCE могут использоваться для связывания данных проверок, выполняемых инструментальными средствами оценки конфигурации, с инструкциями, содержащимися в документах по передовому опыту в области конфигурации.	[b-CCE]

Таблица I.1 – Методы блока обмена, касающегося слабых мест, уязвимости и состояния

Метод	Описание	Справочные документы
Формат обмена результатами оценки (ARF)	Формат обмена результатами оценки (ARF) является открытой спецификацией, которая обеспечивает структурированный язык обмена данными результатов оценки по каждому устройству, осуществляемого между инструментальными средствами оценки, базами данных по ресурсам и другими продуктами, управляющими информацией о ресурсах. Этот формат предназначен для использования инструментальными средствами сбора подробных данных о конфигурации ИТ-ресурсов. Кроме того, формат ARF включает спецификацию сводной отчетности, которая позволяет представлять отчет, содержащий информацию о многих ресурсах, а также язык формулировки задач и запросов, который позволяет запрашивать результаты оценки. Спецификации автоматизированного управления безопасностью описывают сквозной процесс доставки данных оценки в массивы данных, запрашивания оценки этой информации, представления отчетов о результатах этих оценок, а также составления сводных результатов оценки на уровне предприятия.	[b-ARF]

Таблица I.2 – Методы блока обмена, касающегося события, инцидента и эвристики

Метод	Описание	Справочные документы
Описание общих событий (CEE)	В методе описания общих событий представлены стандартные способы описания, регистрации и обмена компьютерными событиями. С помощью общего языка и синтаксиса CEE можно более эффективно осуществлять в масштабах всего предприятия управление регистрацией, сопоставление, свод данных, проверку и обработку инцидентов, а также добиваться в этом более высоких результатов. Главная цель этих мер состоит в стандартизации представления журналов регистрации, создаваемых электронными системами, и обмене этими журналами. В CEE запись и обмен журналами регистрации подразделяется на четыре (4) составляющие: таксономия событий, синтаксис журнала регистрации, транспортирование журнала регистрации, а также рекомендации в отношении регистрации.	[b-CEE]
Формат обмена описаниями инцидентов (IODEF)	В формате обмена описаниями инцидентов определено представление данных, обеспечивающее основу для обмена информацией об инцидентах компьютерной безопасности, которой обычно обмениваются группы CIRT. В IODEF описана модель информации и представлена соответствующая модель данных, определенная в виде схемы XML.	[b-IETF RFC 5070]

Таблица I.2 – Методы блока обмена, касающегося события, инцидента и эвристики

Метод	Описание	Справочные документы
Формат, касающийся фишинга, мошенничества и неправомерного использования	Формат обмена, касающийся фишинга, мошенничества и неправомерного использования, является расширением формата обмена описаниями инцидентов (IODEF), обеспечивающим представление отчетов о фишинге, мошенничестве и неправомерном использовании. Кроме того, эти расширения обеспечивают стандартный формат для обмена информацией об инцидентах, связанных с широким распространением спама. Эти расширения являются достаточно гибкими, чтобы поддерживать информацию, собранную по видам деятельности на всем цикле распространения мошенничества или спама. Имеется возможность представления как простого отчета, так и полного отчета об экспертно-техническом анализе, а также объединения многих инцидентов. ПРИМЕЧАНИЕ. – В настоящей Рекомендации описаны только методы, касающиеся одинаково понимаемых гарантированных средств, предназначенных для обмена информацией о кибербезопасности между объектами кибербезопасности. В ней отсутствует описание видов использования данной информации.	[b-IETF RFC 5901]
Перечень и классификация общеизвестных схем атак (CAPEC)	CAPEC является методом спецификации, предназначенным для определения, описания и составления перечня схем атак. Схемы атак являются высокоэффективным средством, позволяющим получать и представлять информацию о подходах, используемых злоумышленником. Эти схемы являются описаниями общеизвестных методов использования программного обеспечения. Они выводятся из схем проектных решений, применяемых деструктивным, а не конструктивным образом, и вырабатываются на основе углубленного анализа конкретных примеров реальных эксплойтов. Цель CAPEC – обеспечить общедоступный каталог схем атак наряду с комплексной схемой XML и классификационной таксономией.	[b-CAPEC]
Формат перечня и характеристик атрибутов вредоносного программного обеспечения	Формат перечня и характеристик атрибутов вредоносного программного обеспечения (MAEC) является формальным языком, который включает схему, обеспечивающую синтаксис общего словаря использования перечисленных атрибутов и видов поведения, а также формат взаимного обмена структурированной информацией об этих элементах данных. Перечни находятся на разных уровнях абстракции: действия низкого уровня, поведения среднего уровня и механизмы высокого уровня. На самом нижнем уровне MAEC описаны атрибуты, связанные с базовыми функциональными возможностями и низкоуровневым функционированием вредоносного программного обеспечения. На среднем уровне языка MAEC указанные выше действия низкого уровня объединены по группам в целях определения поведения на среднем уровне. На более концептуальном высоком уровне словарь MAEC позволяет создавать механизмы, которые абстрагируют блоки поведения вредоносного программного обеспечения на среднем уровне, основываясь на достижении классификации более высокого порядка.	[b-MAEC]

Таблица I.3 – Методы блока обмена, касающегося политики

Метод	Описание	Справочные документы
Протокол маркировки информации (TLP)	Протокол маркировки информации (TLP) был создан для обеспечения более интенсивного обмена критичной информацией. Отправитель указывает, насколько широко требуется распространять его информацию помимо непосредственных получателей. Протокол TLP обеспечивает простой метод выполнения этой задачи. Этот протокол предназначен для того, чтобы усовершенствовать поток информации между физическими лицами, организациями или сообществами контролируемым и доверенным образом. Протокол TLP базируется на принципе маркировки информации отправителем с использованием одного из четырех цветов, для того чтобы указать на то, какое дальнейшее распространение, если оно необходимо, может осуществить получатель. Если требуется более широкое распространение, получатель должен проконсультироваться с отправителем. Протокол TLP принят в качестве модели доверенного обмена информацией среди сообществ по вопросам безопасности в более чем 30 странах. Для обработки критичной информации используются следующие четыре "уровня обмена информацией": КРАСНЫЙ ЦВЕТ. – Личное пользование. Данная информация предназначена только для указанных получателей. Например, в контексте собрания "КРАСНАЯ" информация предназначена только для присутствующих. В большинстве обстоятельств "КРАСНАЯ" информация передается устно или при личной встрече. ЖЕЛТЫЙ ЦВЕТ. – Ограниченная рассылка. Получатель может обмениваться "ЖЕЛТОЙ" информацией с другими лицами в рамках своей организации, но только на основе принципов доступа к специальной информации. ЗЕЛЕНЫЙ ЦВЕТ. – Рассылка в рамках сообщества. Информация этой категории может распространяться в рамках того или иного конкретного сообщества. Вместе с тем эта информация не может быть опубликована или размещена в интернете и не может быть разглашена за пределами сообщества. БЕЛЫЙ ЦВЕТ. – Неограниченная рассылка. При условии соблюдения стандартных плавил, касающихся авторского права, "БЕЛАЯ" информация может распространяться свободно и без ограничений.	[b-TLP]

Таблица I.4 – Методы блока, касающегося идентификации, обнаружения и запроса

Метод	Описание	Справочные документы
Механизмы обнаружения информации о кибербезопасности при обмене	Эти методы включают: методы и механизмы, которые могут использоваться для определения и локализации источников информации о кибербезопасности; типы информации о кибербезопасности; конкретные экземпляры информации о кибербезопасности; методы, которые могут использоваться для доступа к информации о кибербезопасности, а также принципы политики, которые могут применяться в отношении доступа к информации о кибербезопасности.	
Руководящие указания по администрированию выпуска OID для обмена информацией о кибербезопасности	Описывается пространство имен для общих глобальных идентификаторов кибербезопасности, а также административные требования, применяемые в рамках согласованного выпуска OID; также включены идентификаторы для: • информации о кибербезопасности; • организации кибербезопасности; • политики кибербезопасности.	

Таблица I.4 – Методы блока, касающегося идентификации, обнаружения и запроса

Метод	Описание	Справочные документы
Язык запросов информации о кибербезопасности	В языке запросов информации о кибербезопасности (CYIQL) определено гибкое представление данных, обеспечивающее основу для обмена информацией об инцидентах компьютерной безопасности, которой обычно обмениваются группы реагирования на компьютерные инциденты (CIRT). В данной спецификации описана модель информации для CYIQL и представлена соответствующая модель данных, определенная в виде схемы XML.	

Таблица I.5 – Методы блока, касающегося гарантии идентичности

Метод	Описание	Справочные документы
Доверенные платформы	Вычислительные и коммуникационные продукты со встроенными модулями доверенных платформ (TPM) повышают возможности предприятий, учреждений, правительственных органов и потребителей по осуществлению заслуживающего доверия информационного обмена; в связи с этим модули TPM актуальны для большинства реализаций CYBEX. TPM представляют собой встраиваемые в различные платформы интегральные схемы (ИС) специального назначения, которые позволяют осуществлять строгую аутентификацию пользователя и машинную аттестацию, что является важным для предотвращения ненадлежащего доступа к конфиденциальной и критичной информации, а также для защиты от взлома сетей. Технология модуля доверенной платформы базируется на открытых стандартах, с тем чтобы в среде, состоящей из оборудования разных поставщиков, обеспечивалась функциональная совместимость различных продуктов. Общепринятый стандарт TPM состоит из набора спецификаций, которые разрабатываются и ведутся некоммерческой организацией Trusted Computing Group (TCG), наряду с профилем безопасности, используемым для оценки безопасности в соответствии с общими критериями. Принципы разработки обеспечивают основные понятия о TPM, а также общую информацию относительно функциональной возможности TPM. Разработчик TPM должен проанализировать и реализовать на практике информацию, содержащуюся в главной спецификации TPM (части 1–3), а также проанализировать зависящий от платформы документ, который касается конкретной платформы. В зависящем от платформы документе содержатся нормативные инструкции, которые затрагивают разработку и реализацию TPM. Разработчик TPM должен проанализировать и реализовать требования, в том числе по проверке и оценке, устанавливаемые рабочей группой TCG по вопросам соответствия. TPM должен соответствовать требованиям и пройти любую оценку, предусмотренную рабочей группой по вопросам соответствия. TPM может быть подвергнут более жесткой проверке и оценке.	[b-TPM]

Таблица I.5 – Методы блока, касающегося гарантии идентичности

Метод	Описание	Справочные документы
Доверенное подключение к сети	В рамках мер по обеспечению безопасности ИКТ часто желательно выяснить состояние уровня операционной системы (ОС), а также прикладного программного обеспечения, используемого опорной сетью. Например, когда системе недостаточно корректировок безопасности ОС или сигнатур антивирусов, чрезвычайно важным является получение надежных уведомлений для ограничения ущерба, связанного с сетевыми атаками. Для выполнения данной оценки требуется надежная информация о том, что подключаемая система находится в определенном состоянии. Чтобы не допустить фальсификации информации системой (например, взломанной системой), для успешной оценки требуется аппаратная основа оценки этой системы. В аппаратное обеспечение встраиваются доверенные платформы, которые записывают определенные данные о процессе загрузки и осуществляют их доставку, удостоверяемую цифровой подписью. Кроме того, в настоящее время основные производители чипов дополняют доверенные платформы возможностью "позднего запуска", которая позволяет выполнять доверенный код на более позднем этапе загрузочной последовательности. Это в свою очередь позволяет обеспечить надежную запись событий после аппаратно-зависимого процесса загрузки. Фактически управление конфигурацией сети представляет собой ввод в действие аттестации системы – программных агентов, устанавливаемых на компьютерах предприятия. Агенты периодически направляют отчеты о конфигурации в центральное хранилище, в котором осуществляется аттестация систем и помечаются системы, не соответствующие требованиям безопасности. Несмотря на ценность данных, полученных от этих программных агентов, они могут быть легко изменены злоумышленником. Благодаря повсеместному вводу в действие доверенных платформ для обеспечения более достоверной оценки состояния системы, как правило, существенно повышается уверенность предприятия в своих данных об управлении конфигурацией. Доверенное подключение к сети (TNC) является открытой архитектурой, предназначенной для контроля доступа к сети. Его цель – позволить операторам сетей обеспечить целостность конечной точки при любом подключении к сети. Тем самым обеспечивается функциональная совместимость конечных точек в неоднородной сети.	[b-TNC]
Гарантия аутентификации объекта	Настоящий стандарт предоставляет структуру жизненного цикла аутентификации в целях управления гарантией идентичности объекта, а также связанную с ним информацию об идентичности в заданном контексте. В частности, стандарт обеспечивает методы, позволяющие: 1) количественно оценивать и присваивать идентичностям объекта и относящейся к нему информации об идентичности относительные уровни гарантии аутентификации; и 2) представлять относительные уровни гарантии аутентификации.	[b-NIST EAA]
Система сертификатов с расширенной валидацией	Система сертификатов с расширенной валидацией состоит из интегральной совокупности технологий, протоколов, проверки подлинности идентичности, управления жизненным циклом и аудиторской практики. В ней описываются минимальные требования, которые должны выполняться для того, чтобы выпускать и сохранять сертификаты с расширенной валидацией (EVC), касающиеся рассматриваемой организации. Эта система содержит широкий круг требований в отношении безопасности, локализации и уведомления.	[b-EVCERT]

Таблица I.5 – Методы блока, касающегося гарантии идентичности

Метод	Описание	Справочные документы
Политические требования к сертификационным органам, выпускающим сертификаты открытых ключей	В указанном документе определяются политические требования к сертификационным органам (CA), выпускающим сертификаты открытых ключей, включая сертификаты с расширенной валидацией (EVC). В нем определяются политические требования в отношении работы и управленческой практики сертификационных органов, выпускающих сертификаты и управляющих ими, таким образом, чтобы абоненты, сертифицированные CA субъекты и полагающиеся стороны могли быть уверены в применимости сертификата, сопровождающего криптографические механизмы.	[b-ETSI TS 102 042]

Таблица I.6 – Методы, относящиеся к блоку протокола обмена

Метод	Описание	Справочные документы
Межсетевая защита в реальном времени (RID)	Межсетевая защита в реальном времени (RID) обеспечивает систему для обмена информацией об инцидентах. Стандарт RID обеспечивает набор сообщений координации при инцидентах, необходимых для безопасного обмена документами в формате IODEF между объектами. RID является оболочкой для документов в формате IODEF, включая любые его расширения. Стандартные форматы сообщений и обмена включают опции/параметры безопасности, конфиденциальности и политики, которые необходимы в глобальной схеме координации при инцидентах. RID является уровнем безопасности между документами в формате IODEF и транспортным протоколом. Вопрос о выборе транспортного протокола решается объектами, обменивающимися информацией об инцидентах. Транспортным протоколом может быть указанный транспортный протокол RID (HTTP/TLS), BEEP, SOAP или протокол, который будет определен в дальнейшем.	[b-IETF RFC 6045]
Транспортировка сообщений, касающихся межсетевой защиты в реальном времени (RID)	В этом механизме определена транспортировка сообщений, касающихся межсетевой защиты в реальном времени (RID), в рамках сообщений, содержащих запросы и ответы HTTP, которые передаются поверх протокола TLS.	[b-IETF RFC 6046]
Профиль протокола для расширяемого обмена блоками информации (BEEP) в рамках CYBEX	В методах на основе профиля BEEP для обмена информацией о кибербезопасности определены профили BEEP, используемые в рамках CYBEX. Протокол BEEP является общим ядром прикладного протокола асинхронных взаимодействий на основе соединения, описанным в [b-IETF RFC 3080]. Основу BEEP составляет фреймовый механизм, который позволяет осуществлять одновременный независимый обмен сообщениями между одноуровневыми объектами. Все обмены осуществляются в контексте канала, при увязке с четко определенным аспектом приложения, например безопасностью транспортного уровня, аутентификацией пользователя или обмен данными. Каждому каналу соответствует "профиль", который определяет синтаксис и семантику сообщений, которыми осуществляется обмен.	[b-IETF RFC 3080]

Таблица I.6 – Методы, относящиеся к блоку протокола обмена

Метод	Описание	Справочные документы
Простой протокол доступа к объектам (SOAP) в рамках CYBEX	Протокол SOAP является упрощенным протоколом обмена информацией в децентрализованной распределенной среде. Этот протокол базируется на XML и состоит из трех частей: конверта, определяющего структуру описания того, что содержится в сообщении, и каким образом это следует обрабатывать; набора кодирующих правил для описания экземпляров типов данных, определенных в приложении; а также соглашения, касающегося представления дистанционных вызовов процедур и ответов. Протокол SOAP может потенциально использоваться в сочетании со многими другими протоколами; однако определенные в этом документе увязки описывают только то, как использовать SOAP в сочетании с HTTP и с системой расширения HTTP.	[b-W3C SOAP]

Дополнение II

Онтология обмена информацией о кибербезопасности

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В Дополнении II представлена онтология обмена информацией о кибербезопасности. Она иллюстрирует условия, в которых осуществляется CYBEX, и формирует действенную экосистему кибербезопасности, в которой извлекаемые из отчетов, проверок и опыта знания используются для создания и развития информации о слабых местах и уязвимости, которая в свою очередь может использоваться, вместе с информацией о состоянии системы, для измерения и повышения безопасности.

В онтологии CYBEX определены следующие термины:

1 **Операции кибербезопасности**: методы и процессы, используемые для мониторинга безопасности и управления обеспечением безопасности в рамках определенных рабочих пределов, которые включают:

- сбор и анализ информации, которая может влиять на безопасность;
- обнаружение поведения или событий, которые негативно влияют на безопасность либо по которым можно определить вероятность будущего негативного влияния;
- меры, принимаемые в том случае, если имеет место негативное поведение или событие, с тем чтобы ограничить будущие инциденты, смягчить их последствия и/или предотвратить их;
- обмен информацией по вопросам безопасности, касающейся статуса и состояния систем.

2 **Объект кибербезопасности**: любой объект, который участвует в обмене информацией о кибербезопасности, включая сам информационный объект.

3 **Оперативная информация о кибербезопасности**: любая информация, которая необходима для того, чтобы объекты кибербезопасности выполняли операции кибербезопасности.

Далее в онтологии CYBEX приведено удобное описание методов обеспечения кибербезопасности, указанных в разделе по CYBEX, т. е. показана модель описания обобщенной области операций кибербезопасности. Онтология состоит из набора типов, свойств и отношений (см. рисунок II.1). Сплошными линиями обозначены отношения между типами информации, а стрелки показывают входные информационные сигналы от функциональных объектов к базам знаний/базам данных. Изображенные справа функциональные объекты являются типовыми, и такие объекты, как CIRT, могут выполнять одну или несколько из этих функций.

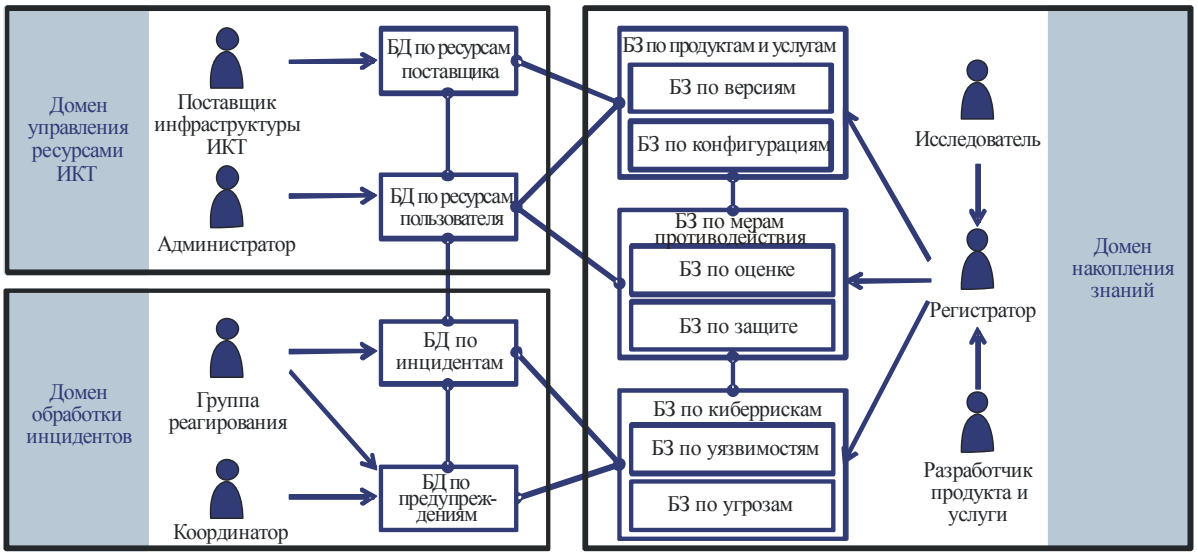

Рисунок II.1 – Модель онтологии CYBEX

В данной онтологии использована модель, определяющая домены операций кибербезопасности, которые далее применяются для идентификации требуемых объектов кибербезопасности, поддерживающих операции в каждом домене. В следующих пунктах приведено подробное описание онтологии, в котором показано, как могут использоваться методы CYBEX для обеспечения этой онтологии.

II.1 Домены операций

Операции кибербезопасности состоят главным образом из трех доменов: обработки инцидентов, управления ресурсами ИКТ и накопления знаний.

Домен обработки инцидентов включает обнаружение и реагирование на инциденты кибербезопасности путем мониторинга инцидентов, компьютерных событий, которые образуют инциденты, а также поведения при атаке, выявленного в инцидентах. Например, домен обнаруживает аномалии в оповещениях от детекторов и далее объединяет подробные данные путем сбора разных журналов. Иногда он выдает оповещения и инструкции, например ранние предупреждения о возможных угрозах для организаций-пользователей.

Домен управления ресурсами ИКТ включает операции кибербезопасности, осуществляемые в рамках каждой организации-пользователя, такие как установка и настройка ресурсов ИКТ организации, а также управление ими. Домен включает как операции по предотвращению инцидентов, так и операции по контролю ущерба, осуществляемые в каждой организации.

Домен накопления знаний включает информацию о кибербезопасности. В нем создаются и накапливаются многократно используемые знания организаций.

II.2 Объекты кибербезопасности

С учетом описанных выше доменов операций можно определить функциональные объекты кибербезопасности, которые необходимы для выполнения операций кибербезопасности в каждом домене.

В домене обработки инцидентов существуют два объекта, выполняющих его операции: группа реагирования и координатор. Группа реагирования является объектом, который осуществляет мониторинг и анализ различных видов инцидентов, например несанкционированного доступа, атак DDoS и фишинга, а также накопление информации об инцидентах. На основе данной информации группа реагирования может осуществлять меры противодействия, например, заносить адреса фишинговых сайтов в черные списки. Координатор является объектом, который координирует деятельность с другими объектами и решает проблемы потенциальных угроз, исходя из известной информации об инцидентах.

В домене управления ресурсами ИКТ существует два объекта операций: администратор и поставщик инфраструктуры ИКТ. Администратор осуществляет административное управление системой своей организации и обладает информацией о своих собственных ресурсах ИКТ. Типичным экземпляром администратора в рамках каждой организации является администратор по ИКТ. Поставщик инфраструктуры ИКТ обеспечивает для каждой организации инфраструктуру ИКТ, которая включает сетевые соединения, услуги облачных вычислений, например программное обеспечение как услугу (SaaS), платформу как услугу (PaaS) и инфраструктуру как услугу (IaaS), а также услуги определения идентичности. Типичными экземплярами являются поставщик услуг интернета (ISP) и поставщик прикладных услуг (ASP).

В домене накопления знаний существует три объекта операций: исследователь, разработчик продукта и услуги и регистратор. Исследователь выполняет исследование информации о кибербезопасности, извлекая и накапливая знания. Разработчик продукта и услуги обладает информацией о продуктах и услугах, например о названиях, версиях, их уязвимостях, корректировках и конфигурации. Типичными экземплярами являются поставщики программного обеспечения, ASP и индивидуальные программисты. Регистраторы – это объекты, которые классифицируют и упорядочивают знания о кибербезопасности, представленные исследователями, разработчиками и поставщиками, таким образом, чтобы они могли использоваться какой-либо другой организацией.

II.3 Оперативная информация о кибербезопасности

С учетом описанных выше доменов операций и объектов, в данном пункте представлены более подробные сведения об оперативной информации о кибербезопасности, обеспечиваемой функциональными объектами в каждом домене операций.

II.3.1 Домен обработки инцидентов

В домене обработки инцидентов существует база данных по инцидентам и база данных по предупреждениям. В базе данных по инцидентам содержится информация об инцидентах, представленная группой реагирования. В ней содержится три вида записей: о событии, инциденте и атаке. Запись о событии включает компьютерные события, например вход в систему привилегированных пользователей. Кроме того, в ней содержится информация о пакетах, файлах и транзакциях, относящихся к инциденту. Как правило, большинство записей предоставляется компьютерами автоматически. Запись об инциденте включает события, которые, возможно, являются инцидентами. Эта запись, как правило, образуется из нескольких записей о событии и их гипотез, которые создаются автоматически и/или вручную. Запись об атаке основывается на анализе инцидентов и включает точную дату и время атак, а также их последовательности.

База данных по предупреждениям включает информацию о предупреждениях кибербезопасности, предоставляемых группой реагирования и координатором. Предупреждения основываются на базе данных по инцидентам, а также на базе знаний по киберрискам.

II.3.2 Домен управления ресурсами ИКТ

В домене управления ресурсами ИКТ находится две базы данных: база данных по ресурсам пользователя и база данных по ресурсам поставщика.

В базе данных по ресурсам пользователя накапливается информация о ресурсах в рамках отдельной организации. В ней содержится такая информация, как список программного и аппаратного обеспечения и их конфигураций, статус использования ресурсов, принципы политики, в том числе политики управления доступом, результаты оценки уровня безопасности, а также топология интранета. Эта информация предоставляется администратором.

В базе данных по ресурсам поставщика накапливается информация о ресурсах, расположенных за пределами отдельной организации. В ней содержится, главным образом, информация о внешних ресурсах и информация о внешней сети. Информация о внешних ресурсах включает информацию о ресурсах, которые используются каждой организацией за пределами своей организации, например список и статус внешних облачных услуг (например, центр данных и SaaS). Информация о внешней сети содержит информацию о сетях, которые соединяют каждую организацию с другими организациями, например об их топологии, информацию о маршрутизации, политике управления доступом, статусе трафика и уровне безопасности. Эта информация предоставляется поставщиком инфраструктуры ИКТ.

II.3.3 Домен накопления знаний

В домене накопления знаний существует три базы знаний: по киберрискам, мерам противодействия и по продуктам и услугам. В этих базах накапливаются знания о кибербезопасности, представляемые исследователем, а также разработчиком продукта и услуги, которые затем упорядочиваются и классифицируются регистратором.

В базе знаний по киберрискам накапливается информация о рисках кибербезопасности. Она включает в себя базы знаний по уязвимостям и по угрозам. В базе знаний по уязвимостям накапливается известная информация об уязвимостях, включая наименования, таксономию и перечень известных уязвимостей. Кроме того, в нее включены уязвимости, обусловленные человеческим фактором, которые исходят от людей как пользователей ИКТ. В базе знаний по угрозам накапливается информация об известных угрозах, которая включает знания об атаках и знания о ненадлежащем использовании. Знания об атаках включают информацию о схемах атак, инструментальных средствах атак (например, вредоносном программном обеспечении) и их тенденциях, например информацию о тенденциях имевших место ранее атак с точки зрения их географии и целей. Кроме того, эти знания включают статистическую информацию об имевших место ранее атаках. Знания о ненадлежащем использовании включают информацию о видах ненадлежащего использования ИКТ, обусловленного действиями физических лиц – пользователей, не имеющих злого умысла. Сюда входит информация об ошибках при вводе с клавиатуры, случаях попадания в фишинговую ловушку, а также о нарушениях требований.

В базе знаний по мерам противодействия накапливается информация о мерах противодействия рискам кибербезопасности. Она включает две базы знаний: по оценке и по обнаружению/защите. В базе знаний по оценке накапливаются известные правила и критерии оценки уровня безопасности ресурсов ИКТ, а также список проверки конфигураций. В базе знаний по обнаружению/защите накапливаются известные правила и критерии обнаружения угроз кибербезопасности и защиты от них, например сигнатуры IDS/IPS и относящиеся к ним правила обнаружения/защиты.

В базе знания по продуктам и услугам накапливается информация о продуктах и услугах. Она включает две базы знаний: по версиям и по конфигурациям. В базе знаний по версиям накапливается информация о версиях продуктов и услуг, включая названия и перечень их версий. В том, что касается версии продукта, в базу знаний также включаются корректировки безопасности. В базе знаний по конфигурациям накапливается информация о конфигурациях продуктов и услуг. В том, что касается конфигурации продукта, в нее включаются названия, таксономия и перечень известных конфигураций.

В каждой из упомянутых выше баз данных и баз знаний могут использоваться различные методы описания информации, показанные на рисунке II.2.

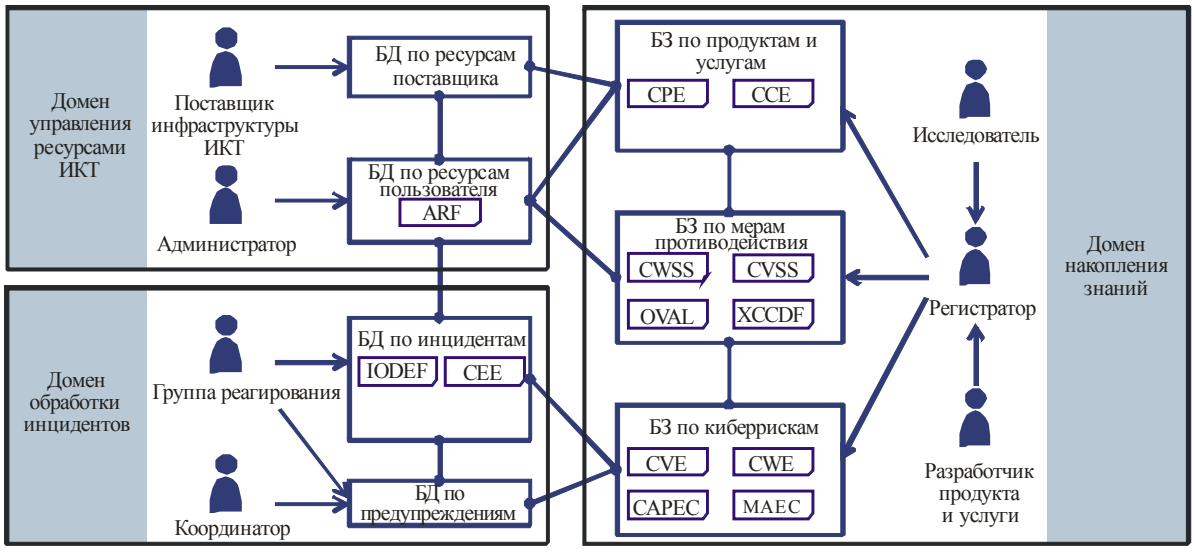

Рисунок II.2 – Подробное изображение модели онтологии CYBEX с указанием методов

Дополнительная информация об онтологии CYBEX представлена в [b-Takahashi].

Дополнение III

Примеры схем автоматизации управления безопасностью в CYBEX

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В Дополнении III представлены два примера схем автоматизации управления безопасностью. Эти средства могут использоваться для создания специальных конкретизаций CYBEX, включающих автоматическую обработку известных безопасных или доверенных "состояний" программного обеспечения, служб и систем, обнаружение вредоносного программного обеспечения, получение информации об инцидентах и эвристике.

Ожидается появление большого числа реализаций, в частности схем автоматизации управления безопасностью, обеспечивающих надлежащую конфигурацию и корректировку систем ИКТ. Первыми двумя известными примерами являются:

1) протокол автоматизации управления данными безопасности (SCAP), разработанный Национальным институтом стандартов и технологий (NIST) США для реализации Базовой конфигурации федеральных настольных систем (FDCC) и пришедшей ей на замену Базовой версии конфигурации для правительства Соединенных Штатов (USGCB); и

2) система автоматизации управления безопасностью, разработанная японским сайтом-порталом JVN.

В настоящем Дополнении приведено краткое описание каждого из этих примеров. Данные реализации инструментальных средств автоматизации управления безопасностью, в общем, имеют вид, показанный на рисунке III.1, и содержат разное количество платформ обмена информацией CYBEX, представленных на этой диаграмме наложенными указателями-стрелками.

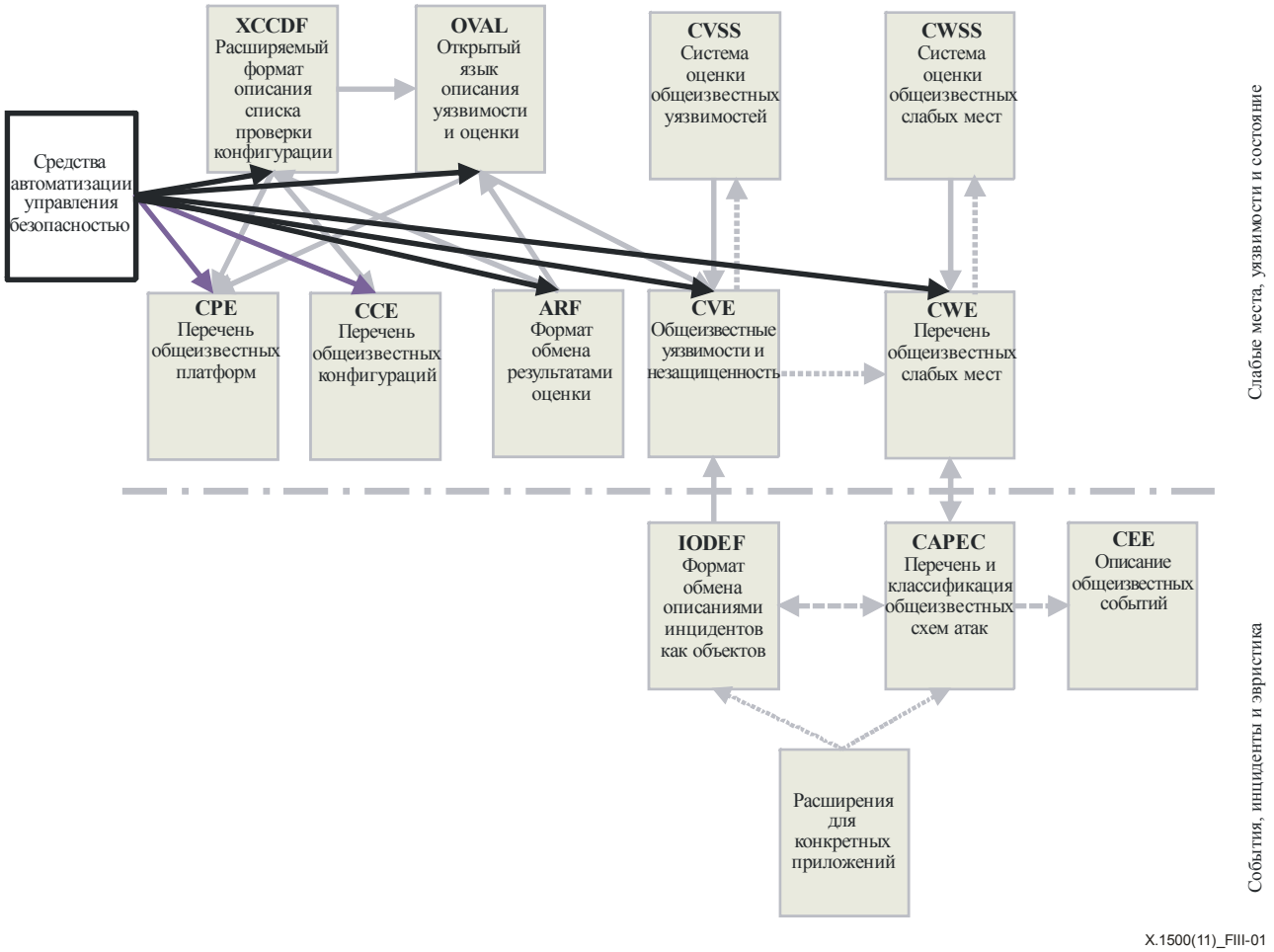

Рисунок III.1 – Автоматизация управления гарантией и целостностью кибербезопасности

III.1 Пример: Базовая конфигурация федеральных настольных систем США/Базовая версия конфигурации для правительства Соединенных Штатов

Базовая конфигурация федеральных настольных систем (FDCC) и пришедшая ей на замену Базовая версия конфигурации для правительства Соединенных Штатов (USGCB), в которых используется Протокол автоматизации управления данными безопасности (SCAP), включают спецификации по организации и выражению в стандартной форме информации о безопасности, а также соответствующие справочные данные, например уникальные идентификаторы уязвимостей. Целью этих двух инициатив является создание базовых версий конфигураций для продуктов ИКТ, которые повсеместно развернуты в федеральных агентствах. Базовая версия USGCB разработана на основе требований Базовой конфигурации федеральных настольных систем. Инициатива USGCB является реализованной в масштабе федерального правительства инициативой, обеспечивающей для агентств руководство по мерам, которые следует принять для улучшения и обеспечения эффективных параметров конфигурации, уделяя первоочередное внимание безопасности.

В технической спецификации USGCB описаны требования и соглашения, которые следует применять для обеспечения согласованного и точного обмена данными SCAP, а также возможности надежной работы этого контента с подтвержденными инструментальными средствами SCAP. Первоначальная версия состоит из шести спецификаций: XCCDF, OVAL, CPE, CCE, CVE и CVSS. Эти спецификации сгруппированы по трем категориям: языки, перечни, а также системы измерения и оценки уязвимости.

В SCAP реализованы 1) определенный формат и номенклатура, посредством которых программные продукты безопасности представляют информацию о недоработках программного обеспечения и о конфигурации безопасности; и 2) справочные данные о конкретных недоработках программного обеспечения и стандартах конфигурации безопасности, известные как данные SCAP. Цели SCAP включают стандартизацию управления безопасностью системы, обеспечение функциональной совместимости продуктов безопасности, а также содействие использованию стандартных выражений для данных о безопасности. В связи с вероятным появлением многих различных видов данных SCAP, предназначенных для разных систем и уровней безопасности, важными требованиями являются структурированное присвоение меток, обнаружение и проверка с точки зрения обеспечения гарантии действующей схемы. В рамках инициативы USGCB создаются данные и руководства, основанные на спецификациях SCAP.

III.2 Пример: JVN – Японский сайт-портал информации об уязвимости

Аббревиатура JVN расшифровывается как Japan Vulnerability Notes (Сообщения Японии об уязвимостях). На этом сайте-портале представлена информация об уязвимости программного обеспечения, используемого в Японии, и иная сопутствующая информация, которая призвана способствовать реализации мер противодействия киберугрозам. Для того чтобы разработчики программного обеспечения имели возможность использовать данные в рамках открытого интерфейса, на портале JVN используется SCAP и размещается местная (национальная) и международная информация, образующая систему автоматизации управления данными безопасности JVN. Как и в национальной базе данных об уязвимостях (NVD), в каждом информационном сообщении об уязвимости содержится номер CVE, оценка CVSS, а также номер CWS. Кроме того, предоставляется CPE-наименование затронутого продукта.

Система состоит из трех компонентов: MyJVN, JVN и JVN iPedia (см. рисунок III.2), каждый из которых подробно описывается ниже.

В компоненте MyJVN содержится информация о мерах противодействия, предоставляемая с помощью прикладного программного интерфейса (API) MyJVN – машинно-читаемого интерфейса, включающего API на базе веба, а также с помощью инструментальных средств MyJVN, например средства проверки версии Version Checker. Этот компонент улучшает использование информации о мерах противодействия уязвимости, накопленной в JVN и JVN iPedia, за счет упрощенного и более эффективного сбора пользователями своей целевой информации, осуществляемого с помощью таких услуг, как настраиваемая фильтрация, автоматический поиск и создание списка проверки. Кроме того, базирующееся на SCAP инструментальное средство MyJVN Version Checker позволяет людям легко проверить, является ли версия программного обеспечения, установленного на их компьютере, его последней версией.

В компоненте JVN содержится информация о мерах противодействия, а также статус японского разработчика для уязвимостей, о которых сообщено Партнерством по раннему предупреждению информационной безопасности. Это партнерство является партнерством государственного и частного секторов, которое было создано в целях содействия обеспечению безопасности программных продуктов и веб-сайтов, а также предотвращения причинения ущерба, вызванного компьютерными вирусами или несанкционированным доступом, большому числу компьютеров. При сообщении информации об уязвимости в IPA (Агентство содействия развитию информационных технологий Японии) – принимающую сторону этого партнерства информация передается в Координационный центр группы реагирования на компьютерные инциденты (JPCERT/CC), являющийся координационным органом. Центр JPCERT/CC определяет затронутые программные продукты и координирует действия с разработчиками. Когда пользователям становятся доступны решения, устраняющие уязвимость, например корректировки или программные обновления, подробная информация об уязвимости вместе с заявлениями разработчиков публикуются в JVN.

В компоненте JVN iPedia содержится информация о мерах противодействия, полученная в отношении программных продуктов, например операционных систем, приложений, библиотек, а также встроенных систем, используемых в Японии. Целью JVN является предоставление общественности информации об уязвимости и мерах противодействия в возможно короткие сроки. Координационный орган взаимодействует с поставщиками в отношении того, когда предоставлять информацию о новых сообщенных уязвимостях. С другой стороны, задачей JVN iPedia является сбор дополнительной информации об уязвимости и мерах противодействия, ежедневно обнаруживаемой в отношении японских программных продуктов, которая не опубликована на JVN.

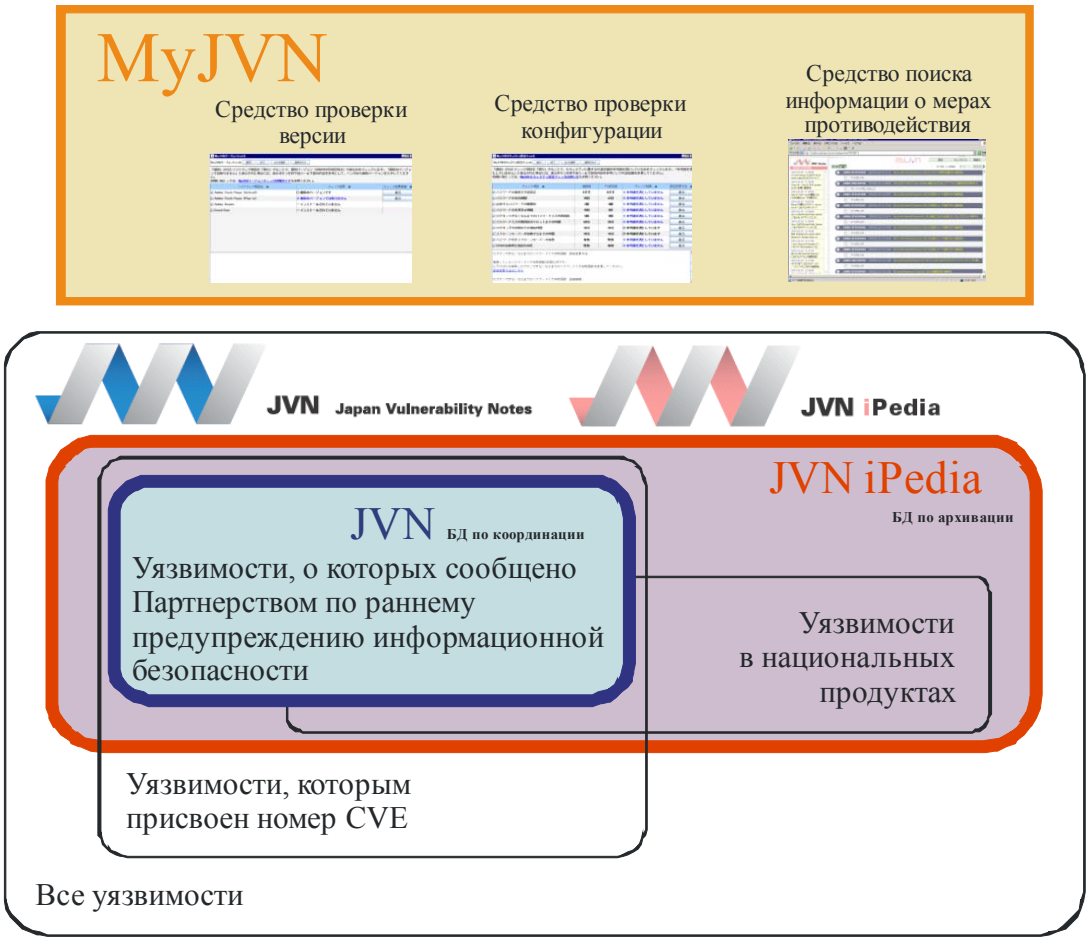

Рисунок III.2 – Концепция системы автоматизации управления данными безопасности JVN

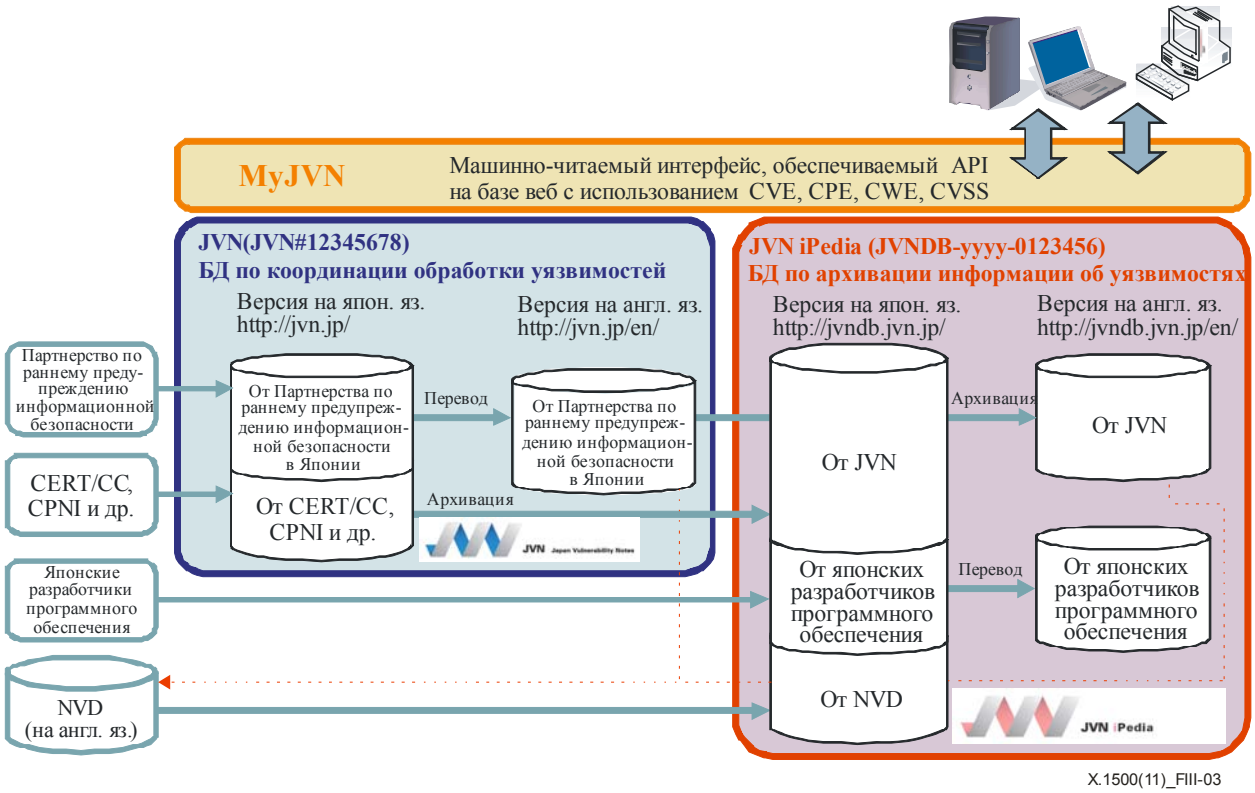

Рисунок III.3 – База данных, содержащая международную и местную информацию

Пользователи, поддерживающие стандартные форматы, например RSS, могут воспользоваться базой данных, содержащей международную и местную информацию (см. рисунок III.3). Из этих трех компонентов MyJVN служит для пользователя интерфейсом, удобному использованию которого содействуют следующие инструментальные средства и API.

Инструментальные средства MyJVN и его API

Инструментальными средствами MyJVN являются инструментальные средства безопасности на основе SCAP, которые улучшают использование пользователями мер противодействия уязвимости и среды обмена информацией. Основными средствами, предлагаемыми в настоящее время, являются:

- **Filtered Vulnerability Countermeasure Information Tool (средство фильтрации информации о мерах противодействия уязвимости)** – Это инструментальное средство способствует улучшенному использованию информации о мерах противодействия уязвимости, накопленной в JVN и JVN iPedia, за счет упрощенного и более эффективного сбора пользователями своей целевой информации, осуществляемого с помощью таких услуг, как настраиваемая фильтрация CPE.
- **Version Checker (средство проверки версии)** – Это средство является онлайновым сканером на базе языка OVAL, который позволяет людям легко проверить, является ли версия программного обеспечения, установленного на их компьютере, его последней версией. С помощью лишь одного щелчка мышью пользователи могут проверить версии нескольких программных модулей. Результаты просты для понимания: "галочка" означает последнюю версию, а "крестик" – устаревшую версию. Если версия программного обеспечения не является последней, пользователь может легко войти на загрузочный сайт разработчика с помощью нескольких щелчков мышью. Средство MyJVN Version Checker поддерживает программные продукты, связанные с использованием интернета, которые были отобраны на основе взаимодействия с поставщиками программного обеспечения.
- **MyJVN Security Configuration Checker (средство проверки конфигурации безопасности)** – Это средство является онлайновым сканером, основанным на XCCDF и OVAL. Оно является бесплатным и удобным в использовании инструментальным средством доступа к настройкам параметров безопасности в Windows, в том числе к политикам учетных записей, таким как минимальная длина пароля, срок действия пароля, автоматическое включение заставки, функция автозапуска для устройства USB и т. д.

- **MyJVN API –** Этот API является программным интерфейсом для доступа и использования информации о мерах противодействия уязвимости, хранящейся в JVN и JVN iPedia. Для того чтобы разработчики приложений имели возможность использовать данные в рамках открытого интерфейса, JVN iPedia приняла SCAP – набор стандартов для описания информации о мерах противодействия уязвимости. С помощью MyJVN API любые клиентские приложения могут получать доступ к данным JVN iPedia, а в различных услугах по управлению уязвимостями теперь может эффективно использоваться информация о мерах противодействия уязвимости.

  Основными функциями API MyJVN являются API услуги фильтрации информации, а также API услуги сотрудничества SCAP. Первый API поддерживает функции "Get list of products" (получить список продуктов), "Get list of vulnerability overviews" (получить список обзоров уязвимостей) и другие, которые используются средством Filtered Vulnerability Countermeasure Information Tool. Второй API поддерживает функции "Get list of OVAL definitions" (получить список определений OVAL), "Get data of OVAL definition" (получить данные определения OVAL) и другие, которые используются средствами MyJVN Version Checker и MyJVN Security Configuration Checker.

  Дополнительная информация о JVN представлена в статье [b-Terada].

Библиография

[b-ITU-T E.409] Рекомендация МСЭ-Т E.409 (2004 г.), *Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1205] Рекомендация МСЭ-Т X.1205 (2008 г.), *Обзор кибербезопасности*.

[b-ITU-T X.1520] Рекомендация МСЭ-Т X.1520 (2011 г.), *Общеизвестные уязвимости и незащищенность.*

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system*.

[b-ETSI TS 102 042] ETSI TS 102 042 (2011), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*.

[b-IETF RFC 3080] IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core*. http://datatracker.ietf.org/doc/rfc3080/

[b-IETF RFC 5070] IETF RFC 5070 (2007), *The Incident Object Description Exchange Format*. http://datatracker.ietf.org/doc/rfc5070/

[b-IETF RFC 5901] IETF RFC 5901 (2010), *Extensions to the IODEF-Document Class for Reporting Phishing*. http://datatracker.ietf.org/doc/rfc5901/

[b-IETF RFC 6045] IETF RFC 6045 (2010), *Real-time Inter-network Defense (RID)*. http://datatracker.ietf.org/doc/rfc6045/

[b-IETF RFC 6046] IETF RFC 6046 (2010), *Transport of Real-time Inter-network Defense (RID) Messages*. http://datatracker.ietf.org/doc/rfc6046/

[b-ARF] Assessment Results Format. https://measurablesecurity.mitre.org/incubator/arf/

[b-CAPEC] Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/

[b-CCE] Common Configuration Enumeration. https://cce.mitre.org/

[b-CEE] Common Event Expression. https://cee.mitre.org/

[b-CPE] Common Platform Enumeration. https://cpe.mitre.org/

[b-CWE] Common Weakness Enumeration. https://cwe.mitre.org/

[b-CWSS] Common Weakness Scoring System. https://cwe.mitre.org/cwss/

[b-EVCERT] CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3

[b-MAEC] Malware Attribute Enumeration and Characterization. https://maec.mitre.org/

[b-NIST EAA] *Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.2, April 2006

[b-OVAL] Open Vulnerability and Assessment Language. https://oval.mitre.org/

[b-Takahashi] Takahashi, T., Kadobayashi, Y., and Fujiwara, H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks, September.

[b-Terada] Terada, Masato, et al. (2009), *Proposal of MyJVN (Web Service APIs) for Security Information Exchange infrastructure*, 21st Annual FIRST Conference on Computer Security Incident Handling, June.
http://jvnrss.ise.chuo-u.ac.jp/jtg/doc/21thFirstConference_paper.pdf

[b-TLP] *CPNI Traffic Light Protocol* (2010), Information Sharing Levels, CPNI Information Exchange, UK, April.

[b-TNC] Trusted Computing Group, *Trusted Network Connect*.

Integrity Measurement Collectors – TCG Version (IF-IMC, Specification Ver. 1.2 Rev. 8, 5 Feb. 2007)

Integrity Measurement Verifiers – TCG Version (IF-IMV Specification Ver. 1.2 Rev. 8, 5 Feb. 2007)

Trusted Network Connect Client-Server – TCG Version (IF-TNCCS TLV Binding Specification Ver. 2.0 Rev. 16, 22 Jan. 2010)

Trusted Network Connect Client-Server Statement of Health – TCG Version (IF-TNCCS-SOH TLV Binding Specification Ver. 2.0 Rev. 10, 23 Jan. 2008)

Policy Enforcement Point – TCG Version (IF-PEP Protocol Bindings for RADIUS Specification Ver. 1.1 Rev. 0.7, 5 Feb. 2007)

Binding for SOAP – TCG Version (IF-MAP Specification Ver. 2.0 Rev. 36, 30 July 2010)

Platform Trust Services Interface – TCG Version (IF-PTS Specification Ver. 1.0 Rev. 1.0, 17 Nov. 2006)

Clientless Endpoint Support Profile – TCG Version (CESP Specification Ver. 1.0 Rev. 13, 18 May 2009)

[b-TPM] Trusted Computing Group, *Trusted Platform Modules*.

Design Principles – TCG Version (TPM Main, Part 1, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-2, 2009-05-15, Information technology – TPM – Part 2)

TPM Structures – TCG Version (TPM Main, Part 2. Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-3, 2009-05-15, Information technology – TPM – Part 3)

Commands – TCG Version (TPM Main, Part 3, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-4, 2009-05-15, Information technology – TPM – Part 4)

The TPM 1.2 specifications have also been adopted as ISO/IEC 11889. Overview – TCG Version (N/A), ISO/IEC Version (11889-1, 2009-05-15, Information technology – TPM – Part 1)

[b-W3C SOAP] W3C Recommendation Simple Object Access Protocol (SOAP), 2007.

SOAP Version 1.2 Part 1: Messaging Framework.

SOAP Version 1.2 Part 2: Adjuncts.

[b-XCCDF] The eXtensible Configuration Checklist Description Format.
http://scap.nist.gov/specifications/xccdf/

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	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

Отпечатано в Швейцарии
Женева, 2012 г.