Международный союз электросвязи

МСЭ-Т X.1243

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(12/2010)

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

Безопасность киберпространства – Противодействие спаму

Система интерактивных шлюзов для противодействия спаму

Рекомендация МСЭ-Т X.1243

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.379
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	
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.1243

Система интерактивных шлюзов для противодействия спаму

Резюме

В настоящей Рекомендации МСЭ-Т X.1243 определяется интерактивная система шлюзов для противодействия спаму как техническое средство противодействия междоменному спаму. Эта система шлюзов позволяет осуществлять оповещение о спаме в разных доменах и препятствует прохождению трафика спама из одного домена в другие.

Дополнительно в настоящей Рекомендации определяется архитектура системы шлюзов, описываются основные элементы, протоколы и функции системы шлюзов и предлагаются механизмы для определения спама, совместного использования информации и особых действий в системе шлюзов для противодействия спаму.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1243	17.12.2010 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 извещения 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

		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	3
6	Архитектура	3
6.1	Объекты и функции противодействия спаму	3
6.2	Определение спама	4
6.3	Действия по противодействию спаму	4
6.4	Обнаружение спама	4
6.5	Оповещение о спаме при помощи однорангового протокола противодействия спаму	4
7	Технологии фильтрации для противодействия спаму	5
7.1	Рассмотрение, не зависящее от технологий	5
7.2	Поддерживаемые методы противодействия спаму	5
8	Обработка однорангового протокола противодействия спаму	9
8.1	Обнаружение однорангового объекта	9
8.2	Настройка одноранговых отношений	9
8.3	Обмен сообщениями по противодействию спаму	9
8.4	Освобождение однорангового объекта	9
9	Модель реализации системы шлюзов для противодействия спаму	10
9.1	Интегрированная модель	10
9.2	Модель на основе домена	10
9.3	Модель обхода	11
Дополнение I – Пример определения сообщения SCPP		12
Библиография		14

Рекомендация МСЭ-Т X.1243

Система интерактивных шлюзов для противодействия спаму

1 Сфера применения

Система интерактивных шлюзов для противодействия спаму представляет собой общий интерактивный механизм для противодействия рассылке разных спамовых сообщений между доменами, включая рассылку спама по электронной почте, SMS спам и пр., позволяет использовать информацию для противодействия спаму совместно в разных доменах и предотвратить как рассылку, так и получение спама. В настоящей Рекомендации поддерживаются разнообразные методы противодействия спаму при помощи фильтров, и предусмотрена гибкость для будущих методов.

До принятия настоящей Рекомендации следует рассмотреть ее соответствие всем имеющим к ней отношение национальным законам и нормативам.

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.509] Recommendation ITU-T X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 спам (spam) [b-ITU-T X.1240]: Значение слова "спам" зависит от того, что понимается под конфиденциальностью в каждой стране, и от того, что представляет собой спам с национальных технологической, социально-экономической и практической точек зрения. В частности, с развитием технологий значение этого слова изменяется, становясь все шире и открывая все новые возможности для злоупотреблений электронными сообщениями. И хотя согласованного на международном уровне определения спама не существует, этот термин обычно используется для обозначения рассылаемых в массовом порядке по электронной почте или подвижной связи незапрашиваемых сообщений, целью которых является, как правило, продвижение продуктов или услуг коммерческого характера.

3.1.2 спаммер (spammer) [b-ITU-T X.1240]: Организация или лицо, создающее и рассылающее спам.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 интерактивная система шлюзов для противодействия спаму (interactive gateway system for countering spam): Интерактивная система шлюзов для противодействия спаму (IGCS) – это объект, который отвечает за обнаружение и блокирование спама. Он выполняет спаренные функции – функция шлюза отправителя (SGF) и функция шлюза получателя (RGF). IGCS должна работать с другими одноранговыми приложениями для реализации полного набора функций для противодействия спаму.

3.2.2 локальная база данных по противодействию спаму (local countering spam database): Этот термин определяет базу данных, которая применяется для хранения информации о спаме, черных списков, правил противодействия спаму для локальных функций шлюза отправителя и шлюза получателя.

3.2.3 модальность (modality): Модальностью называет(ют)ся код(ы) информации, содержащий(ие) информацию, воспринимаемую человеком.

3.2.4 мультимодальное сообщение (multimodal message): Мультимодальным называется мультимедийное сообщение, содержащее информацию с разной кодировкой для взаимодействия посредством множества модальностей.

3.2.5 агент-получатель (receiver agent): Агент-получатель – это сервер, который принимает сообщения для получателей сообщений. В приложениях электронной почты в качестве агента-получателя выступает сервер почтового протокола (POP).

3.2.6 функция шлюза получателя (receiver gateway function): Функция шлюза получателя – это функция принимающей стороны по противодействию спаму, которая определяет и блокирует спам во время получения.

3.2.7 агент-отправитель (sender agent): Агент-отправитель – это сервер, который отправляет сообщения, подготовленные отправителями сообщений. В приложениях электронной почты в качестве агента-отправителя выступает сервер упрощенного протокола передачи сообщений электронной почты (SMTP).

3.2.8 функция шлюза отправителя (sender gateway function): Функция шлюза отправителя – это функция передающей стороны по противодействию спаму, которая определяет и блокирует спам во время отправки сообщений.

3.2.9 одноранговый объект по противодействию спаму (spam-countering peer): В процессе противодействия спаму две IGCS работают совместно, чтобы определить и заблокировать спам, таким образом, одна IGCS противодействует спаму точно так же, как и вторая.

3.2.10 протокол однорангового противодействия спаму (spam-countering peering protocol): Этот протокол создан для обмена сообщениями предупреждения о спаме и черными списками между шлюзами по противодействию спаму.

3.2.11 пользовательский протокол сообщений о спаме (user spam report protocol): Этот протокол создан для того, чтобы получатели сообщений могли сообщить шлюзу о спаме.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения:

E-mail	Electronic Mail	Электронная почта
FE	Functional Entity	Функциональный объект
IGCS	Interactive Gateway system for Countering Spam	Интерактивная система шлюза для противодействия спаму
IM	Instant Message	Мгновенное сообщение
IRC	Internet Relay Chat	Трансляция чатов в интернете
LscDB	Local Spam-Countering Database	Локальная база данных противодействия спаму
POP	Post Office Protocol	Почтовый протокол
RA	Receiver Agent	Агент-получатель
RBL	Realtime Blackhole List	Список нарушителей, проверяемый в режиме реального времени
RGF	Receiver Gateway Function	Функция шлюза получателя
SA	Sender Agent	Агент-отправитель
SCPP	Spam-Countering Peering Protocol	Одноранговый протокол противодействия спаму
SGF	Sender Gateway Function	Функция шлюза получателя
SMTP	Simple Mail Transfer Protocol	Упрощенный протокол передачи сообщений электронной почты
WPF	Weighted Parameter Filter	Фильтр взвешенного параметра

5 Условные обозначения

Функциональный блок: в интерактивной системе шлюзов для противодействия спаму "функциональный блок" определяется как набор функциональных возможностей. Он представлен следующим символом:

6 Архитектура

6.1 Объекты и функции противодействия спаму

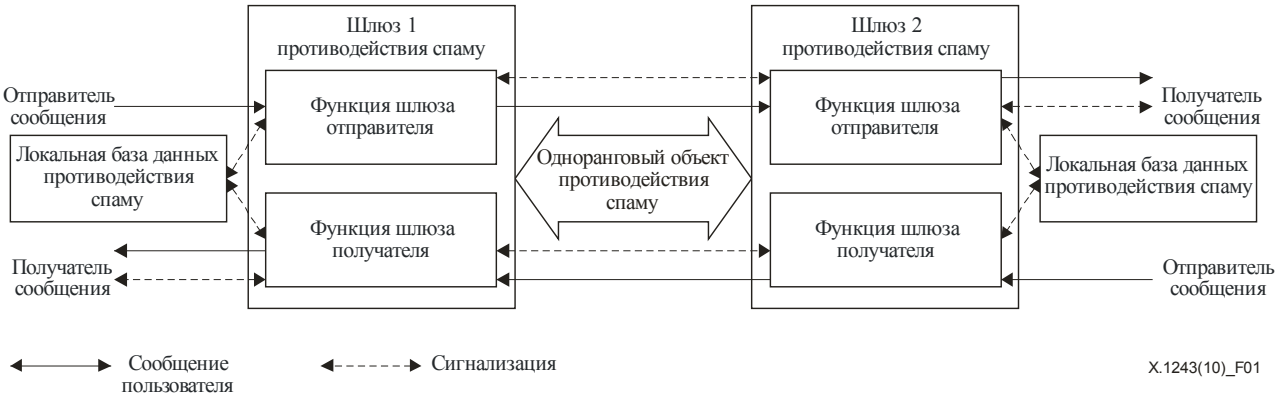

Рисунок 1 – Архитектура интерактивной системы шлюзов для противодействия спаму

Интерактивная система шлюзов для противодействия спаму (IGCS)

Система IGCS состоит из шлюза противодействия спаму и локальной базы данных противодействия спаму. Шлюз противодействия спаму имеет два функциональных подобъекта: SGF и RGF. Эти функциональные объекты действуют и как точки принятия решения, и как точки обязательного выполнения решения. SGF используется для обработки исходящего спама, а RGF используется для обработки входящего спама. Локальная база данных противодействия спаму (lscDB) обеспечивает выполнение правил противодействия спаму для действий по определению спама и противодействию спаму. Локальный шлюз противодействия спаму также отвечает за обновление правил противодействия спаму в lscDB.

В зону ответственности RGF и SGF входят:

RGF в основном выполняет три обязанности:

- предпринимать меры противодействия спаму (блокирование, изолирование или предупреждение и пр.) в отношении известного входящего спама;
- определять новый спам при помощи сообщений от получателей спама и обновлять локальные правила противодействия спаму в lscDB;
- при обнаружении спама оповещать SGF отправителя спама при помощи оповещения.

SGF выполняет две обязанности:

- предпринимать меры по противодействию спаму (блокирование, изолирование или предупреждение и пр.) в отношении известного исходящего спама;
- обрабатывать сообщения о спаме, присланные RGF получателя, и обновлять локальные правила противодействию спаму в lscDB.

Локальная база данных противодействия спаму (lscDB)

lscDB используется для хранения информации по противодействию спаму. В дальнейшем эта информация может быть разделена на следующие три типа.

- информация об идентификации спама: например, адрес источника спама и ключевые слова в предметной области спама;
- правила противодействия спаму: например, черный список и рекомендательный список;
- запись подозрения на спам: образцы подозрительного спама, о которых сообщили RGF и SGF.

6.2 Определение спама

RGF или SGF определяет известный спам на основе информации по определению спама, хранящейся в lscDB. Спам будет разделен на несколько уровней, и по отношению к нему будут предприняты соответствующие действия.

6.3 Действия по противодействию спаму

Как только спам определен, соответствующий RGF или SGF выполняет действия, исходя из уровня определенного спама. Действия по противодействию спаму могут включать в себя, но не ограничиваться:

- предупреждение о спаме: RGF/SGF отправляет предупреждение получателю/отправителю спама;
- изоляцию спама: RGF/SGF изолирует сообщения со спамом и периодически отправляет сводки об изоляции получателю/отправителю сообщения;
- блокирование спама: RGF/SGF блокирует сообщение со спамом.

6.4 Обнаружение спама

6.4.1 Обнаружение спама RGF

Получатель может сообщить о правилах антиспама своему действующему RGF. Правила антиспама включают в себя черный список адресов источников/адресатов, ключевых слов в предметной области электронной почты, но не ограничиваются этим. RGF обновляет определение спама и правила в lscDB. Когда приходит подозрительное сообщение, RGF начинает процесс оценки для принятия решения, является ли сообщение спамом в соответствии с правилами противодействия спаму, хранящимся в lscDB. Если сообщение сочтут спамом, RGF предпримет соответствующие данные.

6.4.2 Обнаружение спама SGF

Процесс обнаружения спама для SGF похож на процесс для RGF. SGF также получает оповещения о спаме от RGF отправителя. SGF рассматривает оповещения RGF и обновляет подтвержденные правила спама в lscDB.

6.5 Оповещение о спаме при помощи однорангового протокола противодействия спаму

6.5.1 Обнаружение однорангового объекта

Когда SA пытается отправить сообщение RA, начинается процедура обнаружения однорангового объекта для обнаружения одноранговой IGCS на тракте доставки сообщения. Процедура обнаружения может инициироваться одной из одноранговых IGCS. Одноранговые отношения устанавливаются после процедуры взаимного опознавания аутентификации одноранговых объектов.

6.5.2 Оповещение о спаме между одноранговыми объектами

После установления одноранговых отношений IGCS может обмениваться оповещениями о спаме с ее одноранговым объектом при помощи однорангового протокола противодействия спаму. Так как спам в основном определяется получателем, RGF получателя отвечает за определение спама и предоставление информации о спаме SGF отправителя. Как только RGF замечает сообщение о спаме, он оповещает SGF отправителя при помощи процесса оповещения о спаме. После получения оповещения о спаме, SGF должен решить принимать или не принимать его в соответствии с локальными правилами противодействия спаму.

6.5.3 Аспект безопасности

В процесс оповещения о спаме для аутентификации однорангового объекта рекомендуется включать механизм сертификации, определенный в [ITU-T X.509]. Рекомендуется, чтобы сообщение оповещения имело цифровую подпись RGF. Рекомендуется принимать сообщения оповещения только от доверенных источников RGF.

7 Технологии фильтрации для противодействия спаму

7.1 Рассмотрение, не зависящее от технологий

IGCS должна поддерживать разнообразные методы противодействия спаму и обеспечивать гибкость для внедрения существующих и будущих методов фильтрации спама. Каждый метод фильтрации может внедряться дополнительно к существующим. Для того чтобы эффективно обнаруживать сообщения со спамом, IGCS может поддерживать несколько методов фильтрации и внедрять их в физическое оборудование сети. Реализация определенных методов фильтрации находится вне зоны рассмотрения настоящей Рекомендации. В данной Рекомендации определяются только интерфейсы, форматы данных для каждого метода фильтрации, чтобы гарантировать взаимодействие при обмене информацией по противодействию спаму между одноранговыми IGCS.

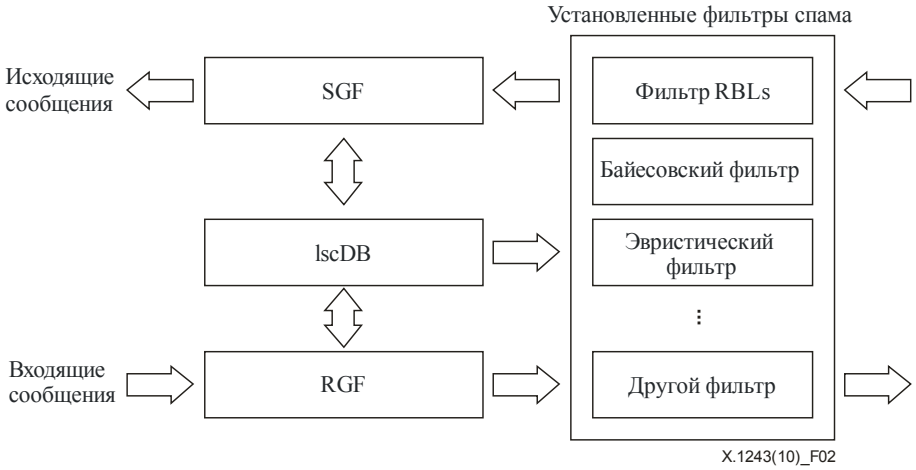

Рисунок 2 – IGCS с множеством фильтров спама

7.2 Поддерживаемые методы противодействия спаму

7.2.1 Список адресатов

Список нарушителей, проверяемый в режиме реального времени (RBL): Список RBL предоставляется разными организациями, которые изучают спам и создают собственные списки адресов пользователей. Система противодействия спаму может использовать эти списки и, сверяясь с этими списками, определять, является ли это сообщение спамом.

Черные списки: Черные списки – это основной механизм управления доступом, который позволяет доступ всем, кроме тех, кто внесен в черный список. Как и RBL, эти списки могут постоянно обновляться, и эта схема также страдает из-за того, что многие сообщения со спамом не содержат адреса источника. Некоторые системы также позволяют пользователям поддерживать рекомендательные списки отправителей, имеющих доступ, но которые могут запрещать пользователям получать желательные сообщения от ранее неизвестных источников.

7.2.2 Эвристическая фильтрация

Эти фильтры основаны на принципе проверки присутствия в сообщении определенных стандартных признаков спама, например исключительное использование HTML, или типа пользователя, которому отправлено сообщение. Эта проверка проводится при помощи процесса обучения на основе комплекса известных сообщений и комплекса электронных писем, про которые известно, что они легитимны.

Эти фильтры обусловливают риск того, что сообщения, использующие технологии спаммеров, например сообщения с очевидным применением HTML, могут считаться спамом.

Этот фильтр может обнаружить большую часть сообщений, и он не нуждается в обучении или настройке. Однако, так как он применяет большое количество проверок, следует знать, что существует возможность изменения конфигурации списка проводимых испытаний и результатов, используемых для классификации сообщений, как спама.

7.2.3 Байесовская фильтрация

Принцип Байесовской фильтрации состоит в том, что ее механизм противодействия спаму обучается на комплексе известных сообщений со спамом и комплексе сообщений, о которых известно, что они легитимны. После процесса обучения, собираются характеристики словаря, используемого в сообщениях со спамом. Байесовская фильтрация для решения о том, является ли новое сообщение спамом или нет, будет использовать Байесовские вероятности. В случае групповой фильтрации, обучение обычно выполняет системный администратор.

Выполняемая на основе алгоритма Байесовских вероятностей Байесовская фильтрация характеризуется большими потерями при вычислении и может ввести проблему масштабируемости в крупной системе противодействия спаму. В небольшом и в высокой степени единообразном окружении (например, в сети предприятия или высшего учебного заведения) ее можно применять. Однако, вне всякого сомнения, это не будет рекомендовано в случае крупного поставщика услуг и особенно поставщика общественных услуг.

Хотя Байесовская фильтрация применялся для противодействия спаму, для нее существуют определенные ограничения, когда спаммеры фальсифицируют информацию о себе.

7.2.4 Мультимодальная фильтрация

Если система IGCS должна выполнять мультимодальную фильтрацию, то в SGF и RGF реализуются мультимодальные фильтры, соответственно при помощи пары функциональных объектов (FE): FE определения модальности, FE фильтрации и других функциональных объектов, например, FE обработки мультимодальных сообщений. Для обеспечения хранения и обмена информацией, следует определить группы данных мультимодальной информации противодействия спаму. lscDB будет хранить мультимодальную информацию противодействия спаму, которая содержит категории (и темы) мультимодального сообщения и критерии фильтрации (которые были введены пользователями или операторами, или получены от одноранговых IGCS).

Если описание мультимодальных метаданных доступно, и считается, что это описание метаданных достойно доверия, мультимодальные приложения могут отфильтровывать мультимодальную информацию на основе описания мультимодального содержания при помощи метаданных. В противном случае при рассмотрении фильтрация должна отдавать предпочтение всей мультимодальной информации, где функциональные объекты должны выполнять следующие задачи:

- базы данных или хранилища, содержащих подходящие категории и критерии фильтрации мультимодальных сообщений. База данных или хранилище могут располагаться в том же здании/домене, что и FE агента интерфейса DB, FE определения модальности, FE мультимодальной обработки и мультимодальный агент пользователя. В другом случае база данных или хранилище могут располагаться в других доменах или зданиях, чем FE фильтрации;
- функциональный элемент определения модальности исследует отправленные или полученные мультимодальные сообщения для определения содержащейся модальности;
- функциональный объект агента DB получает критерии фильтрации от DB в определенных модальностях и категориях сообщений;
- фильтрующий функциональный объект фильтрует мультимодальные сообщения в соответствии с критериями фильтрации. Фильтрующий FE может полностью или частично заблокировать выбранные мультимодальные части обрабатываемого мультимодального сообщения.

На рисунке 3 описана общая архитектура для фильтрации мультимодальных сообщений и необходимые функциональные объекты. Архитектура фильтрации, которая включает в себя FE определения модальности, FE фильтрации, FE агента интерфейса DB и мультимодальный DB. Однако на рисунке 3 показаны другие функциональные объекты, которые обычно не выполняют никаких задач мультимодальной фильтрации, например FE обработки мультимодального сообщения и мультимодальный агент пользователя.

FE мультимодальной обработки сообщений обрабатывает мультимодальные (фильтрованные) сообщения; синхронизирует мультимодальные сообщения, полученные от мультимодального агента пользователя, и мультиплексирует или отправляет отфильтрованные мультимодальные сообщения мультимодальному агенту пользователя. Каждый из различных мультимодальных агентов пользователя имеет определенную модальность, например модальный (особый для устройства) ввод и/или вывод.

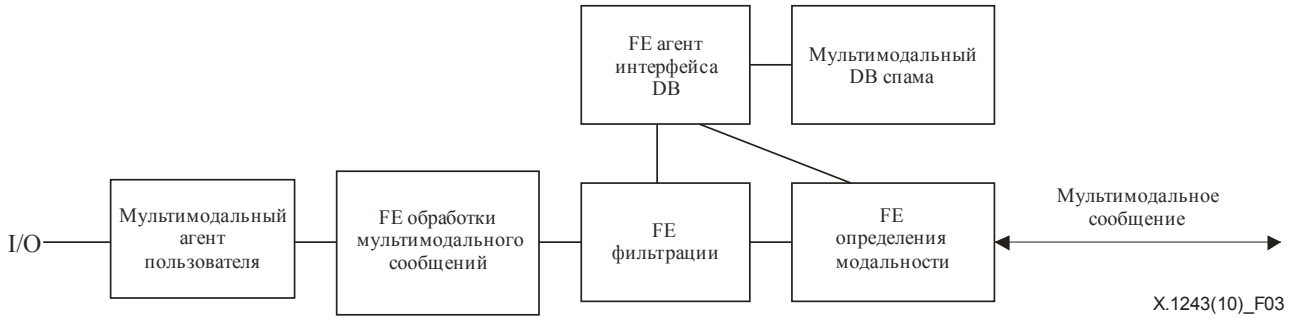

Рисунок 3 – Архитектура мультимодальной фильтрации

На рисунке 4 подробно описана общая архитектура мультимодальной фильтрации при помощи нанесения функциональных объектов на функцию шлюза получателя (RGF). Следующие этапы описывают процедуры, когда FE получают мультимодальное сообщение:

1) RGF получает мультимодальное сообщение.

2) FE обнаружения модальности определяет полученные модальности и тип(ы) сообщения, переданные в полученном мультимодальном сообщении.

3) FE фильтрации может быть настроена статически по правилам фильтрации для всех возможных мультимодальных сообщений, т. е. независимо от конкретного полученного мультимодального сообщения, или может быть настроен динамически с правилом сообщения и/или зависящим от модальности правилом отдельно для каждого полученного мультимодального сообщения.

   a) FE определения модальности может или предложить агенту интерфейса DB определенные модальности и параметры типов сообщения, или FE определения модальности может прикрепить параметры к полученному мультимодальному сообщению.

   b) FE определения модальности отправляет мультимодальное сообщение, возможно помеченное при помощи полученной модальности и параметров типа сообщения, FE фильтрации.

4) В случае если FE фильтрации еще настроен при помощи правил, FE фильтрации передает модальности и параметры типов сообщений агенту интерфейса DB, если только агент интерфейса DB не получил эти параметры напрямую от FE определения модальности.

5) FE агента интерфейса DB запрашивает у мультимодального DB получение соответствующих модальностей и критериев сообщений. FE агента интерфейса DB включает эти значения в определенные правила и предоставляет эти правила FE фильтрации.

6) FE фильтрации применяет доступные правила и осуществляет фильтрацию полученного мультимодального сообщения. В зависимости от конфигурации правил и политики, мультимодальному сообщению разрешается пройти дальше, или оно полностью блокируется или блокируется частично, когда блокируются только определенные модальности в мультимодальном сообщении.

7) FE фильтрации передает прошедшее фильтрацию мультимодальное сообщение FE обработки мультимодальных сообщений, возможно с пометкой об определенных результатах фильтрации (т. е. информация для ввода в журнал или предупреждения безопасности).

8) FE обработки мультимодальных сообщений обрабатывает полученной (прошедшее фильтрацию) мультимодальное сообщение. FE синхронизирует входящие данные, полученные от разных агентов пользователей мультимодальных входящих данных, отправляет мультимодальное сообщение их компонентам модальности и перенаправляет эти части с определенной модальностью агентам пользователей мультимодальных исходящих данных.

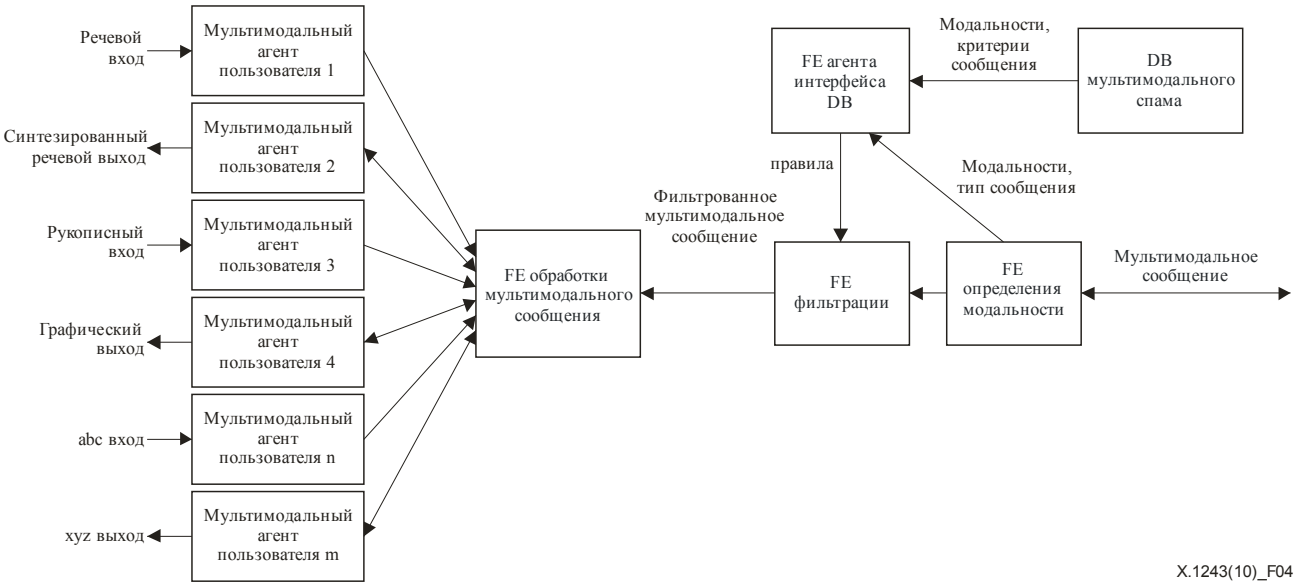

Рисунок 4 – Мультимодальная фильтрация в функции шлюза получателя (RGF)

ПРИМЕЧАНИЕ. – На рисунке 4 описаны разные мультимодальные агенты пользователя. Для RGF может быть необязательно присутствие всех показанных мультимодальных агентов пользователя.

7.2.5 Фильтр подавления спама

Фильтр подавления спама применятся для управления скоростью приема сообщений. Важным параметром фильтра подавления спама является коэффициент подавления спама. Этот параметр является мерой подозрительных сообщений и управляет скоростью приема сообщений. При приеме крайне подозрительного сообщения, этот коэффициент соответственно возрастает, и фильтр подавления спама снизит скорость приема подозрительных электронных писем. Этот параметр обычно создается внешней системой противодействия спаму, например базой данных опыта или репутации. Фильтр подавления спама также влиять на задержку ответа электронной почты, размер транспортного окна и период цикла подавления и т. д.

7.2.6 Фильтр по заголовку электронной почты

Фильтр по заголовку электронной почты (EHF) следит за общением SMTP и гарантирует его соответствие актуальным протоколам. Его можно применять для определения несовместимости протокола и фальсифицированного заголовка электронной почты. Для того чтобы воссоздать сеансы SMTP и отследить состояние протоколов, EHF может потребоваться пакетирование дефрагментации, передачи потока TCP и пр. EHF фокусируется на анализе уровня протокола и предоставляет дополнительную информацию для улучшения общей точности определения спама. Фильтры EHF широко внедрены во многих системах антиспама и в некоторых системах антиспама с открытым кодом.

7.2.7 Фильтр взвешенного параметра (WPF)

Фильтр взвешенного параметра (WPF) применяется для обнаружения спама путем анализа многих параметров. Эти параметры основаны на статистической информации, включая множество сеансов электронной почты, множество серверов адресатов, множество проверок электронной почты, интервал времени отправления сообщений, скорость передачи сообщений, отношение числа проверенных сообщений к числу сообщений, прошедшим проверку, и так далее. Каждый параметр имеет регулируемый порог регулируемое взвешенное значение. Кроме того, также нужен полный набор взвешенных значений, которые проверены в ходе многих экспериментов. Для каждого сообщения будут проверяться все параметры, указанные в правилах. Только те параметры, которые пройдут установленный порог, будут добавлены к измеряемому весу. Если группы параметров проходят заранее определенный порог, то WPF сможет отличить электронные письма со спамом от обычных писем.

8 Обработка одноранговового протокола противодействия спаму

8.1 Обнаружение одноранговового объекта

Процесс обнаружения одноранговового объекта устанавливает одноранговые отношения для двух IGCS. Этот процесс начинается, когда IGCS пытается обнаружить действующую IGCS в тракте доставки сообщения. Когда RGF определяет подозрительное сообщение со спамом, начинается процесс обнаружения одноранговового объекта.

В сообщение об обнаружении одноранговового объекта рекомендуется включать следующую информацию:

- список адресов RGF/SGF исходной IGCS: адрес источника, например IP-адрес источника и пары портов. Для защиты от отказов из-за выхода из строя одного элемента, для получения требуемой избыточности IGCS может объединить несколько RGF и SGF. Список адресов может содержать все адреса RGF/SGF в исходной IGCS;
- адрес IGCS противоположной стороны: IGCS@{адрес прокси сервера или противоположной стороны};
- источник спама: адрес отправителя спама;
- тип подозрительного спама: WELL _KNOWN ,USER_REPORTED или OTHER;
- прикрепленный подозрительный спам: прикрепленный подозрительный спам.

Когда сообщение об обнаружении одноранговового объекта отправлено, исходная IGCS запускает таймер. Если после истечения определенного срока ответного сообщения не получено, значит исходной IGCS не удалось обнаружить одноранговую IGCS. Сообщение об обнаружении одноранговового объекта может содержать следующую информацию:

- список адресов RGF/SGF отвечающей IGCS;
- подтверждение подозрительного спама: для подтверждения того, что подозрительный спам считается спамом отвечающей IGCS.

8.2 Настройка одноранговых отношений

Прежде чем истечет время, если исходная IGCS получила ответное сообщение об обнаружении, она может начать устанавливать одноранговые отношения. Процесс должен состоять из двух основных действий:

- IGCS обновляет список одноранговых объектов: добавляет в список одноранговых объектов список адресов IGCS противоположной стороны;
- список имен поддерживаемых фильтров спама: поддерживаемые фильтры спама на каждой IGSC.

8.3 Обмен сообщениями по противодействию спаму

После настройки одноранговых отношений IGCS начинает обмен сообщениями по противодействию спаму. В этом процессе две одноранговые IGCS обмениваются информацией об общих поддерживаемых фильтрах спама. После получения сообщения в рамках этого обмена, каждая IGCS обновляет свою lscDB.

8.4 Освобождение одноранговового объекта

Если в определенный период времени спам не обнаружен, одна IGCS может прервать одноранговые отношения, отправив сообщение освобождения одноранговового объекта. После получения сообщения освобождения одноранговового объекта, IGCS удалит соответствующую одноранговую информацию или повторно ее использует в соответствии с правилами.

9 Модель реализации системы шлюзов для противодействия спаму

9.1 Интегрированная модель

9.1.1 Описание модели

В интегрированной модели IGCS встроена в систему сообщений, состоящую из RA и SA. Каждая система имеет шлюз (RGF и SGF) и lscDB. Например, в системе электронной почты RA может быть сервером POP3, а SA может быть сервером SMTP. RGF/SGF могут быть реализованы в виде встроенного сервера, предоставляющего и POP3, и SMTP услуги. Для системы электронной почты также требуется lscDB, чтобы обеспечивать выполнение правил противодействия спаму. На рисунке 5 показана интегрированная модель.

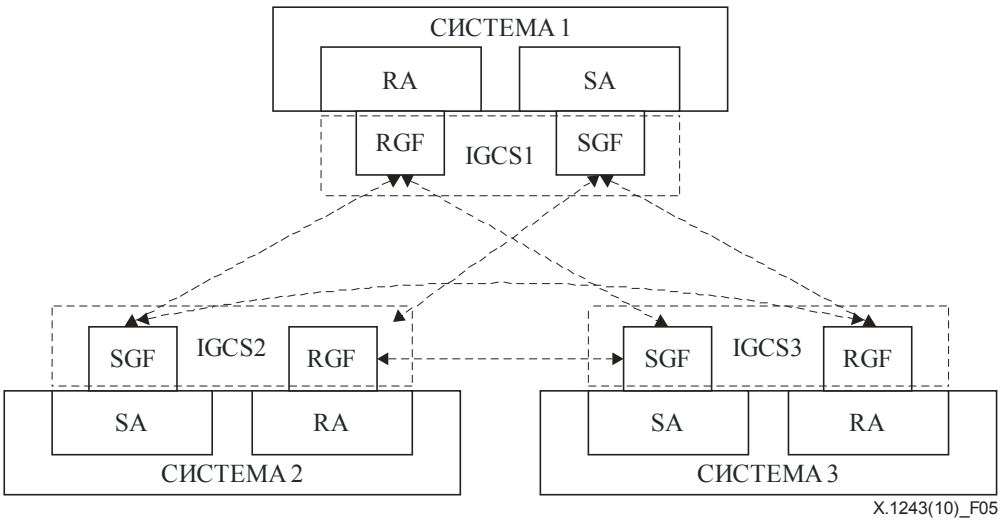

Рисунок 5 – Интегрированная модель IGCS

9.1.2 Варианты применения

Интегрированная модель подходит для модели клиент/сервер, в которой сервер отвечает за отправку/прием множества клиентских сообщений. В этом случае сервер выступает как точка принятия решения и точка обязательного применения решения для действий противостояния спаму.

9.2 Модель на основе домена

9.2.1 Описание модели

В модели на основе домена IGCS действует как прокси по доставке сообщений в домене, в котором может иметься множество SA и RA для выполнения требований по нагрузке. SGF/RGF могут иметь несколько положений, распределенных в домене. Каждое положение SGF/RGF отвечает за несколько SA/RA в домене и за противодействие сообщениям со спамом как в локальном домене, так и между доменами.

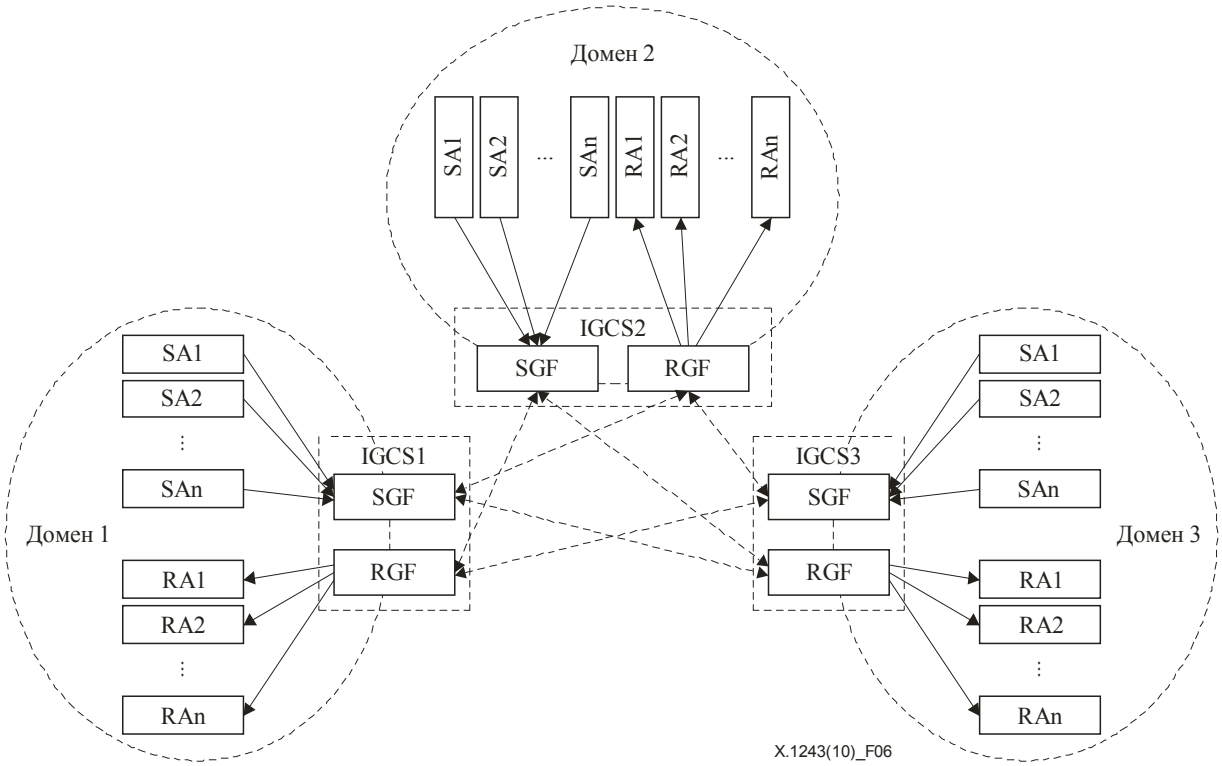

Рисунок 6 – Модель на основе домена

9.2.2 Варианты применения

Модель на основе домена может использоваться для целей противодействия спаму на базе домена. Она особенно подходит для одноранговой системы связи, например для многих популярных приложений IM: IRC и т. п. Для одноранговой модели система на стороне пользователя сама по себе выступает одновременно и как RA, и как SA. Управлять большим количеством RA и SA на стороне пользователей со встроенной моделью IGCS будет очень сложно. Однако модель на основе домена способна решить проблему за счет распределения.

9.3 Модель обхода

9.3.1 Описание модели

В беспроводных сетях также можно развернуть IGCS с беспроводной точкой доступа. Беспроводная точка доступа передает все сообщения IGCS. IGCS оценивает входящие сообщения на основе правил, хранящихся в lscDB, и выпускает нормальные сообщения в беспроводную сеть.

9.3.2 Варианты применения

Модель обхода может использоваться в беспроводной сети. Спам может отфильтровываться прежде, чем он попадет в беспроводную сеть, за счет чего можно снизить бесполезные затраты на доставку трафика спама оконечным пользователям.

Дополнение I

Пример определения сообщения SCPP

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Пример сообщений SCPP на языке ASN.1 приведен ниже и был проверен компилятором ASN.1:

```
СООБЩЕНИЯ SCPP-MESSAGES {itu-t(0) recommendation(0) x(24) igscs(1243)
asn1-module(0) scpp-messages(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- ОПРЕДЕЛЕНИЕ ТЕЛА СООБЩЕНИЯ SCPP
SCPP-PDU ::= SEQUENCE {
     sourceAddress        IGCS-Address,
     destAddress          IGCS-Address,
     igcs-message-body    CHOICE {
               peerDiscovery   PeerDiscoveryDEF,
               peerSetup       PeerSetupDEF,
               dataExchange    DataExchangeDEF,
               peerKeepAlive   PeerKeepAliveDEF,
               peerRelease     PeerReleaseDEF},
     nonStandardData      OCTET STRING OPTIONAL,
     ...
}

-- Определение сообщения Обнаружение одноранговового объекта
PeerDiscoveryDEF::=SEQUENCE {
     setupRequest    BOOLEAN,
     igcsSignature   IGCS-Signature
}

-- Определение сообщения настройки одноранговых сообщений
PeerSetupDEF::=SEQUENCE {
     setupResponse        BOOLEAN,
     sgfList              SEQUENCE OF IGCS-Address,
     rgfList              SEQUENCE OF IGCS-Address,
     supportedFilters     SupportedSpamFilters,
     igcsSignature        IGCS-Signature
}

-- Определение сообщения обмена данными по противодействию спаму
DataExchangeDEF::=SEQUENCE {
     csData               SET OF SpamFilterData,
     ...
}

-- Определение сообщения Существование одноранговового объекта
PeerKeepAliveDEF::=SEQUENCE {
     sgfUpdates      GF-Updates,
     rgfUpdates      GF-Updates,
     filtersUpdates  SupportedSpamFilters
}
-- Определение сообщения Освобождение одноранговового объекта
PeerReleaseDEF::=SEQUENCE {
     peerRelease     ENUMERATED{request(0), confirm(1)},
     nonStandardData OCTET STRING OPTIONAL,
     ...
}
```

```
-- Адреса, поддерживаемые IGCS, включая определение адресов IGCS,SGF,RGF
-- Поддержка IP-адреса, ID электронной почты и других типов адресов
IGCS-Address::=CHOICE{
     ipAddress
     SEQUENCE { ip OCTET STRING(SIZE(4)),
                port INTEGER(0..65535) },
                ip6Address
                SEQUENCE { ip OCTET STRING(SIZE(16)),
                           port INTEGER(0..65535) },

     emailAddress         IA5String(SIZE(1..512)),
     nonStandardAddress   OCTET STRING,
     ...
}

-- Данные подписи для аутентификации
IGCS-Signature::=SEQUENCE {
     igcsID          INTEGER(0..65535),
     signatureData   OCTET STRING,
     ...
}

-- Информация обновления статуса RGF/SGF
GF-Updates::=SEQUENCE {
     gateType        ENUMERATED {sgf(0),rgf(1)},
     gateAdd         IGCS-Address,
     gateRemove      IGCS-Address
}

-- Фильтры спама, поддерживаемые IGCS и соответствующие данные

SupportedSpamFilters::= SEQUENCE {
     supportedFilter SEQUENCE OF SpamFilters

}

SpamFilters::=SEQUENCE{
     filterID        INTEGER(0..128),
     filterName      IA5String(SIZE(1..512))
}

SpamFilterData::=SEQUENCE {
     filterID        INTEGER(0..128),
     filterData      OCTET STRING,
     ...
}

END
```

Библиография

[b-ITU-T X.680] Recommendation ITU-T X.680 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[b-ITU-T X.681] Recommendation ITU-T X.681 (2008) | ISO/IEC 8824-2:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.

[b-ITU-T X.682] Recommendation ITU-T X.682 (2008) | ISO/IEC 8824-3:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.

[b-ITU-T X.683] Recommendation ITU-T X.683 (2008) | ISO/IEC 8824-4:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.

[b-ITU-T X.1231] Рекомендация МСЭ-Т X.1231 (2008 г.), *Технические стратегии противодействия спаму*.

[b-ITU-T X.1240] Рекомендация МСЭ-Т X.1240 (2008 г.), *Технологии, применяемые при противодействии спаму, рассылаемому по электронной почте*.

[b-ITU-T X.1241] Рекомендация МСЭ-Т X.1241 (2008 г.), *Техническая основа противодействия спаму, рассылаемому по электронной почте*.

[b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions*.

[b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3*.

[b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol – Version 4rev1*.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*.

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*.

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*.

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*.

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*.

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	Качество телефонной передачи, телефонные установки, сети местных линий
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, 2011 г.