Международный союз электросвязи

МСЭ-Т X.1233

(09/2021)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Безопасность киберпространства –
Противодействие спаму

Руководящие указания по противодействию распространению спама при мгновенном обмене сообщениями

Рекомендация МСЭ-Т X.1233

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 (1)	
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 (1)	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 (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность умных электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
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
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ IMT-T	X.1800–X.1819

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

Рекомендация МСЭ-Т X.1233

Руководящие указания по противодействию распространению спама при мгновенном обмене сообщениями

Резюме

В Рекомендации МСЭ-Т X.1233 определены предназначенные для поставщиков и пользователей услуг мгновенного обмена сообщениями (IM) руководящие указания по противодействию распространению спама при мгновенном обмене сообщениями (спим), а также по сокращению масштабов распространения спима в киберпространстве и повышению оценки пользователями услуг IM.

В настоящей Рекомендации проанализированы сценарии создания спима при мгновенном обмене сообщениями, определены технические меры и механизмы противодействия спиму, которые могут применять поставщики услуг IM, а также приведены рекомендации по противодействию спиму для пользователей услуг IM.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1233	03.09.2021 г.	17-я	11.1002/1000/14773

Ключевые слова

Противодействие спиму, руководящие указания, поставщик услуг IM, пользователь IM.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например, http://handle.itu.int/11.1002/1000/11830-en.

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 в целях 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/авторскими правами на программное обеспечение, 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 соответствующим базам данных МСЭ-Т, доступным на веб-сайте МСЭ-Т по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

Популярность приложений мгновенного обмена сообщениями (IM) привела к тому, что приложения IM превратились в широко используемое средство распространение спама наряду с голосовой связью, услугой передачи коротких сообщений (SMS) и электронной почтой. Эффективная передача сообщений в реальном времени обеспечивает значительное удобство при общении в социальных сетях. Вместе с тем она создает благоприятные возможности для спамеров, которые отправляют спам при мгновенном обмене сообщениями (спим). Объем являющейся спамом рекламы, порнографического контента и другой незаконно распространяемой информации, такой как сообщения фишинга, вирусы, трояны, черви и шпионское программное обеспечение, которая отправляется с использованием IM, лавинообразно возрастает. Эта практика не только является видом преследования или даже ведет к экономическому ущербу для пользователей, но и существенным образом угрожает безопасности киберпространства. Противодействие спиму становится важным элементом противодействия спаму.

Однако по-прежнему не существует руководства, предназначенного для поставщиков услуг (SP) и пользователей, которые хотели бы противодействовать спиму при эксплуатации или использовании IM. Это означает отсутствие эффективного управления усилиями по противодействию спиму. Поэтому необходимо в срочном порядке разработать соответствующие стандарты, которые будут служить для операторов и пользователей IM руководством по практическим методам и мерам управления, которые могут противодействовать спиму.

Рекомендация МСЭ-Т X.1233

Руководящие указания по противодействию распространению спама при мгновенном обмене сообщениями

1 Сфера применения

В настоящей Рекомендации установлены предназначенные для поставщиков услуг (SP) и пользователей услуг IM руководящие указания по противодействию распространению спама при мгновенном обмене сообщениями (спим). Рассматриваются сценарии распространения IM-спама; технические меры и механизмы противодействия спиму, предназначенные для поставщиков услуг IM; а также меры экстренного реагирования для противодействия спиму, предназначенные для пользователей IM, и т. д.

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 спам, распространяемый при мгновенном обмене сообщениями (спим) (spam over instant messaging (SPIM)) [b-ITU-T X.1244]: Спам, нацеленный на пользователей услуг мгновенного обмена сообщениями.

ПРИМЕЧАНИЕ. – Для целей настоящей Рекомендации термин "спам" в настоящей Рекомендации не определяется.

3.1.2 спимер (spimmer) [b-ITU-T X.1244]: Отправитель спима.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяется следующий термин.

3.2.1 мгновенный обмен сообщениями (instant messaging (IM)): Обмен контентом между несколькими участниками в режиме, близком к реальному времени. Как правило, хотя это не обязательно, контентом являются короткие текстовые сообщения.

ПРИМЕЧАНИЕ. – Основано на [b-IETF RFC 3428].

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

IM	Instant Messaging		Мгновенный обмен сообщениями
IP	Internet Protocol		Протокол Интернет
NO	Network operator		Оператор сети
SMS	Short Message Service		Услуга передачи коротких сообщений
SPIM	Spam over Instant Messaging	Спим	Спам, распространяемый при мгновенном обмене сообщениями
SP	Service Provider		Поставщик услуг

5 Соглашения

Глагольная форма "должен" указывает на требование, которому необходимо неукоснительно следовать, чтобы обеспечить соответствие данной Рекомендации.

Глагольные формы "следует" и "не следует" указывают на то, что из нескольких возможностей одна рекомендуется как в особенности подходящая, без упоминания и исключения при этом других возможностей; что определенный порядок действий является предпочтительным, но не обязательно требуемым; либо (в отрицательной форме) что определенная возможность или определенный порядок действий не рекомендуется, но не запрещается.

Глагольная форма "может" указывает на необязательное требование, которое допустимо. Данный термин не подразумевает, что реализация должна обеспечивать этот вариант.

6 Сценарии распространения спама при мгновенном обмене сообщениями

Спим становится основной проблемой для услуг IM. Спим по-разному влияет на показатели систем IM, например впустую тратит ресурсы, включая память и центральный процессор, объем запоминающего устройства и ресурсы полосы пропускания, а также может создавать значительные проблемы, например распространение вирусов-червей и сетевых атак в целях отказа в обслуживании. Возможны, в том числе, следующие сценарии спима:

– использование автоматизированных средств для регистрации большого количества учетных записей со злонамеренными целями, такими как распространения спима;

– использование учетной записи без разрешения владельца учетной записи для установления сеансового соединения с целевым пользователем для распространения спима;

– отсутствие встроенных механизмов безопасности, например механизма подтверждения при добавлении друзей, что создает среду, в которой возможно быстрое распространение спима;

– раскрытие сообщений, передаваемых по незащищенному каналу доставки; хакеры могут искажать мгновенные сообщения в процессе передачи; в сообщения могут быть вставлены реклама или вредоносные коды, превращая сообщение в спим;

– действующие незаконно производители распространяют подписки на спим среди пользователей для получения коммерческой выгоды.

7 Руководящие указания по противодействию спиму для поставщиков услуг IM

7.1 Настройка функций борьбы со спимом

Поставщик услуг IM должен обеспечивать функции борьбы со спимом при предоставлении услуг IM. Следует, чтобы в число функций борьбы со спимом входили, в том числе, перечисленные ниже:

– автоматическое обнаружение и контроль регистрации пользователей;

– контроль авторизации при добавлении друзей;

– определение и ограничение скорости передачи сообщений;

– фильтрация сообщений на основе черных списков;

– платформа управления жалобами пользователей, которая, помимо прочих функций, имеет простой механизм обратной связи, позволяющий оповестить поставщика услуг IM о полученном спиме.

В то же время поставщик услуг IM должен поддерживать функции борьбы со спимом в процессе работы. Следует, чтобы в число сценариев входили, в том числе, перечисленные ниже:

– ведение баз данных для борьбы со спимом, таких как списки друзей и черные списки, с тем чтобы они были доступными и стабильными;

– сохранение информации о жалобах пользователей в целях повышений точности этой информации;

– настройка пороговых уровней, которые используются в функциях борьбы со спимом, например порогового уровня ограничения скорости передачи сообщений и порогового значения количества жалоб, которые могут поступить в отношении учетной записи, до того как она будет добавлена в черный список.

7.2 Мониторинг и контроль активности

Поставщик услуг IM должен принимать меры для мониторинга следующих видов активности и для подачи сигнала тревоги при обнаружении аномальной активности. Виды активности, которые, в том числе, следует отслеживать, перечислены ниже.

– Действия при ошибке аутентификации. Например, большое количество запросов аутентификации отправляются с одного адреса протокола Интернет (IP). Значительный уровень такой активности может означать, что спимер крадет учетные записи для отправки спима. Это должно вызывать сигнал тревоги, и последующие запросы аутентификации, поступающие с этого IP-адреса, следует отклонять.

– Действия по злонамеренной подаче жалоб. Например, какая-либо учетная запись направляет большое количество жалоб в течение определенного периода времени. Независимо от того, касаются ли эти жалобы разных учетных записей или одной учетной записи, если количество жалоб превышает определенное пороговое значение, это должно вызывать сигнал тревоги, и жалобы, направляемые этой учетной записью, следует игнорировать, тем самым повышая точность жалоб.

– Действия по злонамеренному добавлению учетных записей в черные списки. Например, если некоторые учетные записи добавляют конкретную учетную запись в черный список, следует определить, находятся ли эти учетные записи в списке подозрительных учетных записей. Если большинство из них находятся в списке подозрительных учетных записей, это должно вызывать сигнал тревоги. Эти попытки внести конкретную учетную запись в черный список не следует учитывать при подсчете того, сколько раз рассматриваемая конкретная учетная запись вносилась в черный список, что повышает точность черного списка.

7.3 Аудит и запись

Поставщики услуг IM должны принимать технические меры для аудита и записи поведения пользователей и инцидентов кибербезопасности в целях борьбы со спимом. Записи, аудит которых следует проводить услуге IM, включают, помимо прочего, перечисленные ниже.

– Журналы поведения пользователей, которые включают информацию о проведении регистрации и информацию об аутентификации пользователей. Например, поставщику услуг IM следует записывать хронологию действий пользователей (например, действия по отправке сообщений, превышающие пороговые значения ограничений скорости передачи сообщений, и действия по подаче злонамеренных жалоб). Следует, чтобы в журналы регистрации действий по передаче сообщений включалась, помимо прочего, следующая информация: информация об учетной записи отправителя (например, IP-адрес, имя пользователя, присутствие или отсутствие в списке подозрительных записей или черном списке), информация об учетной записи получателя, тип отношений между отправителем и получателем (например, являются друзьями, не являются друзьями, число членов группы, являющихся друзьями, число членов группы, не являющихся друзьями, друзья из других систем IM и контактные телефонные номера). Поставщикам услуг IM следует проводить анализ этой информации для выявления подозрительных или злонамеренных действий. Следует, чтобы журналы регистрации действий по подаче злонамеренных жалоб включали, помимо прочего, следующую информацию: информацию об учетной записи заявителя (например, IP-адрес, имя пользователя, присутствие или отсутствие в списке подозрительных записей или черном списке), информацию об учетной записи, в отношении которой подается жалоба, а также количество жалоб за определенный период времени. Если количество жалоб превышает пороговое значение, жалобы, направляемые учетной записью данного заявителя, игнорируются, что повышает точность платформы управления жалобами.

– Запись о фильтрации спима, которая включает действия по фильтрации спима и отфильтрованное сообщение. Следует, чтобы запись о действиях по фильтрации спима включала, помимо прочего, следующую информацию: учетную запись отправителя отфильтрованного сообщения (например, IP-адрес, имя пользователя, присутствие или отсутствие в списке подозрительных записей или черном списке), используемые меры фильтрации (например, фильтрация на основе черных списков, контроля скорости передачи или контроля авторизации). Отфильтрованное сообщение следует сохранить, с тем чтобы в случае ошибочной фильтрации была возможна его повторная отправка.

7.4 Экстренное реагирование

Поставщикам услуг IM следует разработать план экстренного реагирования на основные события спима.

Следует, чтобы основные события спима, подлежащие охвату планом экстренного реагирования, включали, помимо прочего, следующие:

– база данных для борьбы со спимом сервера IM подвергается изменению, вторжению, контролю;

– платформа управления жалобами на спим подвергается изменению, вторжению, контролю;

– пороговое значение функции автоматической регистрации подверглась незаконному изменению;

– в течение определенного периода времени осуществляется массовая подача жалоб на спим.

Поставщикам услуг IM следует определить тип и уровень каждого из этих событий спима в соответствии с реальной ситуацией и разработать процесс экстренного реагирования и руководящие указания по экстренным действиям для каждого типа и каждого уровня событий спима.

Поставщикам услуг IM следует создать механизм мониторинга и предупреждения для основных событий спима, обнаруживать основные события спима и своевременно уведомлять соответствующий персонал.

Поставщикам услуг IM следует также обобщать причины основных событий спима после осуществления экстренного реагирования, оценивать эффективность мер экстренного реагирования и своевременно устранять проблему.

7.5 Управление оценкой рисков

Поставщикам услуг IM следует проводить оценку рисков для определения вероятности и степени тяжести событий спима. Следует интегрировать управление рисками в основную операционную деятельность, начиная с оценки управления, далее переходя к оценке безопасности и функциональной оценке. Следует, чтобы управление оценкой рисков включало, помимо прочего, перечисленные ниже действия.

– Поставщикам услуг IM следует проводить оценку управления, включающую, например, разработку политики борьбы со спимом и мониторинг внедрения процессов и стратегий обеспечения безопасности в целях снижения риска спима, кроме того, способствующую реализации этой политики. Поставщикам услуг IM следует также пересматривать и обновлять текущую политику и процедуру оценки рисков с частотой, установленной организацией, или всякий раз при значительных изменениях в системе или операционной среде IM.

– Поставщикам услуг IM следует проводить оценку безопасности, включающую, например, автоматизацию процесса управления уязвимостями с использованием стандартов (например, перечисление дефектов приложений и несоответствующих конфигураций и форматирование контрольных списков и тестовых процедур), с тем чтобы определить наиболее вероятные причины спима (например, уязвимости пароля, небезопасные настройки брандмауэра, трояны, черви) и количественно определить условия, способствующие основным событиям спима.

– Поставщикам услуг IM следует проводить функциональную оценку, включающую, например, обнаружение нелогичной обработки и каскадных ошибок, причина которых может содержаться в коде системы IM (например, автоматическая регистрация пользователя, неограниченная пользовательская скорость отправки в течение определенного периода времени, отсутствие встроенных механизмов безопасности, открытые сообщения по незащищенному каналу доставки), при обновлении системы IM.

– Поставщикам услуг IM следует регулярно проводить оценку рисков или анализировать и обновлять при необходимости свою политику по оценке рисков. Следует, чтобы оценка рисков включала три взаимосвязанных компонента: оценку управления, оценку безопасности и функциональную оценку. Например, оценку управления и оценку безопасности следует выполнять вместе с общей оценкой рисков; функциональную оценку следует проводить до обновления системы IM, во время обновления системы IM или во время обеих этих операций. В то же время поставщикам услуг IM следует либо исправить узаконенные ошибки в определенном организацией времени реагирования, либо внедрить средства контроля для предотвращения использования уязвимостей спимером.

7.6 Меры обеспечения безопасности

Поставщикам услуг IM следует принимать меры обеспечения безопасности для борьбы со спимом. Следует, чтобы меры обеспечения безопасности включали, наряду с прочим, перечисленные ниже.

– Поставщикам услуг IM следует ввести в действие меры защиты от распределенных атак типа отказ в обслуживании для защиты библиотеки черных списков, платформы управления жалобами, методов мониторинга и аудита безопасности, а также для повышения доступности функций борьбы со спимом.

– Поставщикам услуг IM следует ввести в действие меры борьбы с вирусами, троянами и червями для предотвращения заражения сервера и захвата контроля над ним спимерами, которые могут внести изменения в настройки борьбы со спимом или отключить функции борьбы со спимом и после этого отправлять спим.

– Поставщикам услуг IM следует реализовать несколько методов контроля доступа на границах сети, в системах и приложениях системы IM для предотвращения несанкционированного доступа спимеров, которые могут внести изменения в настройки борьбы со спимом или отключить функции борьбы со спимом и после этого отправлять спим.

– Поставщикам услуг IM следует ввести в действие методы обнаружения вторжений и защиты от вторжений для выявления сетевых атак и предотвращения вторжения в систему спимеров, которые могут внести изменения в настройки или отключить функции борьбы со спимом и после этого отправлять спим.

8 Функциональные средства пользователей IM для поддержки борьбы со спимом

Для пользователей IM следует обеспечить возможность настройки клиента IM для защиты от спима при использовании системы IM. Следует предусмотреть в конфигурации в том числе возможности, перечисленные ниже. Пользователь IM должен обладать возможностью:

– использовать механизм подтверждения проверки, включая подтверждение запроса аутентификации и подтверждения добавления в группы, для гарантии того, что все действия утверждены пользователем;

– настраивать параметры, для того чтобы не разрешать прием сообщений или файлов от несанкционированных пользователей;

– своевременно настраивать черный список и не разрешать прием сообщений или файлов, поступающих от подозрительных учетных записей;

– использовать надежный пароль и производить его регулярную замену, с тем чтобы предотвратить кражу его учетной записи и ее использование для отправки спима;

– контролировать выполнение привилегированных функций, отключать и изменять установленные параметры, если они могут стать причиной поступления спима (например, принятие запроса аутентификации постороннего лица).

9 Руководящие указания по противодействию спиму для поставщиков услуг или операторов сетей

Поставщики услуг или операторы сетей (SP/NO) могут способствовать борьбе со спимом с помощью таких средств, как создание единой платформы управления жалобами на спим, создание единой базы данных черных списков для предотвращения поступления спима, тестирование и проверка функций защиты от спима в системе IM, а также предоставление услуг обнаружения спима поставщику услуг IM. Это включает, в том числе, перечисленные ниже меры.

– SP/NO следует создать единую платформу управления жалобами для нескольких услуг IM. Платформа управления жалобами может осуществлять прием от пользователей жалоб на учетную запись, с которой производится отправка спима, и классификацию жалоб по различным услугам IM. Когда число пользователей, подающих жалобу на какую-либо учетную запись IM, достигнет определенного значения, эта учетная запись IM будет отправлена в соответствующую базу данных черных списков для услуг IM.

– SP/NO следует создать единую базу данных черных списков для нескольких услуг IM. База данных черных списков синхронизируется с базой данных черного списка каждой услуги IM в сети. Существует два источника черных списков, в базу данных которых вносится учетная запись, если:
  - на нее поступают жалобы через вышеупомянутую платформу управления жалобами;
  - обнаруживается, что она отправляет спим.
– SP/NO следует предоставлять поставщикам услуг IM услугу регулярной проверки набора номера, чтобы предотвратить отключение функций борьбы со спимом в системе, которое может быть следствием хакерской атаки. Если соответствующая функция не включается после проверки, SP/NO могут отправить поставщику услуг IM сигнал тревоги. Функции проверки набора номера включают, помимо прочего, следующие имитации:
  - выполнение автоматической регистрации и проверку способности системы IM обнаруживать и предотвращать автоматическую регистрацию;
  - учетную запись, отправляющую несколько сообщений за единицу времени (количество сообщений превышает пороговое значение, установленное системой IM), и проверку способности системы IM обнаруживать и отклонять сообщения, отправленные впоследствии с этой учетной записи;
  - учетную запись, занесенную в черной список, для отправки сообщений, и проверку способности системы IM отклонять сообщения, отправленные с этой учетной записи;
  - вредоносные жалобы и проверку способности системы IM обнаруживать и отклонять такие жалобы.
– SP/NO могут предоставлять поставщикам услуг IM услугу обнаружения спима. Им следует заключить с каждым поставщиком услуг IM соглашение об уровне обслуживания, в котором следует определить условия конфиденциальности в целях защиты конфиденциальности пользователей. SP/NO реализуют следующую процедуру для обнаружения спима:
  - развертывание систем обнаружения на ключевых узлах сети и обнаружение заголовка пакетов сообщений IM с разрешения поставщика услуг IM;
  - анализ действий по отправке нескольких сообщений IM учетной записью IM; если количество сообщений, отправленных этой учетной записью IM в течение определенного периода времени, превышает установленное пороговое значение, можно определить, что эта учетная запись отправляет спим;
  - отклонение сообщений IM, отправленных непосредственно учетной записью, упомянутой ранее;
  - включение упомянутой ранее учетной записи в базу данных черных списков.

С помощью услуги обнаружения спима, предоставляемой SP/NO, возможно обнаруживать и отклонять спим почти на границе сети, что позволит не только сохранять пропускную способность сети, но и не допускать потребления ресурсов сервера IM.

Библиография

[[b-ITU-T X.1244] Рекомендация МСЭ-Т X.1244 (2008 г.), *Общие аспекты противодействия спаму в мультимедийных IP-приложениях.*

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session initiation protocol (SIP) extension for instant messaging*. Available [viewed 2021-10-09] at: https://tools.ietf.org/html/rfc3428

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
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	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; 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, а также соответствующие измерения и испытания
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, сети последующих поколений, интернет вещей и умные города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2022 г.