Международный союз электросвязи

МСЭ-Т X.1209

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(12/2010)

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

Безопасность киберпространства – Кибербезопасность

Возможности и контекстные сценарии для совместного использования и обмена информацией о кибербезопасности

Рекомендация МСЭ-Т X.1209

ITU-T

ITU 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.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.1209

Возможности и контекстные сценарии для совместного использования и обмена информацией о кибербезопасности

Резюме

В Рекомендации МСЭ-Т X.1209 описаны сценарии высокого уровня и возможности их поддержки для совместного использования и обмена информацией о кибербезопасности. Настоящая Рекомендация описывает важные возможности для поддержания функциональной совместимости приложений для совместного использования и обмена информацией о кибербезопасности.

Описаны возможности, которые могут использоваться в сценариях/ситуациях поддерживающих совместное участие ранее независимых объектов в различных скоординированных действиях, таких как предотвращение или прекращение целевого поведения или координации действий по анализу и определению.

Перечисленные и описанные цели возможностей должны поддерживать более действенные и эффективные действия по обеспечению безопасности за счет совместного использования и обмена информацией между доверенными сторонами в их совместной работе по контролю, поддержанию и повсеместному управлению безопасностью систем и сетей.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1209	17.12.2010 г.	17-я

Ключевые слова

Информация о кибербезопасности, обмен информацией, совместное использование информации.

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

Рекомендация МСЭ-Т X.1209

Возможности и контекстные сценарии для совместного использования и обмена информацией о кибербезопасности

1 Сфера применения

В настоящей Рекомендации описаны важные возможности для поддержания взаимодействия приложений для совместного использования и обмена информацией о кибербезопасности. Соответственно, в пункте 7 содержатся описания высокоуровневых сценариев применения возможностей, которые используются для установления контекстных рамок для определения возможностей в пункте 8. Для дальнейшего уточнения цели возможностей в пункте 9 содержатся описания возможностей, которые наиболее подходят в каждой ситуации.

Целевой аудиторией настоящей Рекомендации являются лица, участвующие в санкционированных работах по безопасности.

2 Справочные документы

Нет.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 кибербезопасность [b-ITU-T X.1205]: Набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, профессиональная подготовка, передовой 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 следующее:

- доступность;
- целостность, которая может включать аутентичность и неотказуемость;
- конфиденциальность.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 информация о кибербезопасности: Структурированная информация или знания, которые могут включать в том числе сведения о "состоянии" оборудования, программного обеспечения или сетевых систем; данные компьютерной криминалистической экспертизы, связанные с инцидентами или событиями; сведения о сторонах, осуществляющих обмен информацией о кибербезопасности; спецификации кибербезопасности для обмена информацией, включая модули, схемы и присвоенные номера; идентификаторы и атрибуты доверительности для всех предыдущих и выполняемых требований, руководящие указания и данные о практическом применении, но не ограничиваться этим.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
FTP	File Transfer Protocol	Протокол передачи файлов
HTTP	Hyper-Text Transfer Protocol	Протокол передачи гипертекста
HTTPS	Secure-Hyper-Text Transfer Protocol (HTTP over SSL)	Протокол безопасной передачи гипертекста
IPS	Intrusion Prevention System	Система предотвращения вторжения

5 Условные обозначения

Нет.

6 Введение

Кибератаки с применением вирусов, червей и т. д. сокращают скорости своего распространения по сетям, используя различные технологии, принимая все более угрожающие формы. Для того чтобы инцидентам нарушения безопасности из-за таких атак можно было противопоставить систему быстрого реагирования и принимать эффективные контрмеры, были разработаны различные виды решений в области безопасности, включающие антивирусы, обнаружение программ-шпионов, брандмауэр, виртуальные выделенные сети.

Сначала наиболее распространенная линия защиты, используемая службами безопасности против эксплойтов, вирусов, червей и ботнетов имела вид различных дискуссионных форумов, в которых участвовали многие эксперты в сфере безопасности. Обычно за пару дней или неделю дыры в системе безопасности устранялись, уязвимые места залатывались, и все приходило в нормальное состояние.

К сожалению, использование уязвимых мест вирусами, червями и ботнетами может распространяться по сети очень быстро. В течение нескольких секунд целые сети могут быть существенно поражены.

Обмен информацией о кибербезопасности в пределах одной организации может быть осуществлен быстро. Но между организациями обмен широкого спектра информацией при использовании современных методов поддерживается не так хорошо. Нехватка эффективных средств связи может превратить любую организацию в отдельно стоящий островок безопасности.

Поэтому важно совместно использовать информацию о кибербезопасности многими организациями, включая операторов связи, поставщиков услуг связи и центры по обеспечению безопасности. Для того чтобы такой обмен информацией стал возможным, необходимо иметь:

- надежные и безопасные методы быстрого обмена информацией между участниками;
- методы обеспечения защиты персональных данных.

В настоящей Рекомендации приведены продуманные сценарии и дополнительные возможности для безопасного, доверительного и надежного обмена информацией о кибербезопасности между участниками.

7 Сценарии возможностей

Для того чтобы возможности, перечисленные в пункте 8, находились в нужном контексте для правильного понимания настоящей Рекомендации, и для облегчения понимания пяти логических групп следующих возможностей здесь показано пять высокоуровневых сценариев использования, представленных в пяти различных конфигурациях.

7.1 Основной сценарий

Этот основной сценарий применяется ко всем последующим сценариям.

Сценарий: партнеры информационного обмена совместно используют информацию о событиях и инцидентах в области безопасности, полезную для выявления и предотвращения атак на их сети.

Важным аспектом этого сценария является то, что две стороны могут собирать данные аналогичного типа, но из разных источников, и/или в различных форматах, и/или данные аналогичного типа, слегка отличающиеся по содержанию.

7.2 Эксплуатационная политика

Этот сценарий описывает ситуацию, при которой различные партнеры информационного обмена имеют разные ограничения на доступ к различным элементам совместно используемой информации.

Сценарий: партнеры информационного обмена имеют договор о совместном использовании информации о событиях и инцидентах в области безопасности.

Важным аспектом данного сценария является то, что информация, доступная каждому из партнеров информационного обмена может быть ограниченной, и доступ к ней может быть основан на ранее существующих доверительных взаимоотношениях. Другим важным аспектом является то, что доверие к полученной информации может быть связано с существующими доверительными взаимоотношениями.

7.3 Региональная политика

Этот сценарий описывает ситуацию, когда информацией обмениваются несколько партнеров, причем разные партнеры имеют различные правовые и/или регуляторные ограничения для различных элементов одних и тех же типов совместно используемой информации. Этот сценарий, как и предыдущий, также подчеркивает возможность того, что один из партнеров в рамках совместного использования может получить доступ к информации, к которой он сам может не иметь доступа или возможности просмотра.

Этот сценарий отличается от предыдущего источником ограничений, накладываемых на обмен информацией. В предыдущем сценарии источником ограничений является эксплуатационная политика, выбранная каждым партнером, обменивающимся информацией, в то время как в данном сценарии ограничения связаны с эксплуатационной политикой, навязанной извне, например странами региона.

Сценарий: две стороны, работающие в разных регионах, могут обмениваться информацией в соответствии с различными требованиями, принятыми в соответствующих регионах.

Важным аспектом данного сценария является то, что помимо того, что стороны имеют различную эксплуатационную политику, они также могут быть ограничены политикой того региона, в котором происходит обмен информацией.

7.4 Формат обмена

Сценарий: один партнер информационного обмена предоставляет информацию, которая включает в себя вовлеченные порты или диапазон портов, второму партнеру относительно модели нарушения поведения трафика. Совместно используемая информация применяется для выявления отдельных случаев конкретных атак.

Важным аспектом данного сценария является необходимость того, чтобы содержание информации, которой обмениваются партнеры, было понятным и согласованным всеми партнерами информационного обмена.

7.5 Защита конфиденциальности

Сценарии, включенные в этот пункт, касаются различных вопросов, связанных с конфиденциальными данными, эта конфиденциальность может быть корпоративной или персональной. Кроме того, они подчеркивают необходимость в способности самим обеспечить конфиденциальность обмена информацией.

- Сценарий: центр обеспечения безопасности собирает информацию об атаке злоумышленников на одну из управляемых им сетей, систем или, общими словами, управляемых активов. Затем эта информация передается поставщику услуг сети для идентификации источника или источников данной атаки.

  Важным аспектом данного сценария является то, что поставщик услуг сети имеет возможность лично установить подозреваемый источник (источники) атаки, но не обязан сообщать эту информацию центру обеспечения безопасности.
- Сценарий: полный набор информации, собранной одним партнером информационного обмена, может содержать элементы, которые партнер информационного обмена пожелает открыть партнерам по обмену в рамках их организации или деятельности, но не пожелает открыть ее за пределами своей деятельности.

  Важным аспектом данного сценария является то, что стороны, участвующие в обмене информацией, могут принять решение о совместном использовании всей доступной информации или только ее части, или могут каким-либо образом скрыть часть или всю совместно используемую информацию.
- Сценарий: две стороны обмениваются конфиденциальной информацией по сетям "общего пользования".

  Важным аспектом данного сценария является то, что вне зависимости от используемого метода связи должна обеспечиваться конфиденциальность информации об обмене персональными данными.

7.6 Детализация доступа

Этот сценарий описывает ситуацию, при которой в соответствии и в зависимости от различных условий могут совместно использоваться различные типы или элементы информации о безопасности.

Сценарий: услуга публикует информационные сообщения и оповещения как для свободной доставки, так и для доставки по подписке с разными уровнями детализации в зависимости от условий конкретной подписки.

Примером различий между уровнями может служить то, что на одном уровне доступны только первичные данные, а на другом уровне – и первичные данные, и результаты их анализа.

Важным аспектом данного сценария является то, что хотя вся доступная информация может иметь один определенный тип, существуют различные "уровни" информации, доступные другим различным сторонам.

7.7 Проверка источника

Этот сценарий подчеркивает необходимость аутентификации партнеров информационного обмена.

Сценарий: партнер информационного обмена получает информацию от второго партнера и проверяет, что информация действительно пришла от второго партнера.

Важным аспектом данного сценария является то, что сторонам, обменивающимся информацией друг с другом, необходимо проверить, что информация действительно поступила от известного отправителя, а не от третьей стороны, которая пытается замаскироваться под известного отправителя.

7.8 Многоканальное распределение

Хотя этот сценарий похож на сценарий "детализации доступа", он демонстрирует ситуацию, при которой для доступа к информации разных уровней используются различные методы.

Сценарий: партнер информационного обмена делает уведомления и оповещения о безопасности доступными с помощью разных средств и при различных условиях. Эти данные могут быть доступны для бесплатной загрузки из директории с поиском, выборочно доставляться по электронной почте на одном уровне обслуживания, или быть доступными в машиночитаемой форме на другом уровне обслуживания.

Важным аспектом данного сценария является то, что доступ к одинаковым или различным типам информации может осуществляться с помощью разных средств и при различных условиях.

7.9 Совместимость с предыдущими версиями

Сценарий: два партнера информационного обмена уже обмениваются определенной информацией, используя специальные форматы и протоколы. Появляется новый стандарт поддержки существующих методов обмена, который предоставляет новые и дополнительные функции.

Важным аспектом данного сценария является то, что существующие приложения должны в максимально возможной степени поддерживаться, и в то же время, если новые стандарты уже имеются, должно выполняться их обновление.

8 Возможности

В следующем пункте перечислены различные возможности, которые дополняют виды сценариев, перечисленных выше в пункте 7.

8.1 Возможности формата/кодирования

- Формат и структура информации о безопасности должны быть известны и понятны обеим сторонам.
  - Обмен информацией о безопасности имеет неоднородный характер, например сообщения брандмауэра или других устройств безопасности сети, а также различные виды дополнительной специальной информации, такие как отчет о событии и инциденте, анализ и реагирование, обмен данными экспертизы и др.
  - Формат обмениваемой информации представляет собой различные типы информации о безопасности, созданные и применимые в условиях неоднородной системы.
- Различные типы информации о безопасности должны быть доступны для совместного использования. Примерами являются показатели поведения трафика, показателя доступа к системе, источник IP-адреса(ов), источник и/или целевой диапазон портов и т. д.
- Стороны должны иметь возможность охватить различные уровни информации от содержания одиночного пакета до всех пакетов, участвующих в глобальной DDoS-атаке.
- Необходимо, чтобы содержание информации о безопасности было известно и понятно обеим сторонам.
- Необходимо идентифицировать предмет рассмотрения, пригодность и доступность информации.

8.2 Возможности передачи/обмена

- Стороны должны иметь возможность передавать, доставлять и принимать информацию о безопасности в широком и постоянно расширяющемся диапазоне сред распространения и передачи.
- Приложениям, возможно, потребуется поддерживать синхронный и асинхронный обмен между сторонами в ходе совместного использования и обмена информацией о кибербезопасности.
- Приложениям, возможно, потребуется поддерживать пассивный прием сообщений, прием сообщений с опросом и подписку на основе доставки информации.
- Приложениям необходимо поддерживать стабильную работу в ходе обмена и обработки больших объемов информации о безопасности.

- При использовании протоколов обмена необходимо применять и/или основываться на существующих и уже широко используемых протоколах.

8.3 Возможности безопасности

- Совместно используемая или передаваемая информация о кибербезопасности должна быть аутентифицирована и проверена.
- Приложения должны обеспечивать надежность, конфиденциальность, целостность и доступность информации и услуг.
- Должна иметься возможность достоверно аутентифицировать и подтверждать участвующие стороны.
- Приложения должны предотвращать атаки против совместно используемой и передаваемой информации о кибербезопасности, вызванные подделкой и/или фальсификацией информационного содержания или источника/получателя содержащейся информации.
- Стороны-источники должны гарантировать, что к конфиденциальной информации имеют доступ только авторизованные стороны. Это делается для обеспечения конфиденциальности сообщений и относится и к персональным данным, необходимым для личной идентификационной информации, и к частной корпоративной информации, и к любой информации, считающейся важной для сохранения конфиденциальности и доступной только авторизованным лицам.
- Стороны-источники должны управлять доступом на отдельные уровни так, чтобы только авторизованные стороны, имеющие доступ к определенным частям данного участка информации о безопасности, обладали этой возможностью и не имели бы доступа к элементам, к которым не допущены.
- Стороны должны обеспечить защиту информации о безопасности от доступа неавторизованных сторон даже в открытой среде, где информация о безопасности доступна всем, включая неавторизованные стороны.

8.4 Возможности правил

- Стороны должны иметь возможность самостоятельно определить и объявить соответствующие правила, местные и/или региональные, относящиеся к предоставлению и/или доступу к предоставляемой информации по кибербезопасности. Примером этого может служить сокрытие информации о маршрутизации, которая может размещаться в адресах получателей под предлогом того, что это касается "правил".
- Стороны должны иметь возможность предоставлять или иметь доступ к информации о безопасности в порядке, предусмотренном установленными ими правилами в отношении предоставления и/или доступа к информации о безопасности.
- Стороны должны иметь возможность объявить в рамках какой юрисдикции применим данный набор объявленных правил.
- Стороны должны иметь возможность самостоятельно определить и объявить возможные требования юрисдикции и ограничения, касающиеся предоставления и/или доступа к информации о безопасности в пределах своей компетенции.
- Стороны должны иметь возможность предоставлять или иметь доступ к информации о безопасности в порядке, предусмотренном установленными ими соответствующими требованиями юрисдикции.

8.5 Возможность независимости от поставщиков

Для поддержки совместного использования и обмена как можно более широким спектром информации о кибербезопасности приложения должны предоставлять услуги, минимально зависящие от любой определенной системы или определенных данных поставщика. В то же время будет лучше, если любые определенные системы или определенные данные поставщиков будут исключены.

9 Применимость возможностей

Сценарии и возможности, описанные в настоящей Рекомендации, предоставляют набор разрозненных "инструментов", которые можно смешивать и подбирать для создания своего приложения. Некоторые приложения, которые являются наиболее простыми, например сбор данных и/или поиск информации, потребуют только некоторых из перечисленных возможностей, в то время как другие, многофункциональные и предоставляющие более широкий спектр услуг, потребуют объединить и задействовать больше возможностей.

Далее рассмотрены ситуации, в которых отдельные виды возможностей необходимы и когда они могут не быть обязательными.

9.1 Возможности форматирования/кодирования

Для осуществления любого совместного использования и обмена информацией о кибербезопасности, и отправитель, и получатель информации должны иметь четкое представление о содержании информации, которой они обмениваются. Соответственно, возможности форматирования и кодирования должны быть применимы к любому и ко всем сценариям, по которым происходит совместное использование и/или обмен информацией о кибербезопасности.

9.2 Возможности передачи/обмена

Точно так же как и возможности форматирования и кодирования, двум или более партнерам информационного обмена нужен способ получения принимающей стороной информации от передающей стороны.

9.3 Возможности безопасности

Не имеет смысла обмениваться информацией о безопасности без, по крайней мере, некоторого уровня гарантии безопасности, заключающегося в идентификации партнеров информационного обмена и обеспечения безопасности любого канала связи между ними.

Однако различные ситуации и приложения будут иметь различные требования к безопасности, поэтому важно, чтобы те, кто их использует и разрабатывает, учитывали потребности своих конкретных приложений.

К примеру, в приложении, где два партнера информационного обмена работают с выделенной линией связи, в которой реализованы меры по обеспечению их безопасности, в этом случае они мало нуждаются или совсем не нуждаются в специальных мерах по обеспечению безопасности, помимо тех, что уже содержатся в среде передачи.

С другой стороны, если информация доставляется по открытым каналам связи, скорее всего потребуется широкий спектр мер обеспечения безопасности.

9.4 Возможности правил

Не все приложения, поддерживающие функции совместного использования и обмена информацией о кибербезопасности, должны использовать возможность наложения запретов, ограничений и/или санкционирования. Однако во многих коммерческих и деловых ситуациях важно иметь возможность наложить запреты на подобные правила, касающиеся информации.

Как и для возможностей обеспечения безопасности, где условия или ситуации, в которых функции, основанные на правилах, предоставляются вне данного приложения, возможно посредством соглашения об обслуживании или договорного соглашения, способность объявлять и вынуждать исполнять правила в рамках своего же приложения не всегда необходима.

9.5 Возможности независимости от поставщиков

Независимость от поставщиков сильно зависит от ситуации. Если какие-либо из совместно используемых или передаваемых данных созданы продукцией конкретного поставщика с использованием формата обмена и/или протоколов обмена конкретного поставщика, то нельзя говорить о реальной независимости.

С другой стороны, если целью данного приложения является расширение дополнения и поддержка обмена информацией, то важно сохранить нейтральную позицию в отношении определенных способов поставщика и/или информации.

Дополнение I

Краткая информация о совместном использовании и обмене информацией о кибербезопасности

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Настоящее Дополнение описывает концептуальную структуру примера применения информации о кибербезопасности, как показано на рисунках I.1 и I.2. Эти рисунки демонстрируют две различные точки зрения на топологию приложения, использующего возможности, перечисленные в пункте 7. Хотя возможны другие топологии, показанная топология включает применение всех возможностей, в то время как другим возможным топологиям и приложениям может потребоваться лишь какая-либо подгруппа описанных возможностей.

На первом рисунке представлен сценарий с множеством партнеров информационного обмена с различными функциями, приложениями и совместно используемой информацией. На рисунке показаны различные способы того, как приложения, использующие информацию, могут получить доступ к информации, полученной от определенного узла.

Следует отметить, однако, что настоящее Дополнение не предписывает, как именно или с какой целью используется информация, а лишь говорит, что доступ к информации может быть осуществлен различными способами. Кроме того, первый рисунок показывает, что все процедуры обмена между узлами поддерживаются с использованием сообщений стандартизированного формата.

Второй рисунок является видом первого рисунка из третьего измерения, он показывает два примера партнеров информационного обмена, а также описывает наиболее вероятные возможности каждого из них, необходимые для участия в процессе обмена. Повторим, что как и на первом рисунке, конкретным применениям или приложениям может не потребоваться поддержка всех функций всеми перечисленными возможностями, и существует свобода выбора функций, которые требуется включить в данное применение/приложение.

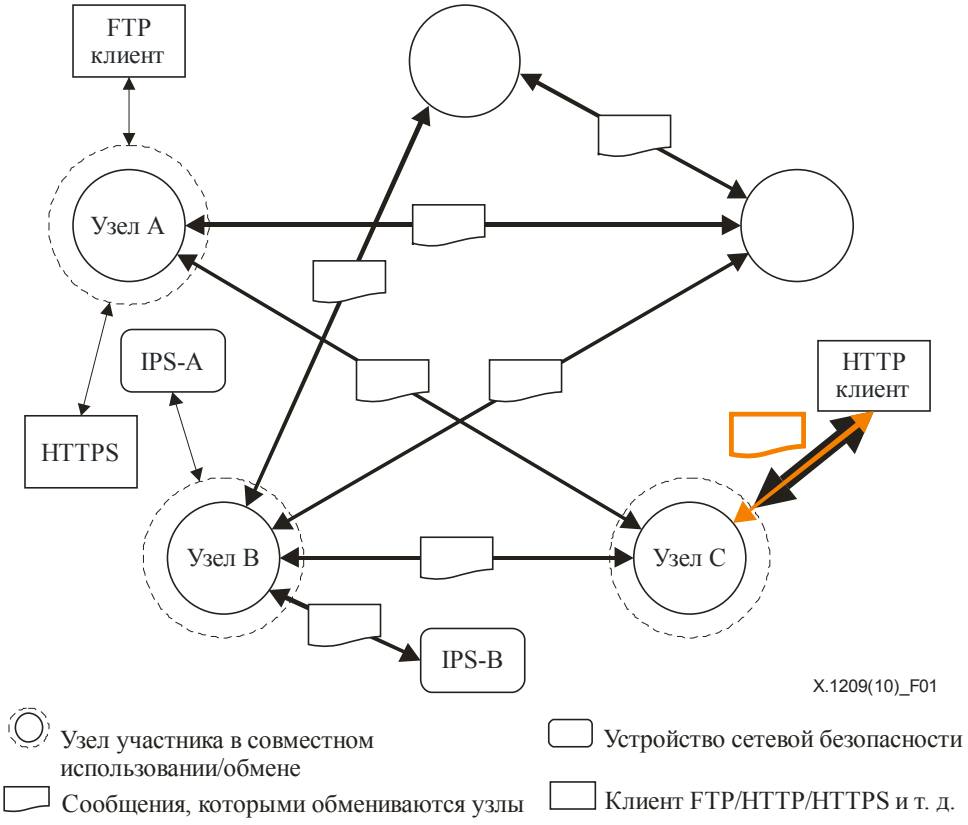

Рисунок I.1 – Пример применения совместного использования и обмена информацией о кибербезопасности

- Все участвующие узлы связываются друг с другом посредством стандартизированных сообщений.

  Следующие возможности играют важную роль в поддержке данной функции:

  – возможности форматирования/кодирования (пункт 8.1);

  – возможности передачи/обмена (пункт 8.2).

- Данные, запрошенные от одного узла, могут фактически быть предоставлены другому узлу.

  Следующие возможности играют важную роль в поддержке данной функции:

  – возможности безопасности (пункт 8.3);

  – возможности правил (пункт 8.4).

- Данный узел может оперировать только протоколами инфраструктуры или может давать доступ к данным инфраструктуры посредством других протоколов/услуг, например FTP или HTTP используются для доступа к данным инфраструктуры через узел A.

  Следующие возможности играют важную роль в поддержке данной функции:

  – возможности форматирования/кодирования (пункт 8.1);

  – возможности передачи/обмена (пункт 8.2);

  – возможности независимости от поставщиков (пункт 8.5).

- Устройства обеспечения безопасности, например система предотвращения вторжения (IPS-A) и другая система предотвращения вторжения (IPS-B), связывающиеся с узлом B, могут иметь доступ к информации о кибербезопасности либо непосредственно, например, IPS-B или через внешнюю службу, например через IPS-A, позволяющую устройствам применять функцию совместного использования и обмена, либо при совместном использовании и обмене информацией о кибербезопасности стандартизированным способом, либо при использовании методов зависимых/собственных устройств.

  Следующие возможности играют важную роль в поддержке данной функции:

  – возможности форматирования/кодирования (пункт 8.1);

  – возможности передачи/обмена (пункт 8.2);

  – возможности независимости от поставщиков (пункт 8.5).

- Устройство обеспечения безопасности может использовать любой протокол или уровень протокола для поддержки доставки сообщений, например TCP/IP, HTTP, HTTPS, SSL, используются клиентами, обслуживаемыми узлом C.

  Следующие возможности играют важную роль в поддержке данной функции:

  – возможности форматирования/кодирования (пункт 8.1);

  – возможности передачи/обмена (пункт 8.2);

  – возможности независимости от поставщиков (пункт 8.5).

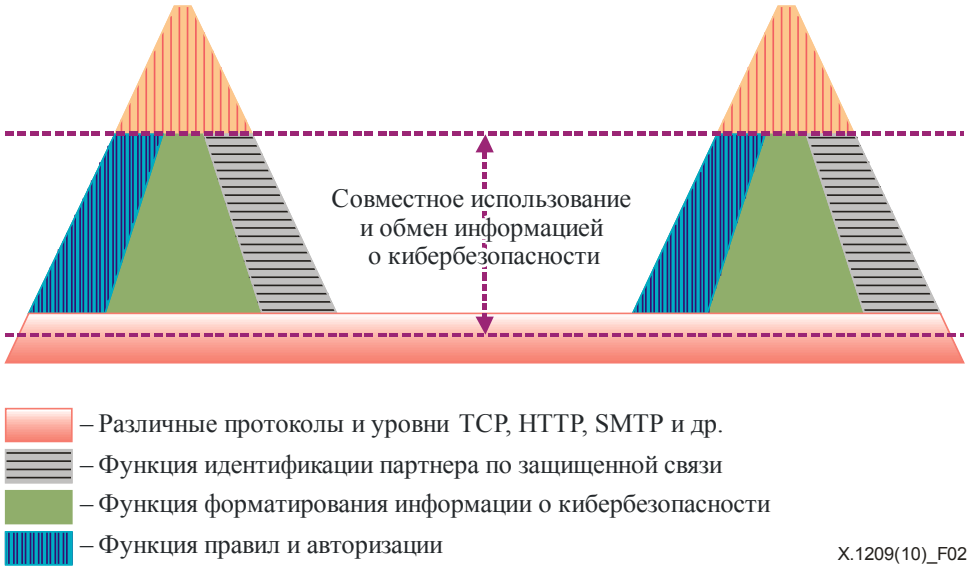

Рисунок I.2 – Вид двух узлов

- Участвующие узлы обмениваются запросами и ответами посредством различных протоколов и уровней протоколов.

  Следующие возможности играют важную роль в поддержке данной функции:

  – возможности форматирования/кодирования (пункт 8.1);

  – возможности передачи/обмена (пункт 8.2).

- Для многих приложений потребуются надежные методы идентификации партнеров по связи.

  Следующие возможности играют важную роль в поддержке данной функции:

  – возможности безопасности (пункт 8.3);

  – возможности правил (пункт 8.4).

- Узлы получают и используют данные, предоставляемые другими узлами.

  Следующие возможности играют важную роль в поддержке данной функции:

  – возможности форматирования/кодирования (пункт 8.1);

  – возможности безопасности (пункт 8.3);

  – возможности правил (пункт 8.4);

  – возможности независимости от поставщиков (пункт 8.5).

- Приложения используют различные функции проверки подтверждения авторизации для удовлетворения различных требований по обеспечению безопасности, необходимых в зависимости от приложения.

  Следующие возможности играют важную роль в поддержке данной функции:

  – возможности правил (пункт 8.4).

- Приложения разных узлов могут использовать информацию об идентификации от других узлов по разным причинам, например, клиент узла A запрашивает доступ к информации о кибербезопасности, доступной на узле B.

  Следующие возможности играют важную роль в поддержке данной функции:

  – возможности правил (пункт 8.4).

- Основными функциями данного участвующего узла являются:
  - прием информации о кибербезопасности;
  - хранение/архивирование информации о кибербезопасности;
  - доставка ответов относительно информации о кибербезопасности.

  Следующие возможности играют важную роль в поддержке данной функции:
  - возможности форматирования/кодирования (пункт 8.1);
  - возможности передачи/обмена (пункт 8.2);
  - возможности правил (пункт 8.4).
- Приложения используют соответствующие инструменты, например проверку аутентификации и авторизации для решения вопросов, связанных с доступом.

  Следующие возможности играют важную роль в поддержке данной функции:
  - возможности безопасности (пункт 8.3);
  - возможности правил (пункт 8.4).
- Приложения используют общую модель данных для решения вопросов, связанных с доступом между узлами.

  Следующие возможности играют важную роль в поддержке данной функции:
  - возможности форматирования/кодирования (пункт 8.1);
  - возможности передачи/обмена (пункт 8.2);
  - возможности независимости от поставщиков (пункт 8.5).
- Приложения используют надежные идентификаторы для связи между узлами, а также между узлами и клиентами.

  Следующие возможности играют важную роль в поддержке данной функции:
  - возможности безопасности (пункт 8.3);
  - возможности правил (пункт 8.4).
- Ответы и запросы между узлами считаются нормой, при этом приложения могут предоставлять интерфейс прикладного уровня между узлами по запросам клиентов и в ответ тем клиентам, которые не использую стандартизированные методы и/или протоколы, используемые между узлами.

  Следующие возможности играют важную роль в поддержке данной функции:
  - возможности форматирования/кодирования (пункт 8.1);
  - возможности передачи/обмена (пункт 8.2);
  - возможности независимости от поставщиков (пункт 8.5).
- Инфраструктура поддерживает функционирование и пассивной модели приема сообщений, и модели приема сообщений с опросом, а также функционирование модели с использованием всех возможностей и модели без изменения состояния в процессе исполнения.

  Следующие возможности играют важную роль в поддержке данной функции:
  - возможности передачи/обмена (пункт 8.2).
- Архитектура приложения может предоставлять "зацепки" в моделях надежной идентификации и идентификации данных, которые требуют приложения.

  Следующие возможности играют важную роль в поддержке данной функции:
  - возможности безопасности (пункт 8.3);
  - возможности правил (пункт 8.4).

Дополнение II

Соответствующая деятельность

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

II.1 Общеизвестная информация о безопасности

Общеизвестная информация о безопасности – это открытая информация о безопасности, предоставляемая некоммерческими организациями, такими как CERT/CC, MITRE или открытыми проектами. Например, информация об общеизвестных уязвимостях и дефектах (CVE), общеизвестный перечень слабых мест (CWE), общеизвестный перечень вредоносного программного обеспечения (CME), общеизвестный перечень и классификация схем атак (CAPEC), общедоступная база данных уязвимостей (OSVDB), сигнатуры, предоставляемые [b-Snort] или [b-Bro], и так далее.

В случае MITRE, CVE является справочником общеизвестной информации об уязвимости и рисках нарушения безопасности. В его основе лежит Национальная база данных уязвимостей (NVD), разработанная Американским национальным институтом стандартов. CWE предоставляет единый измеряемый набор слабых мест программного обеспечения (ПО), который позволяет более эффективно обсудить, описать, выбрать и применить инструменты и услуги программного обеспечения в области безопасности, которые обнаружат эти слабые места в кодах источников и операционных системах. CME предоставляет отдельные, общеизвестные идентификаторы угроз новых вирусов и наиболее распространенных появляющихся угроз вирусов для снижения общественных потерь во время инцидентов с вредоносным ПО. Это не попытка изменить имена поставщиков, используемые вирусами или другими формами вредоносного ПО, а скорее способ облегчить совместное использование возможности нейтрального индексирования вредоносного ПО. CAPEC является общедоступным каталогом схем атак вместе с подробной схемой и классификацией систематизации.

Что касается OSVDB, этот проект является независимой и базой данных с открытыми исходными кодами, созданной обществом для обеспечения безопасности общества. Она представляет собой точную, подробную, актуальную и объективную информацию об уязвимостях безопасности. Также OSVDB будет способствовать более широкой и открытой совместной деятельности между компаниями и частными лицами, чтобы избежать дублирующей работы и снизить расходы, связанные с развитием и поддержанием баз данных уязвимостей внутреннего пользования.

Snort является общедоступной сетевой системой обнаружения и предотвращения вторжений с использованием управляемого правилами языка, которая сочетает в себе преимущества сигнатуры, протокола и методов проверки на основе аномалий. Правила Snort прошли тщательную проверку теми же стандартами VRT (группа обнаружения уязвимостей), которые применяются для пользователей.

Наконец, Bro – проект с открытыми исходными кодами на основе обнаружения сетевого вторжения, который пассивно отслеживает сетевой трафик и следит за подозрительной деятельностью. Правила Bro могут описывать действия, действия, о которых нужно предупреждать, или сигнатуры, описывающие известные атаки, или доступ к известным уязвимостям.

II.2 Новейшая информация о безопасности

Новейшая информация о безопасности – это автоматически создаваемые сигнатуры новейших угроз или атак, аномального трафика, неизвестных червей и т. п. Создание сигнатуры атаки является в настоящее время популярной темой исследования, и были предложены несколько экспериментальных решений, таких как "Early bird" и "Polygraph". Основная роль этих решений состоит в обнаружении кибератак и захвате последовательности байтов, которые являются идентификацией атаки. Услуга сигнатуры "FirstLight" или активная защита от вредоносного ПО Endeavor Security и ZASMIN (инфраструктура управления сигнатурой атаки "Zero-day") ETRI предоставляет новые сигнатуры, которые постоянно обновляются, пересматриваются и расширяются. Эти развивающиеся передовые технологии создания диаграмм дает возможность автоматически создавать сигнатуры на основе трафика атаки. Несмотря на достигнутый прогресс в улучшении качества сигнатур, совместное использование сигнатур все еще находится в зачаточном состоянии.

II.3 Деятельность, связанная с совместным использованием информации о безопасности

II.3.1 Группы реагирования на компьютерные инциденты (CIRTs)

CIRT изучают уязвимость сетевой безопасности, исследуют долгосрочные изменения в сетевых системах, а также разрабатывают информационные и учебные пособия с целью улучшения обеспечения безопасности. Они по-прежнему реагируют на серьезные инциденты в области безопасности и проводят анализ уязвимостей продукта. Наряду со стремительным увеличением масштаба интернета и его использованием для основного функционирования, существуют прогрессирующие изменения в технологиях нарушителей, увеличиваются суммы ущерба, возрастает сложность обнаружения атак, возрастает сложность поимки нарушителей.

II.3.2 Европейское агентство по информационной безопасности

Европейское агентство по информационной безопасности (ENISA) представляет собой первый результат исследования Европейской системой совместного использования информации и предупреждения (EISAS) по информированию малых и средних предприятий (SME) и граждан Европейского Союза об угрозах, уязвимых местах и атаках. В результате исследования получен вывод, что наиболее оптимальный путь в ЕС для облегчения совместного использования информации состоит в принятии на себя роли ведущей содействующей организации при обсуждении и быть "хранителем передового опыта" среди национальных систем совместного использования информации и предупреждения, принимая на себя центральную рабочую функцию. Для того чтобы выполнить исследование предполагалась техническая реализуемость EISAS, которая требовала проверки. В рамках EISAS предлагалась общая модель, состоящая из трех основных компонентов, и эта модель предназначалась для определения областей идентификации, в которых EISAS должна улучшить эффективность существующей деятельности по совместному использованию информации в государствах-членах и ликвидировать пробел в области информации о NIS (сетевая и информационная безопасность). Три компонента – это IGC (компонент накопления информации), IPC (компонент обработки информации) и IDC (компонент распространения информации).

II.3.3 Форум групп реагирования на инциденты и обеспечения безопасности

Форум групп реагирования на инциденты и обеспечения безопасности (FIRST) является главной организацией и признан мировым лидером в области реагирования на инциденты. Государства-члены FIRST дают возможность группам реагирования на инциденты более эффективно отвечать на инциденты в сфере безопасности – реагировать, а также действовать с опережением. Этот форум объединяет различные группы реагирования на инциденты в сфере компьютерной безопасности государственных, коммерческих и образовательных организаций. Этот форум призван способствовать расширению сотрудничества и координации по предотвращению инцидентов, стимулированию быстрого реагирования на инциденты и содействию совместному использованию информации среди своих членов и общества в целом.

II.3.4 Группа реагирования на нарушение компьютерной защиты Азиатско-Тихоокеанского региона

Группа реагирования на нарушение компьютерной защиты Азиатско-Тихоокеанского региона (APCERT) совместно с Группами реагирования на нарушение компьютерной защиты (CERTs) и Группы реагирования на инциденты в сфере компьютерной безопасности (CSIRTs) обеспечивает безопасность в интернете в Азиатско-Тихоокеанском регионе на основе искреннего совместного использования информации, доверии и сотрудничестве. APCERT способствуют совместному использованию информации и обмену технологиями среди ее членов, включая информацию о безопасности, вирусы и вредоносные коды. APCERT также содействует проведению совместных исследований и разработок по вопросам, представляющим интерес для ее членов, а также дает рекомендации, помогающие в решении правовых вопросов, связанных с информацией о безопасности и реагированием на чрезвычайные ситуации в пределах границ региона.

II.3.5 Центр обмена информацией и анализа в области электросвязи

Интернет и другие сети электросвязи составляют основу социально-экономической структуры в мировом масштабе. Обеспечение информационной безопасности становится насущной проблемой в социально-экономической жизни.

Центр обмена информацией и анализа в области электросвязи (Telecom-ISAC) ориентирован на сбор, анализ и совместное использование информации об инцидентах и принимает актуальные меры для обеспечения бесперебойной и стабильной деятельности услуг электросвязи. Более того, ISAC создает форум с широким кругом участвующих членов для совместного использования их знаний и опыта, включая информацию о рисках в отношении безопасности, уязвимостях, решениях в области безопасности и др.

Дополнение III

Соответствующая деятельность

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

[APCERT] Группа реагирования на нарушение компьютерной защиты Азиатско-Тихоокеанского региона, http://www.apcert.org.

[CERT] Группы реагирования на нарушение компьютерной защиты, http://www.cert.org.

[ENDEAVOR] Компания Endeavor Security, http://www.endeavorsecurity.com.

[FIRST] Форум групп реагирования на инциденты и обеспечения безопасности, http://www.first.org.

[MITRE] MITRE, http://makingsecuritymeasurable.mitre.org/.

[Telecom-ISAC] Центр обмена информацией и анализа в области электросвязи, https://www.telecom-isac.jp.

[WIKI] Wikipedia, http://en.wikipedia.org.

Библиография

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

[b-Bro] Bro (ноябрь 2004 г.), *Quick Start Guide Manual*.

[b-EISAS] European information sharing and Alert System (2006/2007), *A feasibility study*.

[b-OSVDB] Open Source Vulnerability DataBase, *Project Aims and Objectives*.

[b-Snort] Snort (май 2008 г.), *Snort User Manual 2.8.2*.

[b-ZASMIN] Information Security Research Division of ETRI, *Zero-day Attack Signature Management Infrastructure*.

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.