Международный союз электросвязи

МСЭ-Т

X.1550

(03/2017)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Обмен информацией, касающейся кибербезопасности – Обмен информацией о политике

Модели контроля доступа для сетей обмена информацией об инцидентах

Рекомендация МСЭ-Т X.1550

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
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

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

Рекомендация МСЭ-Т X.1550

Модели контроля доступа для сетей обмена информацией об инцидентах

Резюме

В Рекомендации МСЭ-Т X.1550 представлены существующие подходы к реализации политики контроля доступа для сетей обмена информацией об инцидентах. В настоящей Рекомендации представлены разнообразные уже установившиеся модели контроля доступа, модели обмена информацией, а также критерии для оценки показателей работы сетей обмена информацией об инцидентах. Рассматриваются основанные на стандартах решения, направленные на содействие реализации различных моделей контроля доступа в рамках различных моделей обмена информацией по вопросам кибербезопасности и в разных условиях среды доверия.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1550	30.03.2017 г.	17-я	11.1002/1000/13198

Ключевые слова

Контроль доступа, авторизация, CERT, CSIRT, CYBEX, IAM, сеть обмена информацией об инцидентах, реагирование на инциденты.

* 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 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

Рекомендация МСЭ-Т X.1550

Модели контроля доступа для сетей обмена информацией об инцидентах

1 Сфера применения

В настоящей Рекомендации представлены существующие подходы к реализации политики контроля доступа для сетей обмена информацией об инцидентах. В настоящей Рекомендации представлены разнообразные уже установившиеся модели контроля доступа, модели обмена информацией, а также критерии для оценки показателей работы сетей обмена информацией об инцидентах. Рассматриваются основанные на стандартах решения, направленные на содействие реализации различных моделей контроля доступа в рамках различных моделей обмена информацией и в разных условиях среды доверия.

2 Справочные документы

Следующие Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые посредством ссылки в настоящем тексте, составляют положения настоящей Рекомендации. На момент публикации указанные издания были в силе. Все Рекомендации и другие справочные документы могут быть пересмотрены; поэтому пользователям настоящей Рекомендации настоятельно предлагается изучить возможность использования самого последнего издания Рекомендаций и других справочных документов, которые перечислены ниже. Список действующих на данный момент Рекомендаций МСЭ-Т публикуется на регулярной основе.

Ссылка на какой-либо документ в настоящей Рекомендации не предоставляет ему, как самостоятельному документу, статус Рекомендации.

[ITU-T X.1500] Рекомендация МСЭ-Т X.1500 (2011 г.), *Методы обмена информацией о кибербезопасности.*

[ITU-T X.1570] Рекомендация МСЭ-Т X.1570 (2011 г.), *Механизмы обнаружения, используемые при обмене информацией о кибербезопасности*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определения которых содержатся в других документах:

3.1.1 контроль доступа (access control) [b-ITU-T X.1252]: Процедура, применяемая для определения того, следует ли предоставлять тому или иному объекту доступ к ресурсам, устройствам, услугам или информации на основе заранее установленных правил и конкретных прав или полномочий, связанных с запрашивающей стороной.

3.1.2 авторизация (authorization) [b-ITU-T M.3345]: Определяет, каким образом и при каких условиях участники управления на основе самообслуживания могут использовать функции самообслуживания и какие действия по самообслуживанию им разрешено выполнять.

3.1.3 обмен информацией об инцидентах (incidents exchange) [ITU-T X.1570]: Передача информации о кибербезопасности между двумя или более объектами кибербезопасности. Такая передача может осуществляться в одном, двух или нескольких направлениях, т. е. многие ко многим.

ПРИМЕЧАНИЕ. − В настоящей Рекомендации термин "обмен информацией об инцидентах" принят эквивалентным термину "обмен".

3.1.4 доверенный домен (trust domain) [b-ITU-T M.3410]: Набор информации и связанных с ней ресурсов, включающий пользователей, сети, хранилища данных и приложения, которые осуществляют обработку данных в этих хранилищах. Различные доверенные домены могут совместно использовать одни и те же физические компоненты. Кроме того, единый доверенный домен может применять различные уровни доверия в зависимости от того, что необходимо узнать пользователю, а также от чувствительности информации и связанных с ней ресурсов.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации содержатся определения следующих терминов:

3.2.1 конфликт политики контроля доступа (access control policy conflict): Определяет действия двух правил, противоречащих друг другу. Объект, реализующий политику, не сможет определить, какое действие выполнять.

ПРИМЕЧАНИЕ. – Настоящее определение основано на описании разрешения конфликта в [b-ITU-T X.1036].

3.2.2 динамическое разрешение конфликта политики (dynamic policy conflict resolution): Стратегии разрешения конфликтов, которые применяются в процессе работы.

3.2.3 сети обмена информацией об инцидентах (incidents exchange networks): Обобщение эксплуатационной инфраструктуры обмена информацией о кибербезопасности (CYBEX) на основе централизованного или федеративного управления.

3.2.4 информация об инцидентах (incidents information): Подмножество информации о кибербезопасности, структурированная информация или структурированные знания, касающиеся экспертно-технического анализа, относящегося к инцидентам или событиям.

ПРИМЕЧАНИЕ. – Настоящее определение основано на описании обмена (информацией о кибербезопасности) в [b-ITU-T X.1570].

3.2.5 статическое разрешение конфликта политики (static policy conflict resolution): Стратегии разрешения конфликтов, которые применяются на этапе разработки.

4 Аббревиатуры и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ABAC	Attribute Based Access Control	Контроль доступа на основе атрибутов
ACL	Access Control List	Список контроля доступа
CERT	Computer Emergency Response Team	Группа реагирования на нарушения компьютерной защиты
CSIRT	Computer Security Incident Response Team	Группа реагирования на инциденты, связанные с компьютерной безопасностью
CYBEX	CYBersecurity information EXchange	Обмен информацией о кибербезопасности
DAC	Discretionary Access Control	Избирательный контроль доступа
IAM	Identity and Access Management	Управления определением идентичности и доступом
IODEF	Incident Object Description Exchange Format	Формат обмена описаниями инцидентов как объектов
IT	Information Technology	Информационная технология
MAC	Mandatory Access Control	Обязательный контроль доступа
PBAC	Policy Based Access Control	Контроль доступа на основе политики
PDP	Policy Decision Point	Пункт выбора политики
PERMIS	PrivilEge and Role Management Infrastructure Standards	Стандарты для инфраструктур управления привилегиями и ролью
RAdAC	Risk-Adaptive Access Control	Адаптированный к риску контроль доступа
RBAC	Role Based Access Control	Контроль доступа на основе ролей
RID	Real-time Inter-network Defense	Межсетевая защита в реальном времени
RIDT	Real-time Inter-network Defense Transport	Транспортирование сообщений межсетевой защиты в реальном времени

STIX	Structured Threat Information Expression	Структурированное выражение информации об угрозе
TAXII	Trusted Automated Exchange of Indicator Information	Доверенный автоматический обмен информацией об индикаторах
TBAC	Task Based Access Control	Контроль доступа на основе задачи
TBAM	Task Based Access Management	Управление доступом на основе задачи
XACML	eXtensible Access Control Markup Language	Расширяемый язык разметки контроля доступа
XML	eXtended Markup Language	Расширяемый язык разметки

5 Условные обозначения

В контексте настоящей Рекомендации "контроль доступа" рассматривается как общий механизм, поддерживающий процедуры авторизации.

6 Общий обзор

Смягчение рисков может потребоваться для снижения финансовых затрат, связанных со смягчением компьютерных атак, а также для обеспечения гарантий безопасности в рамках организации/сотрудничества или службы /системы. Сети обмена информацией об инцидентах функционируют для того, чтобы предотвратить или уменьшить риски, связанные с компьютерными атаками. Практика обмена информацией об инцидентах в области кибербезопасности представляет различные модели обмена информацией, внедренные в среде централизованного или федеративного управления. Обмен информацией об инцидентах основан на определенном уровне доверия, который соотносится со связанными с этим рисками и устанавливает необходимость обеспечивать, чтобы информация конфиденциального или чувствительного характера не предоставлялась для совместного использования ненадлежащим образом. Поэтому некоторые модели контроля доступа являются более эффективными с точки зрения показателей работы, реализации и обеспечения безопасности.

Общий рост и взаимная интеграция глобальных информационных систем стимулировали разработку современных моделей контроля доступа, которые лежат в основе процессов авторизации. Существующие языки политики контроля доступа содействуют развертыванию политики безопасности и создают проблемы, специфичные для различных моделей контроля доступа и эксплуатационных условий.

Механизмы и подходы, представленные в настоящей Рекомендации, могут быть использованы в качестве элементов, которые обеспечивают реализацию политики контроля доступа для лежащего в ее основе обмена информацией о кибербезопасности формата (CYBEX) и транспортных протоколов, таких как: формат обмена описаниями инцидентов как объектов (IODEF) [b-ITU-T X.1541], межсетевая защита в реальном времени (RID) [b-ITU-T X.1580] + транспортирование сообщений межсетевой защиты в реальном времени (RIDT) [b-ITU-T X.1581], структурированное выражение информации об угрозе (STIX) [b-stix] + доверенный автоматический обмен информацией об индикаторах (TAXII) [b-taxii] и другие.

7 Классификация сетей обмена информацией об инцидентах

7.1 Эксплуатационные условия

Сети обмена информацией об инцидентах функционируют в следующей среде:

- единый доверенный домен (централизованное управление);
- федеративные доверенные домены (децентрализованное управление).

7.2 Модели обмена информацией об инцидентах

Ниже представлены модели обмена информацией об инцидентах:

- "Одноранговая" модель, предусматривающая однонаправленный или двунаправленный обмен информацией между двумя участниками.
- "Звездообразная" модель. Этот тип модели часто имеет центральный узел, который принимает данные от участвующих членов (лучей). Центральный узел может либо непосредственно перераспределять поступающие данные другим членам, либо предоставлять дополнительные услуги и направлять новую (и предположительно более полезную) информацию своим членам. При таком подходе центральный узел действует в качестве банка информации, который может содействовать обмену информацией, защищая в то же время опознаватели своих членов. Связанная с этим проблема заключается в том, что обмен информацией в рамках этой модели требует высокого уровня доверия к центральному узлу [b-MITRE Models].
- Модель "универсальной рассылки". Эта модель позволяет любому участнику делиться информацией со всем списком членов, минуя центральный узел. В связи с тем, что члены обмениваются информацией напрямую друг с другом, информация распространяется быстро и может легко передаваться в широких масштабах многим участникам. [b-MITRE Models].

На основе этих трех моделей можно построить следующие ориентированные на услуги модели:

- "Обнаружение-запрос-ответ". Это – двухэтапная модель, в которой на первом (факультативном) этапе используются механизмы обнаружения [ITU-T X.1570] для идентификации централизованных или распределенных источников относящейся к инцидентам информации. На втором этапе потребители получают информацию, запрашивая базы данных, а решения об ответе основываются на модели контроля доступа.
- "Обнаружение-подписка-уведомление". Это – двухэтапная модель, в которой на первом (факультативном) этапе используются механизмы обнаружения [ITU-T X.1570] для идентификации централизованных или распределенных источников относящейся к инцидентам информации. На втором этапе потребители получают данные путем оформления подписки и получают информацию из выбранных источников в форме уведомлений.

7.3 Модели контроля доступа

Модели контроля доступа служат основой политики в области безопасности. На практике они официально фиксируются с помощью конкретных диалектов расширенного языка разметки (XML) (языков политики контроля доступа).

Что касается моделей [b-NIST Models], то представлены следующие модели контроля доступа, начиная с консервативных моделей (учитывающих менее детализированную политику) вплоть до адаптивных моделей (учитывающих более детализированную и зависящую от условий политику):

- **ACL/DAC**. Концепция списков контроля доступа (ACL)/произвольного контроля доступа (DAC) подразумевает, что каждый ресурс в системе, к которому должен контролироваться доступ, определяется как объект, обладающий своим собственным соответствующим списком отображений между набором объектов, запрашивающих доступ к ресурсу, и набором действий, которые каждый объект может предпринять по этому ресурсу.
- **MAC**. Обязательный контроль доступа (MAC) представляет собой наиболее часто используемые системы, в которых приоритетное внимание уделяется конфиденциальности данных. MAC функционирует за счет присвоения классификационного ярлыка каждому ресурсу файла. Классификации включают категорию информации и уровень чувствительности, например, конфиденциальный, секретный или сверхсекретный. Каждый субъект получает аналогичную классификацию, которую называют допуском. Когда субъект пытается получить доступ к какому-либо конкретному ресурсу, система проверяет привилегии субъекта, чтобы определить, можно ли предоставить доступ, а также сравнивает допуск субъекта с классификацией ресурса.
- **RBAC**. При контроле доступа к ресурсу на основе ролей (RBAC) доступ определяется на основе отношений между запрашивающей стороной и организацией или владельцем, осуществляющим контроль над ресурсами; роль или функция запрашивающей стороны определяет, будет ли предоставлен доступ или в нем будет отказано.

- **TBAC/TBAM.** Контроль доступа на основе задачи (TBAC)/управление доступом на основе задачи (TBAM) [b-IEEE TBAC] является продолжением модели RBAC, которое основано на определении задач бизнеса, допускающих более детализированный подход к контролю доступа.
- **ABAC.** Модель контроля доступа на основе атрибутов (ABAC) использует механизмы, такие как ACL, которые содержат атрибуты этих субъектов вместе с операциями, которые разрешается совершать с этим ресурсом. Когда атрибут совпадает с атрибутом в ACL, субъект получает право осуществлять с ресурсом операции, упомянутые для этого атрибута в ACL.
- **PBAC.** Контроль доступа на основе политики (PBAC) представляет собой согласование и стандартизацию модели ABAC на уровне предприятия в поддержку конкретных целей в области управления. Модель PBAC сочетает атрибуты из ресурса, среды и запрашивающей стороны с информацией о конкретном наборе обстоятельств, при которых делается запрос о доступе и используется набор правил, которые устанавливают, разрешается ли доступ согласно политике организации в отношении этих атрибутов в данных обстоятельствах.
- **RAdAC**. Модель адаптируемого к риску контроля доступа (RAdAC) разработана, чтобы обеспечить адаптируемый контроль доступа, учитывающий риски в реальном времени. Эта модель расширяет другие предыдущие модели контроля доступа за счет введения условий среды и уровней рисков в процессе принятия решений о контроле доступа. Она сочетает информацию о том, заслуживает ли доверия человек (или машина), информацию об инфраструктуре корпоративных информационных технологий (ИТ) и факторы риска, связанные с окружающей средой, и использует всю эту информацию для формирования общего количественного измерения риска. Модель RAdAC использует также ситуационные факторы в качестве вклада в процесс принятия решений. Эти ситуационные факторы могли бы включать информацию об уровне текущих угроз, с которыми сталкивается организация, на основе данных, получаемых из других источников, таких как группы реагирования на нарушения компьютерной защиты (CERT), группы реагирования на инциденты, связанные с компьютерной безопасностью (CSIRT), или поставщики систем безопасности. (См. [b-IEEE ARES], [b-NIST RADAC].)

7.4 Уровень доверия

Для того чтобы подчеркнуть зависимость между уровнями доверия и рисками, рекомендуются использовать следующие количественные уровни доверия к сетям обмена информацией об инцидентах: **низкий, средний, высокий**. Разумеется, это подразумевает, что чем выше уровень доверия, тем проще требования и менее детализированный характер контроля доступа. Другими словами, уровень доверия напрямую влияет на уровень сложности механизмов контроля доступа.

Методы оценки количественного и качественного уровней доверия не входят в сферу охвата настоящей Рекомендации.

Рассматривается следующее соотношение между уровнями доверия и моделями обмена информацией:

- Модель "универсальной рассылки" обычно требует **высокой** степени доверия между участниками.
- "Звездообразная" модель обычно требует высокого или среднего уровня доверия (так как "центральный узел" может фильтровать информацию).
- "Одноранговая" модель, как правило, может не требовать высокой степени доверия, так как единственный канал связи можно контролировать с помощью самых разных методов.

Модели обмена информацией более высокого уровня не так явно зависят от степени доверия, но для растущего числа участников и в условиях более сложной среды эти модели могут потребовать применения более передовых моделей контроля доступа.

Следовательно, рассматривается представленная на рисунке 1 классификация:

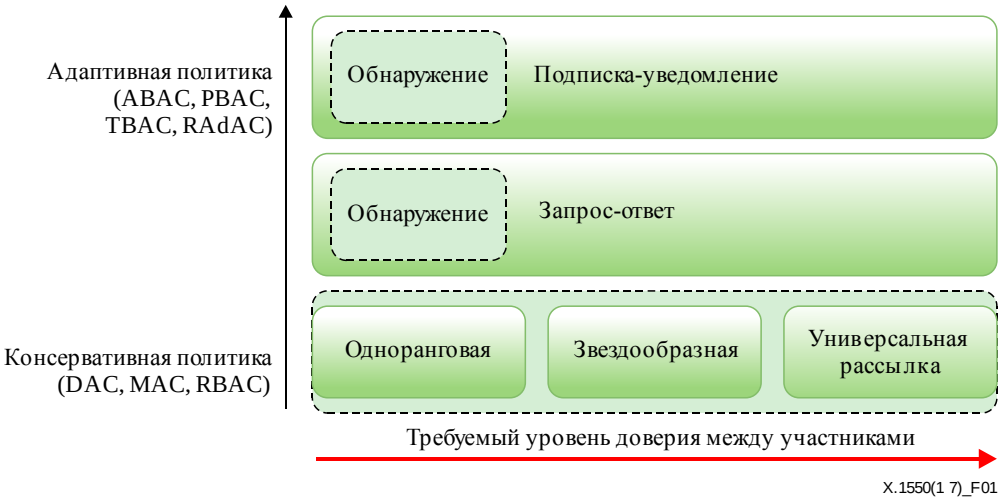

Рисунок 1 – Модели управления доступом, модели обмена информацией и классификация уровней доверия

8 Методы содействия осуществлению политики контроля доступа

8.1 Рекомендации, касающиеся оценки языка, выражающего политику

Наряду с хорошо развитыми языками контроля доступа, которые используются для содействия осуществлению политики контроля доступа в системах управления определением идентичности и доступом (IAM), существуют:

– расширяемый язык разметки контроля доступа (**XACML**). Этот стандарт определяет декларативный язык политики контроля доступа (для модели ABAC), реализуемый в языке разметки, и модель обработки, описывающую то, каким образом оценивать запросы о доступе согласно правилам, определенным в политике.

ПРИМЕЧАНИЕ 1. – XACML 2.0 принят как [b-ITU-T X.1142].

ПРИМЕЧАНИЕ 2. – XACML 3.0 принят как [b-ITU-T X.1144].

– Стандарты для инфраструктур управления привилегиями и ролью (**PERMIS**) представляют собой сложную систему авторизации на основе политики, в которой применяется усовершенствованная версия RBAC (аналогичная ABAC). Политика PERMIS базируется на XML и обеспечивает взаимодействие с XACML, что позволяет PERMIS и XACML беспрепятственно обмениваться пунктами выбора политики (PDP).

Рекомендуется оценивать возможность применения тех или иных моделей контроля доступа в различных условиях и определять минимальные требования для их осуществления с языками политики, такими как [b-ITU-T X.1142], [b-ITU-T X.1144] или [b-UKENT PERMIS].

Пример оценки приводится в таблице 1:

Таблица 1 – Реализация моделей контроля доступа в различных условиях на языках определения политики

Модель/ среда	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBAC	RAdAC
Централи-зованная	[b-ITU-T X.1142]; PERMIS	Экспери-ментальный XACML	[b-ITU-T X.1142]; PERMIS	[b-ITU-T X.1142]; PERMIS*	Экспери-ментальный	[b-ITU-T X.1142]; PERMIS*	[b-ITU-T X.1142]; PERMIS*
Федеративная	[b-ITU-T X.1144]; PERMIS	Экспери-ментальный XACML	[b-ITU-T X.1144]; PERMIS	[b-ITU-T X.1144]; PERMIS*	Экспери-ментальный	–	[b-ITU-T X.1144]

ПРИМЕЧАНИЕ 1. – XACMLv2 [b-ITU-T X.1142] и XACMLv3 [b-ITU-T X.1144] разделены, так как "делегирование", требуемое для большинства федеративных сред, представлено в XACMLv3.

ПРИМЕЧАНИЕ 2. – Известные реализации MAC требуют расширения XACML.

ПРИМЕЧАНИЕ 3. – В настоящее время реализации TBAC/TBAM требуют расширения XACML, что считается экспериментальным.

ПРИМЕЧАНИЕ 4. – PBAC по определению применяется только в централизованной среде, а федеративная среда может потребовать использования RAdAC.

ПРИМЕЧАНИЕ 5. – Звездочка, например PERMIS*, означает, что некоторые ограничения для реализации PERMIS ABAC (и PBAC, RAdAC, если они рассматриваются в качестве расширенной модели ABAC) указаны в [b-UKENT PERMIS].

8.2 Соображения, касающиеся разрешения конфликтов политики

Конфликт политики контроля доступа приводит к противоречивым действиям двух или более правил политики. Базовым механизмом для смягчения конфликтов политики является четкая формулировка правил политики (*статическое разрешение конфликта*). Другой подход основан на оценке политики во время выполнения (*динамическое разрешение конфликта*) [b-UKENT PERMIS].

Если статичное разрешение конфликта считается целесообразным для централизованных систем [b-USB CONFLICT], [b-SPIIRAN POLICY], то в динамичной федеративной среде использование статических методов разрешения конфликта может оказаться проблематичным.

Базовые стратегии статического разрешения конфликта содержит следующие особенности:

- Запрет замен (Deny-override). Конфликтующие правила сочетаются, действию "отказать" отдается предпочтение перед "разрешить";
- Разрешение замен (Permit-override). Конфликтующие правила сочетаются, действию "разрешить" отдается предпочтение перед "отказать";
- Первый применим (First-applicable). Выполняется первое действие между конфликтующими правилами.

Стратегии [b-UKENT PERMIS] для динамического разрешения конфликта политики содержат алгоритмы для отбора надлежащей статической стратегии в отношении контекста текущего запроса доступа.

Рекомендуется оценивать стратегии разрешения конфликта политики с точки зрения показателей эффективности и совместимости с моделями контроля доступа в различных условиях.

Учитывая оценку показателей эффективности для *статического* разрешения конфликта *политики* [b-IJCSIT XACML] в сочетании с динамическим контролем доступа, таким как [b-FUSCAT RADAC], рекомендуется свести к минимуму количество направлений политики, не нарушая уровень гарантии безопасности или используя *динамические* стратегии разрешения конфликта *политики*.

Пример оценки приводится в таблице 2:

Таблица 2 – Разрешение конфликтов политики для моделей контроля доступа в различных условиях

Модель/ среда	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBAC (Прим.)	RAdAC
Централизованная	Статический	Статический	Статический	Статический	Статический	Статический	Динамический
Федеративная	Динамический	Динамический	Динамический	Динамический	Динамический	–	Динамический
ПРИМЕЧАНИЕ. – PBAC по определению применяется только в централизованной среде.							

8.3 Рекомендации, касающиеся оценки показателей работы

Несмотря на то, что языки разметки (такие, как [b-W3C XML], [b-ECMA JSON]) должны считываться человеком, значительный объем устоявшихся и усовершенствованных правил доступа могут представлять трудную задачу с точки зрения формирования и отладки реализуемой политики.

Сложный характер услуг по обмену информацией об инцидентах в сетях обмена информацией об инцидентах может подразумевать использование передовых моделей контроля доступа. Принимая во внимание работу в федеративной среде, это может привести к снижению показателей работы сетей обмена информацией об инцидентах, в результате чего могут возникнуть вопросы в области гарантии безопасности.

Для целей оценки качества/показателей работы/соблюдения политики могут быть рассчитаны соответствующие параметры. Механизмы оценки таких параметров для сетей обмена информацией об инцидентах на входят в сферу охвата настоящей Рекомендации. Однако, рекомендуется набор показателей для такой оценки [b-KIT PERFIAM], [b-NIST METRICS]:

- **Время реагирования**. Время реагирования для компонентов инфраструктуры IAM, компонентов обмена информацией позволяет оценить базовые параметры показателей работы.
- **Неверные решения контроля доступа.** Оценка количества неверных решений по аутентификации или авторизации в напряженных ситуациях обеспечивает информацию о надежности базовой архитектуры IAM.
- **Доверенные компоненты.** Контроль доступа представляет собой деликатную задачу, которая требует определенного уровня доверия между сотрудничающими объектами. Поэтому параметр, перечисляющий доверенные компоненты для принятия решения о контроле доступа, является полезным для определения возможной утечки данных.
- **Распределение политики.** Используется для оценки потенциала и показателей распределения политики в централизованных или федеративных системах контроля доступа.
- **Удобство присвоения привилегий**. Определяет количество этапов, требуемых для присвоения /изменения/устранения/наследования потенциала субъекта или группы.
- **Качество выражения политики.** Определяет, можно ли было бы определить контроль доступа через логические или программируемые выражения.
- **Делегирование потенциала.** Определяет, способна ли система контроля доступа делегировать привилегии субъектам.
- **Сочетание и разрешение политики.** Определяет стратегии сочетания политики, которые используются для разрешения конфликтов (если таковые существуют).
- **Обход.** Определяет, есть ли какие-либо компоненты, которые не учитывают политику контроля доступа.
- **Безопасность.** Определяет потенциал обеспечения безопасности, в частности ограничения на правила контроля доступа, которые используются для предупреждения усиления привилегий.
- **Уровень детализации.** Определяет уровень детализации, которым может управлять система контроля доступа. Может отражать множество атрибутов субъекта, оцениваемых в процессе контроля доступа.
- **Интеграция аутентификации**. Определяет, способна ли система контроля доступа интегрироваться с системами аутентификации.

Библиография

[b-ITU-T M.3345] Рекомендация МСЭ-Т M.3345 (2009 г.), *Принципы управления самообслуживанием*.

[b-ITU-T M.3410] Рекомендация МСЭ-Т M.3410 (2008 г.), *Руководящие указания и требования для систем управления безопасностью в целях обеспечения управления электросвязью*.

[b-ITU-T X.1036] Рекомендация МСЭ-Т X.1036 (2007 г.), *Структура для создания, хранения, распространения и соблюдения политики сетевой безопасности*.

[b-ITU-T X.1142] Рекомендация МСЭ-Т X.1142 (2006 г.), *Расширяемый язык разметки контроля доступа (XACML 2.0)*.

[b-ITU-T X.1144] Рекомендация МСЭ-Т X.1144 (2010 г.), *Расширяемый язык разметки контроля доступа (XACML) 3.0*.

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности*.

[b-ITU-T X.1541] Рекомендация МСЭ-Т X.1541 (2012 г.), *Формат обмена описаниями инцидентов как объектов*.

[b-ITU-T X.1580] Рекомендация МСЭ-Т X.1580 (2012 г.), *Межсетевая защита в реальном времени*.

[b-ITU-T X.1581] Рекомендация МСЭ-Т X.1581 (2012 г.), *Транспортирование сообщений для обеспечения межсетевой защиты в реальном времени*.

[b-IEEE TBAC] IEEE IET Software (2008), *Types for task-based access control in workflow systems*.

[b-IEEE ARES] IEEE (2011), *Sixth International Conference on Availability, Reliability and Security (ARES), An Attribute Based Framework for Risk-Adaptive Access Control Models*.

[b-ECMA JSON] ECMA International (2013), *The JSON Data Interchange Format*.

[b-FUSCAT RADAC] Federal University of Santa Catarina (2014), *A Dynamic Risk-based Access Control Architecture for Cloud Computing*.

[b-IJCSIT XACML] International Journal of Computer Science and Information Technology (IJCSIT) (2010), *Design and evaluation of XACML conflict policies detection mechanism*.

[b-KIT PERFIAM] Karlsruhe Institute of Technology (2009), *Performance Evaluation of Identity and Access Management Systems in Federated Environments*.

[b-MITRE Models] The MITRE Corporation (2012), *Cyber Information-Sharing Models*.

[b-NIST METRICS] NIST Internal Report 7874 (2012), *Guidelines for Access Control System Evaluation Metrics*. [b-NIST Models] NIST Computer Security Division (2009), *A survey of access control models*.

[b-NIST RADAC] NIST Computer Security Division (2009), *Risk-adaptable access control (RAdAC)*.

[b-SPIIRAN POLICY] SPIIRAN (2006), *Conflict Detection and Resolution in Security Policies of Computer Networks*.

[b-stix] OASIS CTI TC (2017), *A structured language for cyber threat intelligence*. <https://oasis-open.github.io/cti-documentation/>

[b-taxii] OASIS CTI TC (2017), *A transport mechanism for sharing cyber threat intelligence*. <https://oasis-open.github.io/cti-documentation/>

[b-UKENT PERMIS] The University of Kent (2013), *Adding privacy protection to policy based authorisation systems*.

[b-USB CONFLICT] IEEE First AESS European Conference on Satellite Telecommunications (ESTEL) (2012), *Conflict detection in security policies using Semantic Web technology*.

[b-W3C XML] W3C (1997), *Extensible Markup Language (XML)*.

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
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 межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2018 г.