Международный союз электросвязи

# МСЭ-Т X.1253

(09/2011)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Безопасность киберпространства – Управление определением идентичности

## Руководящие указания по обеспечению безопасности для систем управления определением идентичности

Рекомендация МСЭ-Т X.1253

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

**СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ**

| | |
|---|---|
| СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ | X.1–X.199 |
| ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ | X.200–X.299 |
| ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ | X.300–X.399 |
| СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ | X.400–X.499 |
| СПРАВОЧНИК | X.500–X.599 |
| ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ | X.600–X.699 |
| УПРАВЛЕНИЕ В ВОС | X.700–X.799 |
| БЕЗОПАСНОСТЬ | X.800–X.849 |
| ПРИЛОЖЕНИЯ ВОС | X.850–X.899 |
| ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА | X.900–X.999 |
| БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ | |
| Общие аспекты безопасности | X.1000–X.1029 |
| Безопасность сетей | X.1030–X.1049 |
| Управление безопасностью | X.1050–X.1069 |
| Телебиометрия | X.1080–X.1099 |
| БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ | |
| Безопасность многоадресной передачи | X.1100–X.1109 |
| Безопасность домашних сетей | X.1110–X.1119 |
| Безопасность подвижной связи | X.1120–X.1139 |
| Безопасность веб-среды | X.1140–X.1149 |
| Протоколы безопасности | X.1150–X.1159 |
| Безопасность одноранговых сетей | X.1160–X.1169 |
| Безопасность сетевой идентификации | X.1170–X.1179 |
| Безопасность IPTV | X.1180–X.1199 |
| БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА | |
| Кибербезопасность | X.1200–X.1229 |
| Противодействие спаму | X.1230–X.1249 |
| **Управление определением идентичности** | **X.1250–X.1279** |
| БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ | |
| Связь в чрезвычайных ситуациях | X.1300–X.1309 |
| Безопасность повсеместных сенсорных сетей | X.1310–X.1339 |
| ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ | |
| Обзор кибербезопасности | X.1500–X.1519 |
| Обмен информацией об уязвимости/состоянии | X.1520–X.1539 |
| Обмен информацией о событии/инциденте/эвристических правилах | X.1540–X.1549 |
| Обмен информацией о политике | X.1550–X.1559 |
| Эвристические правила и запрос информации | X.1560–X.1569 |
| Идентификация и обнаружение | X.1570–X.1579 |
| Гарантированный обмен | X.1580–X.1589 |

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

# Рекомендация МСЭ-Т X.1253

## Руководящие указания по обеспечению безопасности для систем управления определением идентичности


**Резюме**

В Рекомендации МСЭ-Т X.1253 предлагаются руководящие указания по обеспечению безопасности для систем управления определением идентичности (IdM). Руководящие указания по обеспечению безопасности определяют, каким образом должна развертываться и функционировать система IdM для услуг надежного определения идентичности в условиях сетей последующих поколений (СПП) или киберпространства. В руководящих указаниях по обеспечению безопасности основное внимание уделяется предоставлению официальной информации о способах использования различных механизмов обеспечения безопасности для защиты общей системы IdM, а также приводятся надлежащие процедуры обеспечения безопасности, необходимые в случаях взаимодействия двух систем IdM.



**Хронологическая справка**

| Издание | Рекомендация | Утверждение | Исследовательская комиссия |
|---|---|---|---|
| 1.0 | МСЭ-Т X.1253 | 02.09.2011 г. | 17-я |

## ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

## ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

## ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

## СОДЕРЖАНИЕ


| | | Стр. |
|---|---|---|
| 1 | Сфера применения | 1 |
| 2 | Справочные документы | 1 |
| 3 | Термины и определения | 1 |
| 3.1 | Термины, определенные в других документах | 1 |
| 3.2 | Термины, определенные в настоящей Рекомендации | 2 |
| 4 | Сокращения и акронимы | 2 |
| 5 | Условные обозначения | 3 |
| 6 | Базовая информация | 3 |
| 7 | Обзор систем управления определением идентичности | 4 |
| 7.1 | Общая модель систем IdM | 4 |
| 7.2 | Услуги определения идентичности | 5 |
| 8 | Угрозы безопасности в системах IdM | 5 |
| 8.1 | Безопасность систем | 5 |
| 8.2 | Пассивные угрозы безопасности | 6 |
| 8.3 | Активные угрозы безопасности | 6 |
| 8.4 | Угрозы безопасности, касающиеся системы IdM | 7 |
| 9 | Руководящие указания по обеспечению безопасности для систем IdM | 8 |
| 9.1 | Руководящие указания по обеспечению безопасности при развертывании систем IdM | 8 |
| 9.2 | Руководящие указания по обеспечению безопасности при эксплуатации систем IdM | 9 |
| 9.3 | Руководящие указания по обеспечению безопасности для серверов IdM | 10 |
| 9.4 | Руководящие указания по обеспечению безопасности для клиентов IdM | 11 |
| 9.5 | Руководящие указания по обеспечению безопасности для мобильных клиентов IdM | 12 |
| 9.6 | Соображения по обеспечению конфиденциальности в системах IdM | 13 |
| Библиография | | 15 |

# Рекомендация МСЭ-Т X.1253

## Руководящие указания по обеспечению безопасности для систем управления определением идентичности

### 1 Сфера применения

Сфера применения настоящей Рекомендации включает:

– модели и услуги общей системы IdM;

– угрозы и риски обеспечения безопасности, связанные с системой IdM;

– руководящие указания по обеспечению безопасности для развертывания систем IdM;

– руководящие указания по обеспечению безопасности для эксплуатации систем IdM;

– соображения по обеспечению конфиденциальности в системах IdM.

Сфера применения настоящей Рекомендации связана главным образом с услугами управления определением идентичности, основанными на многих доменах. Тем не менее данные руководящие указания применимы также к централизованной системе управления определением идентичности.

ПРИМЕЧАНИЕ. – Лица, осуществляющие внедрение, и пользователи описываемых руководящих указаний должны соблюдать все применимые национальные и региональные законы, нормы и обязательные процедуры. Некоторые конкретные нормы и законодательные акты могут требовать реализации механизмов, предназначенных для защиты идентифицирующих личность данных.

### 2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

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

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

### 3 Термины и определения

#### 3.1 Термины, определенные в других документах

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

**3.1.1 контроль доступа (access control)** [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 атрибут (attribute)** [ITU-T X.1252]: Информация, связанная с объектом, которая означает какую-либо его характеристику.

**3.1.3 аутентификация (объекта) ((entity) authentication)** [ITU-T X.1252]: Процесс, используемый для достижения достаточной меры доверия в связи между объектом и представленной идентичностью.

**3.1.4 полномочия (credential)** [ITU-T X.1252]: Набор данных, представляемых как доказательство утверждаемой идентичности и/или прав.

**3.1.5 идентичность (identity)** [ITU-T X.1252]: Представление какого-либо объекта в виде одного или нескольких атрибутов, которые позволяют однозначно распознать объекты в каком-либо контексте в той мере, в какой это необходимо. В целях управления определением идентичности (IdM) термин "идентичность" толкуется как контекстуальная идентичность (подмножество атрибутов), т. е. разнообразие атрибутов ограничивается рамками с определенными граничными условиями (контекстом), в которых объект существует и взаимодействует.

ПРИМЕЧАНИЕ. – Каждый объект представлен одной целостной идентичностью, которая включает все возможные элементы информации, характеризующие такой объект (атрибуты). Вместе с тем такая целостная идентичность является теоретическим понятием и не может быть описана и практически использована, поскольку число всех возможных атрибутов бесконечно.

**3.1.6 управление определением идентичности (identity management)** [ITU-T X.1252]: Набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и связывание, обеспечение реализации политики, аутентификация и утверждения), используемых для:

- гарантирования информации, подтверждающей идентичность (например, идентификаторов, полномочий, атрибутов);
- гарантирования идентичности объекта (например, пользователей/абонентов, групп, устройств пользователей, организаций, поставщиков доступа к сети и поставщиков услуг, сетевых элементов и объектов, а также виртуальных объектов); и
- обеспечения коммерческих приложений и приложений безопасности.

**3.1.7 пользователь (user)** [ITU-T X.1252]: Любой объект, использующий ресурс, например, систему, оконечное оборудование, процесс, приложение или корпоративную сеть.

**3.1.8 ориентированная на пользователя (user-centric)** [ITU-T X.1252]: Система управления определением идентичности (IdM), при которой пользователю предоставляется право контролирования и обеспечения соблюдения различных видов политики конфиденциальности и безопасности, определяющих обмен между объектами информацией об идентичности, в том числе информацией, позволяющей устанавливать личность (PII) пользователей.

### 3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

**3.2.1 объект (entity)**: Что-либо, что существует отдельно и обособленно и может быть определено в контексте.

ПРИМЕЧАНИЕ. – Объектом может быть физическое лицо, животное, юридическое лицо, организация, активный или пассивный предмет, устройство, применение программного обеспечения, услуга и т. п., или группа таких объектов. В контексте электросвязи примерами объектов являются точки доступа, абоненты, пользователи, сетевые элементы, сети, применения программного обеспечения, услуги и устройства, интерфейсы и т. п.

**3.2.2 клиент IdM (IdM client)**: Клиентская программа, взаимодействующая с сервером IdM для поиска информации об идентичности.

**3.2.3 сервер IdM (IdM server)**: Сервер, управляющий жизненным циклом идентификации пользователей.

**3.2.4 мобильный клиент IdM (mobile IdM client)**: Клиент IdM, который устанавливается и используется в мобильном устройстве.

## 4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

| | | | |
|---|---|---|---|
| DB | Database | БД | База данных |
| DoS | Denial of Service | | Отказ в обслуживании |
| FDDI | Fibre Distributed Data Interface | | Распределенный волоконно-оптический интерфейс данных |
| IdM | Identity Management | | Управление определением идентичности |

| | | | |
|---|---|---|---|
| IdP | Identity Provider | | Поставщик данных идентичности |
| IDS | Intrusion Detection System | | Система обнаружения проникновений |
| IPS | Intrusion Prevention System | | Система предотвращения проникновений |
| LAN | Local Area Network | ЛВС | Локальная сеть |
| NGN | Next Generation Network | СПП | Сеть последующих поколений |
| OS | Operating System | ОС | Операционная система |
| PII | Personally Identifiable Information | | Информация, позволяющая установить личность |
| PIN | Personal Identification Number | | Персональный идентификационный номер |
| PKI | Public Key Infrastructure | | Инфраструктура открытых ключей |
| SP | Service Provider | | Поставщик услуги |
| SSL | Secure Socket Layer | | Уровень защищенных разъемов |
| TTP | Trusted Third Party | | Доверенная третья сторона |
| VPN | Virtual Private Network | ВЧС | Виртуальная частная сеть |

## 5 Условные обозначения

Отсутствуют.

## 6 Базовая информация

За последние десять лет система IdM (управление определением идентичности) превратилась из замкнутой системы в федеративную или ориентированную на пользователя систему IdM. В большинстве разработанных до настоящего времени систем IdM основное внимание уделялось вопросу о том, каким образом можно эффективным и удобным для пользователя способом предоставлять услуги, связанные с определением идентичности. Во многих последних разработках систем IdM предусмотрена реализация определенных аспектов обеспечения безопасности и конфиденциальности.

Вначале система IdM, рассматривавшаяся как замкнутая модель, разворачивалась в корпоративном домене. При этом не обеспечивалась связь между системами IdM, и поэтому отсутствовала возможность обмена информацией об идентичности пользователя для обеспечения полезных услуг в рамках нескольких доменов. Кроме того, идентичность одного пользователя могла дублироваться в нескольких разных системах IdM. Это затрудняет системное администрирование в рамках организации в части обеспечения безопасного и эффективного управления определением идентичности пользователя.

Следующий шаг заключался в осуществлении сбора всей информации об идентичности пользователя в одной системе IdM и распространении ее всякий раз, когда это необходимо. Данный подход привел к так называемой централизованной модели. При применении этой модели в одном сервере собирается слишком большой объем информации пользователя. Этому подходу присущ ряд недостатков, поскольку IdP становится не только единой точкой отказа, но может также не вызывать доверия у всех сторон.

Принятый подход поэтому заключался в том, чтобы позволить каждому IdP управлять своей собственной информацией об идентичности и децентрализовать свою ответственность, распределив ее между различными IdP, которых может выбрать пользователь. Этот подход известен как федеративная модель. В данной модели существует множество IdP, которые могут быть доверенными для пользователя и при необходимости управляют частичной информацией об идентичности пользователей. Информация об идентичности пользователей каждого IdP может использоваться на коллективной основе с частью псевдонима федеративной идентичности. В этой модели устранена проблема единой точки отказа.

Поскольку для пользователя вопросы сохранения конфиденциальности приобретают все бóльшую важность, в технологии IdM основное внимание уделяется пользователям, с тем чтобы обеспечить им полный контроль над информацией собственной идентичности. Эта парадигма носит название модели, ориентированной на пользователя. В такой модели информация об идентичности должна проходить через пользователя, с тем чтобы предоставить ему возможность применить свою

стратегию защиты конфиденциальности в тех случаях, когда два IdP обмениваются информацией об идентичности этого пользователя. Эта модель реализована во многих промышленных продуктах и в ней задействованы другие существующие технологии IdM.

В процессе конвергенции этих систем IdM часто возникает сложная задача, связанная с тем, каким образом гарантировать безопасность конвергированной системы и поддержать баланс между безопасностью и защитой конфиденциальности для обеспечения оптимальных рабочих характеристик. Кроме того, в большинстве разработанных к настоящему времени руководящих указаний по обеспечению безопасности основное внимание, как правило, обращалось на поставщиков данных идентичности и полагающиеся стороны. Поскольку аспекты безопасности и конфиденциальности пользователя становятся обязательными требованиями, необходимо рассматривать безопасность той части системы IdM, которая ориентирована на пользователя, с тем чтобы учитывать растущую обеспокоенность в отношении конфиденциальности пользователя.

# 7 Обзор систем управления определением идентичности

## 7.1 Общая модель систем IdM

### 7.1.1 Система IdM, ориентированная на приложения

В крупномасштабных системах IdM, ориентированная на приложения система IdM означает, что услуги и стратегии определения идентичности предназначены для удовлетворения потребностей поставщиков данных идентичности и полагающихся сторон и оптимизированы в отношении требований со стороны приложений, например, предоставления учетной информации пользователей. В системе IdM, ориентированной на приложения, имеются поставщик данных идентичности и полагающаяся сторона. При предоставлении пользователю услуги определения идентичности между этими двумя объектами, как правило, происходит обмен информацией об идентичности. Исторически сложилось так, что технологии определения идентичности и управления доступом были ориентированы главным образом на аутентификацию конечных пользователей для обеспечения федеративного доступа к приложениям и услугам. Поэтому требование обеспечения безопасности ограничивается рамками домена конкретного приложения.

### 7.1.2 Система IdM, ориентированная на пользователя

Основное внимание в ориентированной на пользователя системе IdM направлено главным образом на конечных пользователей, и система оптимизирована с учетом их потребностей. Это означает, что основной целью системы IdM является обеспечение для пользователей удобных и комплексных услуг определения идентичности. Главная особенность системы заключается в предоставлении пользователю полного контроля над данными о его идентичности. Информация об идентичности пользователя, в случае ее распространения, должна явным образом проходить через пользователя, с тем чтобы дать ему возможность применения при необходимости определенной персональной политики. В системе IdM, ориентированной на пользователя, в вычислительную среду пользователя должна быть включена клиентская программа. Вследствие этого необходимы простые и всеобъемлющие руководящие указания по обеспечению безопасности, которые помогут пользователю безопасно установить и развернуть любое соответствующее программное средство. Программное обеспечение должно контролировать определенную информацию пользователя, связанную с безопасностью.

Модель, в центре которой находится пользователь, отличается от других моделей IdM акцентом на то, что конкретный пользователь, а не какой-либо орган, сохраняет контроль над тем, каким образом создаются, распространяются, обновляются и прекращают действие атрибуты идентичности пользователя. Это означает, что пользователь обладает всеми полномочиями в течение жизненного цикла своей идентичности. Уровень контроля может определяться требованиями к обеспечению конфиденциальности пользователя.

### 7.2 Услуги определения идентичности

#### 7.2.1 Управление жизненным циклом идентичности

Это услуга, управляющая определением идентичности, которая создается, распространяется, обновляется и прекращает существование. Связанная с этой услугой информация сохраняется в базе данных, расположенной на сервере или в локальной машине. Следовательно, доступ к этой базе данных должен предоставляться лишь зарегистрированным пользователям.

#### 7.2.2 Аутентификация

Услуга аутентификации заключается в верификации подлинности законных пользователей или объектов, которые запрашивают доступ к системе или ресурсам. Аутентификация − это ключевая услуга, предоставляемая системой IdM полагающимся сторонам. Во что бы то ни стало должна быть предотвращена возможность взлома пароля и нелегального проникновения.

#### 7.2.3 Авторизация

Услуга авторизации предназначена для принятия решений, касающихся прав доступа пользователя, и исполнения принятых по итогам авторизации решений в соответствии с полномочиями пользователя. Эта услуга необходима для защиты системы определения идентичности от несанкционированного доступа и использования.

#### 7.2.4 Обмен атрибутами

Данная услуга обеспечивает взаимный обмен атрибутами и их синхронизацию. Это одна из наиболее важных услуг по обеспечению безопасности, поскольку обмен тем или иным атрибутом осуществляется по сети связи. При переходе от проводных к беспроводным средствам связи требуются механизмы обеспечения безопасности различных уровней.

#### 7.2.5 Жетон безопасности

Жетон безопасности требуется для совместного пользования объектами информации о безопасности и об идентичности пользователя. Жетон безопасности всегда содержит весьма конфиденциальную информацию, которая не подлежит разглашению, поэтому он обычно защищается механизмами обеспечения безопасности и криптографическими средствами.

## 8 Угрозы безопасности в системах IdM

Следует считать, что большая часть угроз безопасности, возникающих в киберпространстве, существует и в системах IdM, так как они эксплуатируются в киберпространстве. Общие угрозы безопасности в киберпространстве описываются в документе [ITU-T X.1205].

В системах IdM существуют различные угрозы безопасности, которые делают систему уязвимой или приводят к нарушению требований безопасности, подвергая любую организацию серьезной опасности.

### 8.1 Безопасность систем

В целом безопасность систем связана с защитой технических средств и данных пользователя. Цель заключается в том, что технические средства должны быть доступны только зарегистрированным пользователям и для целей, которые определяются владельцами. Кроме того, система должна использоваться для этих же целей. Злоумышленники не должны иметь возможностей лишать законных пользователей права владения ресурсами.

#### 8.1.1 Несанкционированный доступ и использование

Большинство систем не должны быть доступны для использования незарегистрированными пользователями. Система IdM должна обладать весьма жесткими характеристиками, чтобы предотвратить этот тип уязвимости в аспекте безопасности, поскольку любой незарегистрированный доступ к информации об идентичности в системе IdM может привести к дополнительным угрозам безопасности, таким как кража информации и нелегальное проникновение.

### 8.1.2 Ненадлежащее использование

Ненадлежащее использование означает, что пользователь может задействовать систему IdM для обработки или выполнения определенных работ, которые изначально не планировались. Для зарегистрированного пользователя должны быть установлены некоторые ограничения по использованию части системы IdM без надлежащих полномочий. Использование некоторых услуг ограничиваются зарегистрированными пользователями, других − конкретными пользователями, а доступ к некоторым услугам запрещен для всех, кроме администраторов.

### 8.1.3 Отказ в обслуживании

Обычно система IdM является первым пунктом, на который попадает пользователь, чтобы воспользоваться прикладными услугами. Поэтому весьма вероятно, что системы IdM будут мишенью для атак, нацеленных на прекращение предоставления услуг. Для того чтобы системы IdM отказали в обслуживании, могут использоваться самые разнообразные атаки, которые, как правило, легко осуществить, но трудно остановить. Многие атаки такого рода предназначены для потребления огромного объема вычислительных ресурсов, что затрудняет или делает невозможным обслуживание законных пользователей.

## 8.2 Пассивные угрозы безопасности

В случае пассивных угроз безопасности злоумышленник считывает из сети пакеты с информацией, но не вводит в нее свои пакеты. Простейший способ осуществления такой атаки − находиться в той же ЛВС, что и жертва. В наиболее распространенных конфигурациях ЛВС, включая Ethernet, 802.3 и FDDI, любая машина в сети может считывать весь трафик, предназначенный для любой другой машины в той же ЛВС.

Каналы беспроводной связи заслуживают отдельного рассмотрения, особенно в связи с растущей в последние годы популярностью беспроводных ЛВС, таких как сети, использующие стандарт 802.11. Поскольку данные просто передаются на хорошо известных радиочастотах, злоумышленнику остается лишь найти возможность приема этих передач. Такие каналы особенно уязвимы для пассивных атак. Хотя многие каналы такого рода включают криптографическую защиту, это зачастую тот случай, когда данная технология обеспечения безопасности используется с неподходящей конфигурацией.

### 8.2.1 Нарушения конфиденциальности

Атака в отношении конфиденциальности заключается в нарушении любых частных преобразований или сеансов связи, которые осуществляются по линии связи. В интернете все еще весьма часто конфиденциальная информация передается в открытой форме. Любая информация о полномочиях, полученная с помощью такой атаки, может повторно использоваться для последующих атак.

### 8.2.2 Сканирование пароля

Сканирование пароля заключается в овладении передаваемыми по сети паролями пользователя для получения возможности несанкционированного использования ресурсов. Злоумышленник, который может считывать этот трафик, имеет возможность, следовательно, перехватить пароль и повторно его использовать. Другими словами, злоумышленник может инициировать связь с системой IdM для хищения информации об идентичности пользователя.

## 8.3 Активные угрозы безопасности

Если атака включает введение данных в сеть или в систему, такая атака считается активной. Активные атаки являются проникновением в вычислительную сеть, с тем чтобы предпринять попытку уничтожения или изменения данных, хранящихся в системах IdM, которые образуют часть сети. Это одна из наиболее серьезных форм атаки, поскольку многие операции компаний весьма зависимы от этих данных.

### 8.3.1 Взлом защиты путем замещения оригинала

В ходе такой атаки злоумышленник записывает последовательность сообщений из сети и посылает их снова по адресу соответствующей стороны, которая изначально получала их. Следует отметить, что злоумышленнику не требуется пытаться понять эти сообщения. Ему достаточно лишь перехватить и снова передать их.

### 8.3.2 Атака через посредника

Злоумышленник разрывает поток связи, чтобы представить себя в роли передатчика для приемника и в роли приемника для передатчика. Атака такого рода носит весьма серьезный характер, поскольку она маскируется и под передатчик, и под приемник. Поэтому для защиты от атаки через посредника многие методы, обеспечивающие целостность потока связи, оказываются недостаточными. Атаки через посредника возможны в случаях, когда в протоколе отсутствует аутентификация однорангового объекта.

## 8.4 Угрозы безопасности, касающиеся системы IdM

Существуют угрозы, которые конкретно связаны с системами IdM. Эти угрозы перечислены ниже и являются основными слабыми местами в аспекте безопасности, для преодоления которых в любой системе IdM должны быть предусмотрены надлежащие меры противодействия.

### 8.4.1 Угрозы, связанные с паролем

Одна из угроз, связанных с паролем, обусловлена использованием легкораскрываемого пароля. Если пользователь для целей идентификации выбирает легкораскрываемый, т. е. угадываемый пароль, то такой пароль может быть подвергнут словарной атаке. Другая проблема возникает, когда пользователь применяет тот же легкораскрываемый пароль для регистрации на нескольких веб-сайтах. В этом случае любой веб-сайт, имеющий недостаточно высокую степень безопасности, может быть атакован с целью обнаружения паролей его пользователей, а злоумышленник, используя украденные пароли, просто пытается зарегистрироваться на других веб-сайтах.

Еще одной угрозой является сканирование пароля с помощью шпионского программного обеспечения в компьютере. Любой компьютер может быть заражен шпионским программным обеспечением, способным похитить пароль пользователя или администратора.

### 8.4.2 Несанкционированный доступ

Несанкционированный доступ − это термин, который может относиться к ряду различных видов атак. Максимальный результат для нарушителя заключается в получении доступа к ресурсам незаконным образом [ITU-T X.1205].

Система IdM, обеспечивающая услуги аутентификации и определения идентичности, должна находиться в состоянии готовности и быть доступной для всех сторон, которым требуются идентификационные данные пользователя для предоставления прикладных услуг. Поэтому для защиты системы от несанкционированного доступа необходим механизм детального контроля доступа.

### 8.4.3 Перехват

Перехват является трудной для обнаружения угрозой. Целью злоумышленника в этом случае является прослушивание и, главным образом, запись исходных данных о ЛВС предприятия. В рамках этой атаки используется "случайный режим" серийных Ethernet-адаптеров, которые продаются на рынке. Этот режим позволяет злоумышленнику захватывать каждый пакет в сети. В настоящее время в интернете имеется большое количество бесплатных сетевых перехватчиков, которые злоумышленник может использовать для перехвата [ITU-T X.1205].

Системы IdM, использующие проводную или беспроводную сеть, как правило, взаимодействуют с пользователями и другими объектами для обмена полномочиями и информацией (зачастую конфиденциальной), подтверждающей идентичность. Поэтому любая информация, собираемая перехватчиком, может привести к краже идентичности.

### 8.4.4 Фишинг

Это попытка третьей стороны, как правило, с целью финансовой выгоды, завладеть конфиденциальными данными отдельного лица, группы или организации путем подделки (или спуфинга) специального, обычно хорошо известного фирменного знака. Злоумышленник пытается обманным путем вынудить пользователей раскрыть их персональные данные, например, номера кредитных карт, онлайновые банковские реквизиты и иную секретную информацию, которую он/она может затем использовать для совершения мошеннических действий. Веб-сайт фишинга − это сайт, предназначенный для имитации легитимного веб-сайта организации, чей фирменный знак подделывается. Фишинг в системах IdM является серьезной угрозой, поскольку аутентификационные данные жертвы или иная идентифицирующая личность информация, будучи перехваченными злоумышленником, могут использоваться для хищения идентичности или в других мошеннических операциях.

### 8.4.5 Кража идентичности

Это весьма известная проблема обеспечения безопасности, особенно для организаций, которые хранят большие объемы персональных идентифицирующих личность данных и управляют ими. Случаи раскрытия секретной информации, приводящие к потере персональных данных, не только могут подорвать доверие клиента и институциональное доверие и нанести дорогостоящий ущерб репутации любой организации, но несанкционированный доступ к данным может также повлечь за собой весомый финансовый ущерб организациям.

## 9 Руководящие указания по обеспечению безопасности для систем IdM

Руководящие указания по обеспечению безопасности в пунктах 9.1 и 9.2 определяют, каким образом управлять безопасностью при развертывании и эксплуатации общей системы IdM. Эти руководящие указания содержат базовые требования обеспечения безопасности для системы IdM, которая может надежно развертываться и функционировать в различной вычислительной среде. Пункты 9.3, 9.4 и 9.5 посвящены объектам системы IdM, к которым относятся сервер, клиент и мобильный клиент IdM. В пункте 9.6 приводятся соображения относительно обеспечения конфиденциальности в системах IdM.

### 9.1 Руководящие указания по обеспечению безопасности при развертывании систем IdM

В этом пункте излагаются руководящие указания по обеспечению безопасности при установке и развертывании системы IdM. В большинстве случаев подготовка к управлению формированием доверия и управлению ключами является одним из сложных вопросов.

### 9.1.1 Управление формированием доверия

Каждый случай авторизации, выполненный с использованием систем IdM, зависит от степени доверия к тому, что идентичность и соответствующие ей атрибуты достоверны и корректны. Поэтому определение идентичности является полезной процедурой только тогда, когда оно связано с определенными полномочиями. Полномочия устанавливаются на основе доверия. План управления формированием доверия − это первый шаг к успешному развертыванию и функционированию систем IdM.

Инфраструктура открытых ключей (PKI) является одним из главных механизмов формирования доверия для систем управления определением идентичности. Основная цель PKI заключается в предоставлении сертификата открытого ключа, который может использоваться для аутентификации и защищенного канала. В крупных системах IdM настоятельно рекомендуется определить доверенную третью сторону (TTP), используя для этого PKI. Выдаваемый PKI сертификат может использоваться для аутентификации пользователя для системы IdM и шифрования канала связи в SSL. Электронная подпись является еще одним важным применением сертификата.

### 9.1.2 Сетевая безопасность

Важнейшим требованием является обеспечение (с использованием различных средств) защиты сетевой среды. Прежде всего, периметр сети следует защищать с помощью брандмауэра. Любая система IdM должна размещаться внутри периметра брандмауэра. Кроме того, для обеспечения более надежной сетевой среды могут применяться более сложные механизмы обеспечения сетевой безопасности, такие как VPN и IDS/IPS.

### 9.1.3 Защищенная среда хостинга

Среда хостинга − это среда, в которой установлена и функционирует система IdM. В серверах и рабочих станциях, где установлен компонент системы IdM, до установки системы IdM требуется установка антивирусных программ и программ защиты от клавиатурных шпионов. Следует гарантировать то, что до установки и развертывания любой системы IdM среда хостинга не была нарушена в результате любых атак, нацеленных на подрыв безопасности.

### 9.1.4 Защищенное хранение

В устройствах хранения данных, таких как база данных или сервер каталогов, содержится большой объем важной и секретной информации. В ходе процедуры настройки в защищенный компьютер должен быть включен сервер хранения данных и должна быть введена учетная запись администратора в соответствии с надлежащими руководящими указаниями по установке для исключения случаев введения какой-либо вредоносной учетной записи, которая позднее используется для нарушения функционирования системы.

## 9.2 Руководящие указания по обеспечению безопасности при эксплуатации систем IdM

В этом пункте приведены руководящие указания по обеспечению безопасности при эксплуатации системы IdM. Управление аутентификацией и доступом является одним из основных вопросов, которые следует урегулировать.

### 9.2.1 Цифровая подпись

Цифровая подпись − это механизм обеспечения безопасности, который может гарантировать подлинность и целостность подписанного сообщения. В системе IdM существует множество ситуаций, в которых пользователь должен продемонстрировать свое желание осуществлять транзакции в цифровой форме или дать согласие на это. В таком случае применяемая электронная подпись может использоваться в качестве доказательства при верификации целостности данной транзакции.

### 9.2.2 Шифрование

Система IdM требует операции шифрования на различных уровнях функционирования. Прежде всего, необходимо шифровать сообщения, которыми обмениваются объекты, если требуется обеспечить конфиденциальность. В зависимости от эксплуатационной политики IdM необходимо произвести шифрование некоторой информации, сохраняемой в базе данных, в целях обеспечения конфиденциальности и защиты от несанкционированного доступа. Шифрование позволит добиться максимального уровня конфиденциальности для систем IdM, и это в конечном счете обеспечит конфиденциальность пользователя и его информации об идентичности.

### 9.2.3 Аутентификация

Аутентификация − это логическая функция, позволяющая предотвратить несанкционированный доступ незаконного пользователя в систему. В интернете широко используется простая процедура аутентификации по идентификатору/паролю, которая имеет много слабых мест в качестве меры по обеспечению безопасности. Поэтому всякий раз, когда необходимо убедиться в высокой достоверности пользователя, получающего доступ в систему, рекомендуется проводить строгую аутентификацию. При применении взаимной аутентификации могут быть смягчены последствия атак типа фишинг и фарминг.

### 9.2.4 Безопасная связь

Бóльшая часть информации, обмен которой осуществляется между пользователем и системой IdM, обусловливает вопрос неприкосновенности частной жизни и является конфиденциальной по своему характеру. Кроме того, протокольные сообщения между объектами могут переносить секретную и конфиденциальную информацию, которую необходимо шифровать в линиях связи. Безопасная связь может быть достигнута при использовании существующих технологий, таких как SSL и VPN.

### 9.2.5 Управление доступом

Различные объекты, например, администраторы и пользователи, могут иметь доступ к системе IdM для получения определенных услуг и повседневного технического обслуживания. Для защиты системы от проникновения злонамеренных третьих сторон необходим какой-либо надлежащий механизм управления доступом. В большинстве случаев достаточным будет применение произвольной модели избирательного доступа (т. е. списков управления доступом). Однако, если требуется более защищенная и гибкая модель управления доступом, может применяться модель управления доступом на основе ролей, которая способна обеспечить более сложное и многоуровневое управление.

## 9.3 Руководящие указания по обеспечению безопасности для серверов IdM

В этом пункте приведены руководящие указания по обеспечению безопасности, которые относятся к серверу IdM, установленному и эксплуатируемому в больших рабочих станциях или серверах.

### 9.3.1 Обеспечение безопасности операционной системы

Большинство общедоступных серверов IdM работают в операционных системах (ОС) общего назначения. Если конфигурация ОС, используемой сервером IdM, выполнена должным образом, это позволит избежать многих проблем обеспечения безопасности. Поскольку сервер IdM устанавливается на базе действующей ОС, его безопасность зависит в основном от этой ОС. Методы обеспечения безопасности различных ОС варьируются в широком диапазоне; поэтому в данный пункт включены обобщенные процедуры, общепринятые для безопасности большинства ОС. Дополнительные базовые сведения об управлении безопасностью в ОС приводятся в документах [ITU-T X.1205] и [b-NIST SP 800-123].

Для защиты серверов IdM необходимо выполнить следующие основные меры по обеспечению безопасности ОС:

– корректировка и обновление ОС;
– усиление защиты и выбор конфигурации ОС для адекватного решения проблем безопасности;
– установка и выбор конфигурации дополнительных средств управления безопасностью, если это необходимо;
– проверка уровня безопасности ОС, с тем чтобы удостовериться, что ранее принятые меры должным образом решают все вопросы безопасности.

### 9.3.2 Конфигурации аутентификации пользователя

Что касается серверов IdM, зарегистрированные пользователи, которые могут выбирать конфигурацию сервера, должны ограничиваться небольшим числом назначенных администраторов сервера. Для реализации в случае необходимости обусловленных политикой ограничений, администратор сервера должен выбрать конфигурацию сервера для целей аутентификации пользователя путем запроса подтверждения того, что пользователь авторизован для такого доступа. В случае серверов IdM, для которых требуются высокие уровни уверенности и доверия, организации могут также использовать защищенные от умышленных повреждений аппаратные средства аутентификации, такие как жетоны или устройства генерирования одноразовых паролей. В этом случае применение механизмов аутентификации, в которых информация для установления подлинности используется многократно (например, пароли) и передается в открытой форме по ненадежной сети, является серьезным мешающим фактором, поскольку информация может быть перехвачена и использована злоумышленником для маскировки под авторизованного пользователя.

Стандартная конфигурация ОС зачастую содержит учетные записи гостей с паролями и без них. Администратор должен удалять или блокировать неиспользованные учетные записи гостей для исключения их использования злоумышленниками.

### 9.3.3 Конфигурация управления доступом

Большинство серверов IdM предоставляют возможность определять привилегии доступа в индивидуальном порядке согласно полномочиям, содержащимся в информации об идентичности. Любому пользователю, получающему доступ к серверу IdM, не должно даваться разрешение на доступ к информации об идентичности других пользователей. Надлежащая установка функций управления доступом может содействовать предотвращению раскрытия секретной информации или информации ограниченного пользования, которая не предназначена для публичного распространения. Кроме того, возможности управления доступом могут быть задействованы для ограничения использования ресурсов в случае атаки на сервер с целью провоцирования отказа в обслуживании (DoS).

### 9.3.4 Ведение журнала

Ведение журнала − это неотъемлемая часть надежных мер противодействия угрозам безопасности. Весьма важно, чтобы в журнал вносились корректные данные и затем эти журналы тщательно контролировались. Большое значение имеет ведение сетевых и системных журналов, особенно системных журналов в случае шифрованной связи, когда сетевой контроль менее эффективен.

Просмотр журналов является обязательным и эффективным способом обнаружения подозрительной деятельности. Во многих случаях файлы журналов служат единственным местом регистрации фактов подозрительного поведения. Возможности систем для записи информации в журналах должны использоваться в целях обнаружения неудачных и успешных попыток проникновения и в целях запуска устройств сигнализации об опасности, когда требуется проведение дополнительного расследования. Необходимо ввести процедуры и инструменты для обработки и анализа файлов журналов и для просмотра оповещений об опасности.

Следует гарантировать, что функции управления доступом могут осуществить разделение обязанностей путем обеспечения невозможности изменения записей в журналах серверов администраторами серверов и потенциального обеспечения того, что вносить информацию в файлы журналов разрешено только процессу сервера.

## 9.4 Руководящие указания по обеспечению безопасности для клиентов IdM

В этом пункте приведены руководящие указания по обеспечению безопасности при эксплуатации клиентской программы IdM. В случае использования веб-браузера в качестве клиента IdM, уязвимость системы безопасности зависит от самого браузера. Тем не менее некоторые руководящие указания все же могут быть актуальными для обеспечения безопасности клиентской среды.

### 9.4.1 Безопасное распределение клиентской программы

В настоящее время большинство расширений, зависящих от браузеров, загружается из интернета. Если пользователь случайно скачивает неверную клиентскую программу IdM, которая потенциально может нанести вред системе пользователя, то после этого никакие эффективные механизмы обеспечения безопасности не смогут защитить пользователя от злонамеренных действий. Поэтому поставщик клиентской программы IdM должен обеспечить, чтобы распространяемая клиентская программа была защищена в аспекте целостности и предусматривала безопасный способ валидации ее целостности.

### 9.4.2 Целостность клиентской программы

Что касается обеспечения целостности клиентской программы, то ключевым решением для возможных вариантов такой программы является наличие цифровой подписи. Если клиентская программа подписана поставщиком, а подписанный сертификат предоставляется для валидации, то в этом случае пользователь может безопасно загрузить и верифицировать целостность программного кода. Существует альтернативный метод, в котором для обеспечения целостности кода используется хэш-алгоритм. Клиентский код служит входным сообщением для хэш-алгоритма, который создает хэш-значение, являющееся дайджестом клиентского кода. Если хэш-значение

публикуется на веб-сайте безопасным способом, то пользователь может провести валидацию своей клиентской программы путем вычисления хэш-значения загруженной клиентской программы. Однако первый метод решения проблемы целостности является более безопасным, чем последний.

### 9.4.3 Файл клиентской базы данных

Файлы клиентской базы данных (БД) следует хранить безопасным способом. Доступ к БД следует предоставлять только аутентифицированным пользователям. В большинстве случаев клиент IdM имеет дело с информацией о полномочиях пользователя, включая пароли и жетоны безопасности, которая должна храниться в зашифрованном виде для целей обеспечения конфиденциальности. Кроме того, сам файл БД должен быть защищен от несанкционированных изменений и модификаций для поддержания своей целостности. При удалении файла БД из системы на жестком диске не должно оставаться никаких следов для его последующего восстановления.

### 9.4.4 Безопасный пароль

Большинство механизмов обеспечения безопасности зависят в конечном счете от аутентификационного пароля для доступа в систему. Если пользователь применяет легкораскрываемый пароль, который может быть взломан в результате атаки с применением метода полного перебора, то никакие другие механизмы обеспечения безопасности не смогут защитить систему от злонамеренных пользователей. Таким образом, наиболее важная задача для поставщика услуг IdM заключается в обеспечении применения пользователем надежного пароля для регистрации.

### 9.4.5 Удаление клиентской программы

При удалении в пользовательской системе клиентской программы любой пароль, информация о полномочиях и идентичности должны быть необратимо удалены, а также должна быть уничтожена персональная конфигурация для клиентской программы.

## 9.5 Руководящие указания по обеспечению безопасности для мобильных клиентов IdM

В этом пункте приведены руководящие указания по обеспечению безопасности для мобильных клиентов IdM, которые устанавливаются и используются в мобильном устройстве. Мобильное устройство обладает особыми характеристиками, такими как портативность и мобильность. Однако эти характеристики могут превратиться в недостатки в аспекте безопасности, если злоумышленник воспользуется ими в своих интересах.

### 9.5.1 Потеря или кража устройства

Поскольку мобильное устройство является портативным, его очень легко потерять или украсть. Существует много способов проникновения внутрь мобильного устройства для изъятия персональной информации с целью мошенничества с идентичностью. Поэтому введенный в устройство мобильный клиент должен быть подготовлен к любым попыткам нарушения безопасности, которые могут привести к несанкционированному использованию или подделке идентичности. Если устройство потеряно или украдено, то об этом инциденте сообщают поставщику подвижной связи, и, исходя из ситуации, оператор может дистанционно заблокировать устройство, чтобы закрыть доступ к нему. Эти меры принимаются, когда устройство потеряно в дружественной среде, например, дома или на рабочем месте. В любых других случаях оператор должен иметь возможность удаления всей персональной информации или записей идентичности, хранящихся в устройстве, если владелец полагает, что устройство утеряно навсегда или украдено и нет никакой возможности вернуть его.

### 9.5.2 Аутентификация устройства

Если мобильное устройство имеет дисплей небольшого размера для ввода данных, то пользователю очень трудно начинать работу с этим устройством, применяя пароль на основе буквенно-цифровых знаков при каждом использовании устройства. В этом случае в качестве пароля используется PIN (персональный идентификационный номер), который по соображениям удобства во многих ситуациях не применяется. Для преодоления этой проблемы мобильный клиент IdM должен предоставить удобные для пользователя, но достаточно безопасные механизмы аутентификации, подходящие для мобильного устройства. Мобильный клиент должен осуществить аутентификацию

на основе пароля, в случае если в данном устройстве для регистрации пользователя не используются какие бы то ни было механизмы аутентификации.

### 9.5.3 Резервирование базы данных

Бóльшая часть информации об идентичности собирается и обрабатывается мобильным устройством для различных услуг. Однако многие из этих идентификационных данных являются секретной и относящейся к частной жизни персональной информацией, которая нуждается в защите для обеспечения целостности и конфиденциальности. Как отмечалось ранее, это устройство может быть легко потеряно или украдено. Поэтому для мобильного клиента IdM необходимо предусмотреть метод резервирования базы данных, содержащей информацию об идентичности. Это можно сделать двумя способами. Первый способ − зарезервировать базу данных во внешней памяти, например, на SD (защищенная цифровая) карта памяти, если таковая имеется. Второй способ − использовать внешний сервер резервирования для предоставления клиенту услуги резервирования базы данных. В этом случае база данных пользователя может быть всегда восстановлена, даже если устройство потеряно или украдено.

### 9.5.4 Безопасность подвижной связи

Бóльшую часть времени мобильное устройство использует подвижную связь для поддержания связи с другими устройствами. Однако известно, что подвижная связь весьма уязвима для активных и пассивных атак в сети. Мобильный клиент IdM обычно передает секретную персональную информацию по линии подвижной связи. Поэтому для обеспечения целостности и конфиденциальности любая связь с мобильным клиентом с использованием линии подвижной связи нуждается в защите с помощью механизма безопасности на транспортном уровне.

## 9.6 Соображения по обеспечению конфиденциальности в системах IdM

Конфиденциальность представляет крайне важный вопрос в контексте безопасности IdM. Однако в каждой отдельной стране существует множество правил и инструкций в отношении практического применения руководящих указаний по обеспечению конфиденциальности. Поэтому в данном пункте рассматриваются и предоставляются в форме информации некоторые вопросы обеспечения конфиденциальности для систем IdM.

### 9.6.1 Согласие пользователя

В случаях, когда осуществляется сбор идентификационных данных какого-либо пользователя, применяемых в IDP или SP, следует в явной форме получить согласие пользователя для целей распознавания. Лучше всего было бы получать такое согласие в форме цифровой подписи, которую впоследствии, при необходимости, можно использовать для верификации подлинности.

### 9.6.2 Выбор действий в отношении идентичности

Системы IdM в явной форме предоставляют частным лицам возможность выбора того, разрешать или не разрешать сбор, использование, передачу, хранение, архивирование или удаление идентичности. Уровень конфиденциальности пользователя повышается, поскольку последний контролирует процесс управления политикой в отношении своей идентичности и конфиденциальности. Такой ориентированный на пользователя подход должен рассматриваться на этапе проектирования системы IdM.

### 9.6.3 Цель определения идентичности

Перед началом сбора идентификационных данных пользователя система IdM должна простым и понятным образом уведомлять этого пользователя обо всех целях, для которых собирается и используется персональная информация. Кроме того, система должна приложить надлежащие усилия для использования идентичности в тех целях, о которых было заявлено.

### 9.6.4 Ограничение и минимизация определения идентичности

Системы IdM, осуществляющие сбор данных идентичности, должны собирать только те данные определения идентичности, которые необходимы для выполнения определенных ими целей, за исключением случаев согласия конкретного лица или когда это разрешено или необходимо по закону.

Система IdM, осуществляющая сбор данных идентичности, должна тщательно рассматривать и документировать процедуры, в которых четко указано, какие данные определения идентичности необходимы и для каких целей, а также каким образом обеспечить, чтобы весь процесс обработки данных идентичности включал сбор лишь минимально объема таких данных, необходимых для выполнения ее цели.

### 9.6.5 Удаление данных идентичности

Системы IdM должны удалять данные идентичности после выполнения своих заявленных задач и при отсутствии каких бы то ни было других правовых или регуляторных обязательств, требующих более продолжительного периода сохранности этих данных. При удалении данных идентичности необходимо обеспечить, чтобы были удалены также данные идентичности, хранящиеся в связанных системах, таких как система резервирования и система архивирования данных.

### 9.6.6 Определение политики конфиденциальности

Перед эксплуатацией системы IdM может быть определена политика конфиденциальности, например, персональные предпочтения в отношении конфиденциальности и персональная политика авторизации. Такая политика управляет использованием идентичности, представляемой в систему пользователем.

### 9.6.7 Анонимность

Анонимность может быть конечной целью, которая должна быть достигнута в системе IdM с повышенной степенью конфиденциальности. Однако такая функция является весьма сложной и комплексной, для того чтобы ее было возможно предоставлять за небольшую плату. Поэтому в большинстве случаев для удовлетворения требований конфиденциальности системы IdM может быть использован псевдоним.

## Библиография

[b-NIST SP 800-123] Scarfone, K.A., Jansen, W., and Miles, T. (2008), *Guide to General Server Security*, NIST Special Publication SP-800-123.

## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

| | |
|---|---|
| Серия A | Организация работы МСЭ-Т |
| Серия D | Общие принципы тарификации |
| Серия E | Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы |
| Серия F | Нетелефонные службы электросвязи |
| Серия G | Системы и среда передачи, цифровые системы и сети |
| Серия H | Аудиовизуальные и мультимедийные системы |
| Серия I | Цифровая сеть с интеграцией служб |
| Серия J | Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов |
| Серия K | Защита от помех |
| Серия L | Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений |
| Серия M | Управление электросвязью, включая СУЭ и техническое обслуживание сетей |
| Серия N | Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ |
| Серия O | Требования к измерительной аппаратуре |
| Серия P | Оконечное оборудование, субъективные и объективные методы оценки |
| Серия Q | Коммутация и сигнализация |
| Серия R | Телеграфная передача |
| Серия S | Оконечное оборудование для телеграфных служб |
| Серия T | Оконечное оборудование для телематических служб |
| Серия U | Телеграфная коммутация |
| Серия V | Передача данных по телефонной сети |
| **Серия X** | **Сети передачи данных, взаимосвязь открытых систем и безопасность** |
| Серия Y | Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений |
| Серия Z | Языки и общие аспекты программного обеспечения для систем электросвязи |

Отпечатано в Швейцарии
Женева, 2012 г.