ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ

(Проект)

Искусственный интеллект

БОЛЬШИЕ ДАННЫЕ. ОБЗОР И ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ СОХРАННОСТИ ДАННЫХ

(ITU-T Y.3604(2020), IDT)

Настоящий проект стандарта не подлежит применению до его утверждения

Москва Российский институт стандартизации 202

Предисловие

- 1 ПОДГОТОВЛЕН Научно-образовательным центром компетенций в области цифровой экономики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В.Ломоносова» (МГУ имени М.В.Ломоносова) и Обществом с ограниченной ответственностью «Институт развития информационного общества» (ИРИО) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4
- 2 ВНЕСЕН Техническим комитетом по стандартизации ТК 164 «Искусственный интеллект»
- 3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 202_ г. №- ст
- 4 Настоящий стандарт идентичен международному документу ITU-T Y.3604 (02/2020) «Большие данные. Обзор и требования по обеспечению сохранности данных» [Recommendation ITU-T Y.3604 (02/2020) «Big data Overview and requirements for data preservation», IDT].

Наименование настоящего стандарта изменено относительно наименования указанного международного документа для приведения в соответствие с ГОСТ Р 1.5-2012 (пункт 3.5).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных документов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА.

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТР 1.16—2011 (разделы 5 и 6).

Национальный орган Российской Федерации по стандартизации собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее, чем за девять месяцев до истечения срока его действия, разработчику

настоящего стандарта по адресу: 119991, Российская Федерация, Москва, Ленинские горы, д. 1 и в национальный орган Российской Федерации по стандартизации по адресу: 123112, город Москва, Пресненская набережная, дом 10, строение 2.

В случае отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемых информационном указателе «Национальные стандарты» и журнале «Вестник технического регулирования». Уведомление будет размещено также на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет.

© ITU, 2020

© Оформление. ФГБУ «Институт стандартизации», 202_

(Проект)

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1	Область применения			
2	Нормативные ссылки			
3 Термины и определения				
	3.1	Термины, определенные в других документах		
	3.2	Термины, определенные в настоящем документе		
4	Сок	ращения		
5	Согл	оглашения по терминологии		
6 Обзор		ор сохранности больших данных		
	6.1	Общая концепция сохранности данных		
	6.2	Сохранность данных в экосистеме больших данных		
	6.3	Категории данных при сохранности больших данных		
	6.4	Пакеты данных при сохранности больших данных		
	6.5	Функциональные объекты для управления сохранностью больших данных .		
7	Функциональные требования к сохранности больших данных			
	7.1	Отбор данных, подлежащих сохранению		
	7.2	Хранение данных, подлежащих сохранению		
	7.3	Доступ к сохраненным данным		
	7.4	Управление политикой сохранности данных		
8	Обе	спечение безопасности		
При	поже	ние А (справочное) Варианты использования методов сохранности больших данных		
При	поже	ние ДА (справочное) Сведения о соответствии ссылочных международных		
		документов национальным стандартам		
Бибі	пиогр	афия		

Введение

Международный союз электросвязи (МСЭ) является специализированным учреждением ООН в области электросвязи, информационных и коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) является постоянно действующим органом МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов, а также за выпуск Рекомендаций по ним с целью мировой стандартизации электросвязи.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), проводящаяся раз в четыре года, определяет темы для изучения исследовательскими группами 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, входящих в компетенцию MCЭ-T, подготовка необходимых стандартов осуществляется в сотрудничестве с иСО и МЭК.

Примечание – В настоящем стандарте понятие «администрация» используется для краткости, чтобы обозначить как управление электросвязью, так и признанную эксплуатационную компанию.

Соблюдение настоящего стандарта является добровольным. Однако в настоящем стандарте могут содержаться определенные обязательные требования (например, необходимые для обеспечения функциональной совместимости или применимости). Соблюдение настоящего стандарта достигается при выполнении данных обязательных требований. Для выражения требований используются такие слова, как «обязан» или другие императивные формулировки, например «должен», а также их отрицательные эквиваленты. Употребление данных слов не означает, что соблюдение настоящего стандарта является обязательным для какой-либо из сторон.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Искусственный интеллект

БОЛЬШИЕ ДАННЫЕ.

ОБЗОР И ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ СОХРАННОСТИ ДАННЫХ

Artificial intelligence. Big data. Overview and requirements for data preservation

Дата введени	я – с	
	до -	-

1 Область применения

В настоящем стандарте приводится обзор и требования к сохранности больших данных. В документе рассматриваются следующие темы:

- обзор сохранности больших данных;
- функциональные требования к сохранности больших данных;
- варианты использования методов сохранности больших данных.

2 Нормативные ссылки

Следующие рекомендации МСЭ-Т и другие ссылочные документы содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящего стандарта. На момент публикации указанные издания являются действующими. Все рекомендации и другие источники могут быть пересмотрены, поэтому пользователям настоящего стандарта рекомендуется рассмотреть возможность применения самой последней редакции рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время рекомендаций МСЭ-Т регулярно публикуется. Ссылка на тот или иной документ в рамках настоящего стандарта не придает ему, как самостоятельному документу, статус рекомендации.

(Проект)

[ITU-T X.1601], Recommendation ITU-T X.1601 (2015), Security framework for cloud computing (Рекомендация МСЭ-Т X.1601 (2015). Структура безопасности для облачных вычислений)

[ITU-T Y.3600], Recommendation ITU-T Y.3600 (2015), Big data — Cloud computing based requirements and capabilities (Рекомендация МСЭ-Т Y.3600 (2015). Большие данные — Требования и возможности, основанные на облачных вычислениях)

[ITU-T Y.3603], Recommendation ITU-T Y.3603 (2019), Big data – Requirements and conceptual model of metadata for data catalogue (Рекомендация МСЭ-Т Y.3603 (2019). Большие данные. Требования и концептуальная модель метаданных для каталога данных)

3 Термины и определения

3.1 Термины, определенные в других документах

В настоящем стандарте применены следующие термины, определенные в других документах:

3.1.1 **большие данные** (big data): Парадигма, позволяющая осуществлять сбор, хранение, анализ, визуализацию больших наборов данных с неоднородными характеристиками, а также управление ими, потенциально в условиях реального времени.

Примечание — Примерами характеристик наборов данных являются большой объем, высокая скорость, широкое разнообразие и т. д.

[ITU-T Y.3600]

3.2 Термины, определенные в настоящем документе

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.2.1 **сохранность больших данных** (big data preservation): Комплекс мероприятий, стратегий и политик, разработанный сервис-провайдером больших данных (BDSP), для обеспечения доступности и использования ценной информации в экосистеме больших данных.

Примечание — Экосистема больших данных определяет необходимые действия для ролей, предоставляющих или использующих сервисы больших данных, а также взаимоотношения между ними (см. [ITU-T Y.3600]).

- 3.2.2 **сохранность данных** (data preservation): Политики и мероприятия по обеспечению постоянного доступа к данным.
- 3.2.3 **политика сохранности данных** (data preservation policy): Набор правил для контроля мероприятий по сохранности данных.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

BDSP — Сервис-провайдер больших данных;

DAP – Пакет доступа к данным;

DPP – Пакет сохраненных данных;

DSP – Пакет отбора данных.

5 Соглашения по терминологии

В настоящем стандарте:

- ключевые слова «требуется, чтобы» означают требование, которое должно строго соблюдаться и отклонение от которого не допускается, если будет сделано заявление о соответствии этому документу;
- ключевое слово «рекомендуется» означает требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, это требование не является обязательным для заявления о соответствии настоящему документу.

6 Обзор сохранности больших данных

В данном разделе представлен обзор сохранности больших данных. В нем описывается общая концепция сохранности данных, а также иллюстрируется процесс сохранности данных в экосистеме больших данных. В разделе также описываются категории данных, пакеты данных и функциональные объекты для сохранности больших данных.

6.1 Общая концепция сохранности данных

Сохранность данных — это политики и мероприятия, направленные на обеспечение постоянного доступа к данным. Обеспечение сохранности и целостности данных и их метаданных для дальнейшего использования является основополагающим принципом сохранности данных. Целью сохранности данных является защита данных от их потери или разрушения и доступность данных в течение длительного времени.

Потеря или разрушение данных происходит по разным причинам, в том числе изза износа и старения физических носителей данных, исчезновения аппаратного или программного обеспечения, используемого для чтения данных, невозможности прочтения формата файлов, содержащих данные, и т. д.

Сохранность данных расширяет концепцию наличия или обладания данными или резервными копиями данных. Сохранность данных обеспечивает постоянный доступ к данным путем планирования стратегий резервного копирования и восстановления, предшествующих аварийным ситуациям или технологических изменениям.

6.2 Сохранность данных в экосистеме больших данных

В экосистеме больших данных сохранность данных обычно включает в себя комплекс мероприятий, стратегий и политик направленных на обеспечение доступности и использования ценной информации сервис-провайдером больших данных (BDSP).

В дальнейшем термин «сохранность больших данных» используется для обозначения «сохранности данных» в «экосистеме больших данных».

6.2.1 Проблемы сохранности больших данных

Следующие характеристики больших данных (см. пункт 6.1 [ITU-T Y.3600]) порождают проблемы при сохранности больших данных:

- **объем**: характеризует объемы собранных, сохраненных, проанализированных и визуализированных данных, которыми необходимо оперировать с помощью технологий больших данных. С данной характеристикой связаны следующие проблемы:
 - как масштабировать хранилища данных; и
 - как определить данные, подлежащие сохранению.

Примечание — Данные, которые напрямую не используются, могут представлять ценность косвенно, например, для аналитики. Поэтому может быть сложнее принять решение о том, что сохранять и когда предпринимать действия по обеспечению сохранности больших объемов данных.

- **разнообразие**: характеризует различные типы и форматы данных, которые обрабатываются с помощью технологий больших данных. Каждый тип данных может потребовать отдельной программно-аппаратной среды для оперирования данными. С данной характеристикой связаны следующие проблемы:
 - как сохранять различные медиа и контекст их обработки.
- **скорость обработки данных**: характеризует то, как быстро происходит комплектование данных и как быстро данные обрабатываются с помощью технологий больших данных для получения ожидаемых результатов. С точки зрения сохранности больших данных это означает, что:
 - деятельность по обеспечению сохранности должна быть максимально автоматизированной.

6.2.2 Стратегии сохранности больших данных

Согласно рекомендации [ITU-T Y.3600], BDSP поддерживает мероприятия по управлению данными, связанные с происхождением данных, конфиденциальностью данных, безопасностью данных, политикой сохранения данных, владением данными и т. д. Хотя это явно не отмечено, сохранность данных также является одним из видов деятельности по управлению данными и обеспечивает постоянный доступ к данным в соответствии с политикой сохранности данных, которая представляет собой набор правил для контроля мероприятий по сохранению данных.

Для преодоления вышеуказанных проблем BDSP может принять следующие стратегии сохранности больших данных:

- автоматизированные операции: операции по обеспечению сохранности больших данных включают в себя отбор и подготовку данных для сохранения, само сохранение и извлечение сохраненных данных. Из-за огромного объема и высокой скорости обработки больших данных BDSP для повышения эффективности следует поддерживать эти операции и взаимосвязи между ними в «автоматическом» режиме;
- поддержка гибкой политики сохранности данных: сохранность больших данных должна основываться на соответствующей политике. Какие данные следует сохранять, какой тип носителя следует использовать и как долго сохраненные данные

(Проект)

следует хранить — все это примеры положений, которые должны быть определены в гибких политиках сохранности данных. Сохранность больших данных, основанная на соответствующей политике, может помочь BDSP преодолеть проблемы, связанные с объемом и скоростью обработки данных;

- **легкое масштабирование и иерархическое хранение данных**: огромные объемы данных требуют большие хранилища данных. Для поддержания баланса экономичности и эффективности использования хранилища для сохранности данных, BDSP следует применять иерархическую систему хранения данных, где каждый уровень системы должен легко масштабироваться.

6.3 Категории данных при сохранности больших данных

Ниже приведены различные категории данных, учитываемые при сохранности больших данных:

- контент: необработанные данные, подлежащие сохранению;
- **метаданные**: данные о данных или элементах данных, включая их описания, а также данные о владельцах данных, путях и правах доступа и изменчивости данных. Общая концепция метаданных и их применение в экосистеме больших данных описаны в [ITU-T Y.3603]. Для сохранности больших данных необходимы следующие типы метаданных:
 - **дескриптивные метаданные**: описывают структуру и семантику контента (см. пункт 8.2.3 [ITU-T Y.3603]). Они также включают в себя иные метаданные, которые могут потребоваться для понимания контента, такого как программное обеспечение, алгоритмы и т. д.;
 - **нормативно-справочные метаданные**: предоставляют информацию о доступе и для обеспечения поиска (например, тематическая категория и ключевые слова) контента (см. пункт 8.2.3 [ITU-T Y.3603]).;
 - **метаданные о происхождении**: документируют историю контента (см. пункт 8.2.6 [ITU-T Y.3603]);
 - **метаданные о целостности**: обеспечивают проверку целостности данных для защиты контента от недокументированных изменений;
 - **метаданные о правах доступа**: содержат условия доступа к контенту (см. пункт 8.2.3 [ITU-T Y.3603]).
- **метаданные о правилах**: правила, установленные BDSP, которыми следует руководствоваться и которые следует соблюдать при выполнении действий по сохранности больших данных. Репрезентативные правила сохранности больших

данных включают правила отбора данных для хранения, которые определяют какие виды данных BDSP следует хранить, правила определения периода хранения данных, которые определяют, как долго BDSP следует хранить данные, правила хранения сохраняемых данных, которые определяют на каком уровне должны храниться эти данные и при каких условиях их следует перенести на другие уровни хранения и т. д.

Примечание — Например, для автоматизации процесса отбора данных для хранения, BDSP может устанавливать правило отбора данных для хранения, определяющее, какие виды данных подлежат хранению. Параметр данного правила может быть связан с типом данных, размером массива данных, ключевыми словами в наименовании файла и т. д.

6.4 Пакеты данных при сохранности больших данных

Пакеты данных содержат контент и связанные с ними метаданные. При сохранности больших данных выделяются три типа пакетов данных:

- 1) пакет отбора данных (DSP): содержит данные, подлежащие хранению, и связанные с ними метаданные (как правило, дескриптивные метаданные и метаданные о правах доступа), предоставляемые системой управления выбором данных (см. пункт 6.5);
- 2) пакет сохраненных данных (DPP): содержит сохраненные данные и метаданные, генерируемые и поддерживаемые управлением хранением сохраненных данных (см. пункт 6.5);
- 3) пакет доступа к данным (DAP): содержит запрошенные сохраненные данные и связанные с ними метаданные (как правило, включающие дескриптивные метаданные), предоставляемые системой управления доступом к данным (см. пункт 6.5).

Отношения между DPP и DAP могут быть «один к одному», «один ко многим», «многие к одному», «многие ко многим». Например, в соответствии с различными условиями запроса данные DAP могут поступать из одного или нескольких DPP. Отношения между DPP и DSP такие же многозначные, как и отношения между DPP и DAP.

(Проект)

6.5 Функциональные объекты для управления сохранностью больших данных

Функциональные объекты для управления сохранностью больших данных включают управление политикой сохранности данных, управление отбором данных, управление хранением сохраненных данных и управление доступом к данным, как показано на рисунке 6-1. Функциональными объектами являются:

- управление политикой сохранности данных: управляет политикой сохранности данных для обеспечения доступности и пригодности к использованию сохраненных данных;
- управление отбором данных: обеспечивает отбор данных, подлежащих сохранению, и подготовку DSP к хранению в соответствии с установленными правилами;
- управление хранением сохраненных данных: обеспечивает хранение данных, подлежащих сохранению, и поддержку сохраненных данных, включая обновление и миграцию в соответствии с установленными правилами;
- управление доступом к данным: обеспечивает обработку запросов на доступ к сохраненным данным и предоставление запрошенных данных отправителю запроса с помощью DAP.

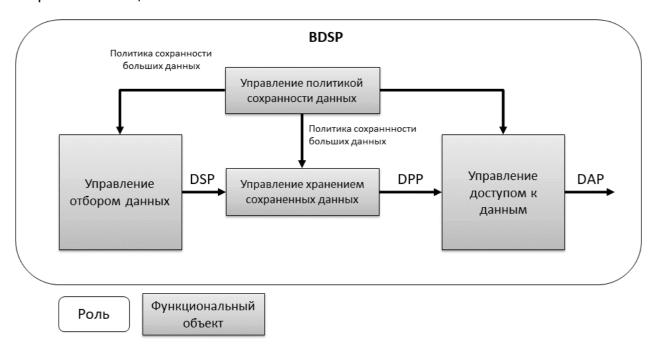


Рисунок 6.1 – Функциональные объекты для управления сохранностью больших данных

Примечание – На рисунке 6.1 представлена одна из ролей BDSP.

7 Функциональные требования к сохранности больших данных

Данный раздел содержит функциональные требования, применимые к сохранности больших данных.

7.1 Отбор данных, подлежащих сохранению

Требования к отбору данных, подлежащих сохранению, включают:

- BDSP следует поддерживать отбор данных, подлежащих сохранению, из исходных данных в соответствии с установленными правилами отбора данных для хранения;

Примечания

- 1 Исходные данные включают в себя все как данные, собранные BDSP вовне, так и результаты обработки данных, сгенерированные внутри BDSP.
- 2 Правила по отбору данных для хранения определяют, какие виды данных BDSP следует сохранять. Параметр данного правила может быть связан с типом данных, размером массива данных, ключевыми словами в наименовании файла и т. д.
- BDSP следует поддерживать извлечение метаданных из данных, подлежащих сохранению;

Примечание — Метаданные, извлеченные из данных, подлежащих сохранению, как правило, включают дескриптивные метаданные, метаданные о целостности и метаданные о правах доступа.

- BDSP следует поддерживать генерацию DSP, который состоит из контента и метаданных.

7.2 Хранение данных, подлежащих сохранению

Требования к хранению данных, подлежащих сохранению, включают:

- BDSP следует поддерживать преобразование DSP в DPP;
- BDSP следует поддерживать выбор надлежащего уровня хранения для DPP в соответствии с установленными правилами хранения сохраняемых данных;

 Π р и м е ч а н и е — Правила хранения сохраняемых данных определяют, на каком уровне должны храниться эти данные и при каких условиях их следует перенести на другие уровни хранения.

(Проект)

- BDSP следует мониторить статистику доступа к DPP для управления иерархией хранилища;
- BDSP следует удалять сохраненные данные в соответствии с установленными правилами определения периода хранения данных

Примечание — Правила определения периода хранения уточняют, как долго BDSP должен хранить данные, подлежащие сохранению.

7.3 Доступ к сохраненным данным

Требования обеспечения доступа к данным, подлежащим сохранению, включают:

- BDSP следует поддерживать проверку полномочий лица, запрашивающего сохраненные данные, при обеспечении доступа к сохраненным данным;
- BDSP следует поддерживать поиск по базе сохраненных данных на условиях фильтрации, предоставляемой лицом, запрашивающим сохраненные данные;
 - BDSP следует поддерживать преобразование DPP в DAP.

7.4 Управление политикой сохранности данных

Требования к управлению политикой обеспечения сохранности данных включают:

- BDSP следует поддерживать установление правил по отбору данных для хранения, чтобы указывать, какие виды данные следует сохранять;
- BDSP следует поддерживать установление правил определения периода хранения данных, чтобы указывать, как долго данные должны храниться;
- BDSP следует поддерживать установление правил хранения сохраняемых данных, чтобы определять на каком уровне должны храниться эти данные и при каких условиях их следует перенести на другие уровни хранения.

8 Обеспечение безопасности

Необходимо учитывать соответствующие требования по обеспечению безопасности [b-ITU-T Y.2201], [b-ITU-T Y.2701] и соответствующие рекомендации МСЭ-Т серий X, Y и M, в том числе требования по контролю доступа, аутентификации, конфиденциальности данных, политике хранения данных, безопасности сети, целостности данных, доступности и защите персональных данных.

Приложение A (справочное)

Варианты использования методов сохранности больших данных

(Данное приложение не является неотъемлемой частью настоящего стандарта).

А.1 Шаблон варианта использования

Разработанные в Приложении I варианты использования должны опираться на следующий унифицированный формат для лучшей читабельности и удобной организации материала.

Таблица А.1 – Шаблон варианта использования

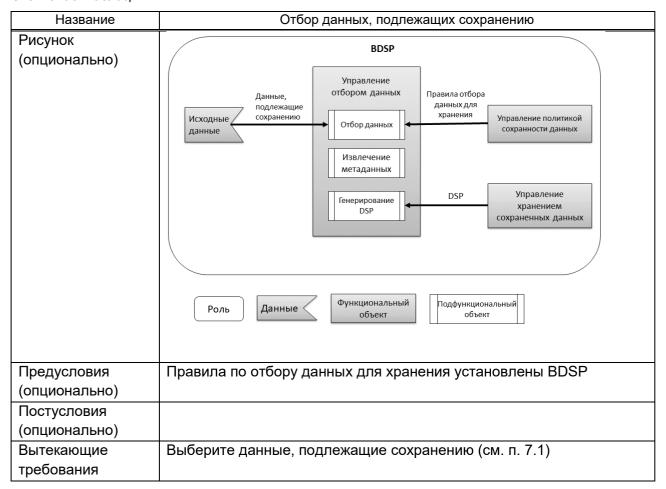
Название	Примечание — Название варианта использования
Описание	Примечание — Описание варианта использования
Роли	Примечание – Роли, задействованные в варианте использования
Рисунок	Примечание — Рисунок для пояснения варианта использования
(опционально)	создается по желанию
Предусловия	Примечание — Необходимые предусловия, которые должны быть
(опционально)	соблюдены до начала варианта использования
Постусловия	Примечание — Постусловие, которое будет выполняться после
(опционально)	завершения текущего варианта использования
Вытекающие	Примечание — Требования вытекают из вариантов использования,
требования	подробное описание которых представлено в соответствующей главе

А.2 Вариант использования: отбор данных, подлежащих сохранению

Таблица А.2 – Отбор данных, подлежащих сохранению

Название	Отбор данных, подлежащих сохранению
Описание	Для подготовки данных, подлежащих сохранению, BDSP выбирает
	данные, основываясь на следующем:
	- BDSP отбирает данные для хранения (т.е. контент) из исходных
	данных в соответствии с правилами по отбору данных для хранения,
	определяющими, какие именно виды данных подлежат сохранению;
	Примечания
	1 Исходные данные включают в себя как все данные, собранные BDSP
	вовне, так и результаты обработки данных, сгенерированные внутри BDSP.
	2 Правила отбора данных для сохранения определяют, какие именно виды
	данных следует сохранять. Параметры данных правил могут быть связаны с
	типом данных, размером массива данных, ключевыми словами в наименовании файла и т. д.
	- BDSP извлекает из данных, подлежащих сохранению, некоторые
	метаданные (например, дескриптивные метаданные, метаданные о
	целостности и метаданные о правах доступа);
	- BDSP генерирует DSP, состоящий из контента и метаданных.
Роли	BDSP

Окончание таблицы А.2



А.3 Вариант использования: создание уровней хранения для сохраненных данных

Таблица А.3 – Создание уровней хранения для сохраненных данных

Название	Создание уровней хранения для сохраненных данных
Описание	Для хранения данных, подлежащих сохранению, BDSP использует
	иерархическую систему хранения, имеющую три уровня: онлайновое
	хранение, когда данные доступны немедленно; почти онлайновое
	хранение, когда данные доступны не сразу, но достаточно быстро;
	офлайновое хранение, когда данные полностью отключены от сети и
	требуют наибольшего времени для обеспечения доступа. Выбор уровня
	хранения данных, подлежащих сохранению, зависит от функции
	управления уровнями хранения и основывается на правилах хранения
	сохраняемых данных.
	Например, существует правило хранения сохраняемых данных,
	определяющее, что объем контента менее 10 Гб следует хранить в
	онлайновом хранении, в противном случае его следует хранить в почти
	онлайновом хранении. Если в течение 3 месяцев доступ к этим данным
	был запрошен менее 3 раз, то их следует переместить на более низкий
	уровень хранения, например, из онлайнового хранения в почти онлайновое
	хранение.
	DSP с 6 Гб контента будет храниться в соответствии со следующими
	процедурами:
	- BDSP преобразует DSP в DPP;

(Проект)

Окончание таблицы А.3



А.4 Вариант использования: доступ к сохраненным данным

Таблица А.4 – Доступ к сохраненным данным

Название	Доступ к сохраненным данным		
Описание	Лицо, запрашивающее сохраненные данные, хочет получить от BDSP		
	доступ к некоторым сохраненным данным. Доступ к сохраненным		
	данным будет осуществляться в соответствии со следующими		
	процедурами:		
	- лицо, запрашивающее сохраненные данные, направляет в систему		
	управления доступом к данным запрос (в соответствии с		
	фильтрационными критериями), чтобы указать, к каким данным оно		
	хочет получить доступ;		

Окончание таблицы А.4

Название	Доступ к сохраненным данным			
	- система управления доступом к данным проверяет, имеет ли дан			
	лицо полномочия на доступ к запрашиваемым данным, и затем			
	отправляет запрос на получение сохраненных данных в управление			
	хранением сохраненных данных;			
	- управление хранением сохраненных данных осуществляет поиск			
	запрошенных сохраненных данных в соответствии с			
	фильтрационными критериями и отправляет полученный(-ые) DPP в			
	систему управления доступом к данным;			
	- система управления доступом к данным преобразует DPP в DAP и			
	отправляет обратно лицу, запрашивающему сохраненные данные			
Роли	BDSP			
Рисунок	BDSP			
(опционально)	Лицо, запрашивающее			
	сохраненные данные Управление доступом к данным Запрос			
	Проверка подномочий сохраненных			
	лица, запрашивающего данных			
	Конвертация DPP в DAP			
	<u> </u>			
	3			
	Запрос сохраненных данных			
	Поиск сохраненных			
	данных			
	Управление хранением сохраненных данных			
	Роль Функциональный Подфункциональный			
	объект			
Пропуспория	Данные, к которым необходимо получить доступ, сохранены BDSP			
Предусловия (опционально)	даппые, к которым необходимо получить доступ, сохранены возе			
Постусловия				
(опционально)				
Вытекающие	Доступ к сохраненным данным (см. п. 7.3)			
требования	доступ к сохраненным данным (см. п. 7.3)			
треоования				

(Проект)

А.5 Вариант использования: управление политикой сохранности данных

Таблица А.5 – Вариант использования: управление политикой сохранности данных

Название	Управление политикой сохранности данных		
Описание	ВDSP реализует управление сохранностью данных на основе политики сохранности данных. BDSP может задавать политику сохранности данных через управление планированием сохранения. Политика сохранности данных состоит из: - правила отбора данных для хранения, которые определяют какие виды данных BDSP следует хранить. Параметры данных правил могут быть связаны с типом данных, размером массива данных, ключевыми словами в наименовании файла и т.д. правила определения периода хранения, которые определяют, как долго BDSP следует хранить данные; правила хранения сохраняемых данных: указывают, на каком уровне следует хранить эти данные и при каких условиях их следует		
Роли	переместить на другие уровни. BDSP		
Рисунок			
(опционально)	Управление политикой сохранности данных Правила отбора данных данных данных данных данных данных для хранения хранения хранения сохраняемых данных		
Предусловия			
(опционально)			
Постусловия			
(опционально)			
Вытекающие	Управление политикой сохранности данных (см. п. 7.4)		
требования			

Приложение ДА (справочное)

Сведения о соответствии ссылочных международных документов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
[ITU-T X.1601]	_	*
[ITU-T Y.3600]	_	*
[ITU-T Y.3603]	_	*

^{*} Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного документа. Перевод данного международного документа находится в Федеральном информационном фонде стандартов

ПНСТ (Проект)

Библиография

[1]	[b-ITU-T Y.2201]	Recommendation ITU-T Y.2201 (2009), Requirements and
		capabilities for ITU-T NGN
[2]	[b-ITU-T Y.2701]	Recommendation ITU-T Y.2701 (2007), Security requirements
		for NGN release 1.

УДК 004.6:006.354 OKC 35.020

Ключевые слова: большие данные, категория данных, пакет данных, сохранность данных, функциональный объект, функциональное требование, стратегия.

Руководитель разработки

Председатель совета директоров

Института развития информационного

общества

Ю. Е. Хохлов

Исполнитель В.А. Дзедик