Международный союз электросвязи

МСЭ-Т X.1641

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2016)

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

Безопасность облачных вычислений – Передовой опыт и руководящие указания в области облачных вычислений

Руководящие указания по безопасности данных потребителей облачных услуг

Рекомендация МСЭ-Т X.1641

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.1641

Руководящие указания по безопасности данных потребителей облачных услуг

Резюме

В Рекомендации МСЭ-Т X.1641 представлены общие руководящие указания по обеспечению безопасности данных потребителя облачных услуг (CSC) в среде облачных вычислений. В Рекомендации проводится анализ жизненного цикла безопасности данных CSC и предлагаются требования безопасности для каждого этапа жизненного цикла данных. Кроме того, в Рекомендации представлены руководящие указания о том, когда следует применять каждое средство безопасности для соответствия передовому опыту в области обеспечения безопасности.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1641	07.09.2016 г.	17-я	11.1002/1000/12853

Ключевые слова

Данные потребителя облачной услуги, средства безопасности данных, жизненный цикл безопасности данных.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует 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.1641

Руководящие указания по безопасности данных потребителей облачных услуг

1 Сфера применения

В настоящей Рекомендации представлены руководящие указания по безопасности данных потребителя облачной услуги (CSC) в среде облачных вычислений для тех случаев, когда ответственность за обеспечение обработки данных при должном уровне безопасности несет поставщик облачной услуги (CSP). Это не всегда так, поскольку для некоторых облачных услуг ответственность за безопасность данных несут сами CSC. В иных случаях ответственность может быть смешанной.

Например, в некоторых случаях CSP может нести ответственность за ограничение доступа к данным, а CSC остается ответственным за принятие решения о том, каким пользователям облачной услуги (CSU) следует предоставить доступ к этим данным, и за режимы работы любых сценариев или приложений, с помощью которых CSU обрабатывает данные.

В настоящей Рекомендации определяются средства безопасности данных CSC, которые могут использоваться на разных этапах всего жизненного цикла данных. Эти средства безопасности могут изменяться при изменении уровня безопасности данных CSC. Вследствие этого, в настоящей Рекомендации представлены руководящие указания о том, когда следует применять каждое средство безопасности для соответствия передовому опыту в области обеспечения безопасности.

2 Справочные документы

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

[ITU-T X.1601] Рекомендация МСЭ-Т X.1601 (2015 г.), *Основы безопасности облачных вычислений*.

[ITU-T X.1631] Recommendation ITU-T X.1631 (2015) | ISO/IEC 27017: 2015, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

3 Определения

3.1 Термины, определенные в других документах

В данной Рекомендации используются термины, определенные в других документах.

3.1.1 аутентификация (authentication) [b-NIST-SP-800-53]: Проверка идентичности пользователя, процесса или устройства, нередко являющаяся необходимым условием обеспечения возможности доступа к ресурсам информационной системы.

3.1.2 облачные вычисления (cloud computing) [b-ITU-T Y.3500]: Парадигма обеспечения возможности сетевого доступа к масштабируемому и гибкому набору совместно используемых физических ресурсов или виртуальных ресурсов со средствами самообслуживания и администрирования по требованию.

ПРИМЕЧАНИЕ. – К примерам ресурсов относятся серверы, операционные системы, сети, программное обеспечение, приложения и оборудование для хранения.

3.1.3 облачная услуга (cloud service) [b-ITU-T Y.3500]: Одна или несколько возможностей, предоставляемых с использованием облачных вычислений, которые активируются через определенный интерфейс.

3.1.4 потребитель облачной услуги (cloud service customer) [b-ITU-T Y.3500]: Сторона, которая состоит в коммерческих отношениях для целей использования **облачных услуг**.

ПРИМЕЧАНИЕ. – Деловые отношения необязательно предполагают финансовые договора.

3.1.5 данные потребителя облачной услуги (cloud service customer data) [b-ITU-T Y.3500]: Класс объектов данных, находящихся под контролем – по юридическим или иным основаниям – потребителя облачной услуги, которые были введены в облачную услугу или получены в результате использования возможностей облачной услуги потребителем облачной услуги или от его имени через опубликованный интерфейс облачной услуги.

ПРИМЕЧАНИЕ 1. – Примером юридического контроля является авторское право.

ПРИМЕЧАНИЕ 2. – Облачная услуга может содержать данные или производить действия с данными, которые не являются данными потребителя облачной услуги; это могут быть данные, предоставленные поставщиками облачных услуг или полученные из другого источника, или же это могут быть общедоступные данные. Однако любые выходные данные, созданные в результате действий с этими данными, которые осуществил потребитель облачной услуги с использованием возможностей облачной услуги, вероятно будут данными потребителя облачной услуги согласно общим принципам авторского права, если в соглашении об облачной услуге явно не предусмотрено обратное.

3.1.6 выведенные данные облачной услуги (cloud service derived data) [b-ITU-T Y.3500]: Класс объектов данных, находящихся под контролем поставщика облачной услуги, которые получены потребителем облачной услуги в результате взаимодействия с облачной услугой.

3.1.7 поставщик облачной услуги (cloud service provider) [b-ITU-T Y.3500]: Сторона, которая предоставляет облачные услуги.

3.1.8 пользователь облачной услуги (cloud service user) [b-ITU-T Y.3500]: Физическое лицо или объект, действующий от его имени, связанные с потребителем облачной услуги, который пользуется облачными услугами.

ПРИМЕЧАНИЕ. – К примерам таких объектов относятся устройства и приложения.

3.1.9 инфраструктура как услуга (infrastructure as a service (IaaS)) [b-IUT-T Y.3500]: Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги, является тип возможностей инфраструктуры.

3.1.10 режим с множеством арендаторов (multi-tenancy) [b-IUT-T Y.3500]: Распределение физических или виртуальных ресурсов, при котором несколько арендаторов и их вычисления и данные изолированы один от другого и недоступны друг другу.

3.1.11 платформа как услуга (platform as a service (PaaS)) [b-ITU-T Y.3500]: Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю услуги, является тип возможностей платформы.

3.1.12 сторона (party) [b-ISO/IEC 20000-1]: Физическое лицо или юридическое лицо, инкорпорированное или неинкорпорированное, либо группа тех или других.

3.1.13 информация, позволяющая установить личность (personally identifiable information (PII)) [b-ISO/IEC 29100]: Любая информация, которая: a) может быть использована для идентификации субъекта PII, к которому такая информация относится; или b) прямо или косвенно связана либо может быть связана с субъектом PII.

3.1.14 субъект PII (PII principal) [b-ISO/IEC 29100]: Физическое лицо, к которому относится информация, позволяющая установить личность (PII).

ПРИМЕЧАНИЕ. – В зависимости от юрисдикции и конкретного закона о защите данных и конфиденциальности, вместо термина "субъект PII" может использоваться его синоним "субъект данных".

3.1.15 программное обеспечение как услуга (software as a service (SaaS)) [b-IUT-T Y.3500]: Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги, является тип возможностей приложения.

3.1.16 арендатор (tenant) [b-IUT-T Y.3500]: Один или несколько пользователей облачной услуги, имеющих общий доступ к набору физических и виртуальных ресурсов.

3.1.17 угроза (threat) [b-ISO/IEC 27000]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

CSC	Cloud Service Customer	Потребитель облачной услуги
CSP	Cloud Service Provider	Поставщик облачной услуги
CSU	Cloud Service User	Пользователь облачной услуги
IaaS	Infrastructure as a Service	Инфраструктура как услуга
PaaS	Platform as a Service	Платформа как услуга
PII	Personally Identifiable Information	Информация, позволяющая установить личность
SaaS	Software as a Service	Программное обеспечение как услуга

5 Условные обозначения

Отсутствуют.

6 Обзор

6.1 Спецификация данных в настоящей Рекомендации

Данные CSC включают персональные данные потребителей, хранящиеся на облачной платформе, и данные, связанные с ними через облачные услуги для CSC, такие как информация учетной записи, регистрационная запись и журнал учета работы.

Ниже более подробно описана разница между терминами CSC (см. п. 3.1.4) и CSU (см. п. 3.1.8).

CSC – это физическое лицо или организация, состоящая в юридических отношениях с CSP. Таким образом, CSC может быть предприятием, филиалом предприятия, государственным учреждением или индивидуальным потребителем.

CSU – это физическое лицо, устройство или приложение, который использует облачную услугу, являющуюся предметом контракта. CSU может быть государственным служащим, приложением, работающим на смартфоне, индивидуальным потребителем или членом домохозяйства, например ребенком. Как правило, CSC назначает некоторых CSU для выполнения функций администраторов и управления отношениями между CSC и CSP. CSU всегда действует от имени CSC. Большинству работников CSU требуется малый объем информации или они могут не иметь никакой информации о том, что или как выполняет CSP, или о том, какие услуги являются предметом контракта CSC, если только CSC не решает, что они должны обладать такой информацией (например, администраторы и внутренние аудиторы).

CSC может включать в себя несколько арендаторов облачной услуг. Арендатор может включать в себя несколько CSU.

6.2 Угрозы безопасности данных для потребителей облачных услуг

В связи с тем что в среде облачной услуги, как правило, существует множество арендаторов, серьезной угрозой для CSC является потеря или утечка данных. Отсутствие надлежащего управления криптографической информацией, например ключами шифрования, кодами аутентификации и правами доступа может нанести серьезный ущерб, например вызвать потерю данных или

неожиданную утечку данных. Основными источниками этой угрозы могут считаться, например, недостаточные средства управления аутентификацией, авторизацией и аудитом, несогласованное использование ключей шифрования или аутентификации, эксплуатационные отказы, проблемы утилизации, вопросы юрисдикции и политические вопросы, надежность центров обработки данных и меры по восстановлению в случае бедствий, которые могут обусловить возникновение проблем.

Что касается безопасности хранимых данных, то поскольку данные всех CSC фактически хранятся в оборудовании CSP, а ресурсы хранения совместно используются разными CSC, это может обусловить некоторые риски, в том числе:

1) привилегированный член CSP может получить несанкционированный доступ и вызвать утечку данных CSC;

2) злонамеренные пользователи или хакеры также могут получить несанкционированный доступ и вызвать утечку данных CSC;

3) трансграничные потоки данных могут стать причиной утечки данных, в особенности конфиденциальных данных;

4) отказы программного и аппаратного оборудования, отключение электроэнергии и стихийные бедствия также могут привести к потере данных.

Безопасность данных тоже является элементом процесса передачи. Во время передачи данные могут быть похищены или искажены, что вызовет, в случае отсутствия надлежащего шифрования данных, нарушение конфиденциальности. Если CSC не используют адекватное шифрование, CSP следует проверять целостность данных и применять соответствующие механизмы шифрования.

Еще одной угрозой является утечка остаточных данных. После того как CSC прекращает свой контракт на использование услуг, его данные стираются, а пространство для хранения высвобождается или перераспределяется другим CSC. Обеспечение невозможности восстановления остаточных данных одного CSC или арендатора другими лежит на CSP.

6.3 Существующие требования, связанные с безопасностью данных

Платформа безопасности облачных вычислений, описанная в [ITU-T X.1601], содержит требования, связанные с безопасностью данных, к которым относятся изолирование данных, защита данных и защита конфиденциальности.

1) Изолирование данных

   В контексте облачных вычислений, арендатор лишен возможности доступа к данным, принадлежащим другому арендатору, даже если эти данные зашифрованы, за исключением случаев, когда доступ санкционирован в явной форме. Изолирование данных может быть реализовано логически или физически, в зависимости от требуемой гранулярности изолирования и конкретного развертывания программного и аппаратного обеспечения облачных вычислений.

   ПРИМЕЧАНИЕ 1. – В среде облачных вычислений изолирование происходит на уровне арендаторов. В рамках данного CSC может существовать множество арендаторов в облаке, например для разделения филиалов, отделов или структурных подразделений.

2) Защита данных

   Защита данных обеспечивает надлежащую защиту данных CSC и выведенных данных, содержащихся в среде облачных вычислений, так чтобы доступ к ним и их изменение могли осуществляться только с санкции CSC (или в соответствии с применимым законодательством). Такая защита может включать некоторое сочетание различных методов, таких как списки контроля доступа, проверка целостности, исправление ошибок/восстановление данных, шифрование и другие надлежащие механизмы. В том случае, когда CSP обеспечивает для CSC шифрование данных на запоминающем устройстве, данная функция может соответствовать шифрованию на стороне клиента (например, в приложении CSP) или шифрованию на стороне сервера.

3) Защита конфиденциальности

Частная информация может включать информацию, позволяющую установить личность (PII), и конфиденциальные корпоративные данные. Сбор, использование, передача, обработка, хранение и уничтожение частной информации регулируются нормативными или законодательными актами в отношении конфиденциальности. Данное ограничение применяется как к CSP, так и к их CSC, а CSC должны иметь возможность постоянного удаления таблицы данных, содержащей частную информацию, даже если CSP не осведомлен о содержании таблицы. Кроме того, может потребоваться, чтобы CSP обеспечивал обработку информации, например поиск данных CSC в преобразованном или зашифрованном виде.

Защита конфиденциальности распространяется на частную информацию, которая может быть получена или выведена в результате деятельности CSC, например тенденции деловой активности, отношения или взаимодействие с другими сторонами, а также уровни и порядок осуществления деятельности.

Защита конфиденциальности отвечает и за обеспечение того, чтобы вся частная информация (включая полученные или выведенные данные) использовалась только в тех целях, которые были согласованы CSC и CSP.

Оценка риска в отношении частной информации (называемая оценкой риска конфиденциальности), может помочь CSP в выявлении конкретных рисков нарушения конфиденциальности, связанных с предполагаемым функционированием. CSP следует определить и реализовать возможности для устранения рисков конфиденциальности, выявленных с помощью оценки риска и обработки частной информации.

ПРИМЕЧАНИЕ. – В некоторых юрисдикциях отдельные физические лица (например, человек-пользователь) рассматриваются отдельно от их работодателей для целей обеспечения конфиденциальности. В таких случаях обеспечивается надлежащая защита конфиденциальности CSU наряду с конфиденциальностью CSC или арендатора.

6.4 Жизненный цикл безопасности данных

В зависимости от реального состояния облачной услуги жизненный цикл безопасности данных CSC включает следующие элементы:

1) Создание: этот элемент лучше, вероятно, назвать создание/обновление, так как он применяется к созданию или изменению элемента данных/содержимого, а не только документа или базы данных. Создание – это генерирование нового цифрового или изменение/обновление существующего содержимого.
2) Передача: это процесс связи при передаче данных из одного места в другое.
3) Хранение: это действие по помещению цифровых данных в какой-либо вид хранилищ для сохранения, и, как правило, оно совершается практически одновременно с созданием.
4) Использование: просмотр, обработка, совместное использование данных или иное действие с данными при выполнении определенной деятельности.
5) Перемещение: это процесс передачи данных между различными хранилищами, форматами или компьютерными системами. Оно является одним из ключевых процессов при реализации, модернизации или объединении любой системы. Перемещение данных осуществляется по многим причинам, включая замену или модернизацию оборудования сервера или аппаратуры хранения данных, объединение веб-сайтов, техническое обслуживание сервера, изменение местонахождения центра данных.
6) Уничтожение: с помощью физических или цифровых средств (например, криптоизмельчение) данные уничтожаются без возможности восстановления.
7) Резервирование и восстановление: пользователи могут создавать резервные копии и восстанавливать данные, используя резервные копии.

7 Руководящие указания о средствах безопасности, относящихся к безопасности данных

В этом разделе представлены руководящие указания о средствах безопасности на этапах жизненного цикла безопасности данных, которые описаны в п. 6.4.

7.1 Средства безопасности на этапе создания

Ниже приведены руководящие указания о средствах безопасности на этапе создания.

a) CSP должны определить категории конфиденциальности данных. Для помощи при классификации данных может использоваться маркировка данных, выполненная пользователем.

b) Данные следует классифицировать согласно степени их конфиденциальности при создании.

c) Для защиты конфиденциальных данных от несанкционированного доступа CSP должны рассматривать механизмы обеспечения цифровых прав предприятий или шифрование.

7.2 Средства безопасности на этапе передачи

Ниже приведены руководящие указания о средствах безопасности на этапе передачи.

a) Для обеспечения безопасности данных аутентификации CSP должны применять технологические методы.

b) CSP должны оказывать помощь пользователям для поддержания безопасной передачи данных, имеющих критическое значение для работы, и данных управления.

c) Нарушение целостности данных во время передачи должно обнаруживаться своевременно, и после обнаружения ошибок должны приниматься необходимые меры для восстановления целостности данных.

7.3 Средства безопасности на этапе хранения

Ниже приведены руководящие указания о средствах безопасности на этапе хранения.

a) CSP должны определять средства контроля доступа, имеющиеся для CSC, в целях применения с пользовательскими данными из хранилищ, такие как определенные в [ITU-T X.1631].

b) CSP должны применять технологию шифрования или другие средства безопасности для обеспечения недоступности содержания хранилища данных аутентификации.

c) CSP должны оказывать помощь пользователям в поддержании обеспечивающего недоступность хранения данных, имеющих критическое значение для работы, и данных управления.

d) CSP должны обеспечивать эффективные методы защиты жестких дисков или применять механизмы фрагментарного хранения в целях недопущения получения неавторизованными пользователями действительных пользовательских данных с жесткого диска, даже в случае его хищения.

e) Нарушение целостности хранимых данных должно обнаруживаться своевременно, и после обнаружения ошибок должны приниматься необходимые меры для восстановления целостности данных.

f) Следует поддерживать дополнительную пользовательскую конфигурацию параметров шифрования, таких как алгоритм, сложность и схемы шифрования.

g) CSP должны оказывать помощь пользователям при выборе механизма шифрования третьей стороны для шифрования ключевых данных.

h) CSP должны поддерживать шифрование данных с использованием защищенных ключей и поддерживать хранение и сопровождение безопасных ключей локально.

i) CSP должны обеспечивать методы эффективной защиты загрузки файлов образа виртуальной машины в целях недопущения возможности ее запуска неавторизованными пользователями на их собственных компьютерных ресурсах с жесткого диска, даже в случае его хищения.

7.4 Средства безопасности на этапе использования

Ниже приведены руководящие указания о средствах безопасности на этапе использования:

a) CSP должны осуществлять авторизацию и верификацию использования данных.

b) Должен выполняться аудит использования конфиденциальных данных, сопровождаемый созданием журналов аудита.

c) CSP должны применять мониторинг злонамеренных действий и механизмы принуждения в рамках сферы своей ответственности и прав для обнаружения угроз и контроля использования данных.

7.5 Средства безопасности на этапе перемещения

Ниже приведены руководящие указания о средствах безопасности на этапе перемещения.

a) Для обеспечения безопасности процесса перемещения данных возможности сетевых соединений следует оценивать до перемещения данных.

b) CSP должны обеспечивать неприкосновенность целостности и конфиденциальности данных в процессе перемещения.

c) CSP должны обеспечивать непрерывное предоставление услуг и бесперебойную работу приложений в процессе перемещения данных.

d) CSP должны надлежащим образом осуществлять мероприятия, связанные с резервным копированием и восстановлением данных, в процессе перемещения данных.

e) CSP должны составить схему перемещения, оценить ее достоинства и недостатки и возникающие риски, после чего разработать в соответствии с этим меры по управлению рисками в рамках подготовки к перемещению данных.

7.6 Средства безопасности на этапе уничтожения

Ниже приведены руководящие указания о средствах безопасности на этапе уничтожения.

a) CSP должны иметь возможность удаления всех ключевых материалов, относящихся к зашифрованным данным.

b) CSP должны применять методы физического уничтожения, такие как размагничивание физического носителя при снятии с эксплуатации оборудования систем хранения.

c) CSP должны применять методы восстановления данных для подтверждения процессов уничтожения.

d) CSP должны иметь возможность обеспечить средства для содействия удалению устаревших данных, являющихся результатом перемещения данных между различными облачными платформами, завершения обслуживания и контракта, или стихийных бедствий.

e) CSP должны обеспечивать средства для удаления всех копий данных.

f) CSP должны гарантировать, что пространство для хранения информации аутентификации пользователя, такой как учетная запись и пароль пользователя, не будет высвобождено или перераспределено другим пользователям до полного удаления этой информации.

g) CSP должны гарантировать, что пространство для хранения ресурсов, таких как файлы, директории и записи баз данных, не будет высвобождено или перераспределено другим пользователям до полного удаления этих ресурсов.

h) CSP должны обеспечивать средства, предотвращающие возможность восстановления уничтоженных данных.

7.7 Средства безопасности на этапе резервного копирования и восстановления

Ниже приведены руководящие указания о средствах безопасности на этапе резервного копирования и восстановления.

a) CSP должны использовать механизмы восстановления содержимого, такие как механизмы предотвращения потери данных, для содействия определению и аудиту данных, для которых требуется резервное копирование.

b) CSP должны поддерживать соответствующий алгоритм шифрования для долговременного (архивного) резервного копирования накопителя данных, например использование длинных ключей шифрования и планирование замены на усовершенствованный алгоритм шифрования.

c) CSP должны обеспечивать функции резервного копирования и восстановления локальных данных. Полной резервное копирование данных следует выполнять не реже одного раза в неделю, а добавочное резервное копирование – не реже одного раза в день.

d) Должен быть создан центр дистанционного аварийного восстановления, оснащенный такими средствами, как линии связи, сетевое оборудование и аппаратура обработки данных и т. д., каковые необходимы для интегрирования в них функций аварийного восстановления.

e) Может быть создан дублирующий центр дистанционного аварийного восстановления. Он должен обеспечивать основные эквивалентные возможности бизнес-деятельности и осуществлять синхронизацию данных в реальном времени по высокоскоростному каналу. Он может одновременно участвовать в операциях бизнес-систем и систем управления, поддерживая при этом непрерывность бизнес-деятельности путем аварийного отключения в аварийных условиях.

f) Для данных, которые классифицированы как важные или конфиденциальные, CSP должны обеспечивать функции дистанционного резервного копирования данных вместе с возможностью оперативного восстановления данных. Одним из вариантов обеспечения этой услуги является сеть, использующая центр аварийного восстановления.

Дополнение I

Руководящие указания по использованию средств безопасности

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В таблице I.1 представлены примеры наборов средств безопасности, которые могут использоваться в целях выполнения руководящих указаний для некоторых сценариев обработки данных, на основе классификации данных и этапов их жизненного цикла.

Таблица I.1 – Пример наборов средств безопасности

Тип	**Жизненный цикл данных**						
	Создание	**Передача**	**Хранение**	**Использо-вание**	**Переме-щение**	**Уничто-жение**	**Резервирова-ние и восста-новление**
IaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), c), d), e), f)
PaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), f), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)
SaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e),f), g), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)

Библиография

[b-ITU-T Y.3500] Рекомендация МСЭ-Т Y.3500 (2014) | ISO/IEC 17788:2014, *Информационные технологии – Облачные вычисления – Обзор и терминология*.

[b-ISO/IEC 27000] ISO/IEC 27000:2014, *Информационные технологии – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Общие сведения и словарь*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Информационная технология – Методы обеспечения безопасности – Схема конфиденциальности*.

[b-NIST-SP-800-53] NIST Special Publication 800-53 Revision 4 (2015), *Security and privacy controls for Federal information systems and organizations*, Available [viewed 2016-12-10] at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты 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, 2017 г.