Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1603

(03/2018)

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

Безопасность облачных вычислений –
Обзор безопасности облачных вычислений

Требования к безопасности данных для услуги мониторинга облачных вычислений

Рекомендация МСЭ-Т X.1603

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.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных системы (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Протоколы безопасности	X.1450–X.1459
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.1603

Требования к безопасности данных для услуги мониторинга облачных вычислений

Резюме

В Рекомендации МСЭ-Т X.1603 проводится анализ требований к безопасности данных для услуги мониторинга облачных вычислений, который включает требования к составу данных мониторинга, жизненный цикл данных мониторинга, требования к безопасности при сборе данных мониторинга и требования к безопасности при хранении данных мониторинга. Требования к составу данных мониторинга включают необходимую сферу охвата мониторинга, которую поставщики облачных услуг (CSP) должны предусмотреть для обеспечения безопасности облака, и наибольшую сферу охвата мониторинга CSP. Жизненный цикл данных мониторинга включает создание данных, хранение данных, использование данных, перемещение данных, представление данных, уничтожение данных и резервное копирование данных. Сбор данных мониторинга определяет требования к безопасности методов сбора данных услуги мониторинга. Хранение данных мониторинга определяет требования к безопасности, предъявляемые к CSP в отношении хранения данных мониторинга.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1603	29.03.2018 г.	17-я	11.1002/1000/13406

Ключевые слова

Облако, безопасность данных, мониторинг.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Стр.

Рекомендация МСЭ-Т X.1603

Требования к безопасности данных для услуги мониторинга облачных вычислений

1 Сфера применения

В настоящей Рекомендации описаны требования к безопасности данных для услуги мониторинга облачных вычислений. В Рекомендации проводится анализ угроз и проблем безопасности данных, связанных с услугой мониторинга в среде облачных вычислений, и приводится описание требований к безопасности данных услуги мониторинга, включая состав данных, жизненный цикл данных, сбор данных и хранение данных. Настоящая Рекомендация может использоваться поставщиками облачных услуг (CSP), которые предоставляют услуги мониторинга потребителям облачных услуг (CSC).

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие 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 возможность (capability) [b-ISO/IEC 19440]: Свойство, заключающееся в способности выполнять данный вид деятельности.

3.1.3 облачные вычисления (cloud computing) [b-ITU-T Y.3500]: Парадигма обеспечения сетевого доступа к масштабируемому и гибкому набору совместно используемых физических или виртуальных ресурсов с предоставлением и администрированием ресурсов на основе самообслуживания по запросу.

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

3.1.4 облачная услуга (cloud service) [b-ITU-T Y.3500]: Одна или несколько возможностей, предоставляемых с использованием облачных вычислений (см. п. 3.1.3), которые активируются с помощью заявленного интерфейса.

3.1.5 потребитель облачной услуги (cloud service customer) [b-ITU-T Y.3500]: Сторона (см. п. 3.1.15), которая состоит в деловых отношениях применительно к использованию облачных услуг (см. п. 3.1.4).

ПРИМЕЧАНИЕ. – Деловые отношения необязательно предполагают финансовые договора.

3.1.6 партнер облачной услуги (cloud service partner) [b-ITU-T Y.3500]: Сторона (см. п. 3.1.15), которая участвует в поддержке деятельности либо поставщика облачной услуги (см. п. 3.1.7), либо потребителя облачной услуги (см. п. 3.1.5), либо обоих или же оказывает помощь в этой деятельности.

3.1.7 поставщик облачной услуги (cloud service provider) [b-ITU-T Y.3500]: Сторона (см. п. 3.1.15), которая предоставляет облачные услуги (см. п. 3.1.4).

3.1.8 пользователь облачной услуги (cloud service user) [b-ITU-T Y.3500]: Лицо или действующий от его имени объект, которые связаны с потребителем облачной услуги (см. п. 3.1.5) и пользуются облачными услугами (см. п. 3.1.4).

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

3.1.9 связь как услуга (communications as a service (CaaS)) [b-ITU-T Y.3500]: Категория облачной услуги, в которой возможностью, предоставляемой потребителю облачной услуги (см. п. 3.1.5), является связь и взаимодействие в реальном времени.

ПРИМЕЧАНИЕ. – В CaaS могут предоставляться два типа возможностей: возможности приложения и возможности платформы.

3.1.10 коллективное облако (community cloud) [b-ITU-T Y.3500]: Модель развертывания облака, в которой облачные услуги (см. п. 3.1.4) обеспечивают исключительную поддержку конкретной группы потребителей облачной услуги (см. п. 3.1.5) и совместно используется этой группой, члены которой имеют общие требования и взаимоотношения один с другим, и при этом как минимум один член этой группы осуществляет контроль над ресурсами.

3.1.11 гипервизор (hypervisor) [b-NIST-SP-800-125]: Компонент виртуализации, осуществляющий управление гостевыми ОС на хост-компьютере и контроль потоков инструкций между гостевыми ОС и физическим аппаратным обеспечением.

3.1.12 инфраструктура как услуга (infrastructure as a service (IaaS)) [b-ITU-T Y.3500]: Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги (см. п. 3.1.5), являются возможности инфраструктуры.

ПРИМЕЧАНИЕ. – Потребитель облачной услуги (см. п. 3.1.5) не осуществляет контроль или управление в отношении внутренних физических или виртуальных ресурсов, но осуществляет контроль над операционными системами, запоминающими устройствами и развернутыми приложениями, которые используют физические и виртуальные ресурсы. Потребитель облачной услуги (см. п. 3.1.5) может также иметь ограниченную возможность контроля над определенными компонентами сети (например, брандмауэрами хост-компьютеров).

3.1.13 режим с множеством арендаторов (multi-tenancy) [b-ITU-T Y.3500]: Распределение физических и виртуальных ресурсов, при котором несколько арендаторов (см. п. 3.1.24) и их вычисления и данные изолированы один от другого и недоступны друг другу.

3.1.14 сеть как услуга (network as a service (NaaS)) [b-ITU-T Y.3500]: Категория облачной услуги, в которой возможность, предоставляемая потребителю облачной услуги (см. п. 3.1.5), является возможностью транспортного соединения и связанными с ним сетевым возможностям.

ПРИМЕЧАНИЕ. – В NaaS могут предоставляться любые из трех типов облачных возможностей.

3.1.15 сторона (party) [b-ISO/IEC 27729]: Физическое лицо или юридическое лицо, инкорпорированное или неинкорпорированное, либо группа тех или других.

3.1.16 информация, позволяющая установить личность (personally identifiable information) [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 прямо или косвенно связана с субъектом PII.

3.1.17 платформа как услуга (platform as a service (PaaS)) [b-ITU-T Y.3500]: Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю услуги (см. п. 3.1.5), являются возможности платформы.

3.1.18 частное облако (private cloud) [b-ITU-T Y.3500]: Модель развертывания облака, где облачные услуги (см. п. 3.1.4) используются на исключительной основе единственным потребителем облачной услуги (см. п. 3.1.5), при этом контроль над ресурсами осуществляет этот потребитель облачной услуги (см. п. 3.1.5).

3.1.19 общественное облако (public cloud) [b-ITU-T Y.3500]: Модель развертывания облака, где облачные услуги (см. п. 3.1.4) потенциально доступны любому потребителю облачной услуги (см. п. 3.1.5), при этом контроль над ресурсами осуществляет поставщик облачной услуги (см. п. 3.1.7).

3.1.20 домен безопасности (security domain) [b-ITU-T X.810]: Совокупность элементов, политика безопасности, орган обеспечения безопасности и набор связанных с безопасностью действий, в рамках которых к набору элементов применяется политика безопасности для указанных действий, а политикой безопасности управляет орган обеспечения безопасности для данного домена безопасности.

3.1.21 инцидент безопасности (security incident) [b-ITU-T E.409]: Инцидент безопасности – это любое неблагоприятное событие, в результате которого некоторый аспект безопасности может подвергнуться угрозе.

3.1.22 соглашение об уровне обслуживания (service level agreement (SLA)) [b-ISO/IEC 20000-1]: Документально оформленное соглашение между поставщиком и потребителем услуги, в котором определяются услуги и целевые показатели обслуживания.

ПРИМЕЧАНИЕ 1. – Соглашение об уровне обслуживания может заключаться также между поставщиком услуги и поставщиком, внутренней группой или потребителем, действующим в качестве поставщика.

ПРИМЕЧАНИЕ 2. – Соглашение об уровне обслуживания может быть включено в договор или в документально оформленное соглашение другого типа.

3.2.23 программное обеспечение как услуга (software as a service (SaaS)) [b-ITU-T Y.3500]: Категория облачной услуги, в которой типом облачных возможностей, предоставляемых потребителю облачной услуги (см. п. 3.1.5), являются возможности приложения.

3.2.24 арендатор (tenant) [b-ITU-T Y.3500]: Один или несколько пользователей облачной услуги (см. п. 3.1.8), имеющих общий доступ к набору физических и виртуальных ресурсов.

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

3.1.26 уязвимость (vulnerability) [b-NIST-SP-800-30]: Слабое место в информационной системе, процедурах обеспечения безопасности системы, внутренних средствах управления или реализации, которое может быть использовано источником угрозы.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 данные мониторинга (monitoring data): Данные мониторинга – это выходные данные услуги облачного мониторинга, которая помогает поставщику облачной услуги (CSP) и потребителям облачной услуги (CSC) управлять облачными платформами и облачными ресурсами.

3.2.2 услуга мониторинга (monitor service): Услуга мониторинга осуществляет контроль качества предоставляемой услуги в части уровней обслуживания согласно их определению в соглашении об уровне обслуживания (SLA) между потребителем облачной услуги и поставщиком облачной услуги.

3.2.3 данные необходимого мониторинга (necessary monitoring data): Данные необходимого мониторинга используются для соблюдения соглашений об уровне обслуживания (SLA). Данные необходимого мониторинга могут помочь поставщику облачной услуги (CSP) поддерживать безопасность и устойчивость платформ облачных вычислений. Данные необходимого мониторинга могут включать, в том числе, данные мониторинга системы управления, данные мониторинга физических ресурсов, данные мониторинга сети и т. д. Данные необходимого мониторинга используются в основном CSP, но также могут использоваться совместно с потребителями облачной услуги (CSC).

3.2.4 данные необязательного мониторинга (optional monitoring data): Данные необязательного мониторинга предоставляются по запросу потребителей облачной услуги (CSC) и служат для обеспечения услуги облачного мониторинга. Данные необязательного мониторинга могут включать, в том числе, данные мониторинга виртуальной машины, данные мониторинга услуги хранения данных, данные облачного мониторинга приложения CSC и т. д.

3.2.5 виртуальная машина (virtual machine (VM)): Действующая изолированная логическая копия реальной машины.

4 Сокращения и акронимы

API	Application Programming Interface		Интерфейс прикладного программирования
BCP	Business Continuity Plan		План обеспечения непрерывности деятельности
CaaS	Communications as a Service		Связь как услуга
CPU	Central Processing Unit	ЦП	Центральный процессор
CSC	Cloud Service Customer		Потребитель облачной услуги
CSN	Cloud Service Partner		Партнер облачной услуги
CSP	Cloud Service Provider		Поставщик облачной услуги

CSU	Cloud Service User		Пользователь облачной услуги
DDOS	Distributed Denial of Service		Распределенная атака типа "отказ в обслуживании"
DNS	Domain Name System		Система доменных имен
DOS	Denial of Service		Отказ в обслуживании
IaaS	Infrastructure as a Service		Инфраструктура как услуга
IAM	Identity and Access Management		Управление определением идентичности и доступом
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
IP	Internet Protocol		Протокол Интернет
IT	Information Technology	ИТ	Информационные технологии
NaaS	Network as a Service		Сеть как услуга
OS	Operating System	ОС	Операционная система
PaaS	Platform as a Service		Платформа как услуга
PII	Personally Identifiable Information		Информация, позволяющая установить личность
PKI	Public Key Infrastructure		Инфраструктура открытых ключей
SaaS	Software as a Service		Программное обеспечение как услуга
SIM	Subscriber Identity Module		Модуль идентификации абонента
SLA	Service Level Agreement		Соглашение об уровне обслуживания
VM	Virtual Machine		Виртуальная машина

5 Соглашения по терминологии

В настоящей Рекомендации:

Ключевое слово "**требуется**" обозначают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

Ключевое слово "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом для заявления о соответствии данное требование не является обязательным.

Ключевое слово "**запрещается**" обозначают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

Ключевые слова "**может факультативно**" означают необязательное требование, которое допустимо, но не имеет какого бы то ни было рекомендательного значения. Этот термин не означает, что вариант реализации поставщика должен обеспечивать выполнение этой функции, и функция может быть активирована по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может предоставлять эту функцию факультативно и при этом заявлять о соответствии спецификации.

6 Обзор

В настоящей Рекомендации проводится анализ требований к безопасности данных для услуги мониторинга облачных вычислений, включая состав данных мониторинга, жизненный цикл данных мониторинга, угрозы и проблемы безопасности, а также требования к безопасности данных мониторинга облачных вычислений.

Состав данных мониторинга определяет два типа данных облачного мониторинга: необходимые и необязательные, а также поясняет сценарии использования.

Жизненный цикл данных мониторинга, а также угрозы и проблемы безопасности определяют контент и угрозы и проблемы безопасности при сборе, хранении, использовании, перемещении, анализе, представлении, разрушении и резервном копировании данных облачного мониторинга.

Требования к безопасности данных мониторинга определяют конкретные требования для каждого этапа жизненного цикла данных облачного мониторинга.

7 Состав данных мониторинга облачных вычислений

В среде облачных вычислений существует два типа данных мониторинга: данные необходимого мониторинга и данные необязательного мониторинга.

Данные необходимого мониторинга – это данные, которые используются для соблюдения соглашений об уровне обслуживания (SLA). Данные необходимого мониторинга могут помочь CSP поддерживать безопасность и устойчивость платформы облачных вычислений. Данные необходимого мониторинга могут включать, в том числе, данные мониторинга системы управления, данные мониторинга физических ресурсов и данные мониторинга сети. Данные необходимого мониторинга используются в основном CSP, но также могут использоваться совместно с CSC.

Данные необязательного мониторинга – это данные, которые предоставляются в ответ на запрос CSC на предоставление услуги мониторинга CSP. Данные необязательного мониторинга могут включать, в том числе, данные мониторинга виртуальной машины, данные мониторинга услуги хранения данных и данные CSC, относящиеся к мониторингу своего собственного приложения в облаке.

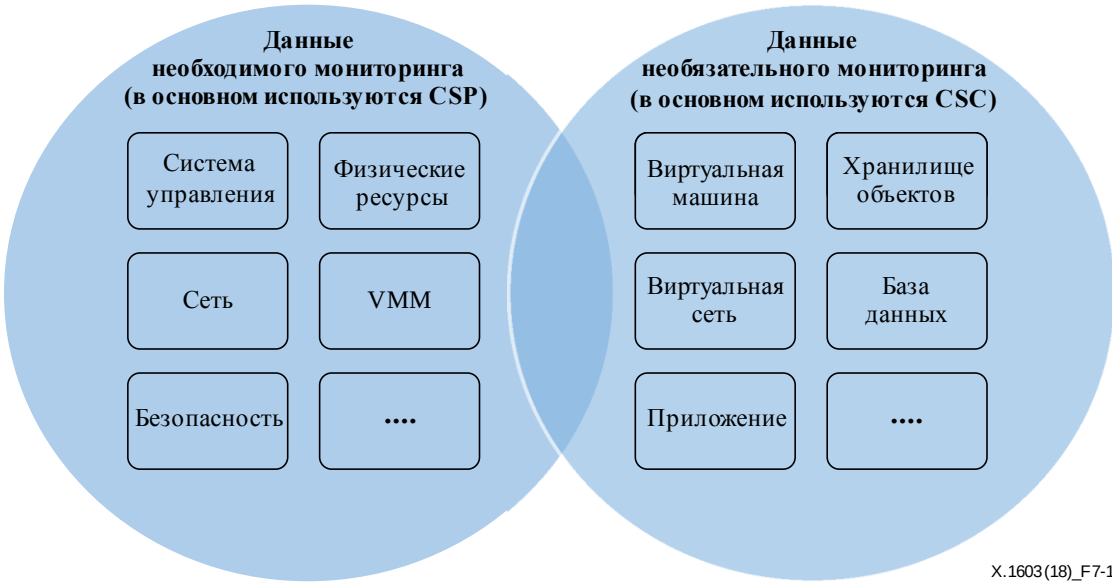

Рисунок 7-1 − Сценарии использования двух типов данных мониторинга данных мониторинга

Данные необходимого мониторинга в основном используются CSP, но их также могут использовать CSC. Например, данные мониторинга физических облачных ресурсов используют в основном CSP для поддержания стабильности облачной платформы, но их также могут использовать CSC, если относящиеся к облаку физические ресурсы предоставлены потребителям в качестве услуги.

Данные необязательного мониторинга предоставляются по запросу CSC и используются в основном также CSC. CSP могут использовать данные необязательного мониторинга для соблюдения SLA. Например, CSC могут запросить данные CSC, связанные с мониторингом их собственных приложений в облаке. Эти данные предоставляются CSP и используются для более эффективного управления своими приложениями в облаке. Например, CSP может использовать данные мониторинга базы данных как услуги (DBaaS) для поддержания безопасности и стабильности ресурсов и услуг базы данных в облаке.

Взаимосвязь этих двух типов данных мониторинга показана на рисунке 7-1.

8 Жизненный цикл данных мониторинга в среде облачных вычислений

В данном разделе описан жизненный цикл данных мониторинга в среде облачных вычислений и разъяснены основные различия между жизненным циклом этих данных и жизненным циклом других данных в среде облачных вычислений.

8.1 Сбор данных мониторинга

Сбор данных мониторинга является результатом получения данных мониторинга и передачи этих данных серверу хранения. Большинство данных мониторинга создается в связи с использованием CSC облачной услуги. Данные необходимого мониторинга могут создаваться также другими функциями мониторинга облачных услуг.

8.2 Хранение данных мониторинга

После выполнения сбора данных мониторинга данные облачного мониторинга могут храниться в облачных ресурсах CSC локально или на серверах хранения данных мониторинга CSP.

8.3 Использование данных мониторинга

Данные мониторинга могут использоваться для поддержания CSP рабочих характеристик и безопасности облачной платформы и облачной услуги; они также могут использоваться для поддержания CSC характеристик и безопасности облачных ресурсов.

8.4 Перемещение данных мониторинга

При перемещении облачных ресурсов данные мониторинга могут перемещаться вместе с облачными ресурсами.

8.5 Анализ данных мониторинга

Данные мониторинга могут анализировать CSP и CSC для понимания статуса ресурсов облачной платформы с целью обеспечения более эффективного управления ими и их большей безопасности.

8.6 Представление данных мониторинга

Рекомендуется предусмотреть возможность представления данных мониторинга в форме, отражающей содержание, с тем чтобы они были пригодны для обеспечения более эффективного управления SLA и безопасности облака. Учитывая, что объем данных облачного мониторинга может быть весьма значительным, рекомендуется обобщать эти данные управляемым и понятным образом.

8.7 Разрушение данных мониторинга

Для поддержания безопасности данных мониторинга требуется, чтобы CSP разрушал данные мониторинга по запросу CSC.

CSP необязательно может разрушать данные мониторинга по истечении соответствующего периода времени с момента создания данных мониторинга.

8.8 Резервное копирование данных мониторинга

Требуется осуществлять резервное копирование данных мониторинга и восстановление данных из резервных копий.

9 Угрозы и проблемы безопасности данных мониторинга облачных вычислений

Угрозы и проблемы безопасности облачных вычислений, разделы 7 и 8, соответственно, в [b-ITU-T X.1601], обусловливают угрозы и проблемы безопасности для CSC и CSP в среде облачных вычислений; к данным облачного мониторинга применимы угрозы и проблемы безопасности, определенные в [b-ITU-T X.1601. Эти угрозы и проблемы безопасности для данных облачного мониторинга включают, в том числе, нижеследующие:

a) потеря и утечка данных;

b) незащищенный доступ к услуге;

c) несанкционированный административный доступ;

d) внутренние угрозы;

e) потеря доверия;

f) потеря управления;

g) потеря конфиденциальности;

h) неготовность услуги;

i) неправомерное присвоение интеллектуальной собственности;

j) совместно используемая среда;

k) конфликт юрисдикций;

l) неудачное перемещение и интеграция.

На каждом этапе жизненного цикла данных мониторинга для данных облачного мониторинга характерны определенные угрозы и проблемы безопасности.

9.1 Угрозы и проблемы безопасности на этапе сбора данных мониторинга

a) Несанкционированный сбор данных: CSP или злоумышленники могут собирать данные мониторинга CSC, не имея разрешения или санкции.

b) Уязвимость интерфейса сбора данных: злоумышленники могут использовать уязвимости интерфейса сбора данных мониторинга.

c) Спуфинг: злоумышленники могут маскироваться под систему управления или сервер хранения данных какой-либо услуги облачного мониторинга и вызывать потерю данных мониторинга.

d) Взлом и перехват: злоумышленники могут использовать атаку через посредника или другие виды сетевых атак для взлома или перехвата данных мониторинга.

e) Незащищенный доступ к услуге: на этапе сбора данных мониторинга незащищенный доступ к интерфейсам сбора данных может вызвать потерю данных мониторинга.

f) Несанкционированный административный доступ: несанкционированный административный доступ к системе сбора данных мониторинга CSP или системе CSC может привести к потере данных мониторинга. Например, злоумышленники могут использовать уязвимость системы для получения несанкционированного административного доступа к системе CSC и изменить IP-адрес пункта сбора данных мониторинга на IP-адрес злоумышленников.

9.2 Угрозы и проблемы безопасности на этапе хранения данных мониторинга

a) Потеря и утечка данных: в связи с тем, что в среде облачной услуги, как правило, существует множество арендаторов, потеря или утечка данных представляет серьезную угрозу и для CSC, и для CSP. Отсутствие надлежащего управления криптографической информацией, например ключами шифрования, кодами аутентификации и правами доступа, может нанести серьезный ущерб, например вызвать потерю данных или неожиданную утечку за пределы облака. Основными угрозами могут считаться, например, недостаточные средства управления аутентификацией, авторизацией и аудитом, несогласованное использование ключей шифрования и/или аутентификации, эксплуатационные отказы, проблемы утилизации, вопросы юрисдикции и политические вопросы, надежность центров обработки данных и восстановление в случае бедствий.

b) Неготовность услуги: сервер хранения данных мониторинга может подвергаться атаке типа "отказ в обслуживании" (DoS) или распределенной атаке типа "отказ в обслуживании" (DDoS); кроме того, может произойти отказ аппаратного оборудования хранения данных мониторинга, который вызовет потерю или разрушение данных.

9.3 Угрозы и проблемы безопасности на этапе использования данных мониторинга

a) Ненадлежащее использование данных: CSP может использовать ненадлежащим образом данные мониторинга CSC. CSP может использовать данные мониторинга для соблюдения SLA

и управления платформой и ресурсами облачных вычислений, однако CSP может использовать данные мониторинга CSC для других целей без разрешения CSC.

b) Внутренние угрозы: сотрудник CSP или CSC может ненадлежащим образом использовать данные мониторинга CSC для неоговоренных целей.

c) Уязвимость системы: данные мониторинга могут быть потеряны в процессе использования данных вследствие уязвимости системы.

d) Прослушивание: злоумышленники могут прослушивать данные мониторинга.

9.4 Угрозы и проблемы безопасности на этапе перемещения данных мониторинга

a) Ненадлежащее использование данных: данные мониторинга могут перемещаться между различными физическими местоположениями. Очень важно не допускать ненадлежащего использования данных в результате передачи данных мониторинга в различные местоположения.

b) Спуфинг: злоумышленники могут маскироваться под систему управления или сервер хранения данных какой-либо услуги облачного мониторинга и вызывать потерю или ненадлежащее использование данных мониторинга.

c) Взлом и перехват: злоумышленники могут использовать атаку через посредника или другие виды сетевых атак для взлома или перехвата данных мониторинга.

9.5 Угрозы и проблемы безопасности на этапе анализа данных мониторинга

a) Ненадлежащее использование данных: CSP может использовать ненадлежащим образом данные мониторинга CSC в процессе анализа данных.

b) Уязвимость системы: данные мониторинга могут быть потеряны вследствие уязвимости системы анализа данных.

c) Атака типа DoS: сервер анализа данных мониторинга может подвергаться атаке типа DoS или DDoS.

9.6 Угрозы и проблемы безопасности на этапе представления данных мониторинга

a) Ненадлежащее использование данных: CSP может использовать ненадлежащим образом (или представлять без разрешения CSC) данные мониторинга CSC в процессе представления данных.

b) Уязвимость системы: данные отчетов и анализа могут быть потеряны вследствие уязвимости системы представления данных.

c) Представление неверных данных: данные мониторинга CSC могут быть представлены в искаженном виде в процессе представления данных.

9.7 Угрозы и проблемы безопасности на этапе разрушения данных мониторинга

a) Спуфинг: злоумышленники могут маскироваться под систему управления услуги облачного мониторинга и вызывать потерю других данных мониторинга.

b) Уязвимость операционной системы: данные мониторинга могут быть потеряны в процессе использования данных вследствие уязвимости системы.

9.8 Угрозы и проблемы безопасности на этапе резервного копирования данных мониторинга

a) Уязвимость операционной системы: вследствие уязвимости системы данные мониторинга могут быть потеряны в процессе резервного копирования данных, в результате чего восстановление данных станет невозможным.

10 Требования к безопасности данных мониторинга облачных вычислений

В данном разделе определены требования к безопасности данных для услуги мониторинга облачных вычислений.

10.1 Требования безопасности при сборе данных мониторинга

Требования к безопасности данных при сборе данных мониторинга включают следующие:

a) требуется, чтобы данные необязательного мониторинга создавались только по запросу CSC;

b) рекомендуется обеспечивать уведомление CSC при создании данных необходимого мониторинга;

c) рекомендуется извещать CSC о составе данных мониторинга;

d) требуется поддерживать целостность и точность данных мониторинга;

e) рекомендуется использовать стандартные методы сбора данных;

f) рекомендуется обеспечивать методы контроля доступа в интерфейсах сбора данных мониторинга, такие как белый список, черный список и т д.;

g) рекомендуется обеспечивать криптографические методы для гарантии безопасности интерфейса сбора данных мониторинга;

h) рекомендуется использовать стандартные сетевые протоколы для связи между облачными ресурсами и серверами хранения данных мониторинга.

В таблице 10-1 представлено сводное сопоставление угроз безопасности при сборе данных мониторинга и требований безопасности.

Таблица 10-1 − Сбор данных мониторинга: соответствие угроз безопасности и требований безопасности

Угрозы безопасности	Требования безопасности
Несанкционированный сбор данных	a), b), c)
Уязвимости интерфейса сбора данных	d), e), f), g)
Спуфинг	d), e), f), g), h)
Взлом и перехват	h)
Незащищенный доступ к услуге	b), d), e), f), g), h)
Несанкционированный административный доступ	d), e), f), g), h)

10.2 Требования безопасности при хранении данных мониторинга

Требования к безопасности данных при хранении данных мониторинга включают следующие:

a) рекомендуется, чтобы CSP обеспечивал надлежащие методы контроля доступа на серверах хранения данных;

b) рекомендуется, чтобы CSP определял максимальный период времени хранения данных мониторинга;

c) рекомендуется, чтобы CSP обеспечивал надлежащие методы кодирования для данных мониторинга.

В таблице 10-2 представлено сводное сопоставление угроз безопасности при хранении данных мониторинга и требований безопасности.

Таблица 10-2 − Хранение данных мониторинга: соответствие угроз безопасности и требований безопасности

Угрозы безопасности	Требования безопасности
Потеря и утечка данных	a), b), c)
Неготовность услуги	a), c)

10.3 Требования безопасности при использовании данных мониторинга

Требования к безопасности данных при использовании данных мониторинга включают следующие:

a) требуется, чтобы CSP четко определял порядок использования данных мониторинга для CSC;

b) рекомендуется, чтобы CSP представлял CSC официальную декларацию об использовании данных мониторинга, например такую, как показана на рисунке 10-1.

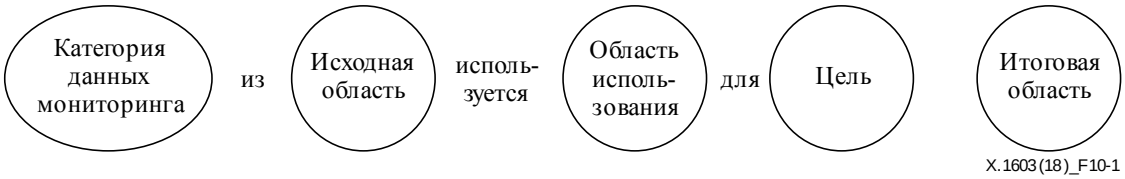

Рисунок 10-1 − Рекомендуемая декларация об использовании данных мониторинга

c) требуется, чтобы CSP обеспечивал уведомление и получал разрешение CSC до использования данных мониторинга в неоговоренных целях;

d) требуется, чтобы CSP поддерживал ведение журнала и аудит использования данных.

В таблице 10-3 представлено сводное сопоставление угроз безопасности при использовании данных мониторинга и требований безопасности.

Таблица 10-3 − Использование данных мониторинга: соответствие угроз безопасности и требований безопасности

Угрозы безопасности	Требования безопасности
Ненадлежащее использование данных	a), b), c), d)
Внутренние угрозы	a), b), c), d)
Уязвимости системы	d)
Прослушивание	d)

10.4 Требования безопасности при перемещении данных мониторинга

Требования к безопасности данных при перемещении данных мониторинга включают следующие:

a) рекомендуется, чтобы CSP обеспечивал уведомление CSC о перемещении данных мониторинга;

b) требуется, чтобы CSP гарантировал защищенную передачу в процессе перемещения данных мониторинга;

c) требуется, чтобы CSP поддерживал ведение журнала и аудит операций по перемещению данных мониторинга.

В таблице 10-4 представлено сводное сопоставление угроз безопасности при перемещении данных мониторинга и требований безопасности.

Таблица 10-4 − Перемещение данных мониторинга: соответствие угроз безопасности и требований безопасности

Угрозы безопасности	Требования безопасности
Ненадлежащее использование данных	a), c)
Спуфинг	b), c)
Взлом и перехват	b), c)

10.5 Требования безопасности при анализе данных мониторинга

Требования к безопасности данных при анализе данных мониторинга включают следующие:

a) требуется, чтобы CSP обеспечивал уведомление CSC о цели анализа данных мониторинга;

b) требуется, чтобы CSP реализовал меры защиты от уязвимостей системы анализа данных мониторинга, например CSP должен предотвращать потерю и утечку данных в системе анализа данных мониторинга;

В таблице 10-5 представлено сводное сопоставление угроз безопасности при анализе данных мониторинга и требований безопасности.

Таблица 10-5 − Анализ данных мониторинга: соответствие угроз безопасности и требований безопасности

Угрозы безопасности	Требования безопасности
Ненадлежащее использование данных	a)
Уязвимость системы	b)
Атака типа DoS	b)

10.6 Требования безопасности при представлении данных мониторинга

Требования к безопасности данных при представлении данных мониторинга включают следующие:

a) требуется, чтобы CSP поддерживал целостность и точность представляемых данных мониторинга;

b) требуется, чтобы CSP реализовал методы аутентификации в целях защиты доступа к представлению данных мониторинга;

c) требуется, чтобы CSP поддерживал меры защиты от уязвимостей системы представления данных мониторинга, например CSP может использовать методы тестирования на защиту от проникновения для предотвращения уязвимостей системы представления данных мониторинга.

В таблице 10-6 представлено сводное сопоставление угроз безопасности при представлении данных мониторинга и требований безопасности.

Таблица 10-6 − Представление данных мониторинга: соответствие угроз безопасности и требований безопасности

Угрозы безопасности	Требования безопасности
Ненадлежащее использование данных	a), b)
Уязвимость системы	b), c)
Представление неверных данных	a), b), c)

10.7 Требования безопасности при разрушении данных мониторинга

Требования к безопасности данных при разрушении данных мониторинга включают следующие:

a) требуется, чтобы CSP обеспечивал надлежащие методы разрушения данных мониторинга;

b) требуется, чтобы CSP предотвращал непреднамеренное разрушение данных мониторинга;

c) требуется, чтобы CSP предотвращал неполное разрушение данных мониторинга;

d) требуется, чтобы CSP уничтожал все конкретные ключи CSC для зашифрованных данных;

e) требуется, чтобы CSP разрушал копии данных мониторинга;

f) требуется, чтобы CSP обеспечивал уведомление CSC о разрушении данных мониторинга.

В таблице 10-7 представлено сводное сопоставление угроз безопасности при разрушении данных мониторинга и требований безопасности.

Таблица 10-7 − Разрушение данных мониторинга: соответствие угроз безопасности и требований безопасности

Угрозы безопасности	Требования безопасности
Спуфинг	a), b), c), d), e), f)
Уязвимость операционной системы	b), c), d), e), f)

10.8 Требования безопасности при резервном копировании данных мониторинга

Требования к безопасности данных при резервном копировании данных мониторинга включают следующие:

a) требуется, чтобы CSP обеспечивал методы резервного копирования для предотвращения потери данных мониторинга;

b) требуется, чтобы CSP поддерживал целостность и точность восстановленных данных мониторинга;

c) требуется, чтобы CSP поддерживал ведение журнала и аудит восстановления данных мониторинга.

В таблице 10-8 представлено сводное сопоставление угроз безопасности при резервном копировании данных мониторинга и требований безопасности.

Таблица 10-8 − Резервное копирование данных мониторинга: соответствие угроз безопасности и требований безопасности

Угрозы безопасности	Требования безопасности
Уязвимость операционной системы	a), b), c)

Библиография

[b-ITU-T E.409] Рекомендация МСЭ-Т E.409 (2004 г.), *Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи.*

[b-ITU-T X.810] Рекомендация МСЭ-Т X.810 (1995 г.), *Информационные технологии – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Обзор*.

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

[b-ITU-T Y.3500] Рекомендация МСЭ-Т Y.3500 (2014 г.), *Информационные технологии – Облачные вычисления – Обзор и терминология*

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[b-ISO/IEC 19440] ISO/IEC 19440 (2007), *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 19944] ISO/IEC 19944 (2016), *Information technology – Cloud services and devices: data flow, data categories and data use*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1 (2011), *Information technology –Service management – Part 1: Service management system requirements.*

[b-ISO/IEC 27000] ISO/IEC 27000 (2016), *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27729] ISO/IEC 27729 (2012), *Information and documentation – International standard name identifier (ISNI).*

[b-ISO/IEC 29100] ISO/IEC 29100 (2011), *Information technology –Security techniques –Privacy framework*.

[b-NIST-SP-800-30] NIST Special Publication 800-30 (2012), *Guide for Conducting Risk Assessments.*

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev.3 (2013), *Recommended Security Controls for Federal Information Systems and Organizations.*

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies.*

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition облачных вычислений.*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2019 г.