Международный союз электросвязи

МСЭ-Т X.1752

(01/2022)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Безопасность данных – Безопасность больших данных

Руководящие указания по безопасности для инфраструктуры и платформы больших данных

Рекомендация МСЭ-Т X.1752

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 (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды (1)	X.1140–X.1149
Безопасность приложений (1)	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 (2)	
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.1350–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределенного реестра (DLT)	X.1400–X.1429
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
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
Киберзащита	X.1590–X.1599
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
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	**X.1750–X.1759**
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800–X.1819

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

Рекомендация МСЭ-Т X.1752

Руководящие указания по безопасности для инфраструктуры и платформы больших данных

Резюме

В Рекомендации МСЭ-Т X.1752 проведен анализ угроз и проблем безопасности, относящихся к инфраструктуре больших данных и платформе больших данных, а также определена эталонная структура для сопоставления руководящих указаний по безопасности и угроз для инфраструктуры и платформы больших данных.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1752	07.01.2022 г.	17-я	11.1002/1000/14806

Ключевые слова

Большие данные, инфраструктура, платформа, руководящие указания по безопасности.

* 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 в целях 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.1752

Руководящие указания по безопасности для инфраструктуры и платформы больших данных

1 Сфера применения

В настоящей Рекомендации содержится описание инфраструктуры и платформы больших данных в соответствии с текущими результатами работ по стандартизации, проводимых в рамках соответствующих форумов. В ней представлена методика оценки угроз и руководящие указания по безопасности, направленные на защиту инфраструктуры и платформы больших данных. В Рекомендации также приведено сопоставление угроз и руководящих указаний по 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 источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

[[ITU-T X.1279] Рекомендация МСЭ-Т X.1279 (2020 г.), *Система расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения.*

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

[ITU-T X.1603] Рекомендация МСЭ-Т X.1603 (2018 г.), *Требования к безопасности данных для услуги мониторинга облачных вычислений.*

[ITU-T X.1605] Рекомендация МСЭ-Т X.1605 (2020 г.), *Требования безопасности к открытой инфраструктуре как услуге (IaaS) в среде облачных вычислений.*

[ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities.*

[ITU-T Y.3605] Recommendation ITU-T Y.3605 (2020), *Big data – Reference architecture.*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 управление доступом (access control) [b-ITU-T X.800]: Предотвращение несанкционированного использования ресурса, в том числе предотвращение использование ресурса несанкционированным способом.

3.1.2 аудит (audit) [b-ITU-T X.800]: Независимый анализ или ревизия системных записей и действий для проверки на адекватность управляющих функций системы, для обеспечения соответствия установленным стратегическим и эксплуатационным процедурам, для выявления нарушения безопасности и для предложения каких-либо изменений в управлении, стратегии или процедурах.

3.1.3 аутентификация (authentication) [b-ISO/IEC 18014-2]: Обеспечение гарантии идентичности объекта.

3.1.4 анализ больших данных (big data analysis) [b- ITU-T Y.2244]: Углубленное исследование больших объемов данных для получения осмысленных результатов, например для определения тенденций или предпочтений.

3.1.5 десенсибилизация данных (data desensitization) [b-ITU-T X.1217]: Процесс сокрытия конфиденциальных данных.

3.1.6 целостность данных (data integrity) [b-ITU-T X.800]: Показатель того, что данные не были изменены или разрушены несанкционированным способом.

3.1.7 брандмауэр (firewall) [b-ISO/IEC 27033-1]: Вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую и, наоборот, при этом пропускается только авторизованный трафик, соответствующий локальной политике безопасности.

3.1.8 балансировка нагрузки (load balancing) [b-ITU-T Y.2052]: Схема, с помощью которой объем трафика можно разделить и сбалансировать в целях эффективного использования сетевых ресурсов (например, полосы пропускания линии).

3.1.9 система обнаружения вторжений (intrusion detection system) [b-ISO/IEC 27039]: Информационные системы, используемые для выявления попыток вторжения, совершаемых или совершенных вторжений.

3.1.10 система предотвращения вторжений (intrusion prevention system) [b-ITU-T X.1361]: Разновидность систем обнаружения вторжений, специально предназначенных для обеспечения возможности активного реагирования.

3.1.11 многофакторная аутентификация (multi-factor authentication) [b-ITU-T X.1158]: Аутентификация с использованием по меньшей мере двух независимых факторов аутентификации.

3.1.12 избыточность (redundancy) [b-ITU-T E.800]: Существование в элементе более чем одного средства для выполнения требуемой функции.

3.1.13 устойчивость (robustness) [b-ITU-T J.1014]: Характеристика определенной функции безопасности ECI, отражающая трудоемкость и/или стоимость усилий, направленных на нарушение защиты, реализуемой данной функцией.

3.1.14 параметры конфигурации обеспечения безопасности (security configuration parameter) [b-ITU-T X.1046]: Набор параметров, описывающих возможности и характеристики функции безопасности, такие как максимальная ширина полосы, максимальное число соединений и т. д., а также защищаемый ею объект и действие по обеспечению безопасности, выполняемое этой функцией.

3.1.15 однократная регистрация входа (single sign-on) [b-ITU-T Y.2201]: Возможность использовать утверждение аутентификации от одного оператора сети/поставщика услуг в сети другого оператора/поставщика услуг для пользователя, запрашивающего доступ к услуге или возможность роуминга в визитной сети.

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

3.1.17 валидация (validation) [b-ITU-T Z.450]: Процесс проверки спецификации на предмет синтаксической и семантической правильности, а также соответствия изложенной в ней логики действий замыслу.

3.1.18 уязвимость (vulnerability) [b-ITU-T X.1524]: Любое слабое место в программном обеспечении, которое может быть использовано для нарушения системы или содержащейся в ней информации.

3.1.19 белый список (whitelist) [b-ITU-T X.1245]: Список идентификаций лиц или источников в услугах связи, где идентификации, включенные в список, являются известными, доверенными или имеют явно выраженное разрешение.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 инфраструктура больших данных (big data infrastructure): Система, состоящая из базовых физических устройств и сетевого окружения в экосистеме больших данных, которая предназначена для реализации услуг больших данных по сбору данных, обработке данных, управлению данными и т. д.

3.2.2 платформа больших данных (big data platform): Система или набор распределенных систем в экосистеме больших данных, предназначенные для выполнения анализа данных, визуализации данных и других функций.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

API	Application Programming Interface	Интерфейс прикладного программирования
BDAP	Big Data Application Provider	Поставщик приложений больших данных
BDIP	Big Data Infrastructure Provider	Поставщик инфраструктуры больших данных
DoS	Denial of Service	Отказ в обслуживании
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
IAM	Identity and Access Management	Управление определением идентичности и доступом
IDS	Intrusion Detection System	Система обнаружения вторжений
IP	Internet Protocol	Протокол Интернет
IPS	Intrusion Prevention System	Система предотвращения вторжений
SSO	Single Sign-On	Однократная регистрация входа
VM	Virtual Machine	Виртуальная машина

5 Соглашения

В настоящей Рекомендации:

ключевое слово "рекомендуется" означает требование, которое рекомендуется, но не является абсолютно необходимым.

6 Угрозы и проблемы безопасности инфраструктуры и платформы больших данных

Как определено в [ITU-T Y.3600] и показано на рисунке 6-1 (на основе рисунка 7-1 в [ITU-T Y.3600]), платформа больших данных предоставляется поставщиком приложений больших данных (BDAP) для выполнения анализа данных, визуализации данных и других функций. Инфраструктура больших данных предоставляется поставщиком инфраструктуры больших данных (BDIP) для реализации услуг больших данных, включая сбор данных, обработку данных, управление данными и т. д.

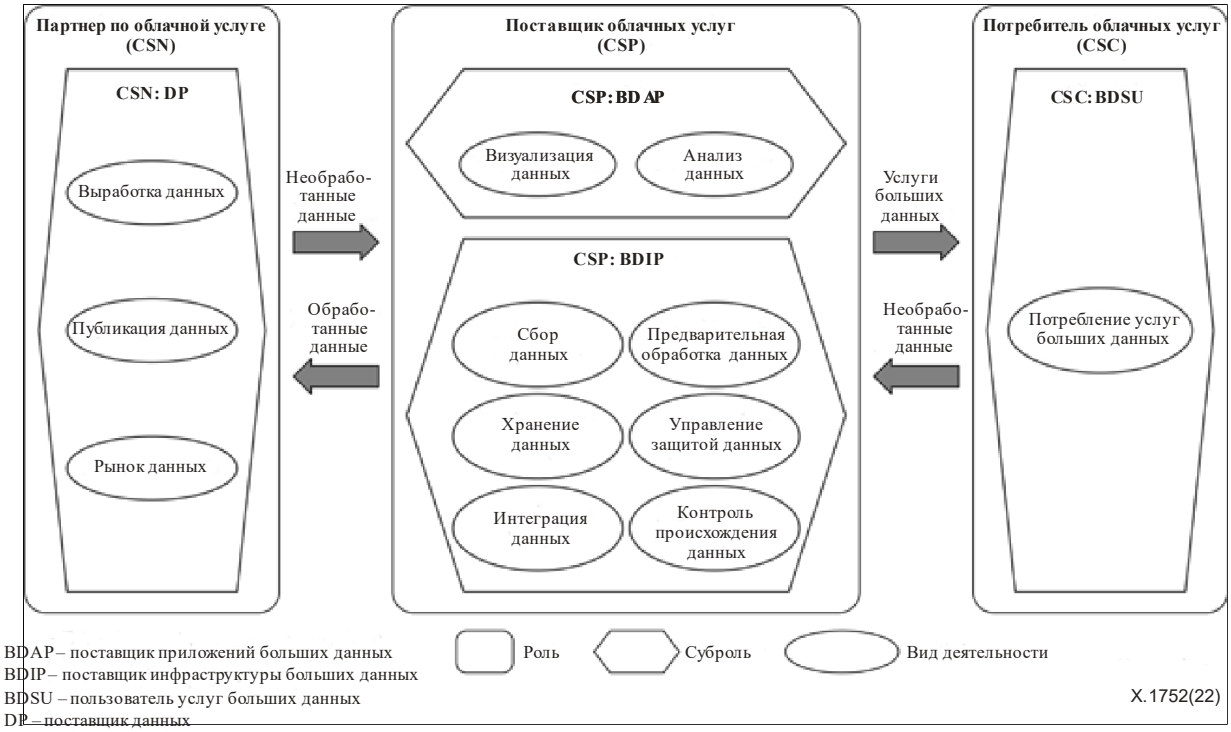

Рисунок 6-1 – Система больших данных на базе облачных вычислений

6.1 Угрозы и проблемы безопасности инфраструктуры больших данных

Угрозы и проблемы безопасности инфраструктуры больших данных охватывают этапы сбора, хранения, интеграции, предварительной обработки данных и управления ими.

6.1.1 Угрозы и проблемы безопасности на этапе сбора данных

К угрозам и проблемам безопасности на этапе сбора данных относится следующее.

a) Несанкционированный сбор данных. Злоумышленники могут собирать данные, не имея разрешения или санкции пользователя.

b) Уязвимость интерфейса сбора данных. Злоумышленники могут воспользоваться уязвимостью интерфейса сбора данных, чтобы получить доступ к процессу сбора данных и вызвать потерю данных.

c) Несанкционированный административный доступ. Несанкционированный административный доступ к системе сбора данных может привести к потере данных. Например, злоумышленники могут воспользоваться уязвимостью системы для получения несанкционированного административного доступа к системе сбора данных, с тем чтобы изменить IP-адрес, на который передаются собранные данные, на IP-адрес злоумышленника.

6.1.2 Угрозы и проблемы безопасности на этапе хранения данных

К угрозам и проблемам безопасности на этапе хранения данных относится следующее.

a) Потеря и 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 за пределы облака. Кроме того, масштабная конвергенция данных из множества источников затрудняет управление доступом при хранении данных. Сложные сценарии хранения и передачи больших данных затрудняют реализацию шифрования данных.

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

c) Угрозы и проблемы безопасности физического хранилища данных. Что касается физической безопасности хранилищ, угрозы и проблемы безопасности в этой области аналогичны тем, которые описаны в пункте 9.3 [ITU-T X.1601] и пункте 7 [ITU-T X.1605].

d) Угрозы и проблемы безопасности оконечного оборудования для хранения данных связаны главным образом с параметрами безопасности аппаратного и программного обеспечения в составе оконечного оборудования, в том числе операционной системы, офисного ПО, браузера, почтовой системы и т. д. К основным таким угрозам и проблемам относятся, в частности, ненадлежащие параметры конфигурации безопасности, несвоевременное обновление параметров конфигурации безопасности и уязвимости в параметрах конфигурации безопасности.

6.1.3 Угрозы и проблемы безопасности на этапе интеграции данных

К угрозам и проблемам безопасности на этапе интеграции данных относится следующее.

a) Ненадлежащее использование данных. Данные могут перемещаться между различными физическими местоположениями. Очень важно не допускать ненадлежащего использования данных вследствие этого процесса.

b) Спуфинг. Согласно определению, данному в [ITU-T X.1279], спуфингом называется попытка объекта выдать себя за другой объект путем демонстрации записанного изображения, другого образца биометрических данных или искусственно полученной биометрической характеристики в целях имитации того или иного индивида. Злоумышленники могут маскироваться под систему управления или сервер хранения данных и вызывать потерю или ненадлежащее использование данных на этапе интеграции.

c) Угрозы безопасности сети на этапе интеграции данных аналогичны угрозам и проблемам безопасности, которые описаны в пункте 9.5 [ITU-T X.1601]. Кроме того, особые проблемы безопасности инфраструктуры больших данных связаны с интегрированным управлением безопасностью в физической сети, виртуальной сети и облачных средах.

6.1.4 Угрозы и проблемы безопасности на этапе предварительной обработки данных

К угрозам и проблемам безопасности на этапе предварительной обработки данных относится следующее.

a) Внутренние угрозы. Сотрудник BDAP может ненадлежащим образом использовать данные пользователя для неоговоренных целей в ходе их предварительной обработки, не имея разрешения пользователя.

b) Уязвимость системы. Данные могут быть потеряны в процессе их предварительной обработки вследствие уязвимости системы.

6.1.5 Угрозы и проблемы безопасности на этапе управления данными

К угрозам и проблемам безопасности на этапе управления данными относится следующее.

a) Уязвимости программного обеспечения. Злоумышленники могут воспользоваться потенциальными уязвимостями системы безопасности программного обеспечения для управления большими данными. Ряд рисков может быть связан с техническими дефектами виртуализации системы; кроме того, не полностью проработанная технология эксплуатации и технического обслуживания может усугубить риски. Наряду с этим модели крупномасштабного распределенного хранения и вычислений, свойственные инфраструктуре и платформе больших данных, повышают риски, связанные с параметрами конфигурации безопасности программного обеспечения, которое используется для управления большими данными.

b) Нарушение управления доступом. Нарушение управления доступом к функциям управления данными может вызвать потерю, утечку или ненадлежащее использование данных.

c) Несанкционированный административный доступ. Несанкционированный административный доступ к системе управления большими данными может привести к потере, утечке или ненадлежащему использованию данных. Например, злоумышленники могут воспользоваться уязвимостью системы, чтобы получить несанкционированный административный доступ к системе больших данных и изменить IP-адрес, на который передаются собранные данные, на IP-адрес злоумышленника.

d) Внутренние угрозы. Неосторожные или недостаточно подготовленные пользователи (или члены семьи, входящие в ближайшее окружение потребителя) либо злонамеренные действия недовольных сотрудников могут привести к потере данных.

6.2 Угрозы и проблемы безопасности платформы больших данных

Угрозы и проблемы безопасности платформы больших данных охватывают этапы визуализации данных и анализа данных.

6.2.1 Угрозы и проблемы безопасности на этапе анализа данных

К угрозам и проблемам безопасности на этапе анализа данных относится следующее.

a) Уязвимость системы. Уязвимость в системе анализа данных может привести к потере данных.

b) DoS/DDoS-атака. Сервер анализа данных может подвергнуться DoS- или DDoS-атаке.

c) Совместное использование приложений для анализа данных. Обычно приложения для анализа данных используются разными пользователями, что может привести к выходу за пределы виртуальной машины, утечке данных и т. д.

d) Незащищенный доступ. Незащищенный доступ к функциям анализа больших данных может вызвать потерю, утечку или ненадлежащее использование данных приложения.

e) Несанкционированный административный доступ. Несанкционированный административный доступ к функциям анализа больших данных может привести к потере данных.

6.2.2 Угрозы и проблемы безопасности на этапе визуализации данных

К угрозам и проблемам безопасности на этапе визуализации данных относится следующее.

a) Ненадлежащее использование данных. В процессе визуализации BDAP может использовать данные не по назначению (или демонстрировать их без разрешения пользователя).

b) Уязвимость системы. Уязвимость в системе визуализации данных может привести к потере отчетных и аналитических данных.

c) Неверное представление данных. Данные могут быть представлены в искаженном виде в процессе визуализации без разрешения пользователя из-за недочетов в политике управления доступом.

7 Руководящие указания по безопасности для инфраструктуры и платформы больших данных

Как определено в [ITU-T Y.3605], в состав многоуровневой структуры, используемой в эталонной архитектуре больших данных, входят четыре уровня и ряд функций, охватывающих несколько уровней. К числу этих четырех уровней относятся:

– уровень доступа;

– уровень приложений;

– уровень обработки; и

– уровень источников данных.

Функции, которые охватывают несколько уровней, называются многоуровневыми.

Эта многоуровневая структура изображена на рисунке 7-1 (на основе рисунка 8-2 в [ITU-T Y.3605]).

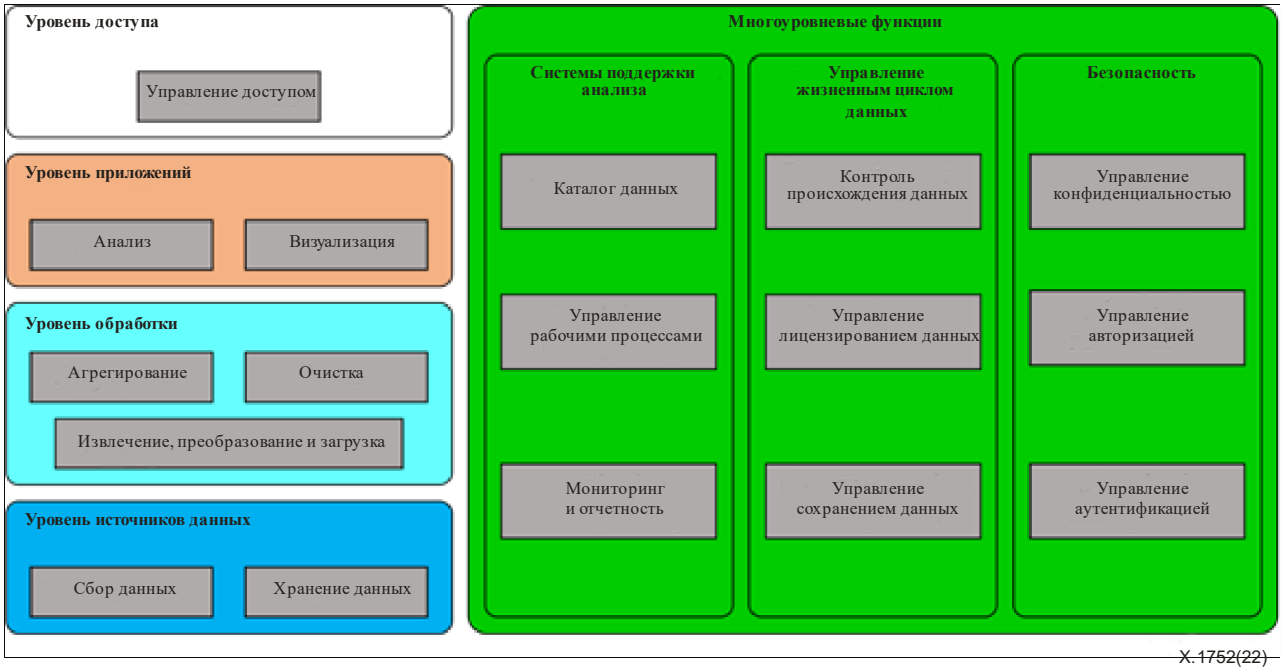

Рисунок 7-1 – Многоуровневая структура больших данных

На основе изображенной на рисунке 7-1 многоуровневой структуры в настоящей Рекомендации разработана архитектура безопасности инфраструктуры и платформы больших данных, показанная на рисунке 7-2.

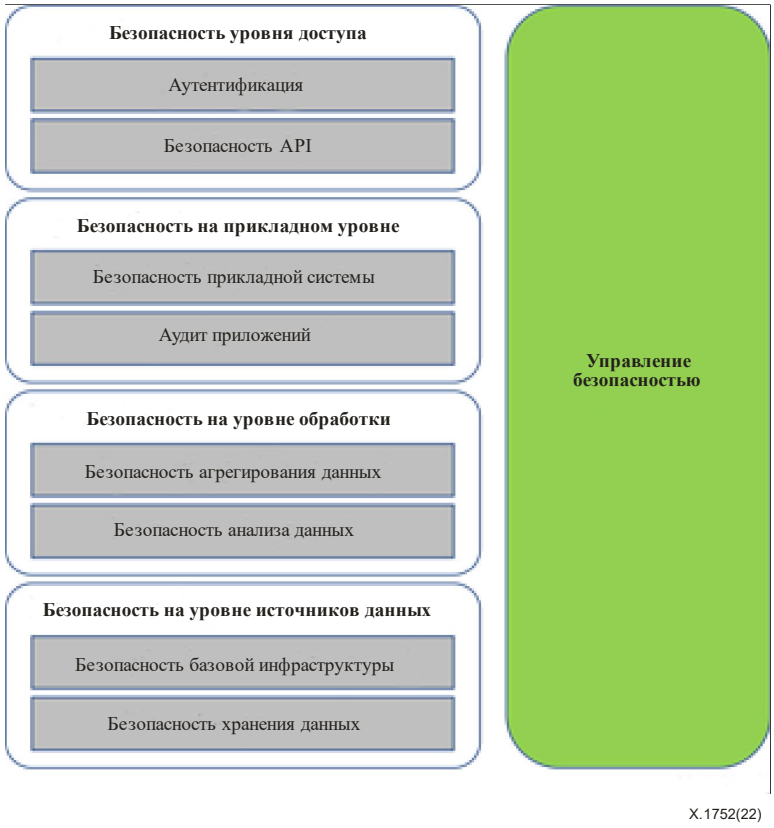

Рисунок 7-2 – Архитектура безопасности инфраструктуры и платформы больших данных

В настоящей Рекомендации содержатся руководящие указания по безопасности для инфраструктуры и платформы больших данных, в том числе:

a) руководящие указания по безопасности на уровне источников данных;

b) руководящие указания по безопасности на уровне обработки;

c) руководящие указания по безопасности на уровне приложений;

d) руководящие указания по безопасности на уровне доступа;

e) руководящие указания по управлению безопасностью.

7.1 Руководящие указания по безопасности на уровне источников данных

Руководящие указания по безопасности на уровне источников данных сосредоточены на вопросах обеспечения безопасности базовой инфраструктуры и безопасности хранения данных.

7.1.1 Руководящие указания по безопасности базовой инфраструктуры

Руководящие указания по безопасности базовой инфраструктуры состоят в следующем.

a) Рекомендуется разделить виртуальную инфраструктуру на внутренний и внешний домены безопасности и реализовать в них разные стратегии обеспечения безопасности в соответствии с текущими потребностями. Рекомендуется предусмотреть эффективные механизмы изоляции между внутренним и внешним доменами безопасности.

b) Рекомендуется реализовать жесткие правила контроля доступа на границе доменов безопасности виртуальной инфраструктуры. Рекомендуется следовать принципу наименьших привилегий, чтобы аутентификация и авторизация в рамках управления доступом пользователей к виртуальной инфраструктуре проводилась на основе их должностных обязанностей.

c) В целях более надежной защиты виртуальной инфраструктуры рекомендуется развернуть в ней программное обеспечение безопасности, например антивирусное программное обеспечение, и периодически обновлять базы данных вирусов и других видов вредоносных программ.

d) На границе между внутренними и внешними сетями рекомендуется развернуть оборудование для обнаружения сетевых атак и защиты от них, например систему предотвращения вторжений (IPS), систему обнаружения вторжений (IDS), брандмауэр, систему защиты от атак DDoS и т. п., и периодически обновлять базы данных сигнатур атак до последней версии.

e) Рекомендуется реализовать строгие правила изоляции и контроля доступа на границе между внутренними и внешними сетями, чтобы предотвратить несанкционированный доступ к базовой инфраструктуре.

f) Рекомендуется проводить мониторинг сетевого трафика базовой инфраструктуры и его глубокий анализ, включая такую важнейшую информацию, как статистические данные сетевых потоков, аномалии сетевого трафика и т. д.

g) При обнаружении атаки рекомендуется отображать информацию о ней, в частности тип атаки, исходный и конечный IP-адреса, временную метку и т. п.

h) Рекомендуется проводить централизованный мониторинг безопасности в режиме реального времени, включая отслеживание текущего состояния различных физических и виртуальных ресурсов.

7.1.2 Руководящие указания по безопасности хранения данных

Руководящие указания по безопасности хранения данных состоят в следующем.

a) Рекомендуется реализовать защищенные компоненты хранения данных, такие как защищенная распределенная файловая система, защищенное индексируемое хранилище и т. д., для обеспечения безопасности среды, в которой хранятся данные.

b) Рекомендуется обеспечить поддержку стратегий изоляции данных различных пользователей в многопользовательской среде.

c) Рекомендуется сформулировать стратегии обеспечения безопасности и регламент управления применительно к хранению данных, например правила контроля доступа, политику безопасной передачи данных, политику обеспечения целостности данных, политику обеспечения согласованности копий, политику шифрования персональных и важнейших данных и т. д.

d) Рекомендуется обеспечить поддержку разнообразных механизмов десенсибилизации данных.

e) Рекомендуется обеспечить поддержку шифрования файловой системы для предотвращения искажения и утечки данных. Рекомендуется также поддерживать распределение по категориям шифрования в зависимости от уровня конфиденциальности данных: нет шифрования, частичное шифрование, полное шифрование и т. д.

f) Рекомендуется предусмотреть функции для обнаружения нарушений целостности хранимых данных и восстановления целостности данных после таких нарушений.

g) Рекомендуется обеспечить поддержку дополнительных параметров конфигурации безопасности, связанных с шифрованием, которые могли бы задаваться по выбору пользователей.

h) Рекомендуется оказывать пользователям помощь в выборе стороннего механизма шифрования важнейших данных.

i) Рекомендуется обеспечить поддержку шифрования данных с использованием защищенных ключей, а также локальное хранение и обслуживание защищенных ключей.

j) Рекомендуется обеспечить поддержку соответствующего алгоритма шифрования для долговременного (архивного) резервного копирования накопителя данных, например использование длинных ключей шифрования и планирование замены на усовершенствованный алгоритм шифрования.

k) Рекомендуется определить временные рамки общего доступа к данным, разрешения на использование данных и удаление данных, а также права на выполнение перечисленных действий.

l) Рекомендуется устанавливать срок действия разрешения на использование данных и уведомлять об этом соответствующих поставщиков и пользователей больших данных.

m) Рекомендуется поддерживать функции удаления, резервного копирования и восстановления данных.

7.2 Руководящие указания по безопасности на уровне обработки

Руководящие указания по безопасности на уровне обработки сосредоточены на вопросах обеспечения безопасности агрегирования и анализа данных.

7.2.1 Руководящие указания по безопасности агрегирования данных

Руководящие указания по безопасности агрегирования данных состоят в следующем.

a) Рекомендуется, чтобы компоненты агрегирования данных поддерживали тот или иной механизм аутентификации, а оконечное устройство источника данных и операторы платформы больших данных прошли аутентификацию и авторизацию.

b) Рекомендуется установить строгий регламент безопасности в отношении процесса агрегирования данных, включая этапы классификации, передачи и временного хранения.

c) Рекомендуется разработать для различных источников данных стратегию классификации данных наряду с соответствующей стратегией управления безопасностью, которые должны регламентировать процесс передачи и временного хранения данных. Для каждого класса источников данных рекомендуется определить соответствующую стратегию управления безопасностью в части обеспечения конфиденциальности, целостности и доступности.

d) Рекомендуется обеспечить поддержку функций ограничения доступа к папке временного хранения в процессе агрегирования данных, чтобы можно было исключить доступ к данным определенных процессов или пользователей и несанкционированное изменение адреса хранения компонентов агрегирования данных.

e) Рекомендуется предусмотреть функции балансировки нагрузки для компонентов агрегирования данных, чтобы можно было распределить нагрузку от интенсивных потоков данных по множеству каналов.

f) Рекомендуется предусмотреть функции обнаружения и защиты (например, IPS/IDC) для компонентов агрегирования данных, чтобы можно было ограничить избыточный или нежелательный сбор данных.

g) Рекомендуется предусмотреть механизмы аварийного переключения и восстановления для компонентов агрегирования данных, чтобы можно было переключить передаваемые потоки данных на резервный компонент.

h) Рекомендуется предусмотреть ведение журналов агрегирования данных и выдачу оповещений в аномальных ситуациях, в том числе при многократном сборе данных, превышении заданного порога интенсивности потоков данных, прерывании потоков данных или превышении заданного объема собранных данных в хранилище.

7.2.2 Руководящие указания по безопасности анализа данных

Руководящие указания по безопасности анализа данных состоят в следующем.

a) Рекомендуется предусмотреть методы аутентификации, чтобы только законные пользователи или приложения могли инициировать запросы на анализ данных.

b) Рекомендуется реализовать модуль контроля доступа для анализа данных в соответствии с политикой идентификации и аутентификации пользователей больших данных, включая управление временными рамками контроля доступа и их валидацию, а также механизм валидации законности доступа к данным.

c) Рекомендуется обеспечить поддержку аудита безопасности анализа распределенных данных, а также определить, какая информация подлежит контролируемому защищенному хранению.

d) Рекомендуется предусмотреть механизм десенсибилизации данных для непрерывного обеспечения безопасности и устойчивости анализа данных, исключающий перебои в деятельности организации, а также значительное снижение производительности системы в результате его использования.

e) Рекомендуется предусмотреть возможность выбора различных механизмов десенсибилизации в соответствии с потребностями различных пользователей и различным характером данных.

f) Рекомендуется обеспечить поддержку настройки механизма десенсибилизации в соответствии с запросами или потребностями пользователей.

g) Рекомендуется предусмотреть возможность динамического добавления и удаления механизмов десенсибилизации, чтобы сделать возможной модернизацию системы без перебоев в работе.

7.3 Руководящие указания по безопасности на уровне приложений

Руководящие указания по безопасности на уровне приложений сосредоточены на вопросах обеспечения безопасности прикладной системы и аудита приложений.

7.3.1 Руководящие указания по безопасности прикладной системы

Руководящие указания по безопасности прикладной системы состоят в следующем.

a) Рекомендуется предусмотреть методы обнаружения и защиты для прикладной системы, такие как брандмауэр, антивирусная система и IDS/IPS.

b) Рекомендуется реализовать механизмы защиты от уязвимостей в прикладной системе.

c) Рекомендуется предусмотреть механизмы аутентификации для предотвращения несанкционированного доступа к прикладной системе.

d) Рекомендуется поддерживать изоляцию между приложениями, чтобы избежать утечки данных в результате анализа связей между данными, инициированного разными приложениями.

7.3.2 Руководящие указания по безопасности аудита приложений

Руководящие указания по безопасности аудита приложений состоят в следующем.

a) Рекомендуется провести аудит работы администраторов с приложениями, чтобы обеспечить возможность отслеживания событий и сбора доказательств при расследовании инцидентов безопасности.

b) Рекомендуется провести аудит работы пользователей с приложением, чтобы обеспечить возможность обнаружения злонамеренного поведения, оповещения о нем и оперативного реагирования на такое поведение.

c) Рекомендуется провести аудит изменения параметров конфигурации безопасности, связанных с оповещениями, оперативным реагированием на злонамеренное поведение и т. д.

7.4 Руководящие указания по безопасности на уровне доступа

Руководящие указания по безопасности на уровне доступа сосредоточены на вопросах обеспечения безопасности механизма аутентификации и интерфейса прикладного программирования (API).

7.4.1 Руководящие указания по безопасности механизма аутентификации

Руководящие указания по безопасности механизма аутентификации состоят в следующем.

a) Рекомендуется обеспечить поддержку услуг расширенной аутентификации, таких как однократная регистрация входа (SSO), многофакторная аутентификация и т. п.

b) Рекомендуется соблюдать жесткие правила в отношении паролей, такие как повышение сложности паролей, регулярное их обновление и т. п.

c) Рекомендуется обеспечить поддержку механизма аутентификации по белому списку, например белый список IP-адресов и т. п.

7.4.2 Руководящие указания по безопасности API

Руководящие указания по безопасности API состоят в следующем.

a) Рекомендуется предоставить администраторам возможность настраивать разрешения на доступ к API, например возможность задавать максимальное число обращений пользователя к API, максимальное число соединений, поддерживаемых API, и т. д.

b) Рекомендуется обеспечить поддержку мониторинга в реальном времени характеристик сетевых потоков между клиентами и API, а также выработку оповещений об аномальном сетевом трафике и возможность реагирования на соответствующие инциденты.

c) Рекомендуется осуществлять валидацию передаваемых в API входных данных для предотвращения различных атак.

d) Рекомендуется обеспечить поддержку передачи основных данных по защищенному (например, зашифрованному) каналу.

e) Рекомендуется обеспечить выполнение анализа и десенсибилизации данных в двух направлениях между клиентами и API до передачи данных.

f) Рекомендуется обеспечить поддержку проверки целостности, а также выявлять искажение и потерю данных в ходе их передачи.

7.5 Руководящие указания по управлению безопасностью

Руководящие указания по управлению безопасностью состоят в следующем.

a) Рекомендуется использовать управление определением идентичности и доступом (IAM) и аудит управления доступом, в том числе документы об эксплуатации и обслуживании, журналы доступа к данным, анализ поведения при доступе, управление ключами и шифрование данных.

b) Рекомендуется применять рациональные и эффективные механизмы обнаружения и защиты, включая избыточность инфраструктуры по безопасности, сканирование на предмет уязвимости, IPS/IDS, брандмауэры и устройства обеспечения безопасности на основе виртуализации.

c) Рекомендуется использовать методы укрепления безопасности для уменьшения поверхности атаки на инфраструктуру и платформу.

d) Рекомендуется регулярно вносить исправления и обновлять версии инфраструктуры и платформы больших данных.

Библиография

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ.*

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995), *Information technology – Open System Interconnection – Security frameworks for open system: Overview.*

[b-ITU-T X.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device.*

[b-ITU-T X.1217] Рекомендация МСЭ-Т X.1217 (2021 г.), *Руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи.*

[b-ITU-T X.1245] Рекомендация МСЭ-Т X.1245 (2010 г.), *Структура противодействия спаму в мультимедийных IP-приложениях.*

[b-ITU-T X.1361] Рекомендация МСЭ-Т. X.1361 (2018 г.), *Структура безопасности интернета вещей на основе модели с использованием шлюза.*

[b-ITU-T X.1524] Рекомендация МСЭ-Т X.1524 (2012 г.), *Перечень общеизвестных слабых мест.*

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

[b-ITU-T Y.2052] Рекомендация МСЭ-Т Y.2052 (2008 г.), *Структура множественной адресации в СПП на базе IPv6.*

[b-ITU-T Y.2201] Рекомендация МСЭ-Т Y.2201 (2009 г.), *Требования к СПП МСЭ-Т и возможности этих сетей.*

[b-ITU-T Y.2244] Recommendation ITU-T Y.2244 (2019), *Service model for a cultivation plan service at the pre-production stage.*

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

[b-ITU-T Y.3502] Рекомендация МСЭ-Т Y.3502 (2014 г.), *Информационные технологии – Облачные вычисления – Эталонная архитектура.*

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens.*

[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.*

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

Отпечатано в Швейцарии,
Женева, 2022 г.