Международный союз электросвязи

МСЭ-Т X.1750

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2020)

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

Безопасность данных – Безопасность больших данных

Руководящие указания по безопасности больших данных как услуги для поставщиков услуг больших данных

Рекомендация МСЭ-Т X.1750

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	X.1140–X.1149
Протоколы безопасности (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.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1389
Безопасность технологии распределения реестра	X.1400–X.1429
Безопасность технологии распределения реестра	X.1430–X.1449
Протоколы безопасности (2)	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
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**
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

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

Рекомендация МСЭ-Т X.1750

Руководящие указания по безопасности больших данных как услуги для поставщиков услуг больших данных

Резюме

Большие данные как услуга (BDaaS) – это категория облачных услуг, которая предоставляет потребителям облачных услуг возможности сбора, хранения, анализа, визуализации данных и управления данными, как определено в Рекомендации МСЭ-Т Y.3600. В результате значительного роста объемов данных и стремительного развития компаний, работающих с большими данными, инфраструктура больших данных стала основным инструментом обеспечения BDaaS. Вследствие этого возникают существенные проблемы безопасности BDaaS. Например, при проектировании программного обеспечения больших данных с открытыми кодами аспекты безопасности не всегда учитываются с самого начала процесса. Новые технологии, вводимые в контексте анализа больших данных, также могут привести к неэффективности традиционных мер обеспечения безопасности. В Рекомендации МСЭ-Т X.1750 проведен анализ проблем безопасности, возникающих в BDaaS, определены функции и обязанности по обеспечению безопасности при предоставлении BDaaS, а также структура безопасности для инфраструктуры больших данных. Наряду с этим определены меры обеспечения безопасности, которые следует соблюдать в отношении услуг и компонентов, связанных с BDaaS.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1750	03.09.2020 г.	17-я	11.1002/1000/14266

Ключевые слова

Большие данные как услуга, руководящие указания по безопасности, меры 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.1750

Руководящие указания по безопасности больших данных как услуги для поставщиков услуг больших данных

1 Сфера применения

В настоящей Рекомендации приведен анализ проблем безопасности, с которыми сталкиваются большие данные как услуга (BDaaS), и даны руководящие указания для поставщиков услуг больших данных (BDSP) по обеспечению безопасности BDaaS. В ней определены роли и обязанности по обеспечению безопасности для компонентов BDaaS, а также структура безопасности для инфраструктуры больших данных, включая платформы, приложения, аналитические инструменты, интерфейсы и экосистему BDaaS. В настоящей Рекомендации также определены меры обеспечения безопасности, которые следует принимать в отношении действий или компонентов, связанных с BDaaS.

Настоящая Рекомендация представляет собой высокоуровневое описание требований по безопасности, предъявляемых к реализациям BDaaS, которые относятся главным образом к BDaaS. В BDaaS задействованы поставщики инфраструктуры больших данных (BDIP) и поставщики приложений больших данных (BDAP). Руководящие указания в отношении BDIP и BDAP, а также подробное руководство по реализации BDaaS выходят за рамки настоящей Рекомендации.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статуса 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), *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[ITU-T X.1641] Рекомендация МСЭ-Т X.1641 (2016 г.), *Руководящие указания по безопасности данных потребителей облачных услуг.*

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

[ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

[ISO/IEC 27036-3] ISO/IEC 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security.*

[ISO 28000] ISO 28000:2007, *Specification for security management systems for the supply chain.*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 большие данные (big data) [b-ITU-T Y.3600]: Концептуальная схема, позволяющая осуществлять с огромными наборами данных, имеющими неоднородные характеристики, операции сбора, хранения, управления, анализа и визуализации потенциально в условиях ограничений, связанных с работой в реальном времени.

ПРИМЕЧАНИЕ. – К примерам характеристик наборов данных относятся большой объем, высокая скорость, большое разнообразие и т. д.

3.1.2 большие данные как услуга (big data as a service (BDaaS)) [b-ITU-T Y.3600]: Категория облачной услуги, в которой возможностями, предоставляемыми потребителю облачной услуги, являются возможности сбора, хранения, анализа, визуализации данных и управления данными с использованием технологий больших данных.

3.1.3 происхождение больших данных (big data provenance) [b-ITU-T Y.3602]: Информация, фиксирующая исторический путь данных в соответствии с операциями жизненного цикла данных в экосистеме больших данных.

3.1.4 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.

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

3.1.6 метаданные (metadata) [b-ITU-T M.3030]: Данные, описывающие другие данные.

3.1.7 проблема безопасности (security challenge) [ITU-T X.1601]: Отличная от непосредственной угрозы безопасности "трудность", включающая косвенные угрозы, которая обусловлена характером и рабочей средой облачных услуг.

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

3.1.9 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 определяется следующий термин.

3.2.1 информационный ресурс (data asset): Источник записанных электронным способом данных, принадлежащий организации или контролируемый ею.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

API	Application Programming Interface	Интерфейс прикладного программирования
ABAC	Attribute-Based Access Control	Управление доступом на основе атрибутов
BDaaS	Big Data as a Service	Большие данные как услуга
BDAP	Big Data Application Provider	Поставщик приложений больших данных
BDIP	Big Data Infrastructure Provider	Поставщик инфраструктуры больших данных
BDSN	Big Data Service Partner	Партнер по услугам больших данных

BDSP	Big Data Service Provider		Поставщик услуг больших данных
BDSU	Big Data Service User		Пользователь услуг больших данных
CSC	Cloud Service Customer		Потребитель облачной услуги
DP	Data Provider		Поставщик данных
IT	Information Technology	ИТ	Информационные технологии
PII	Personally Identifiable Information		Информация, позволяющая установить личность
PKI	Public Key Infrastructure		Инфраструктура открытых ключей
SAML	Security Assertion Markup Language		Язык разметки утверждений безопасности
SDK	Software Development Kit		Комплект инструментов разработки программного обеспечения
SSL	Secure Socket Layer		Протокол безопасных соединений
TLS	Transport Layer Security		Безопасность транспортного уровня
USB	Universal Serial Bus		Универсальная последовательная шина

5 Соглашения

В настоящей Рекомендации:

формулировка "**требуется, чтобы**" означает требование, которое должно строго соблюдаться и от которого не допускается отклонений, если будет сделано заявление о соответствии настоящей Рекомендации;

формулировка "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым, таким образом для заявления о соответствии настоящей Рекомендации это требование не является обязательным;

формулировка "**запрещено, чтобы**" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

формулировка "**может факультативно**" означает необязательное требование, которое допустимо, но не имеет рекомендательного значения. Данный термин не подразумевает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и что функция может быть активирована по желанию оператора сети/поставщика услуг дополнительно. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии спецификациям.

6 Угрозы и проблемы безопасности больших данных как услуги

В этом разделе содержится описание угроз и проблем безопасности BDaaS. Определение BDaaS на основе облачных вычислений дано в [ITU-T Y.3600]. Для BDaaS следует учитывать проблемы безопасности, относящиеся к среде облачных вычислений, которые описаны в разделе 8 [ITU-T X.1601]. Кроме того, в настоящей Рекомендации рассматриваются угрозы и проблемы безопасности, относящиеся к конкретным возможностям и услугам BDaaS, то есть к платформе больших данных как услуге и к программному обеспечению, связанному с большими данными, как услуге (с учетом того, что экосистема BDaaS включает поставщиков данных (DP), BDAP и BDIP), в том числе:

– уязвимости инфраструктуры больших данных и нарушение мер безопасности;
– проблемы хранения и аудита, связанные с неструктурированными данными;
– безопасность и регулирование интерфейса между приложениями, платформами и потоком услуг;
– другие проблемы безопасности, такие как проблемы доверия, аутентификации и визуализации.

На рисунке 6-1 показана структура проблем безопасности BDaaS.

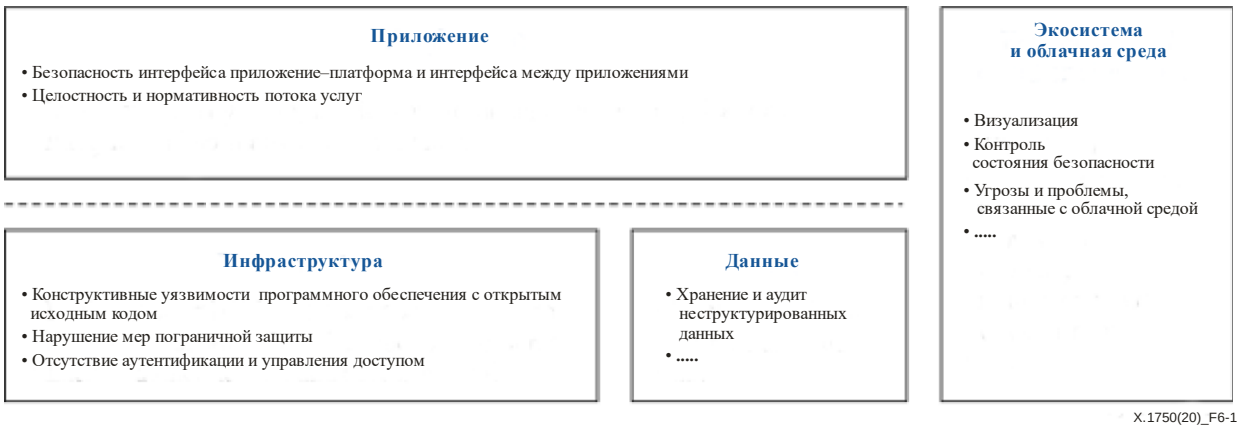

Рисунок 6-1 – Проблемы безопасности больших данных как услуги

6.1 Проблемы безопасности инфраструктуры больших данных

Инфраструктура больших данных может состоять из различных компонентов, получаемых либо из коммерческих источников, либо в виде открытого исходного кода. В конструкции некоторых из этих компонентов проблемы безопасности могут не учитываться изначально, что приводит к потенциальным рискам безопасности, в том числе:

– небезопасному исходному коду и отсутствию механизмов безопасности в компонентах с открытым исходным кодом;

– характеристикам открытой междоменной платформы, стирающим традиционные границы безопасности, что приводит к нарушению мер пограничной защиты;

– отсутствию соответствующих механизмов аутентификации и управления доступом для разных ролей, что может привести к злоупотреблениям.

6.2 Проблемы безопасности приложений больших данных

Инфраструктура больших данных объединяет множество высокоцентрализованных приложений со сложными моделями услуг. К проблемам безопасности приложений больших данных относятся:

– возможное отсутствие проверки безопасности и контроля передачи данных в интерфейсах прикладного программирования (API), комплектах инструментов разработки программного обеспечения (SDK) и интерфейсах между приложениями;

– необходимость отслеживания, контроля и обнаружения выполнения пользовательских приложений для гарантии безопасности бизнес-логики.

6.3 Проблемы безопасности данных

Инфраструктура и приложения больших данных работают с огромными объемами данных. В экосистеме больших данных могут присутствовать такие типы данных, как структурированные, полуструктурированные и неструктурированные данные. Структурированные данные часто хранятся в базах данных, которые могут быть организованы в соответствии с различными моделями, такими как реляционная модель, документальная модель, модель "ключ–значение" и графическая модель. Полуструктурированные данные не соответствуют формальной структуре моделей данных, но содержат теги или маркеры для идентификации данных. Неструктурированные данные не имеют заранее определенной модели данных и не организованы каким-либо установленным образом. В рамках всех типов данных могут существовать данные в разных форматах, таких как текст, электронные таблицы, видеоданные, аудиоданные, изображения и карты (см. [ITU-T Y.3600]). Эти данные используются на этапах хранения, анализа, расчета и других этапах обработки данных. К проблемам безопасности данных относятся:

– требование принятия мер безопасности (включая управление доступом) для обеспечения конфиденциальности данных при поддержке эффективной работы с данными;

– аудит неструктурированных данных;

– риск утечки личной конфиденциальной информации в случае, если данные открыты или ими обмениваются;

– необходимость применять традиционные меры безопасности, описанные в [ITU-T X.1601] к метаданным, так как они имеют те же характеристики, что и данные, публикуемые в интернете.

Проблемы безопасности, связанные с обработкой сведений о происхождении больших данных, включают: зараженные или злонамеренно манипулируемые записи о происхождении данных по всей цепочке обработки, неавторизованные объекты в процессе обработки или обмена информацией о происхождении данных, неаутентичные коды обработки, связанные с происхождением данных, а также проблемы безопасности информации о происхождении данных.

6.4 Проблемы безопасности экосистемы больших данных как услуги

Согласно [ITU-T Y.3600] экосистема BDaaS состоит из ролей и подролей, которые выполняют различные участники/компоненты, предоставляющие и потребляющие услуги на основе больших данных. От экосистемы BDaaS требуется планирование, разработка и реализация мер безопасности на этапе создания, эксплуатации, аудита и других этапах управления предоставлением услуг. К проблемам безопасности больших данных как услуги относятся:

– необходимость постоянного мониторинга действий пользователей, состояния сети, состояния ресурсов и т. д. для борьбы с изменяющимися угрозами;

– появление новых векторов угроз и отсутствие механизмов потенциальной защиты;

– неспособность установить доверие между различными участниками процесса, включая владельцев данных и устройства (для сбора данных);

– безопасность реализации виртуализации, например целостность конфигураций безопасности и виртуальных образов;

– возможность существования сложной цепочки поставок в экосистеме больших данных – повлиять на непрерывность деятельности может даже подрядчик, не заключивший прямой договор с организацией;

– риски, связанные с цепочкой поставок, и необходимость принятия соответствующих мер, включая меры безопасности, описанные в [ISO/IEC 27000], [ISO 28000].

7 Высокоуровневые концепции больших данных как услуги: безопасность и роль BDSP

В [ITU-T Y.3600] определена общая многоуровневая и состоящая из логических функциональных компонентов архитектура технологии больших данных. Возможности обеспечения безопасности услуг больших данных, основанные на этой архитектуре, охватывают как безопасность системы, так и безопасность данных.

В системном аспекте: требования безопасности BDaaS охватывают возможности каждого из соответствующих функциональных модулей: 1) инфраструктуры больших данных; 2) управления приложениями больших данных; 3) безопасности интерфейса; 4) обеспечения и поддержания безопасности платформы больших данных (экосистемы BDaaS).

В частности, в [ITU-T Y.3600] приведено описание BDaaS как состоящей из двух ключевых компонентов:

– BDIP: могут использовать облачные услуги, относящиеся к возможностям облачной инфраструктуры, такие как вычисления как услуга, хранение данных как услуга, инфраструктура как услуга и сеть как услуга, для реализации услуг больших данных, таких как сбор данных, обработка данных и управление данными;

– BDAP: выполняют анализ данных, визуализацию и реализуют другие приложения больших данных.

В аспекте данных: требования безопасности охватывают каждое действие с данными в процессе развития деятельности по предоставлению услуг больших данных. Кроме того, к возможностям безопасности услуг больших данных также относятся требования к безопасности метаданных и безопасности цепочки поставок данных.

Что касается системы BDaaS, в [ITU-T Y.3600] определен контекст системы, включая роли и действия, а также потоки данных и услуг.

Что касается ролей, согласно [ITU-T Y.3600] услуги BDaaS предоставляют BDSP, отвечающие за обеспечение безопасности BDaaS и снижение рисков. Рекомендуется, чтобы при осуществлении деятельности, связанной с BDaaS, BDSP (BDIP и BDAP) учитывали как безопасность системы, так и безопасность данных.

8 Меры безопасности больших данных как услуги

8.1 Меры безопасности для инфраструктуры больших данных

8.1.1 Безопасность системных ресурсов

8.1.1.1 Общие требования

BDSP должны:

– определить стратегии управления безопасностью системных ресурсов, уточнить цели и принципы безопасности системных ресурсов;

– установить политику и процедуры управления созданием и эксплуатацией системных ресурсов, включая планирование, проектирование, снабжение, разработку, эксплуатацию, поддержание и утилизацию;

– создать механизм регистрации системных ресурсов, составить список системных ресурсов, определить область ответственности за безопасность и соответствующих пользователей системных ресурсов и регулярно актуализировать информацию о системных ресурсах;

– создать и внедрить систему классификации и процедуры маркировки системных ресурсов;

– проводить регулярный аудит и обновление информационно-технологических (ИТ) ресурсов и политики управления безопасностью.

8.1.1.2 Дополнительные требования

BDSP следует:

– определить доступные средства контроля за управлением ресурсами, такие как те, что описаны в [ITU-T X.1631], для выполнения инвентаризации и регистрации компонентов, аудита и контроля системных ресурсов;

– установить процедуры оценки рисков для ресурсов системы больших данных, например внедрить процесс идентификации компонентов продуктов или услуг, имеющих решающее значение для поддержания функциональности и, следовательно, требующих повышенного внимания и контроля;

– установить процедуры оценки безопасности цепочки поставок, такие как те, что определены в [ISO/IEC 27036-3] – к ним относятся оценка рисков, связанных с компонентами, которые более недоступны, и систематически повторяющиеся процессы реагирования на уязвимости.

8.1.2 Безопасность информационных ресурсов

8.1.2.1 Общие требования

BDSP должны:

– определить стратегии управления безопасностью информационных ресурсов, уточнить цели и принципы управления безопасностью информационных ресурсов;

– создать механизмы и процедуры управления безопасностью, охватывающие жизненный цикл информационных ресурсов;

– создать методы классификации и ранжирования информационных ресурсов в зависимости от их ценности и значимости, а также руководство по их применению;

– создать механизмы утверждения изменений в стратегиях, процедурах и методах классификации и ранжирования данных, а также в руководствах по их применению;

– разработать спецификации безопасности, механизмы и процедуры управления конфиденциальностью, целостностью и доступностью информационных ресурсов (например, стратегия в отношении паролей, управление ключами);

– составить список информационных ресурсов, определить область ответственности за безопасность данных и соответствующих участников процесса;

– проводить регулярный аудит и обновление стратегий управления безопасностью информационных ресурсов и соответствующих процедур.

8.1.2.2 Дополнительные требования

BDSP следует:

– установить принципы управления безопасностью и политику интеграции данных для всех видов внутренних и внешних информационных ресурсов;

– определить стратегии безопасности, такие как маркировка, многоуровневое управление доступом, шифрование и дешифрование данных, десенсибилизация данных и другие стратегии безопасности, в соответствии с уровнем конфиденциальности информационных ресурсов.

8.1.3 Безопасность процессов в цепочке поставок данных

8.1.3.1 Общие требования

BDSP должны:

– уточнить цели, принципы и сферу охвата системы управления безопасностью цепочки поставок данных;

– разработать политику и процедуры управления безопасностью цепочки поставок данных, включая критерии управления безопасностью для каждого из участников цепочки поставок данных;

– определить цели, схемы поставок и обязанности участников цепочки поставок данных по обеспечению безопасности данных путем заключения соглашений о сотрудничестве;

– регистрировать оборудование и приложения для сбора и распространения данных, осуществлять регистрацию и аудит способов сбора и распространения данных;

– проверять способы потребления данных участниками цепочки поставок данных;

– создать механизм нормализации исходных данных и спецификацию интерфейсов в цепочке поставок данных, регистрировать и проверять важные операции;

– создать организационную структуру эксплуатации и управления цепочкой поставок, основную модель данных цепочки поставок, механизм обработки качества данных и механизм отслеживания данных;

– уточнить обязанности по обеспечению безопасности цепочки поставок данных, гарантировать подлинность и доступность соответствующих информационных услуг;

– обеспечить применение мер безопасности в процессах поставок данных, например при обмене данными и их использовании;

– создать каталоги цепочки поставок данных и словари источников данных, определить ответственного за безопасность процесса поставок данных;

– обеспечить достоверность записей о происхождении данных по всей цепочке распространения;

– четко указать ответственных за обработку информации о происхождении данных;

– внедрить механизмы аутентификации для обеспечения подлинности участников цепочки обработки и обмена информацией о происхождении данных;

– обеспечить подлинность кодов происхождения данных и сохранять ее в обновлениях кода;

– обеспечить конфиденциальность, целостность и доступность информации о происхождении данных, а также соблюдение требований безопасности, описанных в [ITU-T X.1601].

8.1.3.2 Дополнительные требования

BDSP следует:

– определить требования к возможностям обслуживания данных для разных участников цепочки поставок данных в соответствии с их ролями в экосистеме бизнес-цепочки данных;

– регулярно проверять возможности участников цепочки поставок данных по управлению безопасностью данных и оценивать их риски безопасности;

– регулярно оценивать риски безопасности для всего жизненного цикла цепочки поставок данных.

8.1.4 Безопасность метаданных

Следует принять во внимание соответствующие требования к безопасности данных потребителей облачных услуг (CSC), приведенные в [ITU-T X.1641].

8.1.4.1 Общие требования

BDSP должны:

– создать словари данных и соответствующие методы управления согласно архитектуре и набору информационных услуг предприятия, включая предметную область, тип поля, структуру таблицы, а также режимы логического и физического хранения данных;

– создать метаданные безопасности и соответствующие методы управления согласно архитектуре безопасности больших данных, включая политику в отношении паролей, список полномочий и спецификации процессов авторизации;

– определить стратегию управления доступом к метаданным, указать роли метаданных и механизмы контроля авторизации;

– установить процедуры аудита операций с метаданными.

8.1.4.2 Дополнительные требования

BDSP следует:

– построить системы управления метаданными для унифицированного управления метаданными услуг больших данных;

– создать механизм автоматического ранжирования атрибутов безопасности метаданных в соответствии со стратегией классификации и ранжирования ресурсов;

– определить стратегию маркирования, включая привязку данных к владельцу данных, в соответствии с требованиями безопасности метаданных.

8.2 Меры безопасности для приложений больших данных

8.2.1 Приобретение ресурсов платформы

8.2.1.1 Общие требования

BDSP должны:

– обеспечить осведомленность и уведомление пользователей услуг больших данных (BDSU) о системных ресурсах, доступных приложению, таких как сетевое соединение, служба определения местоположения и перечень аппаратных ресурсов типа универсальной последовательной шины (USB) и Bluetooth;

– обеспечить осведомленность и уведомление BDSU о конфиденциальных информационных ресурсах системы, доступных приложению, таких как адресные книги, системные журналы и другие источники конфиденциальной информации;

– гарантировать, что приложение, запрашивающее доступ к ресурсам, имеет достаточную причину для посещения, указанную в документах, предоставленных разработчиком приложения.

8.2.1.2 Дополнительные требования

BDSP следует:

– гарантировать, что приложение ограничивает необязательную внутреннюю и внешнюю связь по сети или связь по сети, инициируемую пользователем, в зависимости от бизнес-требований.

8.2.2 Авторизация и управление доступом

8.2.2.1 Общие требования

BDSP должны:

– создать механизм конкретизации авторизации физического и логического доступа, спецификации и управления таким доступом для приложений больших данных, гарантирующий надлежащую авторизацию доступа к информационным и системным ресурсам, связанным с услугами больших данных;

– установить меры авторизации и управления доступом на основе стратегий управления ресурсами и маркировки ресурсов, а также атрибутов безопасности, чтобы приложение больших данных имело возможность управления детальным контролем доступа;

– разработать стратегию управления информационным потоком для управления операциями инфраструктуры больших данных по импорту данных, их экспорту и обмену ими между различными приложениями больших данных или между приложением больших данных и внешней ИТ-системой;

– внедрить надлежащим образом утвержденный механизм авторизации доступа к данным и системным ресурсам отдельных лиц, групп, ролей, устройств и приложений, связанных с услугами больших данных;

– предоставить пользователям возможность самостоятельно определять стратегию авторизации доступа на основе требований, предъявляемых к услугам, а также получить от каждого пользователя право проверки на основе требований, предъявляемых к услугам, чтобы гарантировать, что его доступ ограничен минимальным диапазоном, соответствующим требованиям сценария услуг.

8.2.2.2 Дополнительные требования

BDSP следует:

– автоматически отслеживать и контролировать сеансы удаленного доступа для обнаружения сетевых атак и обеспечения соблюдения политики удаленного доступа;

– обеспечить механизм управления доступом на основе атрибутов (ABAC) и функции управления авторизацией и управления доступом, ориентированные на объекты данных, а также такие функции, как точка администрирования политики, точка принятия решений в отношении политики, точка применения политики и точка доступа к политике.

8.2.3 Контроль поведения приложений

8.2.3.1 Общие требования

BDSP должны:

– разработать стратегии и процедуры контроля поведения приложений больших данных, охватывающие весь жизненный цикл данных;

– помогать пользователям в настройке правил контроля, способных поддерживать контроль и отчетность по аномальным операциям с критически важными данными;

– иметь возможность для записи, подсчета и анализа информации об аномальном поведении приложения.

8.2.3.2 Дополнительные требования

BDSP следует:

– создать механизмы управления контролем поведения приложений, ориентированные на регуляторные органы и пользователей с особыми требованиями, а также предоставить интерфейс контроля в онлайновом режиме после авторизации;

– создать платформу для регистрации и анализа поведения приложений больших данных и предоставить возможности анализа безопасности, позволяющие идентифицировать поведение пользователей и получать компоненты или интерфейсы протоколов связи услуг больших данных;

– обеспечить системы спецификации контроля поведения и руководства по их эксплуатации.

8.2.4 Стратегии и процедуры безопасности приложений

BDSP должны:

– разработать политику управления выпуском приложений услуг больших данных в рамках письменной процедуры авторизации, а также установить обязанности соответствующих участников процесса; в разрешающем документе должны быть указаны наименование, версия, источник, разработчик, функции, место внедрения, результат оценки безопасности и конкретные требования безопасности в отношении приложения;

– определить защиту передачи данных между приложениями и инфраструктурой больших данных, а также другими аутентичными ИТ-продуктами, например применять схемы безопасности, такие как протокол безопасных соединений (SSL) или безопасность транспортного уровня (TLS), для шифрования конфиденциальных данных при передаче;

– проверять электронные подписи пакетов установки приложений и пакетов обновлений;

– обеспечить возможность запроса приложением текущей версии работающего программного обеспечения либо автономно, либо с использованием соответствующих функций инфраструктуры больших данных;

– гарантировать, что приложение может обрабатывать операции с предсказуемыми ошибками, не влияя на нормальную работу экосистем больших данных;

– разработать политику установки обновлений и исправлений приложений больших данных, гарантирующую, что приложения будут проверять наличие обновлений и устанавливать исправления компонентов;

– следовать спецификациям механизмов безопасности приложений больших данных, избегать записей, нарушающих или обходящих правила безопасности, и записей, не предусмотренных спецификацией;

– разработать механизмы, предотвращающие использование уязвимостей приложения больших данных, например избегать выделения пространства памяти, в котором разрешены как запись, так и выполнение, выделять пространство памяти, в котором разрешены запись и выполнение, только для функций одномоментной компиляции.

8.2.5 Хранение регистрационных данных

8.2.5.1 Общие требования

BDSP должны:

– определить метод постоянного хранения идентификационных регистрационных данных приложения, включая использование функции платформы вместо постоянной памяти для безопасного хранения всех идентификационных регистрационных данных либо реализацию самим приложением функции безопасного хранения идентификационных регистрационных данных;

– уточнить регистрационные данные приложения, такие как ключ, инфраструктура открытых ключей (PKI), секретный ключ или пароль;

– уточнить методы защиты и меры контроля для сбора, хранения и использования информации, позволяющей установить личность (PII);

– определить процесс оценки для метода хранения регистрационных данных приложения, гарантирующий его соответствие стратегиям безопасности и процедурным требованиям систем услуг больших данных.

8.2.5.2 Дополнительные требования

BDSP следует:

– убедиться, что назначение и методы постоянного хранения регистрационных данных указаны в документах спецификации безопасности.

8.2.6 Идентичность и аутентификация

8.2.6.1 Общие требования

BDSP должны:

– предоставить возможность автоматического управления определением идентичности пользователей для выявления идентификационной информации пользователей в приложениях больших данных, гарантирующего установление связей между идентификационной информацией и информацией авторизации пользователей на уровне приложений;

– осуществлять аутентификацию личности пользователя с применением нескольких методов аутентификации для работы с важными данными или важными модулями;

– отображать потенциально полезную открытую информацию об использовании услуг системы больших данных, такую как дата и время последнего входа в систему или последнее место, из которого производился последний вход в систему.

8.2.6.2 Дополнительные требования

BDSP следует:

– осуществлять аутентификацию личности пользователей с применением нескольких методов аутентификации во всех приложениях, где пользователь играет ключевую роль, используя по меньшей мере один метод, основанный на биометрических данных или на цифровом сертификате;

– использовать язык разметки утверждений безопасности (SAML), подобный языкам, применяемым в федерациях идентичностей, для определения идентичности и роли, добавления требований безопасности и конфиденциальности, таким образом поддерживая возможность доступа к услугам больших данных для нескольких идентичностей.

8.2.7 Конфигурация безопасности по умолчанию

BDSP должны:

– гарантировать, что при использовании идентификационных регистрационных данных по умолчанию или в том случае, если идентификационные регистрационные данные не настроены, приложение может предоставить лишь основные функции для настройки новой идентичности; например, при использовании для входа в систему пароля по умолчанию пользователю разрешается лишь войти в интерфейс изменения пароля, и приложение не должно предоставлять ему никаких других функций, пока пароль по умолчанию не будет изменен;

– в режиме установки приложения по умолчанию обеспечить более безопасный функциональный модуль и включить конфигурацию с более высоким уровнем безопасности; например, если приложение может одновременно предоставить модуль входа в систему по паролю и модуль цифрового сертификата, то в режиме установки по умолчанию выбирается установка модуля цифрового сертификата;

– ограничить разрешения на доступ по умолчанию для пользователя приложения по умолчанию; например, препятствовать запуску программы по умолчанию пользователю с минимальными правами доступа;

– гарантировать, что приложение запустит функцию настройки безопасности учетной записи пользователя по умолчанию, включая длину пароля, сложность пароля, ограничение срока действия и стратегию блокировки учетной записи;

– обеспечить запуск необходимых функций контроля событий, например переустановку компонентов или изменение параметров, когда приложение установлено в конфигурации по умолчанию.

8.2.8 Импорт и экспорт данных

8.2.8.1 Общие требования

BDSP должны:

– сформулировать стратегии и процедуры импорта и экспорта данных с учетом таких факторов, как емкость хранилища, темпы роста объема данных, бизнес-требования, носитель для хранения данных и быстродействие хранилища, чтобы избежать потерь важных данных и уменьшить ущерб от потери данных;

– разработать стратегии и механизмы управления экспортом данных, механизмы оценки безопасности при импорте и экспорте данных и процесс утверждения авторизации;

– установить спецификации идентификации носителей экспортируемых данных – идентификация должна соответствовать унифицированным правилам именования и обеспечивать указание номеров носителей, времени экспорта, срока действия и другой важной информации;

– предоставить различные способы обеспечения многоуровневой детализации импорта и экспорта данных, как, например, детализация уровня базы данных, модели или заданных пользователем объектов;

– проводить проверку результатов импорта и экспорта данных, обеспечить целостность и достоверность данных;

– вести регистрацию рабочей информации по импорту и экспорту данных, такой как сведения об операциях, рабочий цикл, среднее число, средний объем, ситуация с передачей и хранением, а также ведение соответствующих записей об изменении;

– внедрить механизмы шифрования, управления доступом и другие технические меры для обеспечения конфиденциальности, целостности и доступности экспортируемых данных;

– регулярно проверять целостность и доступность экспортируемых данных.

8.2.8.2 Дополнительные требования

BDSP следует:

– внедрить платформу расчета индексируемых параметров автоматического управления резервным копированием данных, включая среднюю наработку на отказ, среднее время восстановления и среднее время между отказами, настроить соответствующее программное обеспечение автоматического импорта и экспорта данных;

– обеспечить возможность удаленного импорта и экспорта данных через интернет, регулярно и полуавтоматически выполняя удаленное сохранение пользовательских данных;

– производить автоматическую рекомбинацию и сжатие резервных копий данных в зависимости от популярности данных и т. д., обеспечивая доступность массовых данных;

– поддерживать функцию автоматического сжатия данных для резервного копирования данных пользователя в соответствии с частотой резервного копирования и восстановления данных.

8.3 Меры безопасности интерфейсов

8.3.1 Общие требования

BDSP должны:

– предоставить интерфейсы ролей системного администратора, администратора безопасности, аудитора безопасности и других пользователей и интерфейсы роли регуляторного органа;

– определить требования безопасности и меры контроля безопасности для интерфейса каждой роли, такие как аутентификация идентичности, доступ к авторизации, подпись, отметка времени и протокол безопасности;

– указать ограничения, связанные с безопасностью, для использования каждого класса интерфейсов, такие как удаленные соединения с ограниченными функциями и разрешениями;
– уточнить спецификации безопасности интерфейсов услуг, включая имя интерфейса, параметры интерфейса и требования безопасности интерфейса; эти спецификации содержат ограничения на небезопасные входные параметры и способны обрабатывать исключения;
– обеспечить возможность аудита механизмов доступа к интерфейсу и настраиваемых интерфейсов услуг по предоставлению данных;
– внедрить механизмы безопасности, такие как безопасный канал или шифрованная передача, для защиты междоменных интерфейсов безопасности.

8.3.2 Дополнительные требования

BDSP следует:

– поддерживать требования аудита в процессе доступа к интерфейсам и обеспечивать необходимые функции аудита и регулирования для доступа к интерфейсам;
– внедрить метод шифрованной передачи для передачи по интерфейсу через домены безопасности в системе;
– выполнять необходимый автоматический контроль и обработку при доступе к интерфейсам.

8.4 Меры безопасности для экосистемы больших данных как услуги

8.4.1 Планирование безопасности

Этап планирования безопасности делится на три подэтапа:

– анализ требований – на этом этапе выявляются, уточняются и определяются бизнес-требования и требования безопасности;
– проектирование решений – на этом этапе разрабатываются решения по обеспечению безопасности;
– оценка решений – на этом этапе оцениваются решения безопасности.

По завершении последнего подэтапа BDSP может либо перейти к этапу построения системы безопасности для реализации решений, либо вернуться на подэтап проектирования решений для их корректировки или совершенствования.

8.4.1.1 Анализ требований

8.4.1.1.1 Общие требования

BDSP должны:

– определить объем бизнес-операций услуг больших данных и соответствующие базовые требования безопасности инфраструктуры больших данных;
– определить конкретные угрозы безопасности, уязвимости и риски безопасности, с которыми сталкивается инфраструктура больших данных, а затем уточнить технические и организационные меры для услуг больших данных;
– определить приоритеты реализации требований безопасности для инфраструктуры больших данных.

8.4.1.1.2 Дополнительные требования

BDSP следует:

– организовать анализ требований безопасности и пересмотреть процедуру управления, обеспечив целостность и разумность требований безопасности инфраструктуры больших данных.

8.4.1.2 Проектирование решений

8.4.1.2.1 Общие требования

BDSP должны:

– создать технические спецификации безопасности для инфраструктуры больших данных и четко описать функции, интерфейс и параметры безопасности.

8.4.1.2.2 Дополнительные требования

BDSP следует:

– продемонстрировать эффективность технических спецификаций безопасности и убедиться в том, что в механизме реализации нельзя обойти механизм безопасности;

– своевременно обновлять решения по обеспечению безопасности при изменении требований или совершенствовании технологии до завершения оценки решений.

8.4.1.3 Оценка решений

8.4.1.3.1 Общие требования

BDSP должны:

– регулярно рассматривать предложения по безопасности инфраструктуры больших данных, включая архитектуру и базовые показатели безопасности, при гарантировании соблюдения требований безопасности.

8.4.1.3.2 Дополнительные требования

BDSP следует:

– создать систему оценки безопасности и определить набор ключевых факторов оценки.

8.4.2 Построение системы безопасности

8.4.2.1 Архитектура безопасности

8.4.2.1.1 Общие требования

BDSP должны:

– создать архитектуру безопасности услуг больших данных и обеспечить обоснованность процесса проектирования и реализации служб безопасности больших данных в соответствии с архитектурой безопасности;

– гарантировать, что домен безопасности, описанный в документах архитектуры безопасности, соответствует требованиям приложения больших данных и функциональной архитектуры безопасности;

– гарантировать, что в документах архитектуры безопасности описывается процесс инициализации функций безопасности в приложениях больших данных и в инфраструктуре больших данных, что обеспечивает безопасность инициализации платформы и приложений.

8.4.2.1.2 Дополнительные требования

BDSP следует:

– гарантировать, что в документах, описывающих архитектуру безопасности, достаточно информации, чтобы удостовериться в том, что функция безопасности услуг больших данных способна обеспечить защиту от вмешательства не заслуживающих доверия субъектов;

– гарантировать, что документы, описывающие архитектуру безопасности, обеспечивают достаточный анализ, чтобы доказать, что разработанный механизм функции безопасности услуг больших данных нельзя обойти, а функции безопасности, которыми наделена системы больших данных, реализованы правильно.

8.4.2.2 Функциональная спецификация

8.4.2.2.1 Общие требования

BDSP должны:

– предоставить точные и полные функциональные спецификации и прояснить соответствие между функциональными спецификациями и требованиями к функциям безопасности услуг больших данных;

– гарантировать, что предоставленная функциональная спецификация полностью описывает функции безопасности услуг больших данных и проясняет взаимосвязь между цепочкой поставок данных и компонентами услуг;

– гарантировать, что предоставленная функциональная спецификация описывает цель проекта и метод использования всех прикладных интерфейсов функций безопасности услуг больших данных и предоставляет все соответствующие параметры интерфейсов функции безопасности.

8.4.2.3 Развертывание системы безопасности

8.4.2.3.1 Общие требования

BDSP должны:

– организовать процесс обеспечения безопасности для передачи приложений от разработчиков в систему услуг больших данных;

– описать контролируемые функции и полномочия каждой роли услуг больших данных в процессе развертывания системы безопасности;

– описать доступные функции и интерфейсы для каждой роли услуг больших данных и надлежащим образом указать уровень безопасности, особенно для всех параметров безопасности, контролируемых пользователями;

– описать каждую роль пользователя услуг больших данных и гарантировать, что правила безопасности, описанные в политике и спецификациях безопасности, которые необходимы для обеспечения безопасности операционной среды, реализованы в достаточной степени.

8.4.2.4 Пограничная защита

8.4.2.4.1 Общие требования

BDSP должны:

– планировать домен безопасности и границы системы защиты в соответствии с уровнем безопасности, включая политику контроля безопасности и политику управления;

– планировать домен безопасности и границы системы защиты, связанные с контролем деятельности и изоляцией приложений, включая политику контроля безопасности и политику управления;

– развернуть средства защиты на границах домена безопасности для обнаружения аномальных инцидентов, потенциальных нарушений и т. д., а также защиты от них;

– внедрить сравнительно строгие механизмы защиты между доменами безопасности, например аутентификацию идентичности, управление соединением, политику безопасности при управлении доступом к сети, предотвращение вторжений, фильтрацию информации и проверку целостности границ;

– разработать политику управления обновлением средств защиты и принять необходимые методы для обеспечения реализации этой политики.

8.4.2.4.2 Дополнительные требования

BDSP следует:

– обеспечить персонализированные многопользовательские меры и механизмы пограничной защиты;

– определить домен или субдомен безопасности, механизм изоляции данных между доменами безопасности и механизм управления доступом для авторизованных пользователей или ролей.

8.4.2.5 Управление документами

8.4.2.5.1 Общие требования

BDSP должны:

– реализовать в системе услуг больших данных управление документами, область которого включает организационные стратегии, правила и политику, схемы систем и руководства по внедрению;

– определить процессы создания, проверки, утверждения, публикации и архивного хранения документов, уточнив соответствующие обязанности по обеспечению безопасности в каждом процессе управления документами;

– определить требования к носителям, используемым для хранения документов, и сроку хранения документов, обеспечив их доступность и полноту;

– регулярно пересматривать, обновлять, утверждать и публиковать документы, гарантируя, что пользователям всегда известно о выходе новых версий;

– назначить органы, ответственные за создание и поддержку системы управления документами, и возложить на них ответственность за сопровождение изменения версий документов;

– управлять классификацией системных документов.

8.4.2.5.2 Дополнительные требования

BDSP следует:

– обеспечить платформу для управления документами в рамках системы поставщика услуг, выдавая различные разрешения на просмотр в соответствии с ролями;

– обеспечить необходимое обновление и идентификацию версий соответствующих документов при обновлении продуктов или услуг.

8.4.3 Эксплуатация системы безопасности

8.4.3.1 Управление конфигурацией системы

8.4.3.1.1 Общие требования

BDSP должны:

– сформулировать и выполнять процедуры управления конфигурацией системы, создать организационную структуру управления конфигурацией системы, уточнить роли и обязанности менеджеров по конфигурации, таких как системные администраторы, системные операторы, сотрудники по безопасности, аудиторы, администраторы баз данных и т. д.;

– в соответствии с бизнес-требованиями и объектами управления организовать процессы утверждения, эксплуатации и аудита для управления конфигурацией, например элементы конфигурации хост-систем, элементы конфигурации сети, модули прикладных услуг и другие процессы определения конфигураций системы, конфигураций контента и соответствующие действия по их изменению;

– в соответствии с результатами оценки составить список базовых конфигураций функций безопасности системы больших данных и список содержания ежедневных проверок конфигурации, выполняя необходимую настройку функций безопасности системы больших данных в соответствии с принципом наименьших привилегий;

– в соответствии с соглашением об уровне услуг больших данных выбирать конфигурацию параметров ИТ-продуктов в системе больших данных, регистрировать и поддерживать информацию о текущей конфигурации безопасности системы больших данных;

– в соответствии со стратегиями использования ограничивать стратегии и политику авторизации приобретаемого программного обеспечения, запрещать или ограничивать использование программным обеспечением определенных функций, портов, протоколов или услуг системы больших данных;

– уточнить список контролируемых конфигураций, которые требуют регулярных изменений, и регулярно обновлять важные элементы конфигурации системы больших данных, связанные с информационной безопасностью, такие как база данных вирусов, база данных правил обнаружения вторжений, база данных правил межсетевого экрана и база данных уязвимостей;

– проверять представленные изменения к конфигурациям, управляемым системой больших данных, и утверждать или отклонять их в соответствии с результатами анализа влияния на безопасность и регистрировать решения об изменениях;

– запретить разработчикам системы и интеграторам вносить изменения в систему больших данных, соответствующее оборудование, программное обеспечение и встроенное ПО непосредственно в производственной среде, проводить аудит событий, связанных с конфигурацией и изменениями;

– перед настройкой конфигурации или внесением изменений тестировать, подтверждать и регистрировать контролируемые элементы конфигурации и изменений, а также анализировать элементы системных изменений в целях оценки их потенциального влияния на безопасность услуг больших данных;

– контролировать изменения параметров настройки конфигурации и обоснованно включать функции мониторинга, предупреждения, защиты и другие функции оборудования безопасности;

– обеспечить соответствующие меры реагирования для устранения несанкционированных изменений, охватывающие связанный с изменениями персонал, восстановление установленной конфигурации или прерывание работы затронутой информационной системы в экстремальных ситуациях.

8.4.3.1.2 Дополнительные требования

BDSP следует:

– регулярно или при значительных изменениях в архитектуре предприятия или системы проводить оценку рисков, связанных с управлением конфигурацией, и в соответствии с результатами оценки пересматривать требования к базовой конфигурации и содержание конфигурации, например оценивать риски и пересматривать требования к конфигурации не реже одного раза в год;

– регулярно или при значительных изменениях в архитектуре предприятия или системы оценивать стратегию оценки рисков и ее последствия; по результатам оценки пересмотреть процедуры управления конфигурацией системы, настроить структуру управления организацией, процесс управления конфигурацией и т. д.;

– регулярно проводить обзор конфигураций системы больших данных для выявления ненужных или небезопасных функций, портов, протоколов или элементов конфигурации услуг;

– использовать инструменты конфигурации системы или автоматические механизмы централизованного управления, применения и проверки параметров элементов конфигурации;

– иметь возможность выявлять в режиме реального времени изменения в инфраструктуре больших данных и состоянии виртуальных ресурсов, а также возможность автоматической настройки конфигурации стратегии безопасности услуг системы.

8.4.3.2 Использование сторонних услуг

8.4.3.2.1 Общие требования

BDSP должны:

– разработать политику управления безопасностью для сторонних партнеров по услугам;

– установить механизм допуска, оценки и ранжирования сторонних поставщиков услуг;

– подписать соглашения о сотрудничестве в области компонентов услуг со сторонними поставщиками услуг, уточнить их обязательства и обязанности, например избегать чрезмерного участия сторонних поставщиков услуг в обеспечении безопасности системы больших данных;

– гарантировать, что сторонним поставщикам компонентов услуг понятны меры информационной безопасности системы больших данных и что они правильно реализуют необходимые меры безопасности и проходят проверку сторонних оценочных агентств;

– установить политику безопасности при использовании компонентов услуг сторонних поставщиков услуг, уточнить условия использования и объем доступа со стороны внешних компонентов;

– принять необходимые технические или организационные меры безопасности, чтобы гарантировать, что пользователи больших данных проходят авторизацию и получают доступ к системным и информационным ресурсам через внешние компоненты услуг;

– осуществлять аудит информации, касающейся пользователей, предполагаемых и фактических операций внешних компонентов услуг, и обеспечивать отслеживаемость услуг больших данных.

8.4.3.2.2 Дополнительные требования

BDSP следует:

– осуществлять оценку квалификации и возможностей по обеспечению безопасности сторонних поставщиков услуг и создать механизм совместного реагирования на чрезвычайные ситуации с внешними поставщиками компонентов услуг;

– гарантировать, что внешние поставщики компонентов услуг правильно реализуют необходимые меры безопасности в соответствии со стратегией информационной безопасности и планом безопасности системы больших данных и проходят проверку в сторонних оценочных агентствах;

– ограничить использование конфиденциальных информационных ресурсов во внешних компонентах услуг, включая носители данных, файлы данных и другие информационные ресурсы, контролируемые BDSP, только уполномоченным персоналом.

8.4.3.3 Безопасность цепочки поставок информационных технологий

8.4.3.3.1 Общие требования

BDSP должны:

– разработать политику и процедуры безопасности цепочки поставок ИТ, уточнить механизм фильтрации, коэффициент фильтрации и метод оценки;

– уточнить роли и операции участников цепочки поставок ИТ, связанные с получением данных и услугами системы;

– принять необходимые технические и организационные меры для смены цепочек поставок, обеспечить эффективное реагирование в случае возникновения инцидентов в цепочке поставок.

8.4.3.3.2 Дополнительные требования

BDSP следует:

– создать модель информационной цепочки агрегирования данных, включая извлечение данных, интеграцию и оптимизацию источников данных цепочки поставок;

– установить механизм проверки и оценки цепочки поставок, проводить регулярную оценку рисков и оценку безопасности, например не реже одного раза в год;

– создать механизм управления качеством цепочки поставок данных и обратной связи для его оценки.

8.4.3.4 Управление исправлениями системы

8.4.3.4.1 Общие требования

BDSP должны:

– установить процедуры управления исправлениями, включая загрузку, тестирование, анализ, распространение, установку, архивирование и другие процессы и контент, а также обеспечить стандартизованное управление исправлениями системы;

– создать группу управления исправлениями, следить за информацией о раскрытии уязвимостей и реагировании на события, связанные с безопасностью, выполнять загрузку исправлений, их тестирование, установку и другие задачи в соответствии с графиком;

– создать структуру распространения исправлений системы и управления ими, уточнить механизмы загрузки исправлений и обновления, например процедуры управления исправлениями, инициируемые событиями, связанными с безопасностью системы, или выполняемые через регулярные интервалы времени;

– обеспечить возможность тестирования совместимости исправлений перед их развертыванием и установкой, регистрировать проблемы, возникающие в процессе обновления исправлений;

– обеспечить функцию проверки исправлений, убеждаясь в том, что исправление установлено успешно.

8.4.3.4.2 Дополнительные требования

BDSP следует:

– установить систему управления исправлениями и систему обновления и устанавливать исправления посредством программного обеспечения.

8.4.3.5 План обеспечения непрерывности деятельности

8.4.3.5.1 Общие требования

BDSP должны:

– регулярно оценивать риски, связанные с текущей деятельностью, и информировать пользователей о соответствующих рисках;

– сформулировать и реализовать соответствующий план резервного копирования на случай аварии в соответствии со стратегическими целями предприятия, уточнив уровень возможностей аварийного восстановления системы, предъявляемый к аварийному восстановлению, требования и стратегию восстановления;

– регулярно проводить анализ последствий для деятельности и оценку рисков, организовывать соответствующую учебную подготовку по обеспечению непрерывности деятельности.

8.4.3.5.2 Дополнительные требования

BDSP следует:

– регулярно проводить эксперименты по переключению системы для соответствующей инфраструктуры задействованных услуг больших данных, оптимизировать схемы резервного копирования данных и системных ресурсов в соответствии с фактическими требованиями;

– проводить учения по плану обеспечения непрерывности деятельности для проверки целостности, работоспособности и эффективности этого плана, проверять готовность ресурсов непрерывности деятельности и системы.

8.4.4 Аудит безопасности

BDSP следует проводить регулярный аудит безопасности всей экосистемы BDaaS. Аудит может выполняться внутренней независимой аудиторской группой или сторонними аудиторами (выступающими в качестве партнеров по услугам больших данных (BDSN)). Результаты аудита должны быть соответствующим образом доступны BDSU.

8.4.4.1 Управление стратегией аудита

8.4.4.1.1 Общие требования

BDSP должны:

– сформулировать стратегии и процедуры аудита, охватывающие поведение системы больших данных и действия с данными услуг больших данных, включая цель аудита, объект аудита, операцию аудита, метод аудита, частоту проверок, соответствующие роли и обязанности, обязательства руководства, координацию действий участников цепочки поставок и анализ соответствия;

– сформулировать процесс управления изменениями для стратегий и процедур аудита, подробно записывать статус начала и окончания стратегий и процедур аудита, политику изменения рабочих характеристик, описание изменений и т. д., регулярно рассматривать и обновлять стратегии и процедуры аудита;

– разъяснить привилегии и обязанности пользователей в соответствии со стратегиями и процедурами аудита, установить соответствующую процедуру предоставления привилегий в отношении стратегий и процедур аудита, определения эффективности стратегии аудита и распределения ролей по управлению данными аудита.

8.4.4.1.2 Дополнительные требования

BDSP следует:

– установить процедуры проверки безопасности цепочки поставок и механизмы координации, обеспечить возможность отслеживания событий аудита;

– регулярно проводить проверку и оценку реализации стратегий и процедур аудита;

– назначить независимых аудиторов безопасности системы, которые должны проводить регулярные проверки безопасности услуг больших данных;

– иметь технологии и инструменты анализа соответствия стратегий и процедур аудита на основе данных аудита.

8.4.4.2 Генерирование данных аудита

8.4.4.2.1 Общие требования

BDSP должны:

– сформулировать регламент учета данных аудита, уточнить организационную структуру и формат данных аудита;

– уточнить подвергаемые аудиту события, связанные с действиями системы больших данных, такими как вход пользователей в систему, управление учетными записями, гостевой доступ, изменение стратегии, авторизация привилегированных функций, обновление модулей услуг;

– определить подвергаемые аудиту события, связанные с действиями с данными услуг больших данных, такими как сбор данных, доступ к данным, хранение данных, передача данных, обработка данных, поддержание данных в надлежащем виде и уничтожение данных;

– обеспечить регистрацию данных аудита, включающую по крайней мере время операции, предмет операции, тип операции, объект операции и результаты операции;

– обеспечить возможность проведения детального аудита операций с данными и действий по обслуживанию системы;

– сохранять надежные отметки времени для записи аудита. Степень детализации отметок времени должна соответствовать требованиям аудита;

– обеспечить возможность выбора и проверки подвергаемых аудиту событий;

– регулярно проводить мероприятия по поддержанию в надлежащем виде правил регистрации данных, подвергаемых аудиту событий и записей аудита.

8.4.4.2.2 Дополнительные требования

BDSP следует:

– обеспечить системные интерфейсы для доступа третьей стороны к данным аудита;

– внедрить криптографические технологии для обеспечения невозможности отказа от данных аудита.

8.4.4.3 Защита данных аудита

8.4.4.3.1 Общие требования

BDSP должны:

– обеспечить методы и механизмы управления постоянным безопасным массовым хранением данных аудита;

– обеспечить возможность авторизации доступа к данным аудита, предоставлять полномочия доступа к данным аудита назначенным администраторам аудита;

– внедрить технологии безопасности или меры контроля для обеспечения достоверности данных аудита;

– обеспечивать функцию архивирования данных аудита, поддерживать методы и механизмы автономного хранения зашифрованных данных аудита;

– обеспечить стратегии и методы управления эффективностью хранения данных аудита, сжатия данных и т. д.;

– совершенствовать управление доступом к данным аудита, регистрировать все операции с данными аудита;

– обеспечить возможность десенсибилизации экспортированных данных аудита;

– обеспечить эффективность сохраненных записей аудита, если хранилище данных аудита переполнено, признано недействительным или подверглось атаке.

8.4.4.3.2 Дополнительные требования

BDSP следует:

– обеспечить возможность удаленного резервного копирования и аварийного восстановления;

– быть в состоянии предоставить доказательства подлинности и полноты предоставленных данных аудита.

8.4.4.4 Аналитический отчет по аудиту

8.4.4.4.1 Общие требования

BDSP должны:

– сформулировать стратегии аудита, анализа и представления отчетности и процедуры, касающиеся записей аудита;

– регулярно проверять и анализировать записи аудита, составлять аналитический отчет по аудиту;

– рассылать аналитический отчет определенным ответственным сотрудникам в организации, а если во время аудита обнаружена какая-либо серьезная угроза безопасности или несанкционированное поведение, как можно скорее сообщать об этом руководителям организации.

8.4.4.4.2 Дополнительные требования

BDSP следует:

– отслеживать и анализировать в режиме реального времени события, подлежащие аудиту, поддерживать мониторинг и реагирование на подозрительные действия;

– обеспечить возможность корреляционного анализа записей аудита из разных источников.

Библиография

[b-ITU-T M.3030] Recommendation ITU-T M.3030 (2002), *Telecommunications markup language (tML) framework.*

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

[b-ITU-T Y.3602] Recommendation ITU-T Y.3602 (2018), *Big data – Functional requirements for data provenance.*

[b-NIST SP 800-30] Special Publication NIST SP 800-30 (2012), *Guide for conducting risk assessments.*

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, 2021 г.