Международный союз электросвязи

МСЭ-Т X.1751

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2020)

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

Безопасность данных – Безопасность больших данных

Руководящие указания по обеспечению безопасности при управлении жизненным циклом больших данных операторами электросвязи

Рекомендация МСЭ-Т X.1751

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (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.1379
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного 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.1751

Руководящие указания по обеспечению безопасности при управлении жизненным циклом больших данных операторами электросвязи

Резюме

В Рекомендации МСЭ-Т X.1751 содержится анализ уязвимостей безопасности и представлены руководящие указания по обеспечению безопасности при управлении жизненным циклом больших данных операторами электросвязи.

В результате стремительного развития технологий больших данных ценность данных существенно возросла. Большие данные открывают новые возможности для услуг электросвязи. Ранее данные были разрозненными и в разных системах услуг электросвязи управлялись независимо. При создании услуг на основе больших данных неизбежны тенденции к агрегированию и слиянию данных. В процессе слияния данных в рамках конвергенции потоки данных направляются на платформы и в процессы предоставления услуг. На разных этапах жизненного цикла данных возникают различные уязвимости их безопасности.

В Рекомендации МСЭ-Т X.1751 представлены конкретные характеристики услуг электросвязи на основе больших данных и категории данных, анализируются уязвимости безопасности при управлении жизненным циклом больших данных и содержатся руководящие указания по обеспечению безопасности для операторов электросвязи.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1751	03.09.2020 год	17-я	11.1002/1000/14267

Ключевые слова

Услуги электросвязи на основе больших данных, управление жизненным циклом данных.

* 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.1751

Руководящие указания по обеспечению безопасности при управлении жизненным циклом больших данных операторами электросвязи

1 Сфера применения

В настоящей Рекомендации содержится описание уязвимостей безопасности и устанавливаются руководящие принципы управления жизненным циклом данных для услуг электросвязи на основе больших данных. В настоящей Рекомендации:

– приведены характеристики услуг электросвязи на основе больших данных и категории данных;

– содержится анализ уязвимостей безопасности при управлении жизненным циклом данных для услуг электросвязи на основе больших данных;

– представлены руководящие указания по обеспечению безопасности при управлении жизненным циклом данных для услуг электросвязи на основе больших данных.

Операторы электросвязи могут предоставлять услуги на основе больших данных только при условии получения явного согласия абонентов. Кроме того, операторам электросвязи рекомендуется принимать необходимые меры для защиты данных на всех этапах процесса предоставления услуг на основе больших данных.

Механизмы защиты различных категорий данных не входят в сферу применения настоящей Рекомендации.

2 Справочные документы

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

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

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.

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 Ассоциируемость (linkability) [b-ISO/IEC 20889] – свойство набора данных, дающее возможность ассоциировать (при помощи соединения) запись, относящуюся к субъекту данных, с записью, относящейся к тому же субъекту данных в отдельном наборе данных.

3.1.4 Псевдонимизация (pseudonymization) [b-ISO/IEC 29100] – процесс, применяемый к информации, позволяющей установить личность (PII), в результате которого идентификационная информация заменяется псевдонимом.

3.1.5 Стратегия безопасности (security policy) [b-ITU-T X.800] – набор критериев для предоставления услуг безопасности.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяется следующий термин.

3.2.1 Жизненный цикл данных (data lifecycle) – весь жизненный процесс данных после их создания, включая сбор данных, их передачу, хранение, использование (в том числе анализ и визуализацию), обмен данными и их уничтожение.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

2B	to Business		Для предприятия
2C	to Consumer		Для потребителя
API	Application Programming Interface		Интерфейс прикладного программирования
APP	Application		Применение, приложение
BDaaS	Big Data as a Service		Большие данные как услуга
BSS/OSS	Business Support System and Operation Support System		Система поддержки деятельности предприятия/операций
DB	Database	БД	База данных
FTP	File Transfer Protocol		Протокол передачи файлов
HDFS	Hadoop Distributed File System		Распределенная файловая система Hadoop
IoT	Internet of Things		Интернет вещей
IP	Internet Protocol		Протокол Интернет
JDBC	Java Database Connectivity		Интерфейс взаимодействия Java и баз данных
LBS	Location-Based Service		Услуги, предоставляемые с учетом местоположения пользователя
LDAP	Lightweight Directory Access Protocol		Облегченный протокол доступа к каталогам
MPP	Massive Parallel Processor		Массовый параллельный процессор
OSS	Operation Support System		Система поддержки операций
PII	Personally Identifiable Information		Информация, позволяющая установить личность
REST	Representational State Transfer		Передача репрезентативного состояния

5 Соглашения

В настоящей Рекомендации:

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

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

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

фраза "**может факультативно**" означает необязательное допустимое требование, не имеющее рекомендательного значения. Данный термин не подразумевает, что вариант реализации поставщика должен обеспечивать выполнение этой функции, и функция может быть активирована дополнительно по желанию оператора сети или поставщика услуг. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии настоящей Рекомендации.

6 Обзор

В результате быстрого развития технологий больших данных ценность таких данных существенно возросла. Большие данные открывают новые возможности для операторов электросвязи, которые в течение длительного времени накапливали в так называемых хранилищах данных разнообразные информационные ресурсы, такие как сведения о телефонных вызовах, данные о местонахождении абонентов, персональные данные, данные о пользователях услуг подвижной связи и терминалах. Пользуясь возможностями быстрого создания больших данных, операторы электросвязи постоянно внедряют инновации и вкладывают средства в развитие услуг на основе больших данных.

В услугах электросвязи на основе больших данных задействованы объемы информации, измеряемые терабайтами или даже петабайтами. При этом генерируются данные разного типа – структурированные, полуструктурированные и неструктурированные. В качестве источников используются персональные данные, такие как PII и данные журналов доступа. Такие данные могут быть объектом атак для злоумышленников.

Раньше данные были разрозненными и в разных системах услуг электросвязи управлялись независимо. К тому же эти системы могут быть расположены в разных местах и управляться разными ведомствами. С развитием услуг на основе больших данных операторы электросвязи ломают ведомственные барьеры и собирают данные из разнообразных независимых систем. Конвергенция данных значительно повышает ценность услуг на основе больших данных.

В процессе предоставления услуг на основе больших данных данные проходят через платформу больших данных и разные этапы жизненного цикла, на каждом из которых информация подвергается различным угрозам и рискам в плане безопасности. Например, неправомерный сбор данных может привести к ненадлежащему раскрытию данных. Несанкционированный доступ возможен на этапе хранения данных. Использование конфиденциальной информации может создать риск утечки данных при обмене информацией. Поэтому необходимо провести анализ уязвимостей безопасности и составить руководство по обеспечению безопасности при управлении жизненным циклом для услуг электросвязи на основе больших данных.

В настоящей Рекомендации содержится анализ рисков безопасности и приводятся руководящие указания по обеспечению безопасности при управлении жизненным циклом больших данных в сфере электросвязи.

7 Характеристики услуг электросвязи на основе больших данных и категории данных

7.1 Характеристики услуг электросвязи на основе больших данных

Все больше операторов электросвязи принимают услуги на основе больших данных в качестве важного стратегического направления для внедрения инноваций и развития своих компаний. Например, операторы электросвязи могут развивать услуги на основе больших данных, создавая платформы для работы с большими данными или организуя специализированные рабочие группы.

Операторы электросвязи могут собирать широкий спектр данных об абонентах, относящихся к индивидуальным пользователям, таких как профили пользователей, устройства, частота использования и местоположение. Операторы могут использовать аналитические методы сбора больших данных для разработки услуг, связанных с широким кругом применений, таких как розничная торговля, здравоохранение и "умные" города. Операторы электросвязи могут использовать эти услуги для расширения собственной деятельности или продавать их сторонним поставщикам услуг в других секторах.

Однако разнообразие и типы данных, которые операторы электросвязи используют для этих услуг на основе больших данных, позволяют раскрыть массу подробностей о частных лицах, в том числе PII, конфиденциальные сведения, такие как религиозные убеждения или политические пристрастия, и коммерческую тайну. Этот аспект приобретает особое значение, если операторы электросвязи решают передать такие данные третьим сторонам. Поэтому необходимо, чтобы операторы электросвязи признавали угрозы, возникающие в течение жизненного цикла информации их услуг на основе больших данных, и принимали надлежащие меры безопасности для защиты пользователей.

7.2 Категории данных

Ниже перечислены четыре основные категории пользовательских данных, находящихся в распоряжении операторов электросвязи. Кроме того, с развитием интернета вещей (IoT) и соответствующих услуг глубина и обширность данных еще больше увеличиваются. Это увеличение приводит к новым рискам для доверия и безопасности пользователя, которые операторам связи необходимо устранить в отношении:

1) данных, полученных из системы поддержки деятельности/операций (BSS/OSS) оператора электросвязи, которые охватывают идентификаторы пользователей, продолжительность вызовов, адресатов вызовов, счета за услуги связи, типы услуг и даже типы терминалов;
2) данных, полученных из системы поддержки операций (OSS), которые в основном представляют собой данные о поведении пользователей, в том числе собираемые из мобильного интернета, чатов, игр и веб-серфинга;
3) данных, основанных на информации об услугах, предоставляемых с учетом местоположения пользователя (LBS), которые, в отличие от данных категорий 1 и 2, тесно связаны с фактическим местоположением пользователя и могут применяться для бизнес-маркетинга, определения мобильности населения, обеспечения общественной безопасности и городского планирования;
4) данных для предприятий (2B) и/или для потребителей (2C), генерированные в сценарии IoT, которые состоят из больших данных, относящихся к вещам и к людям, – эти данные имеют большое значение для отраслей здравоохранения, носимых устройств и "умного" дома.

Большие данные, относящиеся к вещам, включают показания счетчиков воды и электроэнергии и газовых счетчиков, данные о климате и загрязнении окружающей среды, собранные с помощью датчиков, и данные отслеживания перемещения грузов.

Большие данные, относящиеся к людям, включают сведения о здоровье, личных финансах и истории покупок.

Следует отметить, что ассоциируемость определенных данных в соответствии с изначальной классификацией этих данных может приводить к более серьезным последствиям для пользователей, чем ожидалось; например, даже анонимизированные данные категории 4, если они анализируются в сочетании с другими данными, могут позволить установить личность как данные PII категории 1. Поэтому при определении способа защиты данных рекомендуется рассматривать ассоциируемость

в качестве ключевого фактора даже в тех случаях, когда данные сразу не классифицируются как PII или другие персональные данные.

В настоящей Рекомендации предлагается защищать данные этих четырех категорий на всех этапах их жизненного цикла в соответствии с руководящими указаниями по обеспечению безопасности.

8 Жизненный цикл данных услуг электросвязи на основе больших данных

Жизненный цикл данных услуг электросвязи на основе больших данных состоит из шести основных этапов: сбор данных, передача данных, хранение данных, использование данных, обмен данными, уничтожение данных. Этап передачи данных может включать в себя несколько подэтапов.

Жизненный цикл данных услуг электросвязи на основе больших данных иллюстрируется на рисунке 1.

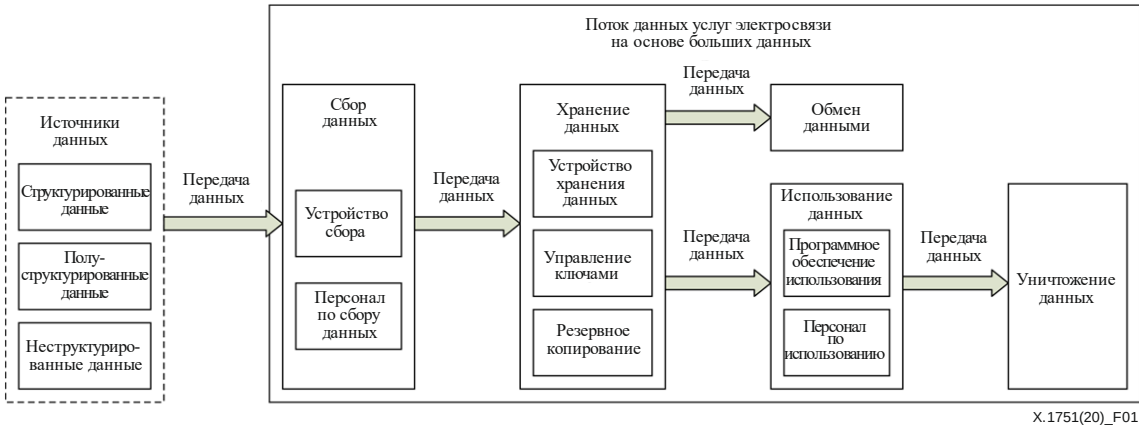

Рисунок 1 – Жизненный цикл данных услуг электросвязи на основе больших данных

Началом жизненного цикла данных услуг электросвязи на основе больших данных является сбор данных, а окончанием – уничтожение данных. Собранные данные могут передаваться, храниться, использоваться и может производиться обмен ими. Передача данных может происходить между различными этапами, например после сбора данные могут передаваться в специализированные устройства хранения (запоминающие устройства); во время использования данные могут передаваться из запоминающих устройств в программное обеспечение или в объект использования; после использования требуется уничтожение данных с истекшим сроком действия или бесполезных данных.

Сбор данных – с помощью специализированных устройств или объектов сбора данные различных типов и категорий собираются для хранения в специальный или временный каталог.

Передача данных – этот процесс включает в себя передачу данных из устройства сбора данных в устройство хранения, и из устройства хранения данные передаются для использования и обмена. Иногда этап уничтожения данных также бывает связан с передачей данных.

Хранение данных – данные хранятся в специальных устройствах, например в базах данных (БД), распределенных файловых системах и дисковых массивах. Для важных данных также требуются шифрование и резервное копирование.

Использование данных – программы и приложения для анализа данных считывают и обрабатывают данные для предоставления различных услуг на основе больших данных. В этом процессе могут быть задействованы разнообразные конфиденциальные персональные данные.

Обмен данными – поставщик услуг или владелец данных предоставляет свои результаты обработки и анализа данных или даже исходные данные другим поставщикам или третьим сторонам.

Уничтожение данных – данные с истекшим сроком действия, особенно в устройствах, в которых хранится важная или конфиденциальная информация, должны полностью уничтожаться с помощью специального механизма обеспечения безопасности.

9 Уязвимости безопасности в течение жизненного цикла данных услуг электросвязи на основе больших данных

На каждом этапе процесса предоставления услуг электросвязи на основе больших данных происходит движение данных. Уязвимости безопасности могут возникать как внутри, так и вне этого процесса. Внутренние уязвимости безопасности связаны с устройствами и системами, такими как устройства сбора данных, устройства хранения и устройства для использования данных. Внешние уязвимости возникают из-за неправильной конфигурации или неправильного использования. Уязвимости для безопасности, связанные с данными, описаны в [b-ITU-T X.1040].

9.1 Этап сбора данных

9.1.1 Уязвимости безопасности, связанные с устройствами и системами

Уязвимые или зараженные вирусами или троянами устройства и системы создают проблемы для безопасности.

9.1.2 Уязвимости безопасности, связанные с неправильной конфигурацией и управлением

1) Управление персоналом

Устройства сбора данных могут неправильно эксплуатироваться или использоваться без разрешения, что создает риск утечки данных.

2) Управление устройствами

Злонамеренная или ошибочная конфигурация устройств сбора данных может привести к несанкционированному сбору и утечке данных.

Данные собираются из различных бизнес-систем, расположенных в разных местах и управляемых разными ведомствами. Вредоносный узел может получить доступ к кластеру устройств и выполнять несанкционированные операции сбора данных.

3) Управление данными

Данные, не относящиеся к заявленной цели использования, являются лишними, и это может привести к утечке данных.

На этапе сбора область временного хранения данных, такая как произвольный каталог на FTP-сервере, не контролируется персоналом по сбору данных и увеличивает риск раскрытия или несанкционированного изменения данных.

9.2 Этап передачи данных

9.2.1 Уязвимости безопасности, связанные с неправильной конфигурацией и управлением

1) Управление персоналом

Администратор без разрешения изменяет порт передачи или конфигурацию передачи, что может привести к утечке данных.

2) Управление устройствами

Собранные данные передаются по незащищенному каналу, что делает их уязвимыми к прослушиванию или изменению.

Интерфейс передачи не аутентифицирован, поэтому происходит неправильное или злонамеренное соединение.

Механизм передачи между различными узлами не обеспечивает защиту конфиденциальности и целостности данных, что приводит к утечкам данных и увеличивает риск изменения, прослушивания и перехвата.

3) Управление данными

Отсутствие защиты конфиденциальности во время передачи данных может привести к перехвату или утечке данных.

Отсутствие защиты целостности во время передачи данных может привести к злонамеренным манипуляциям с данными или их повреждению.

Отсутствие защиты доступности данных во время передачи может привести к перехвату или умышленному изменению данных.

9.3 Этап хранения данных

9.3.1 Уязвимости безопасности, связанные с устройствами и системами

Отсутствие антивирусного программного обеспечения или устаревшее ПО безопасности ведет к раскрытию и искажению конфиденциальных данных.

Неправильно сконфигурированное или необслуживаемое программное обеспечение безопасности оставляет данные незащищенными, что может привести к раскрытию наборов данных, их искажению и уязвимости к состязательным атакам.

9.3.2 Уязвимости безопасности, связанные с неправильной конфигурацией и управлением

1) Управление персоналом

Средства контроля доступа неправильно конфигурированы, так что хранящиеся данные подвергаются риску несанкционированного доступа или изменения. Лица, которым разрешен доступ к определенным хранящимся наборам данных, могут определить PII или другие персональные данные, на доступ к которым у них нет разрешения, благодаря ассоциируемости.

2) Управление устройствами

В среде хранения данных имеются реляционная БД, распределенная файловая система Hadoop (HDFS) и хранилище данных с массовым параллельным процессором (MPP). Неудовлетворительное управление разрешениями приводит к несанкционированному доступу и разглашению данных.

Многие неструктурированные данные хранятся в разных узлах по отдельности, что затрудняет применение единой стратегии безопасности. Несовместимые стратегии безопасности или их конфликты могут привести к незащищенности и утечке данных.

3) Управление данными

Сохраненные данные не зашифрованы, полностью или частично, что повышает уязвимость пользователей в случае пассивного или активного нарушения защиты данных.

Сохраненные данные зашифрованы; однако уязвимости, связанные с алгоритмом шифрования или управлением ключами, повышают риск несанкционированного доступа к сохраненным данным или их изменения.

Во время хранения данных отсутствует активная защита их целостности, что чревато несанкционированным изменением данных даже после их сбора.

Среди сохраненных данных есть устаревшие данные или данные, не имеющие прямого отношения заявленной цели использования и не требующиеся для этой цели. По мере увеличения количества сохраненных данных повышается уязвимость пользователей в случае любого пассивного или активного нарушения защиты данных.

Неполные механизмы резервного копирования и восстановления данных могут привести к недоступности данных.

9.4 Этап использования данных

9.4.1 Уязвимости безопасности, связанные с устройствами и системами

В программном обеспечении для анализа данных, работающем в сети или в облаке, имеются уязвимости, подвергающие риску данные, с которыми работает это ПО.

В программе визуализации ПО анализа данных имеются проблемы безопасности, которые могут использоваться злоумышленниками.

9.4.2 Уязвимости безопасности, связанные с неправильной конфигурацией и управлением

1) Управление персоналом

При отсутствии возможностей аутентификации и авторизации пользователей или программ визуализации визуальные данные могут попасть к фиктивному пользователю или в фальсифицированную программу визуализации, что приведет к утечке данных.

2) Управление устройствами

Отсутствие механизма аутентификации личности для устройств использования данных приводит к возможности подключения к платформе больших данных неавторизованных устройств. Как следствие, происходит утечка данных или неготовность системы для обслуживания предприятия.

3) Управление данными

При использовании программами визуализации персональные данные, включая любые PII и конфиденциальные данные, не анонимизированы и не замаскированы должным образом, что повышает вероятность их распознавания.

Визуализированные данные имеют высокую степень ассоциируемости, что повышает вероятность установления личности или других персональных данных.

Выходные данные, полученные в результате анализа, не хранятся в защищенной среде или сохраняются выходные данные, которые устарели, не имеют прямого отношения к цели использования или не требуются для этой цели. По мере увеличения объема сохраненных данных повышается уязвимость пользователя в случае любого пассивного или активного нарушения защиты данных.

Журналы регистрации данных, создаваемые на этом этапе, хранятся ненадежно, что может использоваться для определения персональных данных в случае взлома.

9.5 Этап обмена данными

9.5.1 Уязвимости безопасности, связанные с устройствами и системами

Уязвимые или зараженные вирусами или троянами устройства и системы обмена данными создают проблемы для безопасности.

9.5.2 Уязвимости безопасности, связанные с неправильной конфигурацией и управлением

1) Управление персоналом

Ответственность за безопасность и возможности пользователей по обмену данными не определены должным образом, что ведет к ненадлежащей защите и утечке данных.

2) Управление устройствами

Нечетко определены объем и границы обмена данными; кроме того, отсутствуют меры контроля безопасности, что ведет к непосредственному раскрытию конфиденциальных данных партнерам.

Канал обмена данными не защищен, что ведет к раскрытию или подлогу важных данных.

3) Управление данными

Неполные записи в журнале обмена данными затрудняют определение причин инцидентов безопасности.

9.6 Этап уничтожения данных

Если на этом этапе данные не были полностью уничтожены, злонамеренный персонал может восстановить конфиденциальные данные, что приведет к утечке данных.

9.7 Взаимосвязь между уязвимостью безопасности и жизненным циклом данных

Уязвимости безопасности возникают на разных этапах жизненного цикла данных услуг на основе больших данных. В таблице 1 приведен обзор взаимосвязей между уязвимостями безопасности и жизненным циклом данных услуг на основе больших данных.

"Да" в ячейке таблицы 1 указывает на то, что на этом этапе существует уязвимость безопасности.

Таблица 1 – Взаимосвязь между уязвимостями безопасности и разными этапами жизненного цикла данных

Уязвимость		Этап жизненного цикла					
		Сбор данных	**Передача данных**	**Хранение данных**	**Использование данных**	**Обмен данными**	**Уничтожение данных**
Уязвимость устройств		Да		Да	Да	Да	
Уязвимость конфигурации и управления	Управление персоналом	Да	Да	Да	Да	Да	
	Управление устройствами	Да	Да	Да	Да	Да	
	Управление данными	Да	Да	Да	Да	Да	Да

10 Руководящие указания по обеспечению безопасности при управлении жизненным циклом данных для услуг электросвязи на основе больших данных

В настоящей Рекомендации подробно описаны механизмы, подходящие для всех категорий данных, определенных в пункте 7.2.

10.1 Этап сбора данных

10.1.1 Руководящие указания по безопасности устройств и систем

Требуется, чтобы программное обеспечение устройств и систем, используемых для сбора данных, своевременно обновлялось и не имело известных уязвимостей.

На устройствах и системах, используемых для сбора данных, должно быть установлено программное обеспечение безопасности, такое как антивирусное ПО и защита от вредоносных программ, совместимое с операционной системой устройства.

10.1.2 Руководящие указания по безопасности конфигурации и управления

1) Управление персоналом

Рекомендуется информировать пользователей о том, какие данные собираются и зачем, а также до начала сбора получить явное согласие пользователей.

Необходимы аутентификация и авторизация персонала, участвующего в процессе сбора данных.

2) Управление устройствами

Рекомендуется указывать механизмы обеспечения безопасности и контрмеры, используемые при сборе данных, например, для строгой аутентификации и авторизации устройств сбора данных. Рекомендуется, чтобы категория данных соответствовала принципам сбора данных.

Услуги на основе больших данных должны быть настроены на достижение намеченной цели. Должны быть определены данные, строго релевантные и необходимые для использования по назначению.

Должны быть указаны устройства, каналы, процессы и методы сбора данных, а также форматы данных.

Требуется обязательная аутентификация доступа для устройств и персонала по сбору данных; необходимо обеспечить обнаружение нештатного поведения и предупредительную сигнализацию при сборе данных.

Место временного хранения данных должно быть строго ограничено, например должен быть запрет на несанкционированный экспорт данных из подобных областей на другие ресурсы хранения, и рекомендуется обеспечить санкционирование изменения области хранения.

Рекомендуется обеспечить защиту передачи собранных данных, включая метаданные, с использованием алгоритмов шифрования, широко используемых и проверенных доверенными третьими сторонами.

Рекомендуется безопасно управлять ключами шифрования и хранить их и по возможности отдавать предпочтение криптографическим протоколам, обеспечивающим прямую секретность.

3) Управление данными

Рекомендуется определить различные категории собранных данных в соответствии с их важностью и степенью конфиденциальности.

Запись в журнале событий и предупреждение о нештатном поведении требуются в случаях, когда:

– число повторов операций сбора и передачи данных превышает установленный порог;

– в процессе сбора данных передача прерывается;

– превышен установленный порог емкости хранилища данных.

10.2 Этап передачи данных

10.2.1 Руководящие указания по безопасности конфигурации и управления

1) Управление персоналом

Необходимо запретить администраторам произвольно изменять параметры портов передачи или конфигурацию интерфейса.

2) Управление устройствами

Требуется, чтобы передача данных осуществлялась по каналу со сквозным шифрованием.

Транспортный интерфейс обеспечивает возможности аутентификации для предотвращения злонамеренных соединений.

3) Управление данными

Рекомендуется обеспечение защиты конфиденциальности и целостности данных на этапе передачи данных.

Рекомендуется незамедлительное выявление нарушения целостности данных в процессе передачи и принятие необходимых мер для ее восстановления после обнаружения ошибок.

10.3 Этап хранения данных

10.3.1 Руководящие указания по безопасности устройств и систем

Требуется, чтобы программное обеспечение устройств и систем хранения данных своевременно обновлялось и не имело известных уязвимостей.

На запоминающее устройство должно быть установлено современное программное обеспечение безопасности.

10.3.2 Руководящие указания по безопасности конфигурации и управления

1) Управление персоналом

Требуется внедрение мер контроля доступа пользователей или приложений, таких как протокол сетевой аутентификации с секретным ключом Kerberos и детальная авторизация.

Рекомендуется выполнение операции с важными данными в режиме коллективного контроля так, чтобы ни один человек не мог иметь всех прав доступа к операциям с важными данными, такими как их пакетный вывод, копирование, уничтожение, публикация и использование.

2) Управление устройствами

Методы авторизации должны предоставлять доступ только лицам, которые необходимы для достижения заявленной цели сбора данных. Должен быть установлен режим разрешений, предотвращающий доступ отдельных лиц к большему количеству данных, чем это абсолютно

необходимо для выполнения ими своих конкретных обязанностей, и учитывающий потенциальную возможность определения персональных данных, вытекающую из ассоциируемости между любыми сохраненными наборами данных и отдельными разрешениями между сотрудниками.

3) Управление данными

a) Минимизация данных

Рекомендуется ограничение хранения данных, включая выходные данные процессов, выполняемых на этапе использования данных, оставив только релевантные и необходимые для достижения заявленной цели данные.

Для всех данных рекомендуется установить четкие максимальные сроки хранения, исходя из минимально возможного времени хранения данных для достижения заявленной цели.

b) Хранение данных в зашифрованном виде

Для обеспечения конфиденциальности важных данных их необходимо хранить в зашифрованном виде. Рекомендуется поддержка иерархической модели шифрования данных; в зависимости от уровня секретности данных используются разные механизмы безопасного хранения.

Рекомендуется использование широко применяемых алгоритмов шифрования, проверенных доверенными третьими сторонами. Рекомендуется безопасно управлять ключами шифрования и хранить их и по возможности отдавать предпочтение криптографическим протоколам, обеспечивающим прямую секретность.

c) Защита целостности данных

Рекомендуется обеспечение механизма определения целостности для выявления повреждения и потери данных в процессе хранения.

Рекомендуется принятие необходимых мер для восстановления целостности данных после обнаружения ошибок [ITU-T X.1641].

Необходимо вести контрольные журналы, в которых документируются любые изменения в хранимых данных. Эти журналы должны надежно храниться, и рекомендуется обнаруживать и регистрировать попытки внести в них изменения.

d) Резервное копирование и восстановление данных

Рекомендуется обеспечение механизмов полного резервного копирования и восстановления данных, чтобы гарантировать пригодность к использованию и целостность данных.

10.4 Этап использования данных

10.4.1 Руководящие указания по безопасности устройств и систем

Рекомендуется, чтобы программное обеспечение устройств и систем своевременно обновлялось и не имело известных уязвимостей.

Рекомендуется устанавливать на устройства и системы современное программное обеспечение безопасности.

10.4.2 Руководящие указания по безопасности конфигурации и управления

1) Управление персоналом

Рекомендуется обеспечение унифицированной аутентификации в разных приложениях (использования данных) для доступа к платформам больших данных, независимо от используемых этими приложениями интерфейсов, таких как интерфейс прикладного программирования для передачи репрезентативного состояния ресурсов (API REST) или интерфейс взаимодействия Java и баз данных (JDBC). Механизмами детальной аутентификации могут служить протокол Kerberos, облегченный протокол доступа к каталогам (LDAP) и др.

Рекомендуется обеспечение механизма детальной авторизации, который будет использоваться различными приложениями для доступа к платформам больших данных, с применением следующих методов:

a) авторизация с высоким уровнем детализации для доступа к платформам больших данных по имени пользователя, адресу Интернет-протокола (IP) и имени приложения (APP);

b) авторизация с высоким уровнем детализации для доступа к ресурсам хранения, таким как программное обеспечение хранилища данных, Hive, нереляционная распределенная база данных с открытым исходным кодом, Hbase, HDFS и БД;

c) авторизация с высоким уровнем детализации по разным операциям базы данных или файловой системы (например, SELECT, INSERT, CREATE);

d) авторизация с высоким уровнем детализации для разрешений на импорт и экспорт данных;

e) авторизация с высоким уровнем детализации для доступа к файлам и каталогам HDFS.

2) Управление устройствами

На этапе использования данных рекомендуется обеспечение механизмов контроля и пресечения вредоносных действий.

Рекомендуется проведение аудиторских проверок безопасности для проверки адекватности использования данных, гарантии соблюдения установленной стратегии безопасности и рабочих процедур, оказания помощи в оценке ущерба и предложения изменений в средствах контроля безопасности, стратегии безопасности и процедурах использования данных.

В стратегии аудиторских проверок безопасности рекомендуется учитывать, какая именно информация об использовании данных должна регистрироваться и при каких условиях, так же как синтаксическая и семантическая спецификация, которая должна использоваться для обмена информацией по аудиту безопасности.

3) Управление данными

Для защиты конфиденциальных данных необходима псевдонимизация данных на этапе их использования. Подробные рекомендации по псевдонимизации данных обобщаются и рассматриваются в пункте, посвященном последующему этапу обмена данными.

Рекомендуется проверка использования конфиденциальных данных с применением журналов аудиторских проверок [ITU-T X.1641].

10.5 Этап обмена данными

10.5.1 Руководящие указания по безопасности устройств и систем

Рекомендуется, чтобы программное обеспечение пользовательских устройств и систем своевременно обновлялось и не имело известных уязвимостей.

Рекомендуется устанавливать на устройства и системы современное программное обеспечение безопасности.

10.5.2 Руководящие указания по безопасности конфигурации и управления

1) Управление персоналом

Пользователи должны быть проинформированы о том, какие данные, включая метаданные и любые данные, получаемые в результате выполняемых на этапе использования данных процессов, будут переданы третьим сторонам и кто эти третьи стороны. Прежде чем передавать какие-либо данные, в том числе выходные данные, необходимо получить явное согласие пользователей.

2) Управление устройствами

Рекомендуется контроль поведения системы экспорта данных.

Когда данные передаются во внешние службы, рекомендуется ограничение их использования во избежание перепродажи.

Рекомендуется, чтобы механизмы обеспечения безопасности были согласованы между соответствующими заинтересованными сторонами (например, операторами, которые обмениваются данными) и включали в себя стратегию безопасности в отношении передачи предоставляемых данных, их хранения, доступа к ним и их уничтожения, а также схему резервного копирования в случае раскрытия этих данных.

3) Управление данными

Псевдонимизация данных – это процесс сокрытия исходных PII и конфиденциальных данных с помощью символов или данных. Целью является защита PII и конфиденциальных данных.

В разных приложениях могут быть настроены разные алгоритмы псевдонимизации. Рекомендуется, чтобы система псевдонимизации данных:

a) поддерживала динамическое добавление и удаление алгоритмов псевдонимизации;

b) поддерживала высокий уровень детализации, то есть чтобы администратор мог настроить ее на конкретную таблицу или столбцы БД;

c) использовала общедоступные алгоритмы, избегая сторонних проприетарных алгоритмов;

d) не оказывала существенного влияния на непрерывность деятельности и рабочие характеристики системы.

10.6 Этап уничтожения данных

10.6.1 Руководящие указания по обеспечению безопасности при управлении данными

Данные на постоянных носителях должны стираться и перезаписываться.

После удаления данных рекомендуется, чтобы пространство для хранения ресурсов в системе, например файлы, каталоги и записи БД, было полностью очищено без возможности восстановления.

Библиография

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

[b-ITU-T X.1040] Recommendation ITU-T X.1040 (2017), *Security reference architecture for lifecycle management of e-commerce business data*.

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

[b-ISO/IEC 20889] ISO/IEC 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques.*

[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, 2021 г.