ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1411 (03/2023)

СЕРИЯ X: Сети передачи данных, взаимосвязь открытых систем и безопасность

Безопасные приложения и услуги (2) – Безопасность технологии распределенного реестра (DLT)

Руководящие указания по обеспечению безопасности блокчейна как услуги (BaaS)

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	X.1000-X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	X.1100-X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	X.1200-X.1299
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	X.1300-X.1499
Связь в чрезвычайных ситуациях	X.1300-X.1309
Безопасность повсеместных сенсорных сетей	X.1310-X.1319
Безопасность умных электросетей	X.1330-X.1339
Сертифицированная электронная почта	X.1340-X.1349
Безопасность интернета вещей (IoT)	X.1350-X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370-X.1399
Безопасность технологии распределенного реестра (DLT)	**X.1400-X.1429**
Безопасность приложений (2)	X.1450-X.1459
Безопасность веб-среды (2)	X.1470-X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	X.1500-X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	X.1600-X.1699
КВАНТОВАЯ СВЯЗЬ	X.1700-X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	X.1750-X.1799
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800-X.1819

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

Рекомендация МСЭ-Т X.1411

Руководящие указания по обеспечению безопасности блокчейна как услуги (BaaS)

Резюме

В Рекомендации МСЭ-Т X.1411 представлены общие руководящие указания по обеспечению безопасности для блокчейна как услуги (BaaS). Сначала проводится анализ угроз безопасности и уязвимостей BaaS, а затем приводятся меры по обеспечению безопасности BaaS. В Рекомендации также рассматриваются требования безопасности и содержатся руководящие указания, относящиеся ко всей деятельности по созданию, эксплуатации и использованию BaaS.

Блокчейн как услуга (BaaS) стал основным направлением разработки в области блокчейна благодаря своим многообещающим возможностям и широкой поддержке, которую это направление получило в отрасли – в особенности со стороны ведущих поставщиков облачных услуг. BaaS предоставляет базовые услуги и ресурсы для приложений на основе блокчейна, однако сталкивается с проблемами безопасности, связанными как с основными технологиями блокчейн, так и с облачными платформами. Соответственно, важны и необходимы руководящие указания по обеспечению безопасности BaaS.

Хронологическая справка *

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор
1.0	МСЭ-Т X.1411	03.03.2023 г.	17-я	11.1002/1000/15110

Ключевые слова

Блокчейн как услуга, облачная вычислительная среда, протокол выработки консенсуса, смарт-контракт, безопасность.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL https://handle.itu.int/ после которого укажите уникальный идентификатор Рекомендации.

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

© ITU 2023

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

Стр.

1 Сфера применения 1

2 Справочные документы 1

3 Определения 1

3.1 Термины, определенные в других документах 1

3.2 Термины, определенные в настоящей Рекомендации 2

4 Сокращения и акронимы 2

5 Соглашения по терминологии 2

6 Обзор вопросов безопасности блокчейна как услуги 3

6.1 Вопросы безопасности BSP 4

6.2 Вопросы безопасности BSD 5

6.3 Вопросы безопасности BSC 6

7 Угрозы безопасности блокчейна как услуги 6

7.1 Угрозы безопасности для BSP 6

7.2 Угрозы безопасности для BSD 7

7.3 Угрозы безопасности для BSC 8

8 Требования безопасности блокчейна как услуги 8

8.1 Конфигурация безопасности специализированной сети блокчейн 8

8.2 Управление идентификацией и доступом 8

8.3 Управление ключами 9

8.4 Защита конфиденциальности 9

8.5 Безопасность механизмов шифрования 9

8.6 Безопасность одноранговых соединений 10

8.7 Безопасность механизма консенсуса 10

8.8 Безопасность смарт-контрактов 10

8.9 Мониторинг ресурсов 11

8.10 Система обнаружения вторжений 11

8.11 Проверка безопасности 12

8.12 Управление сторонними функциями 12

8.13 Безопасность цепочки поставок 12

Библиография 14

Рекомендация МСЭ-Т X.1411

Руководящие указания по обеспечению безопасности блокчейна как услуги (BaaS)

1 Сфера применения

В настоящей Рекомендации даются руководящие указания по обеспечению безопасности блокчейна как услуги (BaaS). В ней содержатся определения и описание структуры, угроз безопасности и уязвимостей, а также меры по обеспечению безопасности блокчейна как услуги. Вопросы безопасности приложений BaaS, построенных на платформе BaaS, 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.

[ITU-T X.1401] Recommendation ITU-T X.1401 (2019), *Security threats of distributed ledger technology*.

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

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 блокчейн как услуга (blockchain as a service – BaaS) [b-ITU-T Y.3530]: Категория облачных услуг, обеспечивающих потребителю облачных услуг возможность создания платформ на основе технологии блокчейн и разработки децентрализованных приложений с использованием этой технологии.

3.1.2 потребитель облачных услуг (cloud service customer) [b-ITU-T Y.3500]: Сторона, которая состоит в деловых отношениях в целях использования облачных услуг.

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

3.1.4 партнер по облачным услугам (cloud service partner) [b-ITU-T Y.3500]: Сторона, которая участвует в поддержке деятельности либо поставщика облачных услуг, либо потребителя облачных услуг, либо обоих или же оказывает помощь в этой деятельности.

3.1.5 консенсус (consensus) [b-ITU-T X.1400]: Соглашение о том, что набор транзакций действителен.

3.1.6 одноранговое взаимодействие (peer-to-peer) [b-ISO 22739]: Соединение, относящееся к сети одноранговых узлов, которые обмениваются друг с другом информацией и ресурсами напрямую без участия центрального узла, а также использующее или представляющее собой такую сеть.

3.1.7 доказательство выполнения работы (proof of work) [b-ITU-T X.1400]: Процесс выработки консенсуса в отношении решения сложной (дорогостоящей, трудоемкой) проблемы, результат которого легко проверить.

3.1.8 смарт-контракт ("умный" контракт) (smart contract) [b-ITU-T X.1400]: Программа, созданная на основе системы распределенного реестра, которая кодирует правила для конкретных типов транзакций системы распределенного реестра таким образом, чтобы эти транзакции можно было проверить и осуществить после выполнения определенных условий.

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

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 атака 51% (51% attack): Атака, при которой злоумышленники контролируют достаточное количество узлов блокчейна или вычислительных ресурсов, чтобы, управляя созданием блоков, отозвать или переписать реестр системы распределенного реестра.

3.2.2 разделение сети (network partition): Сценарий установления сетевых соединений, когда сеть разделяется на два или несколько изолированных участков.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

API	Application Programming Interface		Интерфейс прикладного программирования
BaaS	Blockchain as a Service		Блокчейн как услуга
BSC	Blockchain as a Service Customer		Потребитель блокчейна как услуги
BSD	Blockchain as a Service Developer		Разработчик блокчейна как услуги
BSP	Blockchain as a Service Provider		Поставщик блокчейна как услуги
BSS	Blockchain as a Service Security developer		Разработчик системы безопасности блокчейна как услуги
CPU	Central Processing Unit	ЦП	Центральный процессор
CSC	Cloud Service Customer		Потребитель облачных услуг
CSN	Cloud Service partner		Партнер по облачным услугам
CSP	Cloud Service Provider		Поставщик облачных услуг
DDoS	Distributed Denial-of-Service		Распределенный отказ в обслуживании
GPU	Graphics Processing Unit	ГП	Графический процессор
IAM	Identity and Access Management		Управление идентификацией и доступом
P2P	Peer-to-Peer		Одноранговый
PII	Personally Identifiable Information		Информация, позволяющая установить личность
PoW	Proof of Work		Доказательство выполнения работы
SDK	Software Development Kit		Комплект инструментов разработки программного обеспечения

5 Соглашения по терминологии

В настоящей Рекомендации:

ключевые слова "**требуется, чтобы**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящему документу;

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

ключевые слова "**может факультативно**" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Данный термин не подразумевает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и 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 настоящей спецификации.

В тексте настоящей Рекомендации и приложений к ней иногда встречаются слова "**должен**", "**не должен**", "**следует**" и "**может**", и в таком случае их следует понимать соответственно как "требуется", "запрещается", "рекомендуется" и "возможно". Такие фразы или ключевые слова, фигурирующие в дополнении или материалах, явно помеченных как информационные, должны толковаться как не несущие нормативного смысла.

6 Обзор вопросов безопасности блокчейна как услуги

Блокчейн как услуга предоставляет как разработчикам, так и потребителям услуг на основе технологии блокчейн интегрированную среду разработки, которая позволяет создавать, разрабатывать, тестировать, размещать, развертывать и эксплуатировать приложения, связанные с блокчейном. В результате потребители услуг BaaS могут использовать основные компоненты блокчейна на платформе BaaS для эффективной эксплуатации и простого развертывания сетей и приложений на основе технологии блокчейн.

Поскольку базовая платформа и услуги на основе блокчейна построены на базе облачных услуг, в процессе функционирования BaaS участвуют три основные стороны, роли которых соответствуют ролям, характерным для облачных услуг.

- **Поставщик блокчейна как услуги (BSP)**. Подобно поставщику облачных услуг (CSP) в среде облачных вычислений, роль BSP охватывает инфраструктуру блокчейна и поставщиков платформ, которые обеспечивают функционирование блокчейна как услуги. BSP упрощает разработку и эксплуатацию блокчейнов и приложений в отношении хранения, передачи данных, вычислений и поддержки со стороны сети, предлагая базовые ресурсы и функции, относящиеся к блокчейну. BSP отвечает за безопасность основных ресурсов блокчейна и разработку инструментов, предоставляемых другим ролям BaaS.
- **Разработчик блокчейна как услуги (BSD)**. Подобно партнеру по облачным услугам (CSN) в среде облачных вычислений, BSD занимается разработкой и эксплуатацией основных компонентов BaaS, помогая BSP в предоставлении услуг на основе блокчейна. BSD отвечает за безопасность разработанных основных компонентов.
  - **Разработчик системы безопасности блокчейна как услуги (BSS)** – это BSD особого типа. BSS помогает BSP в повышении уровня безопасности BaaS в качестве стороннего поставщика услуг обеспечения безопасности. В число услуг обеспечения безопасности, предоставляемых BSS, входят управление идентификацией и доступом (IAM), проверка, обнаружение вторжений и др.
- **Потребитель блокчейна как услуги (BSC)**. Подобно потребителю облачных услуг (CSC) в среде облачных вычислений, BSC – это клиенты блокчейна, которые запрашивают, получают доступ и используют услуги или ресурсы блокчейна посредством функций, предоставляемых BSP напрямую или косвенно через приложения и услуги, предоставляемые BSD. BSC несет ответственность за соблюдение правил безопасности, установленных BSP при эксплуатации его сети и приложений на основе технологии блокчейн. BSC также рекомендуется сотрудничать с BSP в области мониторинга безопасности специализированных сетей блокчейн и при необходимости сообщать о событиях безопасности.

Порядок взаимодействия между этими ролями показан на рисунке 1.

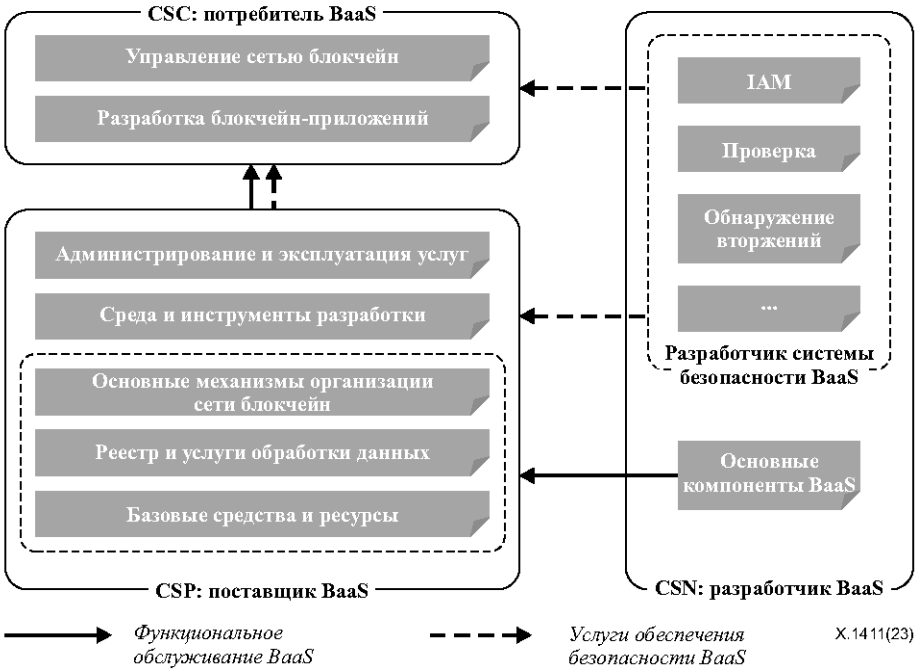

Рисунок 1 − Функции и взаимодействие ролей в системе блокчейна как услуги

6.1 Вопросы безопасности BSP

BSP предоставляет основные функции блокчейна, включая смарт-контракты, протоколы выработки консенсуса, одноранговые (P2P) соединения, алгоритм шифрования, записи транзакций, управление реестром, управление узлами и ресурсами, а также поддержку стандартизированных интерфейсов разработки и служб безопасности. Ниже рассматриваются функции BSP и связанные с ними проблемы безопасности.

6.1.1 Базовые средства и ресурсы

BSP обеспечивает базовые средства для предоставления основных вычислительных, коммуникационных и других ресурсов в целях поддержки сети и разработки блокчейн-приложений. Это могут быть физические или виртуализированные устройства, такие как виртуальные машины и контейнеры.

Для базовых средств характерны такие проблемы, как риски условий окружающей среды для физических объектов, внедрение закладок, обобщенные ресурсы арендаторов и т. д.

6.1.2 Регистр и услуги обработки данных

BSP предоставляет услуги обработки данных как внутри блокчейна, так и вне его. К ним относятся такие услуги, как хранение, управление, обработка клиентских запросов и предоставление BSC системных данных. Реестр данных внутри блокчейна гарантирует защиту от несанкционированного доступа, а база данных вне блокчейна поддерживает эффективные службы обработки данных.

BSP необходимо решить следующие проблемы обеспечения безопасности данных:

– неготовность услуг обработки данных, включая несогласованное хранение данных внутри блокчейна и вне блокчейна, связанное с изолированными участками сети, потеря данных, вызванная выходом из строя базы данных и хранилища данных, несанкционированные изменения реестра данных и т. д.; – утечка конфиденциальной информации, в том числе несанкционированный доступ к индивидуальным данным, извлечение из данных конфиденциальной информации, безуспешное уничтожение личных данных и т. д.

6.1.3 Основные механизмы организации сети блокчейн

BSP предоставляет набор вариантов основных механизмов организации сети блокчейн для упрощения создания сетей блокчейн. К основным механизмам организации сети блокчейн относятся протоколы выработки консенсуса, протоколы P2P-соединений и алгоритмы шифрования. BSC может выбрать определенный набор компонентов сети среди всех вариантов и установить соответствующие параметры для быстрого создания специализированной сети блокчейн.

BSP отвечает за решение проблем безопасности основных механизмов организации сети блокчейн. Указанные проблемы влияют на безопасность специализированных сетей блокчейн и даже блокчейн-приложений, построенных на платформе BaaS, поскольку BSC напрямую использует основные механизмы организации сети блокчейн для разработки сетей и приложений на основе технологии блокчейн. В данном случае возможны такие проблемы безопасности, как несанкционированный доступ к ресурсам блокчейна, образование изолированных участков сети, вредоносные узлы и т. д. Например, образование изолированных участков сети, вызванное неготовностью услуг на основе блокчейна, может привести к недопустимой задержке при попытке выработки консенсуса в распределенной сети блокчейн.

6.1.4 Среда и инструменты разработки

BSP предоставляет интегрированную среду разработки, содержащую интерфейс прикладного программирования (API), набор инструментов разработки и другие средства разработки для упрощения разработки блокчейн-приложений. Поскольку естественным механизмом блокчейна при разработке блокчейн-приложений является смарт-контракт, BSP также упрощает внедрение смарт-контрактов и предоставляет набор смарт-контрактов для реализации обычных функций, таких как управление идентификацией и доступом.

К числу связанных с этим проблем относятся ненадлежащий контроль доступа к API, несовместимые интерфейсы, несвоевременное выполнение смарт-контрактов и т. д.

6.1.5 Администрирование и эксплуатация услуг

BSP отвечает за мониторинг и оповещение о состоянии услуг на основе блокчейна по отношению к физическим объектам, узлам блокчейна, сетевым соединениям и выделенным ресурсам, а также за IAM и другие функции управления безопасностью. BSP также поддерживает и администрирует связанные с блокчейном функции, которые предоставляет BSD.

К соответствующим проблемам безопасности относятся недоступные функции управления, ненадлежащее управление доступом, несанкционированный административный доступ, резкое увеличение потребляемых ресурсов и риски, относящиеся к связанным с блокчейном компонентам, которые предоставляет BSD.

6.2 Вопросы безопасности BSD

BSD разрабатывает основные компоненты BaaS для BSP или предоставляет услуги обеспечения безопасности для всех ролей.

6.2.1 Разработка основных компонентов BaaS

BSD предоставляет основные компоненты BaaS, такие как смарт-контракты, криптографические алгоритмы, протоколы выработки консенсуса и алгоритмы шифрования, в качестве стороннего поставщика.

К числу соответствующих проблем и угроз безопасности относятся несовместимые интерфейсы, небезопасные структуры протоколов, закладки в реализациях протоколов и т. д.

6.2.2 Услуги обеспечения безопасности

BSS выступает в качестве стороннего поставщика услуг обеспечения безопасности для всех ролей в экосистеме BaaS. Например, BSS может обеспечивать обнаружение вторжений для BSP, проверку кода для BSD и IAM для BSC.

К проблемам безопасности относятся устаревшие правила безопасности, ошибочные действия сотрудников BSS и т. д.

6.3 Вопросы безопасности BSC

BSC использует услуги, предоставляемые BSP и BSD, для создания индивидуальной сети и приложений на основе технологии блокчейн. Существует два типа BSC: администратор, который создает и администрирует специализированные сети блокчейн, и участник, который присоединяется к специализированной сети блокчейн. Один и тот же BSC может быть администратором одной специализированной сети блокчейн и участником другой.

BSC всех типов сталкиваются с проблемами безопасности, связанными с управлением ключами и их использованием. Администратор также сталкивается с проблемами безопасности, связанными с настройкой и администрированием специализированных сетей блокчейн, такими как неправильная настройка узлов, соединений и других ресурсов блокчейна.

7 Угрозы безопасности блокчейна как услуги

Угрозы для BSP, BSD и BSC можно разделить на три группы:

– небезопасные технические конструкции, ошибки реализации и ненадлежащее управление базовыми ресурсами, основными функциями и системами услуг на основе блокчейна;– небезопасное взаимодействие между BSC, BSD и BSP, включая несовместимые интерфейсы и небезопасную цепочку поставок;– неправомерные действия сотрудников, в том числе ненадлежащее использование и хранение паролей.Угрозы безопасности для каждой роли описаны в пунктах 7.1–7.3.

7.1 Угрозы безопасности для BSP

7.1.1 Угрозы для облачных услуг

Поскольку BSP предоставляет базовые ресурсы блокчейна на основе облачных услуг, он сталкивается с проблемами и угрозами, характерными для облачных услуг, как описано в разделах 7 и 8 [ITU-T X.1601]. Например, несанкционированный доступ к участку ресурса другого арендатора в обобщенной среде облачных услуг может привести к разветвлению блокчейна в системе блокчейна этого арендатора в результате перезаписи или пересмотра его реестров данных.

7.1.2 Угрозы для основных механизмов сети блокчейн

Угрозы для протоколов выработки консенсуса, протоколов P2P-соединений и механизмов шифрования могут быть вызваны уязвимостями в конструкции протоколов, ошибками при реализации механизмов и ненадлежащим управлением. Подробности содержатся в разделе 6 [ITU-T X.1401].

7.1.3 Ненадежные услуги передачи данных

К угрозам для распределенного реестра данных относятся нехватка ресурсов блокчейна, ошибки в системе хранения и небезопасное управление хранилищем данных, что может привести к несогласованной записи, потере, подлогу или утечке данных. Например, в процессе работы сети блокчейн система и данные блокчейна специализированной сети блокчейн увеличиваются в объеме. Если BSP не предоставит специализированной сети блокчейн достаточных ресурсов хранения для увеличившихся объемов данных, такая сеть перезапишет новые данные поверх старых или просто удалит новые данные, что приведет к потере данных в специализированной сети блокчейн. Другой пример: отказы в системе передачи или хранения данных могут привести к несогласованному хранению данных в распределенных реестрах. Если отказы сохраняются достаточно долго, результирующие изолированные участки сети вызывают непредвиденные задержки при создании блоков, обработке запросов данных и предоставлении других услуг по передаче данных.

7.1.4 Угрозы для среды разработки

Интегрированная среда разработки, среда компиляции, смарт-контракты, API-интерфейсы, комплекты инструментов разработки программного обеспечения (SDK) и другие средства разработки, предоставляемые BSP, подвержены угрозам в процессе проектирования, реализации, настройки и эксплуатации этих средств разработки. Например, ошибки аутентификации API могут привести к несанкционированному доступу и использованию базового ресурса блокчейна. Кроме того, смарт-контракты подвержены уязвимостям безопасности в логической структуре, при реализации контрактов

и управлении кодом; например, переполнение целочисленных регистров и потеря значимости в смарт-контракте приводит к ложным результатам исполнения.

7.1.5 Небезопасные сторонние функции

BSP поддерживает сторонние функции, предоставляемые BSD, и интегрирует их в платформу BaaS посредством API. Ошибки и вредоносные программы в таких сторонних функциях, а также несовместимые API и ненадлежащий контроль доступа к API могут привести к нарушению работы системы BaaS.

7.1.6 Небезопасный доступ к системе

Под небезопасным доступом к системе понимается отсутствие контроля или ненадлежащий контроль доступа к объектам блокчейна, реестру данных, сети и приложениям. Это может привести к фальсификации данных блокчейна, вторжению в специализированные сети блокчейн и утечке конфиденциальной информации.

7.1.7 Внутренние угрозы

Сотрудники BSP могут случайно или преднамеренно совершать вредоносные действия, например сообщать пароли неуполномоченным лицам, оставлять пароли в небезопасных местах, раскрывать личную информацию и т. д. Внутренние угрозы могут привести к утечке конфиденциальной информации, несанкционированному доступу к специализированным сетям блокчейн и неготовности услуг на основе блокчейна.

7.1.8 Ненадежная цепочка поставок

Для платформы услуг на основе блокчейна используются программные и аппаратные компоненты, поставляемые различными поставщиками. Прекращение поставок программного и аппаратного обеспечения подорвет возможности вычислений, установления соединений и других ресурсов, используемых для предоставления услуг на основе блокчейна. В этом случае доступность таких услуг оказывается под угрозой. Например, доказательство выполнения работы (PoW) протокола выработки консенсуса основано на конкуренции вычислительных способностей между активными узлами блокчейна, поэтому прекращение поставок устройств, обеспечивающих возможности вычислений и установления соединений, может повлиять на результаты консенсуса в сетях блокчейн на основе PoW.

Кроме того, вредоносное ПО и уязвимости в программном и аппаратном обеспечении, а также в архитектуре блокчейна с открытым исходным кодом могут привести к несвоевременному созданию блоков, отказу в обслуживании, утечке или неправомерному использованию данных и т. д.

7.1.9 Угрозы для физической среды

Пожар, наводнение, гроза и другие стихийные бедствия, воздействующие на базовые средства, могут привести к недоступности средств установления соединений, выполнения вычислений и других базовых ресурсов. Например, преднамеренное или случайное отключение электроэнергии может привести к переходу участков блокчейна в автономный режим. В этом случае в процессе выработки консенсуса участвует меньшее число узлов блокчейна, что приводит к неверным результатам консенсуса и дополнительной задержке при создании блоков.

7.2 Угрозы безопасности для BSD

7.2.1 Угрозы для сторонних функций

BSD предоставляет основные компоненты блокчейна, механизмы обеспечения безопасности блокчейна и функции разработки блокчейн-приложений в качестве стороннего поставщика. К соответствующим угрозам относятся уязвимости, присущие основным компонентам блокчейна, ошибки реализации этих сторонних функций, несовместимые интерфейсы и небезопасный контроль доступа к интерфейсам.

Кроме того, вредоносные действия сотрудников BSD также могут привести к утечке конфиденциальной информации, внедрению закладок в сторонние функции и ложному срабатыванию функций безопасности.

7.3 Угрозы безопасности для BSC

7.3.1 Утечка и потеря ключей

BSC управляет ключами самостоятельно или через стороннюю службу. Ненадлежащее хранение ключей, повреждение файла ключа или ненадежные сторонние службы управления ключами могут привести к потере или утечке ключей, что чревато потерей активов BSC, раскрытием конфиденциальной информации и нарушением работы специализированных сетей блокчейн.

7.3.2 Неправильное администрирование специализированных сетей блокчейн

BSC создает собственные специализированные сети блокчейн и развертывает механизмы безопасности, основанные на функциях блокчейна, предоставляемых BSP и BSD. Соответственно, специализированным сетям блокчейн могут угрожать неправильные конфигурации настройки таких сетей и механизмов безопасности. Например, если BSC выделяет недостаточно ресурсов хранения для работы специализированной сети блокчейн, такая сеть может перестать обновлять данные блокчейна, что в конечном итоге приведет к несогласованности реестров данных блокчейна.

8 Требования безопасности блокчейна как услуги

8.1 Конфигурация безопасности специализированной сети блокчейн

Рекомендуется, чтобы BSP давал рекомендации по настройке специализированной сети блокчейн в целях выполнения требований безопасности BSC. Кроме того, рекомендуется, чтобы BSP давал рекомендации по развертыванию необходимых механизмов безопасности в специализированных сетях блокчейн.

a) Требуется, чтобы BSP указывал рекомендуемый диапазон общего количества узлов.

b) Требуется, чтобы BSP указывал минимальное количество активных узлов во избежание угроз "атака 51%" и других известных угроз для сети блокчейн.

c) Требуется, чтобы BSP указывал минимальное количество соседей каждого узла во избежание разделения сети блокчейн.

d) Рекомендуется, чтобы BSP указывал рекомендуемые типы узлов, а также количество и права узлов каждого типа.

e) Рекомендуется, чтобы BSP указывал минимальный ресурс хранения, центральный процессор (ЦП) и графический процессор (ГП) для узлов каждого типа.

f) Рекомендуется, чтобы BSP указывал рекомендуемые протоколы выработки консенсуса и одноранговое взаимодействия в соответствии с конфигурациями узлов.

g) Рекомендуется, чтобы BSP предоставлял базовые функции безопасности, включая IAM и управление ключами, для специализированной сети блокчейн.

h) BSP может факультативно дать оценку безопасности конфигураций специализированной сети блокчейн. BSP должен предоставить BSC соответствующие предложения и решения по безопасности.

8.2 Управление идентификацией и доступом

Рекомендуется, чтобы BSP предоставлял функции управления идентификацией и доступом для системы BaaS и специализированной сети блокчейн. Функции управления идентификацией и доступом предназначены не только для защиты идентификационных данных, но и для облегчения управления доступом, аутентификации и авторизации.

a) Требуется, чтобы BSP предоставлял функции регистрации и отмены регистрации идентификационных данных для системы BaaS.

b) Рекомендуется, чтобы BSP предоставлял функции регистрации и отмены регистрации идентификационных данных для специализированной сети блокчейн.

c) Требуется, чтобы BSP обеспечивал управление доступом к учетным записям в системе BaaS, позволяя различать BSP, BSC и BSD.

d) Рекомендуется, чтобы BSP обеспечивал управление доступом к учетным записям в специализированной сети блокчейн. В любой специализированной сети блокчейн должны присутствовать одна или несколько ролей потребителей с разными правами доступа.

e) Требуется, чтобы BSP обеспечивал аутентификацию доступа к системе BaaS. Каждое лицо может получать доступ к ресурсу только в соответствии со своими правами доступа.

f) Рекомендуется, чтобы BSP обеспечивал аутентификацию доступа к специализированной сети блокчейн.

g) BSP может факультативно предоставить отдельные функции управления доступом, такие как функции управления доступом на основе ролей.

h) BSP может факультативно отслеживать частоту обращений для определенного IP-адреса, учетной записи, устройства и т. п. Обращениями считаются регистрация, отмена регистрации, обновление ключа и другие действия.

8.3 Управление ключами

Рекомендуется, чтобы BSP предоставлял функции управления ключами для обеспечения безопасности создания, хранения, распространения, использования, резервного копирования, восстановления и отзыва ключей.

a) Требуется, чтобы BSP предоставлял исчерпывающие схемы управления ключами, а также разъяснение информации по ключам и процедуре управления.

b) Требуется, чтобы BSP оценивал безопасность алгоритмов на основе случайных чисел и других параметров, используемых для создания ключей. Алгоритмы на основе случайных чисел должны удовлетворять требованиям в отношении степени случайности и непредсказуемости.

c) Рекомендуется, чтобы BSP поддерживал сторонние функции управления ключами. Безопасность сторонних функций управления ключами должна оцениваться и гарантироваться до их предоставления BSC.d) Рекомендуется, чтобы BSP предоставлял функции отзыва ключей исключенных и подозрительных учетных записей.e) Рекомендуется, чтобы BSP предоставлял функции восстановления утерянных ключей. Доступ к функциям восстановления ключей предоставляется только аутентифицированным учетным записям. f) Рекомендуется, чтобы BSP периодически требовал обновления ключей BSC. Период обновления должен зависеть от уровня защиты.g) Рекомендуется, чтобы BSC разворачивал в специализированной сети блокчейн функцию управления ключами.h) Требуется, чтобы BSC осваивал и соблюдал безопасные процедуры использования, хранения, восстановления и отзыва ключей в соответствии с функцией управления ключами, развернутой в специализированной сети блокчейн.i) Рекомендуется, чтобы BSC сообщал BSP о подозрительном использовании ключа, как указано в функции управления ключами.j) BSP может факультативно использовать двухстороннюю или многостороннюю схему хранения ключей для основных и секретных ключей.**8.4 Защита конфиденциальности**

Рекомендуется, чтобы BSP обеспечивал защиту при сборе, доступе и других операциях с информацией, позволяющей установить личность (PII).

a) Требуется, чтобы BSP соблюдал национальные и местные законы, правила и нормы, относящиеся к защите конфиденциальности, например при сборе и хранении PII.b) Требуется, чтобы BSP обеспечивал деидентификацию отображаемой PII.c) Требуется, чтобы BSP принимал меры безопасности, гарантирующие возможность полного удаления PII из блокчейна по требованию BSC, например с использованием технологии блокчейн на основе алгоритма Chameleon Hash, или хранил PII вне блокчейна.

d) Рекомендуется, чтобы BSP приглашал профессиональные организации для проверки операций с PII, требующих защиты.

8.5 Безопасность механизмов шифрования

Рекомендуется, чтобы BSP обеспечивал безопасность механизмов шифрования, применяемых в специализированных сетях блокчейн.

a) Требуется, чтобы BSP поддерживал основные алгоритмы шифрования, безопасность которых подтверждена публично.

b) Требуется, чтобы BSP приглашал профессиональные организации для проверки безопасности механизмов шифрования.

c) Рекомендуется, чтобы BSP поддерживал механизмы шифрования, предоставляемые BSD. Рекомендуется, чтобы BSD предоставлял результаты оценки безопасности механизмов шифрования.

8.6 Безопасность одноранговых соединений

Рекомендуется, чтобы BSP обеспечивал защиту одноранговых соединений от ненадежных и вредоносных узлов.

a) Требуется, чтобы BSP предоставлял схемы аутентификации для управления доступом к одноранговым сетям.

b) Требуется, чтобы BSP использовал технологию шифрования для установления безопасных каналов передачи данных между распределенными узлами.

c) Требуется, чтобы BSP поддерживал одноранговые протоколы с гарантированной надежностью и масштабируемостью. Надежность означает, что отсоединенные узлы после восстановления соединения сохраняют согласованность с другими узлами. Масштабируемость означает, что протоколы поддерживают динамическое или статическое добавление или удаление узлов с сохранением нормальной работы сетей блокчейн.

d) Требуется, чтобы BSP поддерживал протоколы одноранговой сети в любом узле, который имеет более одного соседа.

e) Рекомендуется, чтобы BSP поддерживал протоколы одноранговой сети, в которой отсоединение любого узла не приводит к образованию изолированных участков сети.

f) Рекомендуется, чтобы BSP предоставлял топологию одноранговой сети в режиме реального времени.

g) Рекомендуется, чтобы BSP подавал сигнал, если в одноранговой сети появляются изолированные участки или вредоносные узлы.**8.7 Безопасность механизма консенсуса**

Рекомендуется, чтобы BSP гарантировал безопасность структуры и работы механизма консенсуса.

a) Требуется, чтобы BSP предоставлял алгоритмы выработки консенсуса, безопасность которых доказана или оценена публично.

b) Требуется, чтобы BSP поддерживал BSC при развертывании алгоритмов выработки консенсуса, предоставляемых BSD.

c) Требуется, чтобы BSP предоставлял BSC оценки безопасности алгоритмов выработки консенсуса. Оценка безопасности должна включать пороговое количество узлов, участвующих в выработке консенсуса, рекомендуемую частоту проверок консенсуса и другие параметры.

d) Требуется, чтобы до присоединения к консенсусу BSP гарантировал, что узлы, участвующие в выработке консенсуса, аутентифицированы.

e) Требуется, чтобы BSP контролировал процесс достижения консенсуса и оценивал период выработки консенсуса, количество участвующих узлов и результат консенсуса.

f) Рекомендуется, чтобы BSP подавал сигналы и предлагал решение, когда контролируемый процесс выработки консенсуса оценивается как аномальный.

8.8 Безопасность смарт-контрактов

Рекомендуется, чтобы BSP обеспечивал управление всем жизненным циклом смарт-контрактов, включая их создание, внедрение, обновление, инициирование, исполнение и отмену.

a) Требуется, чтобы BSP предоставлял спецификации кода, требования к логике и другие нормативные указания по смарт-контрактам.

b) Рекомендуется, чтобы BSP предоставлял надежную изолированную среду для выполнения смарт-контрактов, такую как "песочница".

c) Требуется, чтобы BSP обеспечивал надлежащее управление доступом к смарт-контрактам для ограничения возможности вредоносных операций и предотвращения заражения вредоносными смарт-контрактами других контрактов.

d) Требуется, чтобы BSP поддерживал механизмы реагирования на чрезвычайные ситуации в отношении безопасности смарт-контрактов.

e) Требуется, чтобы BSP ограничивал сложность смарт-контрактов с точки зрения потребления ресурсов и времени выполнения.

f) Рекомендуется, чтобы BSP отслеживал и контролировал чрезмерное потребление ресурсов блокчейна смарт-контрактами.

g) Рекомендуется, чтобы BSP поддерживал расторжение смарт-контрактов, когда они превышают предел расходуемых ресурсов.

h) Рекомендуется, чтобы BSP предоставлял технические решения для предотвращения атак "распределенный отказ в обслуживании" (DDoS) по отношению к смарт-контрактам.

i) Рекомендуется, чтобы BSP обязывал BSD применять средства автоматического обнаружения уязвимостей в исходном коде и байт-коде смарт-контрактов.

j) Рекомендуется, чтобы BSP обязывал BSD следить за действиями смарт-контрактов в целях обнаружения и раннего предупреждения об их аномальном поведении.

8.9 Мониторинг ресурсов

Рекомендуется, чтобы BSP отслеживал потребление ресурсов в BaaS и подавал сигнал при аномальном состоянии ресурса.

a) Рекомендуется, чтобы BSC позволял BSP отслеживать потребление ресурсов узлами специализированных сетей блокчейн в отношении устройств хранения данных, вычислительных устройств, ЦП, сетевых соединений, состояния активности, времени активности и других параметров.

b) Рекомендуется, чтобы BSP подавал BSC сигнал, когда узлы специализированной сети блокчейн сталкиваются с нехваткой ресурсов. BSP должен предоставить BSC решения для устранения нехватки ресурсов.

c) Рекомендуется, чтобы BSC позволял BSP отслеживать в специализированных сетях блокчейн параметры состояния сети, такие как скорость создания блоков, количество генераторов блоков, размеры блоков и др.

d) Рекомендуется, чтобы BSP подавал BSC сигнал о необходимости вмешательства при выявлении аномального состояния сети. BSP должен представить BSC соответствующий анализ аномалии, информацию об аномальном узле и рекомендуемые решения.

8.10 Система обнаружения вторжений

Рекомендуется, чтобы BSP предоставлял и обновлял механизмы предотвращения проникновения вредоносного кода и других вторжений.

a) Требуется, чтобы BSP предоставлял правила безопасности и библиотеки уязвимостей смарт-контрактов. BSP должен предоставить интерфейсы доступа в общей форме для обнаружения уязвимостей.

b) Требуется, чтобы BSP устанавливал программное обеспечение для защиты от вредоносных программ или программное обеспечение настройки с соответствующими функциями обнаружения и удаления вредоносных программ.

c) Рекомендуется, чтобы BSP обеспечивал предотвращение возможности проникновения вредоносного кода в каждом узле блокчейна и устранения вредоносного кода до получения доступа к сети блокчейн.

d) Рекомендуется, чтобы BSP представлял положение о механизмах предотвращения проникновения вредоносного кода, включая периодическое обновление библиотеки вредоносных программ и регулярное выявление и удаление вредоносного кода.

e) Рекомендуется, чтобы BSP обязывал BSD регулярно оценивать эффективность технических мер борьбы с атаками вредоносных программ.

8.11 Проверка безопасности

Рекомендуется, чтобы BSP обязывал одного или нескольких BSD проводить проверки безопасности инфраструктуры блокчейна, исходного кода и других основных функций.

a) Рекомендуется, чтобы BSP выбирал нескольких BSD для проведения оценки безопасности и проверки базового программного обеспечения блокчейна, сети и других рабочих сред до ввода в эксплуатацию услуг на основе блокчейна, чтобы гарантировать контролируемость рисков безопасности на уровне инфраструктуры.

b) Рекомендуется, чтобы BSP обязывал по крайней мере одного BSD проводить проверки безопасности исходного кода, фокусируясь главным образом на рисках и проблемах качества на уровне исходного кода.

c) Рекомендуется, чтобы BSD представлял BSP отчеты о проверках исходного кода с указаниями на соответствие/нарушение и предложениями по пересмотру указанного исходного кода.

d) Рекомендуется, чтобы BSP обязывал BSD оценивать функции IAM, гарантируя отсутствие таких рисков, как утечка секретных ключей и информации пользователей.

8.12 Управление сторонними функциями

Рекомендуется, чтобы BSP гарантировал безопасное осуществление операций сторонними функциями в соответствии с заданными требованиями.

a) Требуется, чтобы BSP выяснял требования безопасности и функциональные требования сторонних поставщиков.

b) Требуется, чтобы BSP заключал соглашения о сотрудничестве в области компонентов услуг со сторонними поставщиками услуг и уточнял их обязательства и обязанности.

c) Рекомендуется, чтобы BSP контролировал или проверял услуги сторонних поставщиков и оценивал их в соответствии с подписанным соглашением.

8.13 Безопасность цепочки поставок

Рекомендуется, чтобы BSP гарантировал устойчивость своей цепочки поставок в отношении ненадежных поставщиков и смены поставщиков.

a) Требуется, чтобы BSP разрабатывал правила и процедуры управления безопасностью цепочки поставок, включая критерии управления безопасностью участников цепочки поставок.

b) Требуется, чтобы BSP регулярно оценивал уязвимость своей цепочки поставок в инфраструктуре и использование программного обеспечения с открытым исходным кодом в системе.

c) Рекомендуется, чтобы BSP информировал BSC о рисках, связанных с цепочкой поставок, в системе блокчейна как услуги.

Требуется, чтобы BSP подтвердил разнообразие своих поставщиков необходимого программного и аппаратного обеспечения.

Таблица 1 − Требования безопасности BaaS

Угрозы безопас-ности		Требования безопасности												
		Конфигурация безопасности	**IAM**	**Управление ключами**	**Защита конфиден-циальности**	**Безопас-ность механизмов шифрования**	**Безопас-ность P2P-соеди-нений**	**Безопас-ность механизма выработки консенсуса**	**Безопас-ность смарт-контрактов**	**Мониторинг ресурсов**	**Система обнару-жения вторжений**	**Проверка безопас-ности**	**Управление сторонними функциями**	**Безопас-ность цепочки поставок**
BSP	7.1.1	✓	✓	✓	✓				✓			✓	✓	✓
	7.1.2					✓	✓	✓	✓		✓	✓	✓	✓
	7.1.3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	7.1.4							✓	✓	✓	✓			
	7.1.5										✓	✓	✓	✓
	7.1.6		✓	✓										
	7.1.7		✓										✓	
	7.1.8											✓	✓	✓
	7.1.9												✓	
BSD	7.2.1			✓	✓	✓	✓	✓		✓	✓		✓	
BSC	7.3.1		✓	✓										
	7.3.2	✓								✓			✓	

Библиография

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology − Cloud computing − Overview and vocabulary*.

[b-ITU-T Y.3530] Recommendation ITU-T Y.3530 (2020), *Cloud computing − Functional requirements for blockchain as a service*.

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies − Vocabulary*. https://www.iso.org/standard/73771.html

[b-ISO/IEC 27000] ISO/IEC 27000:2018(en), *Information technology − Security techniques − Information security management systems − Overview and vocabulary*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

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, 2023 г.