Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

F.747.10

(01/2022)

СЕРИЯ F: НЕТЕЛЕФОННЫЕ СЛУЖБЫ ЭЛЕКТРОСВЯЗИ

Мультимедийные службы

Требования к системам распределенного реестра для услуг, использующих защищенный человеческий фактор

Рекомендация МСЭ-Т F.747.10

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ F

НЕТЕЛЕФОННЫЕ СЛУЖБЫ ЭЛЕКТРОСВЯЗИ

ТЕЛЕГРАФНАЯ СЛУЖБА	
Эксплуатационные методы для международной службы передачи телеграмм общего пользования	F.1–F.19
Сеть гентекс	F.20–F.29
Коммутация сообщений	F.30–F.39
Международная служба обмена сообщениями	F.40–F.58
Международная служба телекс	F.59–F.89
Статистика и публикации по международным телеграфным службам	F.90–F.99
Службы связи с работой по расписанию и с арендованными каналами	F.100–F.104
Фототелеграфная служба	F.105–F.109
ПОДВИЖНАЯ СЛУЖБА	
Подвижные службы и многоадресные спутниковые службы	F.110–F.159
ТЕЛЕМАТИЧЕСКИЕ СЛУЖБЫ	
Факсимильная служба общего пользования	F.160–F.199
Служба телетекс	F.200–F.299
Служба видеотекс	F.300–F.349
Общие положения для телематических служб	F.350–F.399
СЛУЖБЫ ОБРАБОТКИ СООБЩЕНИЙ	F.400–F.499
СПРАВОЧНЫЕ СЛУЖБЫ	F.500–F.549
ДОКУМЕНТАЛЬНАЯ СВЯЗЬ	
Документальная связь	F.550–F.579
Программируемые интерфейсы связи	F.580–F.599
СЛУЖБЫ ПЕРЕДАЧИ ДАННЫХ	F.600–F.699
МУЛЬТИМЕДИЙНЫЕ СЛУЖБЫ	F.700–F.799
СЛУЖБЫ ЦСИС	F.800–F.849
УНИВЕРСАЛЬНАЯ ПЕРСОНАЛЬНАЯ ЭЛЕКТРОСВЯЗЬ	F.850–F.899
ДОСТУПНОСТЬ И ЧЕЛОВЕЧЕСКИЕ ФАКТОРЫ	F.900–F.999

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

Рекомендация МСЭ-Т F.747.10

Требования к системам распределенного реестра для услуг, использующих защищенный человеческий фактор

Резюме

В Рекомендации МСЭ-Т F.747.10 представлены общие требования и функциональные возможности систем распределенного реестра (DLS) для услуг, использующих защищенный человеческий фактор.

В настоящей Рекомендации описаны требования к модели услуг распределенного реестра, использующих защищенный человеческий фактор, которые могут реализовать противоречивые цели защиты конфиденциальности и использования больших персональных данных, содержащих человеческий фактор. В настоящей Рекомендации описаны также функциональные возможности совместно используемых узлов распределенного реестра, содержащих защищенный человеческий фактор, для выполнения машинного обучения без дешифрования зашифрованных данных, содержащих человеческий фактор. Однако вычислительная нагрузка машинного обучения в случае зашифрованных данных может быть чрезмерной. Для решения этой проблемы данная модель услуг распределенного реестра, использующих защищенный человеческий фактор, обеспечивает процедуры, позволяющие применять две или более пары ключей шифрования и уведомлять о типе ключа. Кроме того, в настоящую Рекомендацию включены требования по поддержанию целостности для услуг, использующих защищенный человеческий фактор, для того чтобы поддерживать безопасность распределенного реестра и его проверку с самого начала для распространения персональной информации, содержащей человеческий фактор. Следовательно, применение системы распределенного реестра при распространения персональной информации, содержащей защищенный человеческий фактор, может обеспечить прозрачное отслеживание от процесса распределения до пути конечного использования.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т F.747.10	17.01.2022 г.	16-я	11.1002/1000/14644

Ключевые слова

Модель услуг распределенного реестра, расширение защиты конфиденциальности, защищенный человеческий фактор, отслеживание прозрачности.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Стр.

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 3

6 Базовая информация 3

7 Общие требования к системам распределенного реестра для услуг, использующих защищенный человеческий фактор 4

7.1 Функциональные требования к совместно используемым узлам общедоступного распределенного реестра 4

7.2 Требования к аутентификации для нового участвующего узла 4

7.3 Требования безопасности для системы распределенного реестра 5

7.4 Требования по поддержанию целостности для системы распределенного реестра 6

8 Функциональные возможности системы распределенного реестра для услуг, использующих защищенный человеческий фактор 6

8.1 Структура распределенного реестра при распространении персональных данных, содержащих человеческий фактор 6

8.2 Две функции в структуре распределенного реестра для распространения персональных данных, содержащих человеческий фактор 7

8.3 Методики обслуживания системы распределенного реестра 8

Приложение А – Применение модели услуг распределенного реестра, использующих защищенный человеческий фактор 10

Библиография 11

Рекомендация МСЭ-Т F.747.10

Требования к системам распределенного реестра для услуг, использующих защищенный человеческий фактор

1 Сфера применения

В настоящей Рекомендации представлено описание требований к системам распределенного реестра (DLS) для услуг, использующих защищенный человеческий фактор, которое включает следующие части:

- базовая информация;
- общие требования к DLS для услуг, использующих защищенный человеческий фактор;
- функциональные возможности DLS для услуг, использующих защищенный человеческий фактор.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все рекомендации и другие источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. 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.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 блок (block) [b-ISO 22739]: Структурированные данные, которые состоят из данных блока и заголовка блока.

3.1.2 консенсус (consensus) [b-ISO 22739]: Соглашение между узлами DLT, о том что 1) транзакция подтверждена; и 2) что распределенный реестр содержит согласованный набор и порядок следования подтвержденных транзакций.

3.1.3 цифровая подпись (digital signature) [b-ISO 22739]: Данные, которые, когда они присоединены к цифровому объекту, дают возможность пользователю этого цифрового объекта удостоверить его источник и целостность.

3.1.4 распределенный реестр (distributed ledger) [b-ISO 22739]: Реестр, используемый совместно набором узлов DLT и синхронизируемый между узлами DLT с помощью механизма консенсуса.

3.1.5 технология распределенного реестра (distributed ledger technology) [b-ISO 22739]: Технология, которая обеспечивает возможность работы и использования распределенных реестров.

3.1.6 вилка (fork) [b-ITU-T TS FG DLT D1.1]: Создание двух и более различных версий распределенного реестра.

3.1.7 хеш-значение (hash value) [b-ISO 22739]: Строка битов, которая является результатом криптографической хеш-функции.

3.1.8 здоровье (health) [b-WHO]: Состояние физического, душевного и социального благополучия при отсутствии болезней и физических дефектов.

3.1.9 реестр (ledger) [b-ISO 22739]: Хранилище информации, содержащее записи транзакций, которые считаются окончательными, полными и неизменяемыми.

3.1.10 дерево Меркла (Merkle tree) [b-NIST]: Структура данных, в которой данные хешируются и суммируются до получения единого хеш-корня, представляющего полную структуру данных.

3.1.11 майнинг (mining) [b-ITU-T F.751.0]: Деятельность, предусматривающая получение вознаграждения, которая осуществляется на уровне некоторых механизмов консенсуса.

3.1.12 узел (node) [b-ISO 22739]: элементарный компонент, который служит основой структуры данных.

3.1.13 общедоступная система распределенного реестра (public distributed ledger system) [b-ITU-T F.751.0]: Система DLT, общедоступная для использования.

3.1.14 транзакция (transaction) [b-ISO 22739]: Наименьшая единица рабочего процесса, которая представляет собой одну или несколько последовательностей действий, необходимых для получения результата, соответствующего управляющим правилам.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 глубина блока (block depth): Уровень блока, добавленного к цепочке системы распределенного реестра, начиная от начального блока.

3.2.2 электронные записи, в которых содержится человеческий фактор: Систематизированная совокупность информации о человеке и населении, в которой учитывается человеческий фактор и которая хранится в электронном виде в цифровом формате.

3.2.3 человеческий фактор (human factor): Принципы создания оптимальных условий жизни в отношении благополучия, безопасности и здоровья человека, включая развитие существующих технологий и освоение новых.

ПРИМЕЧАНИЕ. – На основе [b-ISO 6385] и [b-Wickens].

3.2.4 персональные данные, содержащие человеческий фактор (personal human factor information): Информация, собираемая путем прямого измерения характеристик человеческого тела и окружающей его среды, которая передается на персональные устройства, учитывающие человеческий фактор, или иные устройства по сети связи для использования в электронных записях, содержащих человеческий фактор.

3.2.5 персональное устройство, учитывающее человеческий фактор (personal human factor device): Тип устройства, которое измеряет характеристики человеческого тела и окружающей его среды, и выполняет обмен собранной информацией с другими устройствами, учитывающими человеческий фактор.

3.2.6 защищенный человеческий фактор (secure human factor): Человеческий фактор, который находится в информационной безопасности.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

CPU	Central Processing Unit	ЦП	Центральный процессор
DLS	Distributed Ledger Systems		Системы распределенного реестра
DLT	Distributed Ledger Technology		Технология распределенного реестра
IP	Internet Protocol		Протокол Интернет
PDLS	Public Distributed Ledger Systems		Общедоступные системы распределенного реестра
UUID	Universally Unique Identifier		Универсальный уникальный идентификатор
VRF	Verifiable Random Function		Верифицируемая случайная функция

5 Соглашения

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 настоящей Рекомендации;

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

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

6 Базовая информация

В последние годы объем персональных данных, содержащих человеческий фактор, значительно увеличился в связи с развитием персональных устройств сбора медицинских данных и увеличением объема данных, вносимых в персональные медицинские карты, которые находятся в ведении больниц. Одна из лучших моделей управления персональными данными, содержащими человеческий фактор, и обмена ими – модель услуг распределенного реестра. Характеристики систем распределенного реестра обеспечивают надежность благодаря использованию распределенной базы данных с большим количеством задействованных узлов, а также прозрачность извлеченных данных благодаря использованию цифровых подписей и хеш-значений. Однако данные, содержащие человеческий фактор, имеют высокий уровень конфиденциальности в аспекте защиты информации. Следовательно, требуется, чтобы к модели услуг общедоступного распределенного реестра применялись требования по защите персональных данных, содержащих человеческий фактор (см. рисунок 1).

Рисунок 1 – Модель услуги распределенного реестра, использующей человеческий фактор

В настоящей Рекомендации определены требования безопасности для модели услуг распределенного реестра, использующих человеческий фактор, которые могут реализовать цели защиты конфиденциальности и использования больших персональных данных, содержащих человеческий фактор. В Рекомендации также представлены функциональные требования к совместно используемым узлам распределенного реестра для выполнения машинного обучения без дешифрования зашифрованных данных. Описаны требования к стимулам в модели услуг распределенного реестра для улучшения качества жизни путем автоматизации распределения продуктов медицинского назначения непосредственно потребителям и производителям. Применение технологии распределенного реестра прежде всего обеспечивает возможность отслеживать производство и распространение медицинской информации и управлять ими. Иными словами, применение технологии распределенного реестра при распространении персональных данных, содержащих человеческий фактор, может обеспечить прозрачное отслеживание от процесса распределения до пути конечного использования. По этой причине отдельные лица, представленные отдельными узлами, которые участвуют в системе

распределенного реестра, могут доверять распространяемой информации и использовать эту информацию. Наряду с этим возможно обеспечить метод абсолютного блокирования незаконного распространения персональных данных, содержащих человеческий фактор.

7 Общие требования к системам распределенного реестра для услуг, использующих защищенный человеческий фактор

В настоящем разделе определены требования к безопасному управлению перемещением в распределенных реестрах, которые могут реализовать противоречивые цели защиты конфиденциальности и использования больших персональных данных, содержащих человеческий фактор. В разделе представлены функциональные требования к совместно используемым узлам распределенного реестра для выполнения машинного обучения без дешифрования зашифрованных данных. Например, гомоморфное шифрование – это криптографический метод, с помощью которого возможно выполнять все вычисления, производимые компьютером, даже без дешифрования зашифрованных данных. И в случае анализа данных, содержащих подлежащие защите персональные данные, дополнительно может выполняться машинное обучение без утечки персональных данных или потери данных.

7.1 Функциональные требования к совместно используемым узлам общедоступного распределенного реестра

Ниже приведены функциональные требования к совместно используемым узлам общедоступного распределенного реестра:

- требуется, чтобы на узлах хранились данные цепочки распределенного реестра, которая образуется с первого блока;
- требуется, чтобы статус завершения поступал на другие узлы, когда узел выполнит распределенный алгоритм подтверждения при верификации транзакции;
- в целях верификации действительности распределенного реестра, сгенерированного в каждом цикле, требуется, чтобы узел проверял действительность сгенерированного блока путем его сравнения с целевым хеш-значением;
- требуется, чтобы каждый узел обновлял и поддерживал совместно используемые данные, такие как списки открытых ключей всех других узлов, а также распределенный реестр;
- требуется, чтобы узел распространял транзакцию на другие узлы до фазы соглашения (например, завершение подтверждения транзакции) в процессе верификации транзакции.
- требуется, чтобы узел выполнял шифрование данных требующей безопасности транзакции, используя криптографические ключи (например, сертификат открытого ключа [b-ITU-T X.509], гомоморфное шифрование [b-ISO 18033-6], верифицируемая случайная функция (VRF) [b-IETF draft-irtf-cfrg-vrf-08]), и сообщал тип ключа шифрования;
- требуется, чтобы узел определял потребность в дешифровании: если дешифрование необходимо, узел выполняет дешифрование данных и их передачу запрашивающему узлу; если дешифрование не требуется, узел выполняет шифрование данных с помощью открытого ключа запрашивающего узла и их передачу.

7.2 Требования к аутентификации для нового участвующего узла

Рекомендуется, чтобы существующие узлы обеспечивали функции, описанные в пунктах 7.2.1–7.2.3, для аутентификации новых участвующих узлов в общей системе распределенного реестра.

7.2.1 Требования к запросу аутентификации нового узла

- Рекомендуется, чтобы новый узел до осуществления запроса имел для использования по крайней мере две пары ключей шифрования (например, сертификат открытого ключа [b-ITU-T X.509], ключи гомоморфного шифрования [b-ISO 18033-6]).
- Рекомендуется, чтобы новый узел выполнял шифрование сообщения запроса с помощью своего собственного закрытого ключа и отправлял узлу зашифрованные данные вместе со своим открытым ключом.

– Рекомендуется, чтобы каждый узел при верификации и передаче аутентифицированной информации обновлял список верифицированных открытых ключей новых и существующих узлов и сохранял список открытых ключей общей системы распределенного реестра для участия.

7.2.2 Функциональные требования к аутентификации узла

– Рекомендуется, чтобы узел выполнял верификацию действительности путем дешифрования зашифрованных данных, переданных новым желающим участвовать узлом вместе с открытым ключом, шифрования верифицированной информации и списка открытых ключей с использованием открытого ключа этого нового узла и передачи зашифрованной информации.

– Рекомендуется, чтобы узел содержал список открытых ключей всех узлов, участвующих в общей системе распределенного реестра, и обновлял свой соответствующий список открытых ключей каждый раз, когда он выполняет аутентификацию нового узла.

– Каждый раз, когда узлу рекомендуется обновлять свой список открытых ключей, требуется зашифровать список открытых ключей с помощью своего собственного закрытого ключа и отправить его всем узлам, участвующим в общей системе распределенного реестра.

– Рекомендуется, чтобы узел постоянно хранил верифицированную информацию об узлах, участвующих в общей системе распределенного реестра, а также время верификации и адрес участвующего узла.

7.2.3 Требования к существующим узлам в отношении верификации аутентификации нового узла

– Рекомендуется, чтобы существующие узлы выполняли верификацию цифровой подписи списка открытых ключей, отправленного узлом, и обновляли его на основе нового списка открытых ключей.

– Рекомендуется, чтобы существующие узлы выполняли верификацию участия аутентифицированного нового узла путем проверки нового списка открытых ключей.

7.3 Требования безопасности для системы распределенного реестра

Рекомендуется, чтобы существующие узлы соответствовали положениям настоящего раздела.

– Требуется, чтобы попытки манипулировать информацией в существующем совместно используемом распределенном реестре верифицировались с использованием электронной подписи и отклонялись в распределенном реестре.

– Требуется, чтобы среди основных цепочек, используемых в системе распределенного реестра, те цепочки, содержимое которых отличается от содержимого самой длинной цепочки до произвольной глубины блока b в момент создания нового блока, отклонялись в распределенном реестре. Здесь b – число, больше 1.

– Требуется, чтобы данные отклонялись в процессе создания распределенного реестра, если к системе распределенного реестра добавляются данные с дублированными адресами (например, IP, UUID).

– Требуется, чтобы общий случайный источник (например, криптографическое одноразовое случайное число [b-NIST]) был одинаковым для блоков любой глубины блока d. Требуется, чтобы блоки, добавленные к блокам с глубиной блока d, обновляли общий случайный источник, создавая новую глубину блока g. Рекомендуется, чтобы после обновления хеш-значение вновь добавленного блока использовалось в качестве случайного источника.

ПРИМЕЧАНИЕ. – Здесь глубина блока d и глубина блока g означают любые блоки, глубина которых больше 1.

– Требуется, чтобы цепочки, содержащие блоки, хеш-значения которых отличаются от хеш-значений предыдущих блоков и значений корня дерева Меркла, отклонялись в распределенном реестре.

– Рекомендуется, чтобы в случае возникновения узла с ошибкой среди узлов, составляющих систему распределенного реестра, узлы без ошибок сохранялись, если они превышают предварительно определенный уровень консенсуса для DLS.

7.4 Требования по поддержанию целостности для системы распределенного реестра

Рекомендуется, чтобы существующие узлы соответствовали положениям настоящего раздела.

- Рекомендуется, чтобы каждый узел подавлял попытки манипулирования информацией в существующем совместно используемом распределенным реестре. Рекомендуется при обнаружении такой атаки суммировать число узлов для получения коэффициента мощности хеширования. Рекомендуется сравнить текущее количество деревьев блоков с пороговым значением, для того чтобы рассчитать уровень безопасности и передать всем узлам (путем широковещательной рассылки) соответствующую информацию и адреса узлов.
- Рекомендуется, чтобы каждый узел удалял из системы распределенного реестра самые длинные цепочки, обычно используемые в системе распределенного реестра, и цепочки с различающимся содержимым.
- Рекомендуется, чтобы каждый узел удалял цепочку, содержащую блоки, хеш-значения или значения корня дерева Меркла которых отличаются от значений предыдущих блоков в распределенном реестре, и рассчитывал суммарное количество узлов, которые подверглись атакам, для того чтобы определить, безопасен ли распределенный реестр, и передавал (путем широковещательной рассылки) соответствующую информацию и адрес узла.
- Рекомендуется, чтобы в случае возникновения узла с ошибкой или поддельного узла среди компонентов системы распределенного реестра, каждый узел удалял его и суммировал количество узлов, подвергшихся попытке внести ошибку или совершить атаку, для того чтобы определить коэффициент мощности хеширования. Рекомендуется, чтобы в распределенном реестре количество безопасных узлов поддерживалось на уровне, превышающем пороговое значение, а также рекомендуется передавать (путем широковещательной рассылки) соответствующую информацию и адреса узлов.
- Рекомендуется, чтобы каждый узел отклонял данные в процессе создания распределенного реестра, если к данным системы распределенного реестра добавляются новые данные с дублированными адресами.

8 Функциональные возможности системы распределенного реестра для услуг, использующих защищенный человеческий фактор

В качестве стимула требуется улучшать качество жизни в модели услуг распределенного реестра путем автоматизации прямого распространения персональных данных, содержащих человеческий фактор. Применение технологии распределенного реестра прежде всего обеспечивает возможность отслеживать производство и распространение содержащей человеческий фактор информации и управлять ими. Иными словами, применение технологии распределенного реестра при распространении персональных данных, содержащих человеческий фактор, может обеспечить прозрачное отслеживание от процесса распределения до пути конечного использования. По этой причине отдельные лица, представленные отдельными узлами, которые участвуют в системе распределенного реестра, могут доверять распространяемой информации и использовать эту информацию. Наряду с этим возможно обеспечить метод абсолютного блокирования незаконного распространения персональных данных, содержащих человеческий фактор.

8.1 Структура распределенного реестра при распространении персональных данных, содержащих человеческий фактор

По соглашению, первой транзакцией реестра является специальная транзакция, открывающая новый стимул (например, монеты криптовалюты [b-ITU-T F.751.0]), который будет выплачен создателю реестра. Этот стимул с самого начала передается узлам в качестве вознаграждения за поддержание распределенного реестра для целей распределения персональных данных, содержащих человеческий фактор. Рекомендуется заранее согласовать методы предоставления и распределения этих стимулов, учитывая, что узлы работают как распределенные системы. Причиной постоянного добавления определенного количества новых стимулов является компенсация узлам (майнерам), которые потребляют ресурсы, для того чтобы работала система распределенного реестра. Эти узлы потребляют вычислительную мощность центрального процессора (ЦП), память и монеты.

8.2 Две функции в структуре распределенного реестра для распространения персональных данных, содержащих человеческий фактор

Для того чтобы сократить время ожидания и при этом увеличить скорость майнинга, факультативно может применяться метод декомпозиции структуры базового распределенного реестра на три функции. Этот метод можно рассматривать как выбор основной цепочки в протоколе распределенного реестра (например, метод выбора самой длинной цепочки), который ведет к выбору безопасного реестра из всех реестров на каждой глубине иерархии дерева реестра. Здесь глубина реестра определяется как расстояние от исходного реестра (количество соединенных блоков в реестре).

Реестр в распределенном реестре служит трем целям, а именно: выбор капитана, добавление транзакций в основную цепочку и голосование за реестр-предок через отношение родитель-потомок. Представляя реестр как концептуальное действие, мы разделяем его на две функции (см. рисунок 2). Функция предложения связывает транзакции одинаковой глубины в дереве исходного реестра. Функция голосования выбирает часть реестра путем голосования за транзакции одинаковой глубины в дереве реестра. Выбранный реестр берет частичные реестры транзакций и формирует конечный реестр. Функция голосования работает на той же глубине дерева реестра и создает связь родитель-потомок. Следовательно, связь родитель-потомок исходного реестра имеет две функции, которые явным образом разделены: 1) обеспечение некоторого порядка реестров в части транзакций на одинаковой глубине; 2) функция голосования, которая помогает голосовать один за другого для проверки реестра. Общая структура распределенного реестра для распространения персональных данных, содержащих человеческий фактор, показана ниже, на рисунке 2.

Распределенная природа DLS обусловливает проблемы нарушения стабильности. В DLS каждый узел может зарегистрировать транзакцию, но, в итоге, выбор узла является результатом работы алгоритма консенсуса [b-ITU-T F.751.0]. Требуется учитывать проектное решение DLS как один из нескольких факторов, влияющих на стабильность, и рекомендуется, чтобы распределенный реестр восстанавливал стабильную услугу, применяя в системе адаптивную обработку. Для того чтобы разрешить проблему нарушения стабильности DLS, общий случайный источник (например, криптографическое одноразовое случайное число [b-NIST]) сохраняется одинаковым для глубины блока d, и блоки, следующие за блоками глубиной d, должны обновлять общий случайный источник, создавая новую глубину блока g. После обновления хеш-значение вновь добавленного блока используется в качестве случайного источника. При d=1 происходит возврат к базовому правилу обновления, которое выполняет ветвление каждой "эпохи", при этом уязвимость к атакам (сбалансированным) заражения наивысшая. Для того чтобы обычным порядком повысить порог безопасности, можно увеличить значение d. При d=∞ все блоки в качестве общего случайного источника используют одноразовое случайное число исходного блока. Это протокол с самой длинной цепочкой, который не допускает ветвления, оставляя зараженному владельцу секретного ключа возможность личного прогнозирования в отношении цепочки.

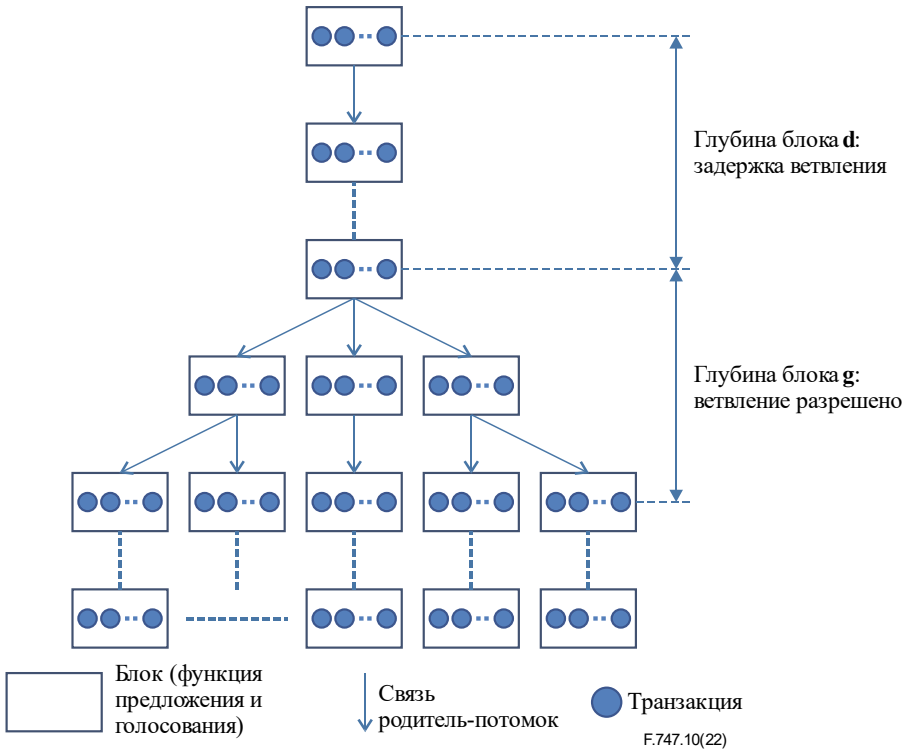

Рисунок 2 – Структура модели услуг распределенного реестра

8.3 Методики обслуживания системы распределенного реестра

Данное представление функционального разделения распределенного реестра намного сложнее по сравнению с традиционным распределенным реестром, но оно может улучшить характеристики распределенного реестра благодаря более оперативному достижению консенсуса. Эта функция быстрого получения консенсуса может увеличить количество реестров в транзакциионной части, не нарушая безопасность распределенного реестра в функции предложения. Следовательно, количество реестров будет ограничено только пропускной способностью базовой сети связи. Может выполняться факультативное подтверждение консенсуса с малой задержкой и высокой надежностью, так как функция голосования по нескольким транзакциям будет выполнять голосование параллельно с реестром предложения для оперативного подтверждения. Управление системой распределенного реестра для персональных данных, содержащих человеческий фактор, является простым благодаря существенному увеличению общей скорости генерации реестров, а количество частичных реестров функции предложения по глубине может быть небольшим.

Такая система распределенного реестра может поставить под угрозу прозрачность, если в процессе выбора реестра мощность хеширования сосредотачивается в функции предложения конкретной транзакции. Как показано на рисунке 3, высокая мощность хеширования злоумышленника в конкретном реестре функции предложения может существенно повлиять на безопасность. На рисунке 3 представлен пример цепочки реестров, которая разрушена или заражена в результате сосредоточения мощности хеширования злоумышленника. Если бы злоумышленник мог собрать больше вычислительной мощности ЦП, памяти и монет в одном месте, чем все защищенные узлы, злоумышленник должен был бы решать, использовать ли эту мощность для кражи стимулов честных узлов или для сотрудничества. Необходимо предусмотреть такую политику стимулов, чтобы злоумышленнику выгоднее было следовать правилам, чем подрывать прозрачность системы распределенного реестра с персональными данными, содержащими человеческий фактор. Требуется, чтобы такой стимул был адаптирован к распределению между всеми участвующими узлами. Злоумышленник может предусмотреть такое правило, которое сделает более выгодным связь со всеми другими узлами. Такое правило рекомендуется, для того чтобы поддерживать количество честных узлов больше порогового уровня (например, CD $(1 + \alpha)/(\alpha - 1)/\log(\alpha)$), в зависимости от коэффициента мощности хеширования злоумышленника (α). Здесь C и D – пропускная способность и задержка сетей связи.

Из приведенной формулы следует, что если значение α близко к 0, мощность хеширования злоумышленника слабая, то есть можно говорить об отсутствии проблемы нарушения безопасности систем распределенного реестра даже при малом количестве блоков дерева избирателя. Однако, если значение α близко к 1, то есть мощность хеширования злоумышленника высокая, количество блоков дерева избирателя должно увеличиваться экспоненциально. На этом этапе можно заметить, что уязвимость безопасности становится очень высокой.

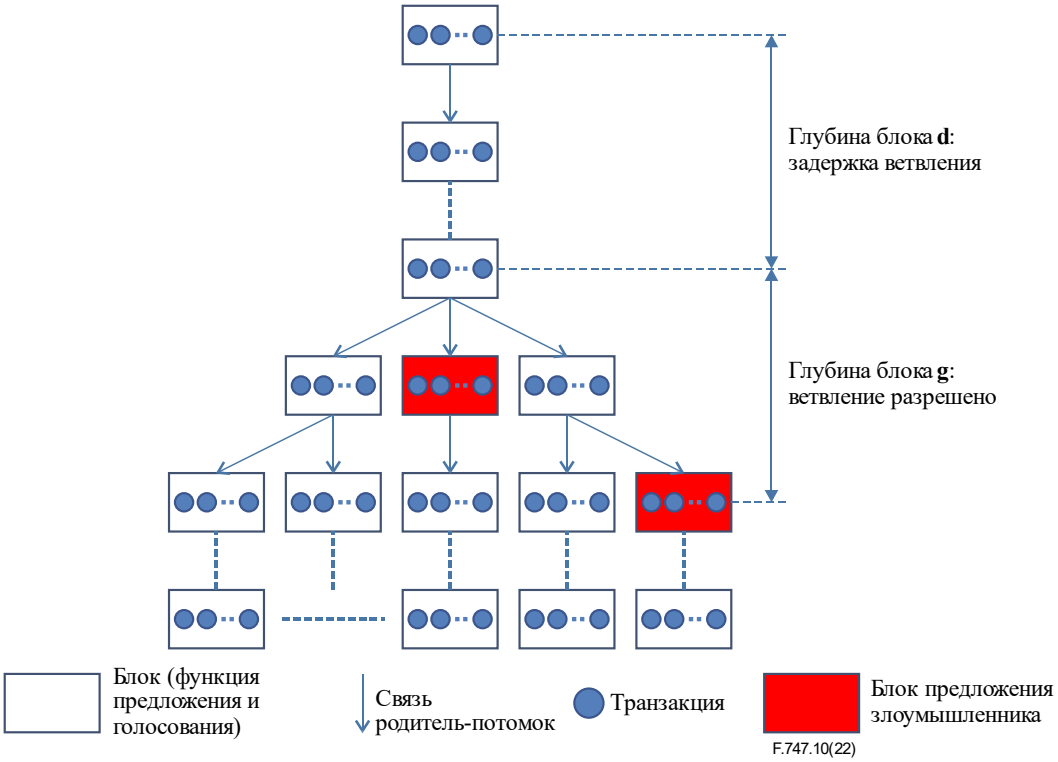

Рисунок 3 – Пример предотвращения заражения в модели услуг распределенного реестра

В процессе выбора блока предложения рекомендуется определить функцию блока путем регулирования мощности хеширования и монет. В это же время можно заметить, что если злоумышленник обладает высокой мощностью хеширования и большим количеством монет, безопасность весьма уязвима. Если бы злоумышленник мог собрать больше вычислительной мощности и монет, чем все защищенные узлы, пришлось бы принимать решение, использовать ли эту мощность для кражи стимулов честных узлов или для сотрудничества. Рекомендуется предусмотреть такую политику стимулов, чтобы злоумышленнику более выгодно было следовать правилам, чем подрывать систему и легитимность своего собственного богатства. Используя политику, направленную на предотвращение концентрации прибыли в каком-либо конкретном блоке предложения, рекомендуется установить такое правило, которое сделало бы для злоумышленника более выгодным распределение прибыли между всеми другими узлами.

Приложение A

Применение модели услуг распределенного реестра, использующих защищенный человеческий фактор

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Сценарий использования распределенного реестра, показанный на рисунке A.1, может обеспечить безопасное и прозрачное управление не только персональными данными, содержащими человеческий фактор, которые находятся в ведении больниц, но также и данными, содержащими человеческий фактор, которые хранятся у отдельных лиц, например на персональных устройствах сбора медицинских данных. В примере использования персональных медицинских данных, представленном на рисунке A.1, надежность может быть обеспечена путем использования распределенного реестра, в котором участвует несколько узлов, а для обеспечения прозрачности данных поиска могут использоваться цифровые подписи и хеш-значения. Однако персональные данные, содержащие человеческий фактор, могут быть весьма чувствительными в аспекте защиты данных. Такие секретные данные регистрируются в зашифрованном виде с использованием метода шифрования, способного обрабатывать большие данные. Процедура обеспечения мобильности для секретных персональных данных, содержащих человеческий фактор, отвечает требованиям и процедурам общей системы распределенного реестра, которые описаны в разделе 7.2, с использованием алгоритма шифрования (см рисунок A.1). Кроме того, требуется, чтобы система распределенного реестра для персональных данных, содержащих человеческий фактор, работала таким образом, чтобы удовлетворять требованиям функции стимулов, которые описаны в разделе 8.3, для активации обслуживания.

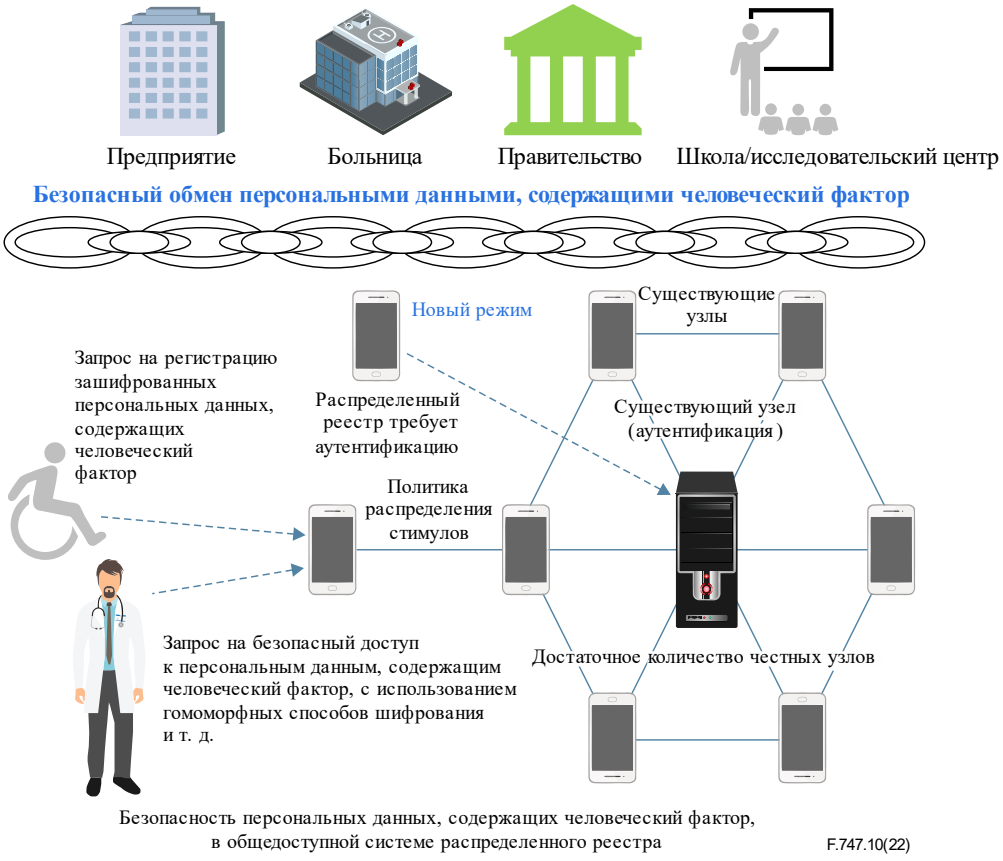

Рисунок A.1 – Сценарии для модели защищенных услуг распределенного реестра

Библиография

[b-ITU-T F.751.0] Рекомендация МСЭ-Т F.751.0 (2020 г.), *Требования к системам распределенного реестра.*

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

[b-ITU-T TS FG DLT D1.1] Technical Specification ITU-T FG DLT D1.1 (2019), *Distributed ledger technology terms and definitions.*

[b-IETF draft-irtf-cfrg-vrf-08] IETF draft-irtf-cfrg-vrf-08 (2020), *Verifiable Random Functions (VRFs)*. https://tools.ietf.org/html/draft-irtf-cfrg-vrf-08

[b-ISO 6385] ISO 6385:2016, *Ergonomics principles in the design of work systems.*

[b-ISO 18033-6] ISO 18033-6:2019, *IT Security techniques – Encryption algorithms – Part 6: Homomorphic encryption.*

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary.*

[b-NIST] NISTIR 8202 (2018). *Blockchain Technology Overview*.

[b-WHO] World Health Organization (2006), *Constitution of the World Health Organization – Basic Documents, Forty-fifth edition, Supplement.*

[b-Wickens] Wickens, D., Gordon, S., Liu, Y. (1997), *An Introduction to Human Factors Engineering*. pp. 2-7. New York, NY: Longman.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2022 г.