ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 27.018— 2021 (МЭК 62673:2013)

НАДЕЖНОСТЬ В ТЕХНИКЕ

Методы оценки и обеспечения надежности коммуникационной сети

(IEC 62673:2013, Methodology for communication network dependability assessment and assurance, MOD)

Издание официальное

Москва
Российский институт стандартизации
2021

Предисловие

1 ПОДГОТОВЛЕН Закрытым акционерным обществом «Научно-исследовательский центр контроля и диагностики технических систем» (ЗАО «НИЦ КД») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 119 «Надежность в технике»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 8 октября 2021 г. № 1102-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту МЭК 62673:2013 «Методы оценки и обеспечения надежности коммуникационной сети» (IEC 62673:2013 «Methodology for communication network dependability assessment and assurance», MOD) путем внесения технических отклонений, объяснение которых приведено во введении к настоящему стандарту.

Международный стандарт разработан Техническим комитетом по стандартизации ТК 56 Международной электротехнической комиссии (МЭК).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте, приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

Содержание

Введение

На надежность коммуникационной сети большое влияние оказывают проектирование и реализация функций обслуживания сети, которые направлены на обеспечение удовлетворенности пользователей качеством обслуживания.

Эволюция сети, рост услуг и функциональное обновление в коммуникациях долгое время были проблемами для поставщиков коммуникационных услуг, причем не только по широкому спектру существующих услуг, но и для тех видов деятельности, которые связаны с услугами, используемыми конечными пользователями.

Для поддержания жизнеспособного бизнеса в области услуг коммуникационных сетей целесообразно при создании сети обеспечить:

- предоставление необходимых функций услуг сети;
- адекватные мощность и возможности сети;
- безопасность услуг;
- качество услуг;
- надежность услуг.

В настоящем стандарте рассмотрен один из наиболее важных вопросов, касающихся оценки и обеспечения надежности услуг коммуникационной сети. В стандарте рассмотрены стратегии обеспечения надежности сети и методы поддержания и улучшения работы сети.

В настоящем стандарте рассмотрены общие методы оценки и обеспечения надежности коммуникационных сетей. В стандарте также представлены методы оценки и обеспечения обслуживания коммуникационных сетей при разработке их надежности в соответствии с МСЭ-Т[1)] (см. также *[1]*).

В стандарте представлен подход к анализу и оценке надежности сети, который обеспечивает надежность сети при проектировании для успешного ее изготовления.

Целью настоящего стандарта является формирование экономически эффективного решения для достижения показателей надежности сети и обеспечения преимуществ надежной сети при предоставлении услуг.

В настоящем стандарте ссылки на международные стандарты заменены ссылками на национальные стандарты.

[1)] МСЭ-Т — Международный союз электросвязи. Сектор стандартизации по телекоммуникациям.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

НАДЕЖНОСТЬ В ТЕХНИКЕ

Методы оценки и обеспечения надежности коммуникационной сети

Dependability in technics.
Methodology for communication network dependability assessment and assurance

Дата введения — 2022—01—01

1 Область применения

В настоящем стандарте приведены общие методы оценки и обеспечения надежности коммуникационных сетей (сетей связи, телекоммуникационных сетей) на всех стадиях жизненного цикла сети. В стандарте представлены стратегии оценки надежности сети и методы анализа топологии сети, оценки надежности способов оказания услуг и оптимизации конфигураций сети с целью обеспечения надежности сети и надежности ее услуг. В стандарте также рассмотрены стратегии обеспечения надежности сети и методы проверки работоспособности сети, управления отключением сети и тестовыми случаями для улучшения и поддержания предоставления услуг сети.

Настоящий стандарт применим поставщиками коммуникационных услуг, проектировщиками и разработчиками сетей, а также обслуживающим персоналом и операторами сети для обеспечения надежности работы сети и оценки надежности предоставления коммуникационных услуг.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 27.015 (МЭК 60300-3-15:2009) Надежность в технике. Управление надежностью. Руководство по проектированию надежности систем

ГОСТ Р 27.101 Надежность в технике. Надежность выполнения задания. Термины и определения

ГОСТ Р 27.102 Надежность в технике. Надежность объекта. Термины и определения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по *[2]*, *ГОСТ Р 27.101*, *ГОСТ Р 27.102*, а также следующие термины с соответствующими определениями:

3.1.1 **коммуникационная сеть** (communication network): Система коммуникационных узлов и соединений, обеспечивающая передачу аналоговых и цифровых сигналов.

Пример — Телекоммуникационные сети, интернет, интранет, экстранет, широкополосные сети (WAN), локальные сети (LAN) и компьютерные сети с использованием информационных технологий.

Примечания

1 Сеть имеет свои границы. Все узлы на границе сети называются концами. В некоторых приложениях термин «узел» используют вместо термина «конец» в качестве точки доступа к сети, а также для соединений линий передачи данных.

2 «Магистральная» коммуникационная сеть состоит из основной сети и высокоскоростных линий передачи (национальных или международных), соединяющих основные узлы коммуникационной сети (соединение линий передачи) в различных точках страны или региона.

3.1.2 **надежность, надежность сети** (dependability, network dependability): Способность выполнять требуемые функции в соответствии с установленными требованиями к коммуникации и эксплуатации сети.

3.1.3 **готовность, готовность сети** (availability, network availability): Способность быть в состоянии работать в соответствии с установленными требованиями.

Примечания

1 Готовность зависит от сочетания свойств безотказности, восстанавливаемости и ремонтопригодности сети, а также от выполнения технического обслуживания.

2 Готовность может быть определена количественно с использованием соответствующих показателей.

3.1.4 **безотказность, безотказность сети** (reliability, network reliability): Способность работать в соответствии с установленными требованиями без отказов в течение заданного периода времени в заданных условиях.

Примечания

1 Продолжительность периода времени может быть выражена в единицах, соответствующих сети.

2 Надежность выполнения услуг сети (предоставления пользователю услуг сети по его запросу) зависит от комбинации свойств безотказности, восстанавливаемости, ремонтопригодности и обеспеченности техническим обслуживанием составляющих сеть элементов.

3 Заданные условия включают аспекты, влияющие на безотказность, такие как: режим работы, уровень нагрузки, условия окружающей среды.

4 Безотказность может быть количественно оценена с использованием соответствующих показателей.

3.1.5 **ремонтопригодность, ремонтопригодность сети** (maintainability, network maintainability): Способность сохранения или восстановления сети до состояния, позволяющего работать в соответствии с установленными требованиями в заданных условиях эксплуатации и заданном уровне технического обслуживания.

Примечания

1 Заданные условия включают аспекты, влияющие на ремонтопригодность, такие как: места технического обслуживания, процедуры технического обслуживания и ресурсы технического обслуживания.

2 Ремонтопригодность может быть количественно оценена с использованием соответствующих показателей.

3.1.6 **обеспеченность техническим обслуживанием, обеспеченность техническим обслуживанием сети** (maintenance support, network maintenance support). Обеспеченность ресурсами, необходимыми для выполнения технического обслуживания сети.

Примечание — Ресурсы включают человеческие ресурсы, вспомогательное оборудование, материалы и запасные части, средства технического обслуживания, документацию, информацию и информационные системы технического обслуживания.

3.1.7 **результативность обеспеченности техническим обслуживанием, эффективность обеспеченности техническим обслуживанием сети** (maintenance support performance, network maintenance support performance): Результативность организации технического обслуживания сети.

Примечание — Показатель обеспеченности техническим обслуживанием может быть количественно оценен с использованием соответствующих показателей.

3.1.8 **восстанавливаемость, восстанавливаемость сети** (recoverability, network recoverability): Свойство объекта восстанавливаться после отказа без корректирующего технического обслуживания.

Примечания

1 Восстанавливаемость может требовать или не требовать внешних действий.

2 Восстанавливаемость может быть количественно оценена с использованием такого показателя, как вероятность восстановления в течение определенного периода времени.

3.1.9 **элемент, элемент сети** (element, network element): Подсистема или компонент коммуникационной сети.

Пример — Терминалы, узлы и коммутаторы.

Примечания

1 Элементом сети может быть ввод данных человеком для выполнения своей сервисной функции.

2 Элементы сети объединены сетевыми соединениями.

3.1.10 **соединение, сетевое соединение** (link, network link): Электрическое, беспроводное или оптическое соединение узлов сети.

3.1.11 **работа, работа сети** (performance, network performance): Способность (сети) поставлять сервисные функции, связанные с коммуникациями между пользователями.

Примечание — См. *[3]*.

3.1.12 **управление, управление сетью** (management, network management): Применение организованных процессов и ресурсов для управления работой, конфигурацией, учетом, неисправностями и безопасностью сети.

3.1.13 **сервисная функция, функция услуги сети** (service function, network service function): Программа или приложение, взаимодействующее с пользователями сети или внутренней инфраструктурой сети для передачи или обмена данными и информацией в сети.

Примечание — Функция услуги сети может состоять из аппаратных и программных элементов и может включать в себя взаимодействия между людьми для реализации конкретной функции.

3.1.14 **услуги сети** (network services): Обеспечение выполнения функций услуг сети и коммуникационных услуг, оказываемых пользователям сети.

Примечания

1 Коммуникационные услуги — это услуги сети, на которые подписаны конечные пользователи.

2 Услуга — это коммуникационная функция, которая позволяет передавать информационные сигналы пользователя между пользовательскими сетевыми интерфейсами.

3.1.15 **качество услуги** (quality of service): Совокупность характеристик выполнения услуги, определяющих степень удовлетворенности пользователя услугой.

3.1.16 **отказ сети** (network failure): Потеря способности сети выполнять требуемые функции.

Примечание — Отказ сети может быть вызван, например, отказом оборудования, стихийными бедствиями или действиями человека.

3.1.17 **неисправность сети** (network fault): Состояние неспособности сети выполнять требуемые функции по внутренней причине.

Примечания

1 В условиях работы сети неисправность может быть естественной из-за ненормальных условий или неисправности, вызванной отказом элемента сети, или вызванной внешними средствами, такими как неисправность устройств ввода.

2 Состояние ухудшения работы сети — это ситуация, когда один или несколько показателей работы сети не соответствуют требованиям.

3.1.18 **поставщик услуг, провайдер услуг** (service provider): Организация, предоставляющая услуги коммуникационной сети.

Пример — Телефонные компании, операторы передачи данных, операторы мобильной связи, интернет-провайдеры и операторы кабельного телевидения.

Примечание — Сетевым провайдером или общим провайдером является организация, которая предоставляет продукт или услугу, используя свои технические средства или технические средства других провайдеров, и предлагает услуги широкой аудитории.

3.1.19 **пользователь** (user): Сторона, которая использует услуги поставщика услуг для прямого доступа к сети.

Примечания

1 Пользователь может быть источником или получателем информации пользователя или и тем, и другим.

2 В некоторых случаях пользователя услуг связи также называют абонент.

3.1.20 **целостность, целостность сети** (integrity, network integrity): Способность гарантировать, что содержимое данных не заражено, не повреждено, не потеряно и не изменено между передачей и приемом.

Примечание — Пропускная способность — это интенсивность (объем передаваемой информации в единицу времени) успешной доставки сообщений по каналу связи услуги сети.

3.1.21 **надежность работы, надежность работы сети** (dependability performance, network dependability performance): Способность сети обеспечивать или демонстрировать характеристики надежности работы в эксплуатации в соответствии с целями предоставления услуг сети.

Примечания

1 В контексте настоящего стандарта надежность работы сети связана с обеспечением услуг сети «из конца в конец сети» (E2E).

2 Услуга сети (E2E) — это обеспечение выполнения услуги сети, устанавливающей соединения передающих и принимающих концов коммуникационной сети.

3.1.22 **надежность услуги, надежность услуги сети** (dependability of service, network dependability of service): Результат обеспечения требуемой надежности работы сети для пользователей коммуникационных услуг.

Примечания

1 В контексте настоящего стандарта надежность услуги сети относится к обеспечению сквозных услуг сети (E2E).

2 Сквозная услуга сети — это обеспечение услуги связи, установленной между передающим и принимающим концами коммуникационной сети.

3.1.23 **безопасность услуги, безопасность услуги сети** (security of service, network security of service): Результат обеспечения необходимой безопасности коммуникационных услуг для пользователя.

3.1.24 **путь услуги, путь услуги сети** (service path, network service path): Путь, установленный последовательностью соединений и узлов для обеспечения пользователя коммуникационной услугой.

3.1.25 **поток услуг, поток услуг сети** (service flow, network service flow): Поток информации и данных по пути услуг.

3.1.26 **сценарий услуги** (service scenario): Способ обеспечения пользователей функциями услуг сети и их применением при эксплуатации коммуникационной сети.

3.1.27 **отключение сети** (network outage): Состояние сети, при котором она не способна выполнять свою основную функцию.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

E2E — из конца в конец;

FRACAS — отчет об отказах, анализ системы и корректирующие действия;

FRU — объект, возвращенный в эксплуатацию;

HAZOP — исследование опасности и работоспособности;

MTTR — среднее время восстановления узла/соединения;

ND — надежность сети;

NFIT — тест введения неисправности в сеть;

NFMECA — анализ видов, последствий и критичности отказов сети;

OAMP — эксплуатация, администрирование, техническое обслуживание и подготовка к работе;

QoS — качество услуги;

RBD — структурная схема расчета надежности;

SLB — логический блок услуги.

4 Обзор методов надежности сети

4.1 Необходимость применения методов надежности сети

Коммуникационная сеть — это система, состоящая из систем, которые взаимодействуют с другими сетями для достижения нескольких целей выполнения услуг. Коммуникационная сеть сложна, а составляющие ее системы постоянно изменяются и развиваются. Для оценки и обеспечения надежности сети необходимы соответствующие методологические и технические подходы.

С точки зрения оценки надежности сети классические методы анализа и оценки надежности имеют ограниченную область применения. Существующие методы надежности часто непригодны для моделирования сложной топологии сети и сложны для анализа множества конфигураций сети и путей услуг сети при подтверждении выполнения установленных требований. Селективные методы, такие как SLB, NFMECA и сетевое моделирование, подходящие для анализа и оценки надежности сети, могут обеспечить более эффективные сетевые решения. Данные методы являются важными процессами обеспечения устойчивости услуг сети и надежности работы сети.

Общий подход к обеспечению надежности работы сети и надежности услуг заключается в построении структуры безотказности сети, установлении эффективных схем маршрутизации, обеспечении эффективного управления неисправностями и обеспечении технического обслуживания сети, а также сборе данных об эффективности и обратной связи с пользователями для оценки и улучшения качества услуг сети. Данный процесс включает в себя анализ функций услуг сети для экономически эффективной реализации и оценку дополнительных свойств услуг сети для повышения надежности услуг. Данный подход, хотя и является адекватным для оценки жизненного цикла системы аппаратных и программных элементов сети, при установлении показателей надежности работы сети не подходит для работы с маршрутизацией подключения пользовательских услуг. Традиционному подходу к обеспечению безопасности не хватает быстроты реагирования на динамику рынка адаптивных конфигураций сети. Это влияет на цели предоставления услуг сети при обеспечении надежности работы сети и гарантии надежности услуг в высоко конкурентном глобальном коммуникационном бизнесе.

Существует много разработанных ранее методов обеспечения надежности, но лишь некоторые из них обеспечивают методологию, соответствующую результативной работе сети и надежности услуг. Это связано, прежде всего, со сложным характером эволюции сети; инновационной топологией разработки передовых функций услуг сети и уникальными методами, необходимыми для практического применения методов надежности. В то время как существует множество факторов, которые могут повлиять на надежность сети на стадиях ее жизненного цикла, наиболее значимое влияние может быть оказано на ранних стадиях концепции и определения, проектирования и разработки и изготовления и интеграции. Новые дополнения к существующей сети требуют применения анализа сценариев существующей системы на стадии концепции и определения до инвестиций в последующие стадии проектирования и разработки, изготовления и интеграции. Объем потребностей на стадиях эксплуатации и технического обслуживания, улучшения и обновления и вывода из эксплуатации должен быть включен в сценарий анализа существующей системы. Необходимо постоянно проводить мониторинг, анализ и оценку надежности работы сети и надежности услуг сети для оптимизации сетевых операций и формирования экономически эффективных коммуникационных услуг. Стратегии обеспечения надежности сети и применения методологии являются ключевыми факторами, способствующими расширению и поддержанию непрерывного предоставления коммуникационных услуг с точки зрения бизнеса.

4.2 Цели обеспечения надежности сети

Способность сети обеспечивать коммуникации пользователей при непрерывной и бесперебойной работе услуг в значительной степени зависит от надежности сети. Надежность подразумевает, что предоставление функций услуг сети заслуживает доверия, и сеть способна выполнять необходимую

услугу по запросу. Для достижения требуемой работы сети и обеспечения надежности услуг сети необходимо использовать соответствующие методы оценки надежности сети. Настоящий стандарт поддерживает инженерные требования к проектированию сетей и выполнению процессов, а также обеспечивает соответствующую методологию анализа и оценки надежности коммуникационных сетей. К настоящему стандарту применимы положения *ГОСТ Р 27.015* в части надежности систем (см. также *[2]* в части разработки надежности сетей). Термины, относящиеся к качеству коммуникационных услуг, приведены в *[4]*.

При разработке и изготовлении коммуникационных сетей существует несколько важных влияющих факторов, которые касаются операторов сетей и поставщиков услуг для поддержания жизнеспособного бизнеса. Они включают в себя:

- функции услуг сети для удовлетворения потребностей пользователей;
- возможности работы сети в соответствии с запросами услуги;
- безопасность услуги;
- качество услуги (QoS) *[5]*;
- надежность услуги.

При оценке и обеспечении надежности сети следует отметить, что:

a) функциональные параметры сети, такие как пропускная способность и возможность подключения, ухудшаются во времени из-за отказов, и это влияет на надежность сети;

b) устойчивость сети при нарушении ее работы из-за внешнего вторжения и/или внешних прерываний работы влияет на защиту критической инфраструктуры сети от критических воздействий.

4.3 Сценарии услуги сети

Существует два сценария услуг сети, связанных с обеспечением надежности сети:

a) Надежность услуги подключения конечных пользователей к сквозным услугам сети (E2E) (см. А. 2). Цель состоит в определении характеристик надежности работы сети на услугах сети E2E с точки зрения конечных пользователей сети. Услуга сети E2E — это важнейшая услуга для удовлетворения потребностей конечных пользователей, основанная на способности работы сети при выполнении услуг. В сценарии услуг сети E2E надежность услуг устойчива на схемах маршрутизации, а способность сети работать связана с установленными путями услуг, выбранными для соединений E2E. Надежность услуги ощущают конечные пользователи, она отражает требования потребителей и удовлетворенность пользователей.

b) Целью надежности работы сети, включая все концевые узлы (далее — сети в целом) (см. В.2), является определение показателей надежности работы сети с точки зрения оператора сети или поставщика услуг сети. Сеть в целом может работать в соответствии со сценарием выполнения услуг, где поставщик услуг имеет полный контроль над частной сетью и несет ответственность за обеспечение надежности работы сети, соответствующей услугам сети в целом. Сеть в целом также может работать в соответствии со сценарием услуг с несколькими поставщиками услуг, каждый из которых контролирует определенный сегмент всей сети, когда общая сеть — это сеть коммутации. Оператор сети несет ответственность за работу сети. Отдельные поставщики услуг несут ответственность за свой вклад в выполнение услуг сети, в соответствии с соглашениями об уровне услуг с сетевым оператором при обеспечении качества услуг (QoS).

Сценарии выполнения услуг сети, связанные с E2E, и выполнение услуг сети в целом являются взаимозависимыми и взаимодополняющими. Следует отметить, что без надежной работы приемлемые пользовательские услуги не могут быть выполнены или гарантированы, а без удовлетворенности пользователей надежностью услуг поставщик услуг испытывает трудности в поддержке потребностей пользователей в обслуживании и может потерять пользователей, следовательно, это влияет на его доход. Соответствующая информация обратной связи от пользователей сети и данные о работе сети, собранные и проанализированные в соответствии с этими двумя сценариями, облегчают планирование ресурсов и контроль обеспечения качества услуг абонентам или пользователям, а также поддерживают надежность услуг сети в целом.

Надежность работы сети и надежность услуг отражают сценарии услуг сети и условия работы при ведении бизнеса. Это достигается с помощью оценки и обеспечения надежности работы сети при ее разработке и обеспечения надежности услуг при работе сети.

Стратегии оценки надежности сети и обеспечения ее надежности изложены в 4.4 и 4.5. Методы надежности и методы использования сети приведены в разделе 5.

4.4 Методы оценки надежности сети

Оценка надежности — это процесс оценки, позволяющий определить состояние работы сети для обеспечения надежности услуг. Ниже описаны стратегии оценки надежности сети, соответствующие сценариям выполнения услуг сети.

a) Стратегия оценки надежности сети E2E

Надежность сети E2E зависит от топологии сети, схем маршрутизации и выбора путей выполнения услуг для обеспечения соединений при обслуживании пользователя. Для оценки надежности сети E2E необходимо проанализировать пути маршрутизации услуг, связанных со сценариями выполнения услуг. Все оборудование и все соединения каждого пути выполнения услуг должны быть оценены для обеспечения и выполнения надежной услуги. Оценка надежности сети E2E охватывает различные сценарии выполнения услуг сети в публичных и частных сетях.

Стратегия оценки сети E2E должна предусматривать технический подход к оценке надежности услуги. Это относится к многочисленным путям выполнения услуг, которые необходимо проанализировать для оптимизации надежности услуги. Сложная конфигурация сети требует применения уникального метода моделирования и методологии, состоящей из диаграмм логических блоков услуг (SLB) (см. пункт А.3) для облегчения оценки надежности услуг сети E2E.

b) Стратегия оценки надежности сети в целом

Сеть в целом, работающая в соответствии со сценарием услуг, состоит из множества взаимодействующих сетей, предлагающих различные функции услуг нескольких поставщиков услуг. Обеспечение надежности работы сети — это совместные усилия поставщиков услуг в рамках соглашений об уровне обслуживания для обеспечения качества услуг. Вероятность безотказной работы функции сети в целом может быть смоделирована с помощью RBD *[6]* или аналогичных методов. Оценка надежности сети в целом может быть практически установлена только после выполнения услуг сети с помощью обследования работы сети и обработки данных обратной связи об удовлетворенности потребителей для получения соответствующих данных о работе сети. Это связано со сложностью эволюции сети, в которую постоянно добавляют новые функции услуги для улучшения работы и устраняют устаревшие или нерентабельные услуги. Публичная коммутационная сеть является примером того, как надежность работы сети может быть оценена путем анализа и оценки сообщаемой частоты отключений обслуживания пользователей, продолжительности отключений и жалоб потребителей на услуги. Результаты оценки включают классификацию отключений, связанных с выявленными причинами отказов, и их влияния на обслуживание абонентов или пользователей сети.

Сеть в целом может быть частной сетью и принадлежать одному оператору, который имеет полный контроль за предоставлением услуг сети. Защищенная сеть передачи данных, состоящая из автоматических банкоматов для предоставления распределенных банковских услуг, является примером частной сети. Для оценки надежности работы частной сети в целом необходимо определить все элементы сети и их взаимосвязи, а также оценить все соответствующие характеристики надежности работы на соответствие установленным критериям. Технические процессы оценки надежности сети анализируют и оценивают как систему с граничными условиями. При разработке новой сети следует рассмотреть процесс жизненного цикла сети и выполнить инженерные работы по обеспечению надежности в соответствии с рекомендуемыми руководящими принципами *[1]*. Для проектов по улучшению и обновлению сети важно учитывать унаследованные проблемы существующих конфигураций сети для оптимизации работы обновленной сети. Статистические данные об эксплуатации сети должны быть собраны и проанализированы для подтверждения работы сети в соответствии с целями услуг сети.

4.5 Стратегии обеспечения надежности сети

Стратегии обеспечения надежности сети — это планируемые мероприятия, включающие систематические процессы по обеспечению надежности сети при ее работе и предоставлению потребителю надежных услуг. Стратегии обеспечения надежности сети отражают соответствующие технические области применения конкретных сетей. Они включают в себя управление работой сети и регулярные мероприятия по техническому обслуживанию и поддержке сети. Стратегии обеспечения надежности конкретной сети обобщают с точки зрения эксплуатации сети.

a) Обеспечение надежности услуг для конечных пользователей

Существуют два отдельных стратегических вопроса, касающихся обеспечения надежности услуг: один касается вклада в обслуживание способа доставки функций оборудования сети и функциональной совместимости; другой касается поставки услуг в виде передачи информации и данных, в том

числе пропускной способности в соответствии с использованным способом доставки услуг согласно конфигурации сети. Стратегии конкретных применений сосредоточены на способе доставки и обеспечении целостности данных.

b) Обеспечение целостности данных

Целостность данных является основой для генерации достоверной информации и передачи данных по путям услуг, которые представляют собой способ доставки в соответствии с конфигурацией сети. Установленная стратегия обработки данных ориентирована на надежность работы сети и способность предотвращения потери данных, их повреждения или угрозы безопасности.

c) Улучшение работы функций и процессов поддержки сети

Функции работы сети и процессы сопровождения имеют тенденцию к ухудшению без должного обслуживания и регулярного обновления. Это приводит к постепенному ухудшению работы сети, к частым отключениям сети и увеличению продолжительности простоев; следовательно, влияет на работу сети и качество услуг. Стратегия обеспечения технического обслуживания сети для обеспечения надежности заключается в постоянном улучшении для оптимизации функций сети и упрощения процедур процессов обслуживания сети. Цель состоит в улучшении критических параметров работы сети, связанных с такими свойствами, как восстанавливаемость, готовность, безотказность, ремонтопригодность и обеспеченность техническим обслуживанием. Непрерывное улучшение сети имеет важное значение для поддержания операций обслуживания сети и обеспечения удовлетворенности конечных пользователей. Стратегия гарантии работы сети предусматривает корректирующие и превентивные меры, чтобы избежать повторения проблем работы сети.

5 Применение методологии надежности сети

5.1 Процессы жизненного цикла сети

5.1.1 Применение процессов жизненного цикла

Применение процессов жизненного цикла сети включает в себя действия по обеспечению надежности для достижения целей работы сети. Стадии жизненного цикла сети включают концепцию и определение, проектирование и разработку, изготовление и интеграцию, эксплуатацию и техническое обслуживание, улучшение и обновление, и вывод из эксплуатации. Определены соответствующие методы анализа и оценки надежности сети. Цель состоит в обеспечении выполнения требований к надежности сети путем разумного применения соответствующих методов обеспечения надежности работы сети для достижения требуемой надежности услуг.

Конкретные сети отличаются друг от друга границами и условиям выполнения услуг. Следует установить сценарий функционирования сети, обеспечивающий выполнение основных услуг сети. Соответствующие методы анализа и оценки должны быть определены на ранних этапах разработки концепции сети, чтобы максимизировать преимущества надежной работы сети. Данный процесс помогает обеспечить надежность предоставления услуг сети и удовлетворенность пользователей. Технический подход и процесс выполнения описаны здесь для облегчения применения методологии. Для анализа услуг сети должны быть определены соответствующие входные и выходные данные. Своевременное реагирование на собранные данных, анализ и интерпретация результатов оценки, а также оценка риска, как часть процесса обеспечения надежности, должны стать основой для рекомендаций по улучшению надежности сети.

5.1.2 Применение процесса оценки риска

Оценка риска *[5], [6], [7]* — это процесс, охватывающий идентификацию риска, анализ риска и количественную оценку риска. Оценка риска обеспечивает понимание влияния риска, причин и последствий риска, которые являются полезными входными данными для принятия решений на стадиях жизненного цикла сети. Информация, полученная в результате процесса оценки риска, может внести значительный вклад в принятие важных деловых и проектных решений, в том числе при принятии основных обязательств в отношении ресурсов. Эту информацию используют для поддержки анализа влияния бизнеса, связанного с рисками и преимуществами. Анализ влияния бизнеса необходимо проводить в сочетании с анализом сценариев выполнения услуг при рассмотрении инвестиционных рисков и планов восстановления для предотвращения возможных потерь или повреждений критических функций сети.

Конкретные действия по обеспечению надежности при проектировании часто включают в себя применение вероятностных распределений и методов статистического анализа. Риски, связанные с

такой проектной деятельностью, требуют использования соответствующих методов оценки риска для рассмотрения возможных преимуществ и вероятных негативных последствий, возникающих в результате применения проекта, влияния бизнеса и технических проблем при работе с неопределенностями. Процесс оценки риска представляет собой основанный на фактических данных подход к определению уровня экспозиции риска. Оценка риска должна основываться на соответствующих данных и практическом опыте.

Процесс оценки риска включает в себя:

- признание возможных положительных и отрицательных последствий идентифицированного риска,
- понимание источников причин и последствий риска, и вероятности реализации последствий,
- принятие решения о значимости риска, если он находится в пределах установленных критериев риска.

После завершения оценки риска может быть принято решение об обработке риска. Обработка риска включает в себя выбор и согласование одного или нескольких релевантных вариантов изменения вероятности возникновения и воздействия риска и реализации этих вариантов. Примеры включают в себя устранение риска, принятие риска без каких-либо действий или изменение уровня риска. Могут быть также приняты решения о сохранении риска или разделении его с другой стороной посредством договора или страхования.

Типы методов оценки риска *[8]*, применимых к инженерной деятельности по обеспечению надежности, могут быть сгруппированы следующим образом:

- анализ сценариев — примеры: анализ первопричин, анализ дерева неисправностей, анализ дерева событий, анализ влияния на деятельность, анализ причин и воздействий, анализ причин и последствий;
- функциональный анализ — примеры: FMECA *[9]*, техническое обслуживание, ориентированное на безотказность *[10]*, HAZOP *[11]*;
- статистические методы — примеры: моделирование Монте-Карло *[12]*, марковский анализ *[13]*.

Приведенные выше методы оценки риска являются установленными стандартизованными методами анализа, рекомендованными для применения *[12]*. Подробное описание методов оценки риска приведено в *[8]* и *[12]*. Они не приведены в настоящем стандарте.

5.1.3 Применение методологии надежности

Существуют два основных аспекта применения методологии надежности, связанных с жизненным циклом сети.

a) Оценка надежности сети

Оценка надежности сети — это применение анализа, тестирования (испытаний), верификации и сравнительной оценки при разработке сети. Эти методы используют на ранних стадиях жизненного цикла сети (концепции и определения, проектирования и разработки, реализации и интеграции). Цели оценки сосредоточены на выполнении требований к надежности работы сети до введения сети в эксплуатацию и предоставления услуг. Некоторые из методов оценки, такие как FRACAS и оценка риска, являются основной частью процессов анализа и оценки, установленных для облегчения сбора информационных данных о сети для прогнозирования тенденций изменения надежности на стадиях эксплуатации и технического обслуживания сети и поддержки решений по улучшению и обновлению сети. Применение методов оценки надежности описано в 5.3.

b) Обеспечение надежности сети

Обеспечение надежности сети — это подходы и процессы, выполняемые на стадиях эксплуатации и технического обслуживания, улучшения и обновления сети. Цели обеспечения надежности сети сосредоточены на конкретных проблемах надежности работы сети, требующих решения при ее эксплуатации. Это позволяет улучшить работу сети и выполнение услуг. Мероприятия по обеспечению надежности действуют вместе с управлением работой сети, системами управления неисправностями сети и регулярными мероприятиями по техническому обслуживанию и поддержке сети, за счет инженерных усилий по обеспечению надежности. Применение методов обеспечения надежности и технические подходы описаны в 5.4.

В таблице 1 представлено соответствие методов применения с основными действиями по обеспечению надежности на каждой стадии жизненного цикла сети.

Таблица 1 — Краткое описание действий по обеспечению надежности сети и методов их применения

Стадии жизненного цикла сети	Действия по обеспечению надежности сети (ND)	Типичные методы выполнения
Концепция и определение	Анализ требований надежности сети	Анализ сценариев выполнения услуги; анализ воздействий на деятельность
Проектирование и разработка	Распределение вероятности безотказной работы по составным частям сети; прогнозирование показателей надежности сети; анализ и оценка показателей надежности сети	Моделирование сети (RBD, SLB и моделирование); NFMECA; FRACAS; анализ первопричин; анализ причин и последствий
Изготовление и интеграция	Проверка свойств надежности сети; разработка тестовых случаев надежности сети; валидация соответствия услуг надежности сети	NFMECA; FRACAS; анализ причин и последствий
Эксплуатация и техническое обслуживание	Оценка реализации надежности сети; управление неисправностями сети и ведение записей об инцидентах; ведение записей о техническом обслуживании сети	FRACAS; проверка работоспособности сети; контроль отключений сети; управление тестовыми случаями; техническое обслуживание, HAZOP, ориентированное на безотказность
Улучшение и обновление	Анализ требований к улучшению и обновлению услуг; оценка надежности услуг после их улучшения и обновления	Анализ сценария выполнения услуг (включая рассмотрение юридических услуг); проверка работоспособности сети; контроль отключений сети; управление тестовыми случаями; анализ воздействий на деятельность; анализ причин и последствий
Вывод из эксплуатации	Уведомление пользователей о прекращении работы сети; распоряжение устаревшим оборудованием	Анализ причин и последствий; анализ воздействий на деятельность

5.2 Характеристики надежности работы сети

Применение методов, приведенных в таблице 1, для оценки надежности требует идентификации соответствующих характеристик работы сети. Эти характеристики отражают способность сети работать в соответствии с соглашениями о требованиях к уровню качества услуг. Анализ характеристик надежности работы сети должен предусматривать установление критериев отказа сети и определение параметров надежной работы сети.

а) Установление критериев отказа сети

Критерии отказа для услуг E2E и услуг сети в целом должны быть установлены для обеспечения возможности измерения параметров надежности работы сети. Критерии обеспечивают количественные показатели оценки параметров работы сети для определения состояния выполнения услуг и условий отказа. Отказы сети классифицируют для выявления вероятных причин отказов, что облегчает анализ первопричин отказов и способствует повышению надежности сети. Следует принимать во внимание фиксируемые вероятность возникновения отказов сети и частоту инцидентов, связанных с отказами.

Ниже приведены типичные отказы сети, которые необходимо рассмотреть.

1) Связанные с оборудованием отказы сети состоят из отказов отдельных элементов сети, соответствующих отказам узла и соединения оборудования или программного обеспечения, вызывающих прерывание в работе сети. FRU — элемент сети, такой как набор схем или восстанавливаемый сборочный узел оборудования, используемый при выполнении услуги сети. FRU — объект, изымаемый из

эксплуатации в случае отказа или по другим причинам для замены в соответствии с соглашениями об услугах сети или требованиями к сопровождению сети. Анализ интенсивности замен FRU дает представление о критических проблемах отказов в эксплуатации.

2) Связанные с трафиком отказы сети состоят из отказов, связанных со сценариями замен при выполнении услуг сети и перегрузкой трафика. Эти отказы вызваны ограничениями возможностей оборудования сети, неправильной работой резервных путей услуг, неверным дублированием узлов и соединений сети, а также внезапными скачками расхода трафика, которые создают ситуацию перегрузки в сети.

3) Связанные со стихийными бедствиями отказы сети включают отказы, вызванные ошибками человека и стихийными бедствиями, вызывающими отказ сети. Катастрофы, вызванные действиями человека, являются следствием технологических или антропогенных опасностей, таких как разрушение конструкций, пожар или отключение электроэнергии. Стихийные бедствия являются результатом наводнения, землетрясения или извержения вулканов. Все катастрофы влияют на жизнь человека и его имущество, нанося экономический ущерб и ущерб окружающей среде.

4) Отказы сети, связанные с безопасностью, состоят из отказов, вызванных недостаточным уровнем защищенности от несанкционированных проникновений в сеть, таких как взлом, кибератаки или саботаж.

5) Отказы сети, связанные с запланированной деятельностью, состоят из отказов, произошедших во время плановых мероприятий по техническому обслуживанию сети, вызванных неправильным выполнением процедур технического обслуживания или неправильным осуществлением процесса технической поддержки.

6) Отказы сети, связанные с человеческим фактором, состоят из отказов, вызванных непреднамеренными ошибками человека, такими как ошибки оператора, неправильное выполнение процедур или преднамеренное нанесение ущерба и уничтожение имущества.

b) Определение параметров надежности работы сети

В таблице 2 обобщены важные параметры для оценки характеристик надежности работы сети. Соответствующие параметры надежности работы сети определены для услуг сети в целом и услуг сети E2E. Эти параметры надежности отражают ключевые характеристики надежности работы сети и требования к предоставлению услуг сети в целом и услуг сети E2E.

Таблица 2 — Параметры надежности сети

Услуги сети в целом: параметры надежности работы сети (интерес поставщиков услуг)	Услуги сети E2E: параметры надежности работы сети (опыт конечных пользователей)
Коэффициент готовности услуг сети в целом (% продолжительности работоспособного состояния); количество абонентов или пользователей, пострадавших из-за отключения услуг сети; продолжительность неработоспособного состояния сети (минуты/год); время обнаружения неисправности (минуты); время восстановления (минуты); интенсивность замен FRU (кол-во/месяц)	Коэффициент готовности услуг сети E2E (% продолжительности работоспособного состояния); продолжительность неработоспособного состояния пути услуги (минуты/год); неуспешный доступ к услуге (частота/год); допустимая задержка услуг (частота/год); преждевременное отключение услуг (частота/год); задержка медиа-услуг (минуты/год)

5.3 Методы оценки надежности сети

5.3.1 Общие методы анализа и оценки надежности

Оценка надежности охватывает анализ и оценку и часто представляет собой итеративный процесс. Методы анализа и оценки надежности обеспечивают широкий спектр методов для применения к надежности сети. Многие из классических методов надежности используют на всех этапах жизненного цикла сети для анализа надежности элементов сети и операций выполнения услуг. Примеры, такие как анализ видов, последствий и критичности отказов *[9]*, анализ структурной схемы надежности *[6]*, марковский анализ *[13]* и методы проектирования безотказного программного обеспечения *[14]* формируют основу оценки надежности сети. Однако следует отметить, что классические методы обеспечения безотказности имеют ограниченную область применения. В частности, существующие методы надежности часто непригодны для моделирования сети со сложной топологией и трудны для анализа множества конфигураций сети. Для обеспечения надежности сети вводят новые методы, более адаптированные к динамическим схемам маршрутизации услуг сети.

Следующие методы, указанные в таблице 1, обеспечивают рекомендуемую методологию и процессы оценки надежности работы сети и услуг сети.

5.3.2 Анализ сценариев выполнения услуг

a) Описание и назначение

Анализ сценариев выполнения услуг — это прикладной метод идентификации профиля эксплуатации и анализа требований к услугам. Цель состоит в определении топологии сети и функций услуг, относящихся к предоставлению запланированных услуг сети для оценки надежности. Прикладной метод облегчает перевод потребностей пользователей, полученных из различных маркетинговых источников, в технические требования в процессе анализа требований к надежности сети. Анализ влияния на бизнес проводят в сочетании с применимым анализом сценариев для оценки экспозиции рисков и определения соответствующих действий плана восстановления.

b) Критерии выбора и условия использования метода:

- появление новых требований к услугам, наличие неизвестных или изменение существующих требований;
- необходимость улучшения существующего профиля эксплуатации для обеспечения конкурентоспособных свойств услуг;
- необходимость установления требований к ресурсам для поддержания функционирования и развития сети;
- использование анализа сценариев выполнения услуг для планирования первоначальных потребностей пользователей в обслуживании и определения последующих потребностей в обслуживании, когда требования к услугам изменились или определены новые.

c) Процедура выполнения:

- определение соответствующей топологии сети, соответствующей требованиям к услугам. Сети переходят в разные топологические формы и содержат разные активные пути передачи услуг по сети с резервными путями и механизмами защиты для облегчения доступа к услугам и их транспортировки;
- определение функций услуг, таких как голос, данные и видео для предоставления услуг сети;
- определение использования функций услуг и требований к их выполнению;
- определение профиля использования, отражающего частоту доступа, время и продолжительность сеансов связи;
- определение влияния на бизнес и необходимости соответствующего плана восстановления;

d) Требования к данным

Варианты топологии, альтернативные пути выполнения услуг, расположение механизмов защиты и точек доступа.

e) Интерпретация результатов

Представление существенной информации профиля эксплуатации услуг сети, рисков и преимуществ, а также входных данных для моделирования и разработки требований к надежности.

5.3.3 Моделирование сети

a) Описание и назначение

Моделирование сети — это прикладной метод создания графических символьных представлений узлов и соединений сети, а также взаимосвязей для установления конфигурации сети. Цель состоит в определении подходящих путей выполнения услуг сети для предоставления услуг пользователям. Процедура облегчает идентификацию соответствующих узлов и соединений сети и связанных с ними механизмов защиты, участвующих в конкретном потоке обслуживания для оценки надежности услуг E2E. Моделирование сети позволяет выбирать альтернативные пути выполнения услуг для анализа и оценки надежности при оптимальной маршрутизации. Сеть услуг E2E — это коммуникационная сеть предоставления услуг. В приложении А описан метод SLB, специально разработанный для обеспечения надежности E2E.

Для сети в целом применение моделирования создает узлы и соединения всей сети в целом в соответствии с конфигурацией сети при оценке надежности работы сети. Цель состоит в определении общего коэффициента готовности работы сети, чтобы отразить возможности и мощность сети в обеспечении работы сети в целом в соответствии с соглашениями об уровне обслуживания и качества услуг. Общие методы моделирования включают, но не ограничиваются ими, RBD, марковский анализ, моделирование системы и комплексный анализ сети. Сеть в целом рассматривают как расширение концепции системы, где применяют аналогичный процесс моделирования. В приложении В приведен пример оценки работы сети в целом.

b) Критерии выбора и условия использования метода:

- необходимо установить структуру анализа и оценки сети;
- необходимо определить критические элементы сети для конфигурации сети;
- необходимо количественно оценить коэффициент готовности сети и установить границы допустимых простоев;
- моделирование сети используют, когда необходимо установить топологию сети и схемы маршрутизации, они изменены или ожидается их изменение для целей планирования обслуживания;

c) Процедура выполнения:

- создание узлов (и соединений) сети, а также взаимосвязей на основе топологии сети для установления конфигурации сети;
- определение функций услуг, связанных с путями выполнения услуг;
- выбор подходящего пути выполнения услуг и определение узлов и соединений сети, а также связанных с ними механизмов защиты, участвующих в потоке услуг;
- анализ каждого пути выполнения услуг для определения вероятности безотказной работы услуги E2E и коэффициента готовности предоставления функций услуг;
- оптимизация конфигурации услуг сети при обеспечении надежности E2E услуг, путем определения основного пути услуг альтернативных путей услуг;
- для моделирования сети в целом необходимо определить, изучить и оценить соответствующие показатели безотказности, ремонтопригодности, обеспеченности техническим обслуживанием и восстанавливаемости узлов и соединений сети. Готовность конфигурации всей сети должна быть проанализирована для определения общей продолжительности неработоспособного состояния за год непрерывной работы сети.

d) Требования к данным

Показатели надежности каждого выбранного пути обслуживания, вероятность безотказной работы узлов и соединений и связанных с ними механизмов защиты, коэффициент готовности выбранных путей выполнения услуг и продолжительность путей выполнения услуг.

e) Интерпретация результатов

Применение моделирования сети является основой для разработки требований к надежности сети. Моделирование позволяет распределять вероятность безотказной работы сети, прогнозировать надежность сети, выполнять анализ и оценку проекта, а также оценивать услуги E2E.

5.3.4 Анализ видов, последствий и критичности отказов

a) Описание и назначение

NFMECA — прикладной метод, заимствованный из классического процесса FMEA (Failure Mode and Effects Analysis — анализ видов и последствий отказов) для анализа элементов сети и функций услуг. Целью является выявление критических видов отказов в узлах и соединениях сети для определения влияния отказов на функции услуг следующего более высокого уровня. NFMECA позволяет оценить критичность отказов, которые могут повлиять на надежность работы сети и на обслуживание пользователей. Для анализа более сложных сетей в качестве дополнения к методу NFMECA могут быть использованы другие методы, такие как анализ дерева отказов и сеть Петри.

b) Критерии выбора и условия использования метода:

- установление конфигурации сети и доступность подробной информации об элементах сети;
- выполнение количественной и качественной оценки причинно-следственных связей для определения критичности воздействия услуг;
- необходимо выявление критических элементов сети для повышения безотказности сети;
- обоснование решения об использовании резервирования или других приемов обеспечения отказоустойчивости проекта;
- NFMECA используют, если обнаружены или возможны критические последствия услуг.

c) Процедура выполнения:

- использование информации о топологии сети для идентификации узлов и соединений сети, путей услуг на каждом уровне анализа видов отказов;
- определение соответствующих видов отказов, связанных с каждым узлом (например, перегрузка) и соединением (например, прерывание интерфейса) по базе реальных данных, выбранных из хранилища данных сети. Данные об отказах отражают опыт обслуживания конечных пользователей, в том числе доступность услуг, непрерывность обслуживания и отключение услуг;

- определение влияния отказов на неработоспособное состояние услуги, в том числе продолжительности неработоспособного состояния пути услуги, продолжительности неработоспособного состояния сети и продолжительности неработоспособного состояния передающей сети;

- определение результирующей критичности отказа и оценка влияния на услуги сети E2E.

d) Требования к данным

Экспериментальные данные (собранные и накопленные) о видах отказов сети и их последствиях в хранилищах данных сети.

e) Интерпретация результатов

Результаты NFMECA могут быть использованы в качестве исходных данных для обновления оценки надежности сети в зависимости от продолжительности неработоспособного состояния сети и усилий технического обслуживания сети. Результаты NFMECA также используют для разработки тестовых случаев для NFIT, где это оправдано.

5.3.5 Проверка сети путем введения неисправности

a) Описание и назначение

NFIT — прикладной метод верификации влияния отказов сети путем преднамеренного введения неисправностей для проверки последствий и полученных результатов. Цель состоит в проверке эффективности применения в конструкции резервирования, механизмов защиты и возможности управления отказами сети в целом.

b) Критерии выбора и условия использования метода:

- критичность неисправности известна и вызывает опасения;

- определено вероятное место неисправности;

- необходимо определить критичность влияния неисправности на выполнение услуг сети;

- необходимо проверить частоту возникновения неисправностей;

- NFIT используют при обнаружении критических последствий услуг и необходима верификация с помощью тестовых случаев.

c) Процедура выполнения:

- определение объекта NFIT планируемого тестового случая;

- определение метода введения неисправности на целевом тестовом уровне. Различные уровни OSI *[15]* имеют различные типы неисправностей (см. раздел 4);

- выполнение тестового случая. Наблюдение во время испытаний за всеми связанными элементами сети и путями услуг. Определение области и степени воздействия неисправности. Выполнение записей о результатах испытаний.

d) Требования к данным

Записи результатов испытаний и наблюдений.

e) Интерпретация результатов

Оценка влияния неисправности на функции услуг сети, время восстановления услуг и возможности отказоустойчивости. Предоставление информации об эффективности применения тестового случая, области влияния неисправности, результативности управления неисправностями сети.

5.3.6 Система отчетности, анализа и корректирующих действий при отказах

a) Описание и назначение

FRACAS — это метод сбора соответствующих данных о зафиксированных инцидентах, действиях технического обслуживания, результатах диагностики и анализа для разработки рекомендаций о корректирующих действиях. Цель состоит в формализации базы данных репозитория для сбора и хранения хронологических данных о надежности работы сети, используемых при проектировании сети и улучшении ее услуг.

b) Критерии выбора и условия использования метода:

- создание информационной базы данных об отказах;

- установление процедуры записей об отказах;

- необходимость сбора хронологических данных об отказах для установления тенденции изменения надежности работы сети,

- необходимость обоснования решений по проектированию сети и улучшению процедур;

- FRACAS используют в процессе всего срока службы сети для поддержания надежной базы данных репозитория и отслеживания хронологических данных о работе сети.

c) Процедура выполнения:

- определение информации об отказах и записей об инцидентах для ввода FRACAS;

- классификация записей об инцидентах для принятия мер на основе установленных критериев технического обслуживания, таких как срочность, процедура или график выполнения для исполнения этих мер в период следующего обновления;

- анализ и оценка критичности основных проблем отказа, влияющих на выполнение услуг и предоставление рекомендуемых решений, таких как изменение конструкции, замена составных частей или управление конфигурацией,

- выполнение рекомендаций по разрешению проблем;

- выполнение записей и мониторинг состояния FRACAS для постоянного улучшения;

- FRACAS, как правило, автоматизирован для облегчения обновления данных, последующих действий и улучшения процесса.

d) Требования к данным

Обеспечение классификации данных об отказах и обслуживание базы данных.

e) Интерпретация результатов

Установление тенденции изменения надежности работы сети и хронологии действий по улучшению сети.

В приложении С показана оценка показателей надежности сети в условиях эксплуатации. Приведен пример типичных категорий отказов сети общего пользования для оценки надежности.

5.4 Методы обеспечения надежности сети

5.4.1 Область применения методов обеспечения надежности

Область применения методов обеспечения надежности охватывает три области, указанные в 4.5. Применение методов специально ориентировано на действия при эксплуатации сети с точки зрения надежности. Процесс обеспечения надежности сети широко использует установленные процессы управления сетью для обеспечения сопровождения управления работой сети, управления отказами сети и качеством услуг. Цель состоит в повышении и поддержке надежности работы сети.

Методы обеспечения надежности — это рекомендуемые технические подходы, основанные на отраслевой практике, по обеспечению устойчивости надежности работы сети при эксплуатации и своевременного удовлетворения потребностей в поддержке надежности услуг сети. Общая ответственность за работу сети для достижения качества услуг и удовлетворенности потребителей лежит на операторах сети и поставщиках услуг. Обеспечение надежности в нормальных и аварийных условиях работы сети ориентировано в первую очередь на обеспечение надежности услуг для конечных пользователей сети, поддержке качества услуг. Безопасность услуги соответствующего качества дополняет деятельность по обеспечению надежности. Надежность работы сети обеспечивает проектирование сети и выполнение услуг, которые могут оказывать существенное влияние на безопасность работы сети.

Методы обеспечения надежности сети сгруппированы в соответствии со стратегиями обеспечения надежности. Представленные в настоящем стандарте методы являются типичными примерами обеспечения выполнения услуг сети при ее эксплуатации, такими как проверка работоспособности сети и контроль отключений сети. Системы управления неисправностями сети используют при поддержке больших сетей для идентификации неисправностей, сбора данных и анализа тенденций работы сети. Ниже приведены технические подходы к решению проблем обеспечения надежности.

5.4.2 Обеспечение надежности услуг

a) Цель

Обеспечение надежности в пути выполнения услуг сети и обеспечения передачи и пропускной способности данных.

b) Описание применения методологии

1) Путь выполнения услуги — это способ передачи информации. Узлы и соединения сети, связанные с путем выполнения услуги, должны быть объединены с соответствующими устройствами защиты для обеспечения успешной передачи информации и перенаправления на альтернативные пути в случае неисправности основного пути выполнения услуги. Приоритеты выбора пути выполнения услуги должны быть определены заранее. Существует несколько схем выбора путей, подходящих для конструкции сети, которые включают в себя устройства защиты, такие как методы резервирования путей (с использованием нагруженного резервирования или резервирования замещением), мажоритарного голосования и приоритетного голосования. Анализ безотказности устройства защиты имеет важное значение для соответствующего применения. Для оценки влияния неисправности и ее последствий необходима оценка риска защищенного пути выполнения услуг сети.

2) Работоспособность сети отражает надежность предоставления услуг конечным пользователям. Факторы, способствующие обеспечению работоспособности, включают доступность услуг для конечного пользователя, возможность сохранения обслуживания и прекращение обслуживания при установлении и завершении или начале и окончании сеанса связи. Задержки доступа связаны с невозможностью установить соединения сети по различным причинам. Стабильность удержания услуги зависит от пропускной способности сети и условий расхода трафика во время связи. Неудачное отключение услуги приводит к потере доступных ресурсов сети и ошибкам в начислении платы абонентам или пользователям. Эффективность выполнения услуг сети зависит от надежности работы сети и безотказности, скорости и точности разъединений. Планирование сети должно решать проблемы работоспособности с точки зрения надежности работы сети для максимизации использования ресурсов сети.

5.4.3 Обеспечение целостности данных

a) Цель

Обеспечение целостности пропускной способности данных и защиты данных.

b) Описание применения методологии

1) Целостность данных зависит от механизмов, реализованных в элементах сети и функциях услуг, предназначенных для обнаружения и предотвращения неправильного перехода потока данных между функциями процессов сети. Целостность данных также зависит от механизмов, используемых для проверки точности и достоверности входных и выходных данных. Характеристикой целостности надежности работы сети является способность сети обеспечивать защищенный проход содержимого данных. Целостность отражает обеспечение работы сети, гарантирующей, что содержимое данных не загрязнено (не включает посторонней информации), не повреждено и не изменено при преобразовании входных данных в выходные данные.

2) Существует много методов, используемых для управления защищенной информацией и сохранения целостности данных. Их применение зависит от специфики требований в отношении системы управления информацией, целостности данных и уровня потребностей в их безопасности, возможности поиска и скорости восстановления данных, эффективности примененной технологии и стоимости изготовления в рамках процесса обеспечения безопасности сети. Подходы к обеспечению целостности и безопасности данных для реализации определены в *[1]*. Примеры сохранения данных включают резервное копирование и дублирование данных, хранение данных в различных местах и репликацию данных в разных форматах. Примеры защиты данных включают аутентификацию, кодирование и шифрование данных и сообщений, обнаружение вирусов и защиту брандмауэра для предотвращения атак на сеть.

5.4.4 Обеспечение функций работы сети и поддержка процесса улучшения

a) Цель

Обеспечение функций работы сети и поддержка процесса улучшения.

b) Описание применения методологии

1) Применимая методология обеспечения надежности использует установленные процессы управления сетью для решения различных задач обеспечения надежности работы сети, связанных с планированием сети, измерениями и оптимизацией работы сети. Деятельность по обеспечению надежности включает в себя идентификацию и решение проблем, зависящих от времени работы сети, таких как задержка во времени при доставке кадров (пакетов информации) и ее подтверждении, потеря пакетов, повторные передачи и измерение пропускной способности трафика. Цель состоит в обеспечении работы трафика в отношении скорости, безотказности и пропускной способности в соответствии с проектом и конфигурацией сети для максимального использования ресурсов и предотвращения перегрузки сети.

2) Применяемая методология обеспечения надежности использует установленные процессы управления неисправностями сети для обнаружения, изоляции и устранения неисправностей при эксплуатации сети, компенсации изменений окружающей среды и оказания помощи в техническом обслуживании и диагностических мероприятиях. Цель состоит в обеспечении надлежащей диагностики неисправностей сети, сборе и ведении записей о работе сети для базы данных, а также использовании источника данных о неисправностях для разработки рекомендаций по улучшению поддержки услуг сети.

3) Применяемая методология обеспечения надежности использует установленные процессы системы отслеживания состояния сети, технического обслуживания и материально-технического обеспечения, а также соответствующие базы данных для анализа и оценки категорий отказов при определении продолжительности и частоты простоев сети из-за неработоспособного состояния. Соответствующие данные используют для установления влияния простоев в соответствии с причинами отказов на конеч-

ных пользователей услуг сети. Целью является обеспечение надлежащей оценки тенденций работы сети, удовлетворенности потребителей и качества услуг.

5.4.5 Методы обеспечения надежности сети

a) Проверка работоспособности сети

Проверка работоспособности сети — это метод мониторинга и контроля правильности и эффективности устранения текущих проблем эксплуатации сети. Проверку проводят для обеспечения надежности услуг. Проверка работоспособности сети является основным методом обеспечения надежности работы сети. Процесс проверки работоспособности основан на анализе проблем эксплуатации, возникающих в работе сети, которые контролируют или проверяют на регулярной основе (например, раз в две недели) с помощью серии моделирований сети в течение определенного периода времени. Это делают путем установления последовательности временных соединений для исследования возникновения проблем в соответствующем сценарии и профиле эксплуатации при проверке состояния работы сети и обеспечении работоспособности сети в эксплуатации.

Сценарий работы сети постоянно изменяется во времени из-за различных требований к трафику, изменений в использовании услуг, адаптации топологии и конфигурации сети, а также активации защитного механизма для снижения последствий неисправностей в работе сети и перенаправления сетевых путей, ограниченных пропускной способностью соединений. Метод проверки работоспособности сети используют в сочетании с системой управления неисправностями сети и информацией базы данных FRACAS для непрерывной работы сети. Процесс проверки работоспособности сети включает в себя анализ сценария и профиля эксплуатации при решении проблем, возникающих для поддержания надежности работы сети при эксплуатации.

Процедуры проверки работоспособности сети:

1) определение текущей топологии и конфигурации сети для анализа каждого сценария;

2) определение возникшей проблемы эксплуатации и регистрация времени при мониторинге сценария;

3) анализ ключевых элементов сети, участвующих в снижении последствий возникшей проблемы эксплуатации, для ее решения и поддержания функционирования сети,

4) определение надежности сети с точки зрения показателей готовности и безотказности и потребностей в поддержке услуг в соответствии со сценарием работы сети;

5) создание файла конфигурации сети в качестве входа при моделировании сети, включая всю информацию о зависящем от времени сценарии, необходимую для моделирования;

6) оценка результатов моделирования для определения надежности работы сети, результативности и правильности схем резервирования и маршрутизации для каждого исследуемого сценария;

7) анализ документов и оценка результатов для различных исследуемых сценариев при создании серии профилей проверки работоспособности сети для управления эксплуатацией сети и ее непрерывного улучшения.

Целесообразно проверять, верифицировать и валидировать результативность и правильность работы сети при предоставлении услуг сети на основе знания сценариев и проблем эксплуатации.

b) Контроль отключения сети

Управление отключением сети — это метод выявления и классификации проблем эксплуатации сети с помощью записей об инцидентах операторов сети и поставщиков услуг. Это позволяет определить состояние непрерывной работы сети и влияния услуг на удовлетворенность потребителей. Цель состоит в сборе статистик отключений сети и данных о продолжительности неработоспособного состояния оборудования для проверки соответствия надежности работы сети отраслевым показателям. Соответствующая информация о статистиках простоев сети способствует разработке надлежащих мер по смягчению последствий и контролю воздействия услуг в процессе эксплуатации сети.

Практика отрасли связи устанавливает стандартные требования к представлению отчетов о проблемах в эксплуатации. Критерии измерения простоев элементов сети (например, оборудования) устанавливают отраслевые стандарты *[16]*, *[17]*. Информацию о простоях сетевого оборудования фиксируют и сообщают в соответствии с уровнем соглашений об обеспечении услуг сети. На надежность работы сети влияют неисправности оборудования, приводящие к полному или частичному отключению услуг. Неисправности оборудования могут привести к деградации сети. Это также может поставить под угрозу целостность данных во время работы сети. Для управления отключением сети необходимо записывать информацию о простоях, влияющих на услуги сети. Данные о простоях, собранные с помощью записей об инцидентах, имеют решающее значение для установления причинно-следственных связей при определении соответствующих источников отказов, вызывающих неработоспособное состояние услуг

сети. Простои, вызванные неработоспособным состоянием, характеризуют данные о продолжительности неработоспособного состояния. Кроме того, фиксируют дополнительную информацию об источнике отключения, частоте его возникновения и влиянии количества пострадавших абонентов или пользователей. Информация о простоях сети позволяет процессу обеспечения надежности сети обосновать и рекомендовать корректирующие или предупреждающие действия для обеспечения устойчивой работы сети и непрерывного улучшения ее обслуживания.

Управление отключением сети контролирует потерю функциональности оборудования в системах сети. Информация об отключениях представляет собой данные о продолжительности неработоспособного состояния сети для определения воздействия услуг на оборудование сети. Цель состоит в сокращении продолжительности периодов простоев, связанных с ними затрат и влияния услуг для повышения дохода и удовлетворенности клиентов.

Оборудование сети классифицируют для облегчения сбора данных и назначения показателей простоев. Категории оборудования сети включают, например: коммутацию, сигнализацию, передачу и общие функции.

К показателям отключения сети относятся следующие:

1) показатели влияния услуг — частота отключений (простоев) сети и продолжительность неработоспособного состояния, влияющая на количество абонентских линий при предоставлении услуг сети в связи с частичным или полным отключением от всех источников, выраженная в минутах на абонентскую линию за год;

2) показатель воздействия неработоспособного состояния элемента (оборудования) — частота простоев сети и продолжительность неработоспособного состояния из-за неисправности оборудования для оценки показателей готовности, безотказности и потребностей в техническом обслуживании, выраженная в минутах на категорию оборудования за год.

Данные об отключениях группируют для облегчения составления статистики отключений.

- Область услуг сети, на которую влияет:
  - полное отключение,
  - частичное отключение.
- Причина простоя:
  - простои, связанные с изготовителем оборудования или поставщиком услуг;
  - простои, вызванные процедурной ошибкой;
  - простои, вызванные ошибкой программного обеспечения;
  - другие причины.

c) Контроль перегрузок

Включение контроля перегрузок направлено на поддержание работоспособности сети в эксплуатации для обеспечения продолжения выполнения услуг сети. Контроль перегрузок включает в себя контроль входов трафика в коммуникационную сеть. Цель состоит в том, чтобы избежать перегрузок трафика, вызывающих коллапс сети, посредством мониторинга и регулирования избыточных запросов на обработку или возможностей соединений промежуточных узлов сети. Методология использует процедуры экономии ресурсов, такие как снижение скорости отправки пакетов данных.

Ключевые компоненты общей схемы предотвращения перегрузки включают реализацию функциональных устройств управления для обнаружения перегрузки, обратной связи о перегрузке, селектора обратной связи, фильтра сигналов, функции принятия решений и алгоритмов увеличения/уменьшения нагрузки.

Для предотвращения перегрузки сети и коллапса метод требует:

- установления условий перегрузки;
- наличия в маршрутизаторах механизма переупорядочивания или отбрасывания пакетов в заранее установленных условиях перегрузки;
- применения сквозных механизмов регулирования потока данных, разработанных в конечных точках, для обеспечения надлежащего реагирования на состояние контроля перегрузки.

d) Управление тестовым случаем

Для управления серьезными проблемами эксплуатации сети иногда необходимо воссоздать проблемную ситуацию, зеркально отражающую окружающие условия, для проверки в лаборатории или в офисе, дублируя конкретную систему и сценарий работы сети. Для управления решением задачи генерируют тестовый случай. Тестовый случай — это способ, позволяющий облегчить получение результатов в рамках процесса обеспечения качества.

Тестовые случаи разрабатывают для моделирования реальных условий эксплуатации, в которых могут возникнуть конкретные области, требующие изучения, или потенциальные проблемы. Тестовый случай — это набор входов, условий выполнения и ожидаемых результатов, разработанный для тестирования с целью проверки соответствия определенному требованию. Спецификация тестового случая представляет собой документ, устанавливающий входы, ожидаемые результаты тестирования и установленные условия выполнения теста.

NFIT рассматривают как метод тестовых случаев для решения проблем эксплуатации.

Приложение А
(справочное)

Пример оценки надежности сети E2E

А.1 Общие положения

Целью оценки надежности сети E2E является определение пути выполнения услуг сети в зависимости от ее надежности. Результатом оценки является показатель готовности или общая продолжительность неработоспособного состояния E2E-соединений за год. Метод SLB (балансировка нагрузки на сервер) приведен для демонстрации методов, используемых для обеспечения решений в области надежности при анализе путей выполнения услуг сети.

А.2 Описание топологии сети и путей выполнения услуг сети E2E

Пути выполнения услуг сети определяет топология сети. Топология сети учитывает следующее:

- сценарии выполнения услуг и требования к голосовым, числовым видеоданным или другим услугам сети;
- критичность предоставления услуги;
- соответствующие узлы и соединения для установления основного пути выполнения услуги E2E;
- резервные пути услуг на случай отказа основного пути.

На рисунке А.1 показан пример типичной топологии сети, в которой указаны соответствующие узлы и соединения E2E, а также их взаимосвязи в топологической конфигурации. На схеме указаны следующие обозначения узлов сети: A, I, K — переключатели (коммутаторы) обмена; B, C, D, E — маршрутизаторы; F, G, H, J — центры обработки данных, в которых хранятся соответствующие данные регистрации для доступа пользователя к данным и его аутентификации для облегчения соединений E2E. Соединения сети располагаются между узлами и устанавливают связи между ними. Результирующий путь выполнения услуги E2E должен установить связь A с J, инициированную конечным пользователем в A.

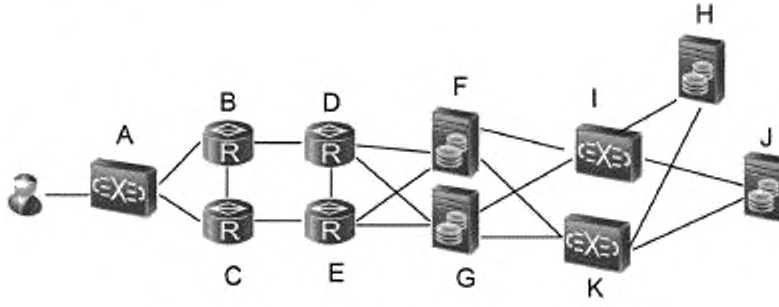


Рисунок А.1 — Пример типичной топологии сети E2E

Сценарий выполнения услуги можно объяснить следующей последовательностью действий:

- конечный пользователь использует доступ к A, чтобы установить связь с J;
- основной путь услуги, показанный сплошной линией «__», следует по узлам и соединениям A-B-D-F-I-H-I-J для установления искомой связи с J;
- когда выполнение услуги достигает узла I, он требует аутентификации H, чтобы разрешить продолжение выполнения услуги, представляя цикл I-H-I, уникальный для информационных потоков в коммуникационных технологиях;
- если в H разрешение предоставлено, выполнение услуги продолжается от I к J для завершения соединения E2E. Следует отметить, что H является критическим узлом, требующим высокой безотказности работы оборудования.

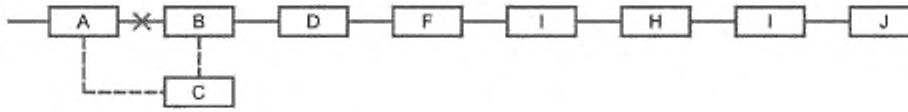
Из набора информации, предоставленной на данный момент, резервные пути услуги, показанные пунктирными линиями «----», могут быть установлены на основе сведений об узле и отказах соединений, обозначенных знаком «X» в топологической конфигурации. При установлении путей услуг сети E2E приходится иметь дело с унаследованными проблемами, когда существующие сети взаимодействуют с новыми сетями для завершения подключения E2E. Символ в виде стрелки «--->» используют только тогда, когда SLB слишком длинные и подключаются к новому соединению SLB для завершения построения пути услуги сети E2E.

А.3 Построение пути услуги сети E2E

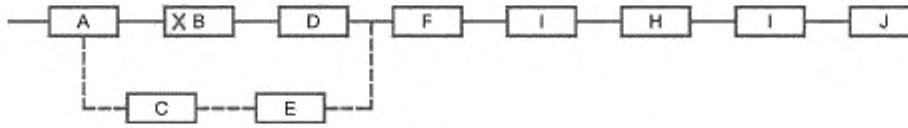
Построение пути услуги сети E2E начинают с основных и резервных путей услуги и строят с помощью схем SLB, как показано в перечислениях a)—k).

a) Основной путь услуги

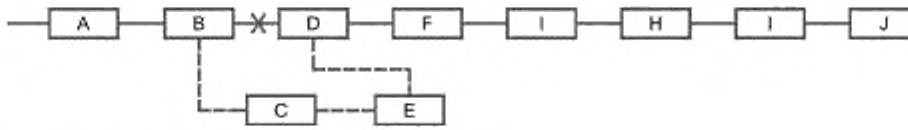
b) Резервный путь услуги при отказе соединения между узлами A и B



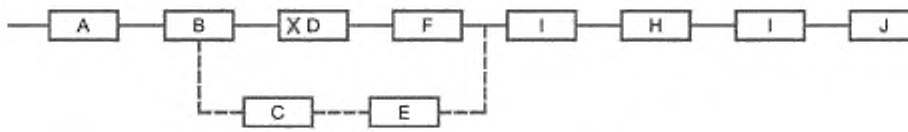
c) Резервный путь услуги при отказе узла B



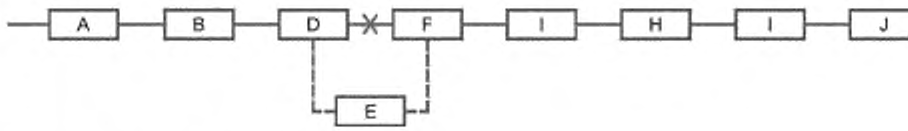
d) Резервный путь услуги при отказе соединения между узлами B и D



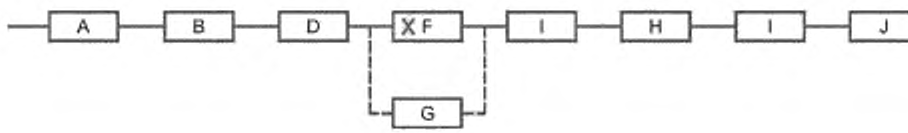
e) Резервный путь услуги при отказе узла D



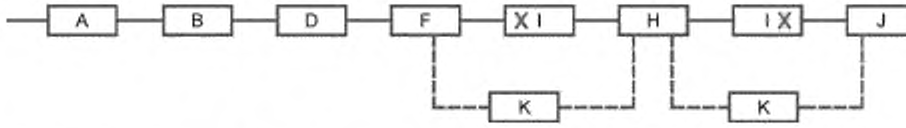
f) Резервный путь услуги при отказе соединения между узлами D и F



g) Резервный путь услуги при отказе узла F



h) Резервный путь услуги при отказе узла I



Из данного набора схем SLB можно определить показатели готовности или общую продолжительность неработоспособного состояния за год путей услуг сети E2E с использованием стандартных математических процедур и экспериментальных данных, установленных или оцененных для каждого узла и соединения в соответствии с топологией сети E2E. Высокая эксплуатационная готовность услуг сети E2E означает, что основной путь услуги доступен для эксплуатации, все резервные пути услуги также доступны по запросу, и переключение пути при необходимости должно быть успешным.

Каждый путь услуги от A до H представляет собой простую последовательную модель RBD, позволяющую определить показатели готовности пути от A до H. Готовность пути услуги E2E определяет комбинация готовности основного пути и резервных путей.

Коэффициент готовности пути услуги E2E A_{E2E} может быть определен по вкладу продолжительности неработоспособного состояния следующим образом:

$$A_{E2E} = 1 - \frac{DT_{E2E}}{8760 \cdot 60}, \qquad (A.1)$$

где DT_{E2E} — продолжительность неработоспособного состояния пути услуги E2E мин/год, выполняемая по формуле

$$DT_{E2E} = \sum_i f_i \cdot [r_i \cdot dt_i + (1 - r_i) \cdot MTTR_i], \qquad (A.2)$$

где f_i — частота отказов i-го узла/соединения на основном пути (раз/год);

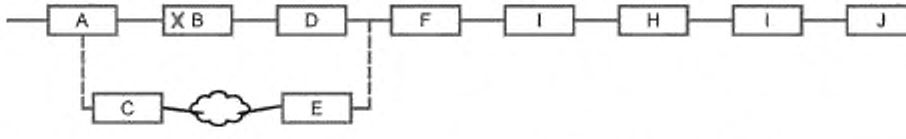
r_i — коэффициент восстановления после отказа сети i-го узла/соединения основного пути;

dt_i — продолжительность неработоспособного состояния i-го узла/соединения основного пути при отказе, когда услуга успешно выполнена;

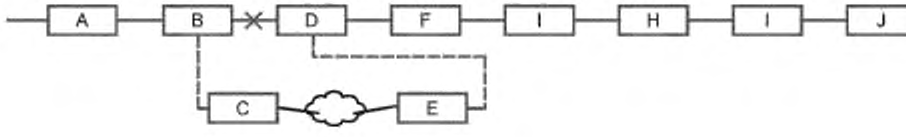
$MTTR_i$ — среднее время восстановления i-го узла/соединения основного пути, когда услуга не выполнена.

В топологии сети иногда встречается топологическая конфигурация с маршрутизацией через всю взаимодействующую сеть, которая уже существует в эксплуатации. Метод SLB может включать такую взаимодействующую сеть для моделирования пути услуги сети E2E. Для этого взаимодействующую сеть представляют в виде «облака» с символом ⬭, включенным в путь услуги SLB. «Облако» рассматривают как узел сети в топологической конфигурации. Например, если маршрутизатору C необходимо установить связь через транспортную сеть, чтобы достичь маршрутизатора E, соответствующие резервные пути услуги для c), d) и e) могут быть представлены соответствующими схемами SLB, указанными в i), j) и k).

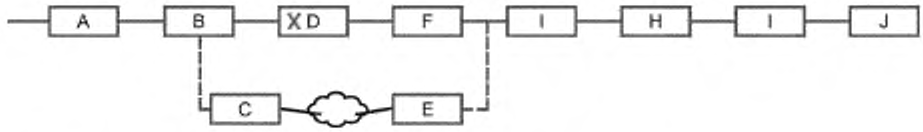
i) Резервный путь услуги через «облако» при отказе узла B



j) Резервный путь услуги через «облако» при отказе соединения между узлами B и D



k) Резервный путь услуги через «облако» при отказе узла D



Метод SLB имеет следующие ключевые особенности при применении:

- SLB разработан специально для моделирования сетей связи;
- SLB используется для идентификации и отслеживания критических путей услуги E2E для дальнейшего анализа;
- SLB учитывает поток услуг, а также топологию сети;
- SLB включает ситуацию наличия обратного контура при моделировании топологической конфигурации сети, уникальной для информационных потоков в коммуникационных технологиях;
- SLB работает главным образом с единичными отказами; наличие нескольких отказов на путях сети редко бывает, но может возникать, например, при перегрузке и нарушении продвижения, что требует особого рассмотрения в каждом конкретном случае;
- SLB позволяет проведение дальнейших исследований чувствительности, таких как задержка пакетов, джиттер, потери и восстановление в реальном и нереальном времени, для облегчения планирования и выбора стратегий защиты услуг сети;
- SLB представляет собой логическую схему простого построения путей выполнения услуг E2E;
- SLB облегчает разделение сети для построения соответствующих путей выполнения услуг сети E2E, задействованных в существующих сетях, взаимодействующих с новыми сетями;
- База данных об отказах SLB использует результаты оценки или экспериментальные данные о работе услуг сети E2E для поддержки оценки продолжительности неработоспособного состояния сети;
- SLB можно компьютеризировать для облегчения итеративного анализа отказов сети E2E и оценки их влияния на работу сети.

А.4 Анализ путей выполнения услуг сети E2E

Предпосылкой анализа пути выполнения услуги E2E является определение места отказа и типа отказа в рассматриваемом сетевом пути. Типичные отказы сети включают:

- отказы оборудования;
- неполадки в ОАМР;
- неисправность оборудования и перебои в подаче электроэнергии;
- процедурные ошибки;
- перегрузка трафика
- аварии и экологические инциденты;
- проникновение в систему безопасности и злонамеренные атаки на сеть.

Расположение отказов узлов и соединений сети может существовать на любом уровне сети, как описано в эталонной модели OSI *[15]*. Ниже приведены примеры некоторых возможных симптомов отказа сети:

- прикладной уровень: отказ при передаче файлов по электронной почте;
- уровень представления: отказ в шифровании и преобразовании данных;
- уровень сеанса: отказ поддержки порядка запуска/остановки связи;
- транспортный уровень: отказ доставки сообщения;
- уровень сети: отказ маршрутизации данных;
- уровень линии данных: отказ передачи фреймов от узла к узлу;
- физический уровень: отказ оборудования в узле или кабельной линии сети.

По этим симптомам можно отследить ответственные узел или соединение сети для определения основных причин их отказа. Соответствующие последствия отказа также могут быть установлены по результатам испытаний сети или на основании наблюдений в условиях эксплуатации, касающихся степени и критичности воздействия отказа для конечных пользователей сети и предоставления соответствующих функций услуг сети. Эти данные наиболее ценны для сбора и хранения в базе данных для текущей и будущей оценки показателей ОАМР.

Например, отказ сети, вызывающий перегрузку сообщений и частые прерывания выполнения услуг сети E2E, связан с совместимостью версий программного протокола, используемого на уровне приложений. После определения причины отказа протокол обновляют до последней версии, тем самым восстанавливая нормальное выполнение услуг сети E2E.

Общий процесс анализа называют NFMECA.

Соответствующую информацию об отказах фиксируют в базе данных FRACAS в качестве общего хранилища данных о режимах отказов и их последствиях. База данных FRACAS может быть эффективно использована в качестве источника опытных данных для диагностики отказов сети и аналогичных симптомов отказа для ускорения со-

ответствующих корректирующих действий. База данных FRACAS — ценный инструмент поддержки прогнозирования показателей готовности сети и продолжительности неработоспособного состояния сети. База данных FRACAS должна быть связана с системой управления неисправностями сети, чтобы облегчить общее хранение данных и обмен информацией, где это применимо.

А.5 Оценка путей выполнения услуг сети E2E

Знания, полученные в результате NFMECA, могут быть использованы для принятия решений и оценки рисков проекта, таких как:

a) рекомендации по перепроектированию целевого пути выполнения услуг сети E2E для улучшения проекта сети и обеспечения надежности;

b) разработка тестовых случаев для NFIT при проверке возможных последствий идентифицированного отказа путем инициирования тестов введения неисправности в соответствующий путь услуги сети E2E. Для создания тестовых случаев используют данные NFMECA и другую соответствующую информацию.

Процесс реализации проекта целевого пути услуг сети E2E в соответствии с a) представляет собой процесс перепроектирования, который строго следует процессу жизненного цикла проектирования/разработки и изготовления/интеграции. Соответствующие стадии жизненного цикла сети описаны в *[1]*.

Оценка целевого пути услуг сети E2E в соответствии с b) предназначена для разработки соответствующих тестовых случаев для применения NFIT. NFIT выполняет тесты для моделирования реальных условий эксплуатации пути услуг сети E2E посредством введения неисправности и изучения результатов тестирования. Цель состоит в определении степени экспозиции риска при проведении перепроектирования. NFIT — это попытка проверки и подтверждения неопределенности возможного результата до выполнения фактических действий по перепроектированию пути услуг сети E2E. В зависимости от графика реализации проекта и бюджетных ограничений деятельность NFIT в соответствии с b) обеспечивает дополнительную уверенность в процессе перепроектирования в соответствии с a) и предоставляет тестовую информацию, помогающую в принятии решений при проектировании. Адаптация проекта и компромиссы полезны при принятии решений.

Тестовый случай представляет собой набор входов условий выполнения и ожидаемых результатов, разработанных для конкретного объекта тестирования. В этом случае верификация целевого перепроектирования пути услуг сети E2E заключается в достижении работы сети при обеспечении надежности услуг. Введение неисправности является методом верификации, при котором преднамеренную неисправность вводят в целевой путь выполнения услуг сети E2E для определения ожидаемых результатов тестирования. Результат теста представляет собой объективные свидетельства в поддержку решения о перепроектировании.

NFIT также обеспечивает средства оценки эффективности процесса тестирования, результирующего охвата неисправностей сети, коэффициента готовности пути услуг сети и влияния на надежность работы сети.

В рамках процесса, оценки путей выполнения услуг сети E2E, могут быть определены следующие данные:

a) продолжительность неработоспособного состояния услуг сети:

- сумма продолжительности неработоспособного состояния, вызванного отказами каждого узла сети;
- сумма продолжительностей неработоспособного состояния, вызванных отказами каждого соединения сети;

b) коэффициент готовности услуг сети;

c) виды отказов:

- узел сети: отключение услуги, частичное отключение услуги, прерывистое обслуживание, мгновенное отключение услуги, деградация услуги;
- соединение сети: обрыв соединения.

d) информация о параметрах сети:

Параметр сети	Источник
- продолжительность неработоспособного состояния услуг сети за год (мин/год)	рассчитанный результат
- количество узлов в сети	топология сети
- количество соединений в сети	топология сети
- частота отказов *i*-го узла	статистика FRACAS
- частота отказов на линии *i*-го соединения	бизнес-статистика
- продолжительность отключения *i*-го узла услуги (минуты)	результаты NFIT
- продолжительность отключения соединения услуги (минут)	результаты NFIT
- интенсивность восстановлений сети	результаты NFIT
- среднее время восстановления *i*-го узла	статистика FRACAS
- среднее время восстановления *i*-го соединения	статистика оператора

Приложение В
(справочное)

Пример оценки надежности сети в целом

В.1 Общие положения

Целью оценки оператором сети надежности сети в целом является определение надежности работы сети в целом. Результатом оценки является показатель готовности или общая продолжительность неработоспособного состояния сети в целом за год. Существует много способов оценки с использованием комбинации методов моделирования сети и методов прогнозирования, а также используя данные эксплуатации, относящиеся к характеристикам отказов сети для установления тенденции отказов во времени.

В.2 Описание топологии сети и сети в целом

Топология сети такая же, как и для сети E2E, за исключением того, что два конечных пользователя на узлах A1 и A2 соединены связью, чтобы проиллюстрировать работу сети в целом. Сеть представлена на рисунке В.1.

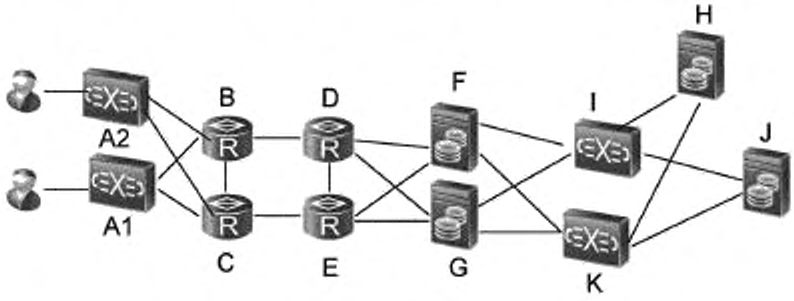


Рисунок В.1 — Пример типичной топологии сети в целом

Сценарий выполнения услуги можно описать следующим образом:

- поставщик услуг заинтересован в определении показателей готовности/безотказности сети в целом;
- предполагается, что все элементы сети от A до J включительно должны выполнять свои функции в любое время на непрерывной основе.

В.3 Анализ модели готовности сети в целом

Готовность сети в целом может быть определена с помощью вычисления средней продолжительности неработоспособного состояния в виде взвешенной суммы продолжительностей неработоспособного состояния E2E. При этом использованы те же математические символы, что и в приложении А.

Коэффициент готовности услуги сети A_N в целом можно определить следующим образом:

$$A_N = 1 - \frac{DT_N}{8760 \cdot 60}, \qquad (B.1)$$

где DT_N — общая продолжительность неработоспособного состояния сети в целом, выполняемая по формуле

$$DT_N = \sum_i DT_{E2Ei} \cdot P_i \qquad (B.2)$$

где DT_{E2Ei} — продолжительность неработоспособного состояния услуг i-го состояния сети (минуты в год);

P_i — количество пользователей i-го пути услуги, деленное на количество пользователей сети в целом.

В.4 Оценка сети в целом

Оценка услуг сети в целом аналогична оценке услуг сети E2E, но с учетом всех путей услуг сети E2E.

NFMECA и NFIT проводят аналогично процессу оценки E2E, но с разными целями с точки зрения поставщика услуг сети или оператора.

Приложение С
(справочное)

Оценка надежности работы сети в эксплуатации

С.1 Цель

Оценка работы сети в эксплуатации показана на примере. Цель состоит в описании процедуры определения влияния прерываний работы сети и продолжительности прерываний работы, на количество пользователей, использующих услуги сети.

Данный пример иллюстрирует методы, используемые для анализа и оценки сети на основе данных о работе сети, собранных за два года исследований работы общенациональной коммутируемой телефонной сети *[18]*. Числовые данные представлены для иллюстрации целей по индикации величины параметров работы сети. Процентные значения приведены для представления относительных вкладов в отключение сети и результирующего воздействия сетевых услуг.

С.2 Анализ данных

Статистика работы сети показывает в общей сложности 303 отключения сети в течение двух лет работы услуг сети. От 303 отказов сети пострадало более миллиона абонентов или пользователей, общая продолжительность простоя составила 3196,5 мин. Прерывания в выполнении услуг характеризуют суммой прерываний телефонных услуг. Они сгруппированы по различным категориям отказов. В таблице С.1 приведены данные об отказах сети.

Таблица С.1 — Общие данные об отказах сети общенациональной коммутируемой телефонной сети

Источник отказа сети	Категория отказа	Количество отключений (прерываний работы)	Количество затронутых пользователей	Продолжительность неработоспособного состояния сети (мин)
Оборудование	Аппаратный отказ программного обеспечения	56 44	95 690 118 200	159,8 119,3
Трафик	Функции (перегрузка)	18	276 760	1 123,7
Стихийные бедствия	Стихийные бедствия	32	159 000	828,2
Безопасность	Вандализм	3	853 930	456,0
График работы	Техническое обслуживание	0	0	0
Человеческий фактор	Процедуры (ошибки человека)	150	265 996	509,5

Влияние услуг характеризуют совокупной продолжительностью неработоспособного состояния в пользовательских минутах по категориям.

Пользовательские минуты = (Количество пользователей, затронутых категорией отказа) × (продолжительность отключения категории в минутах).

На рисунке С.1 представлены прерывания работы сети и результирующее влияние на услуги сети.

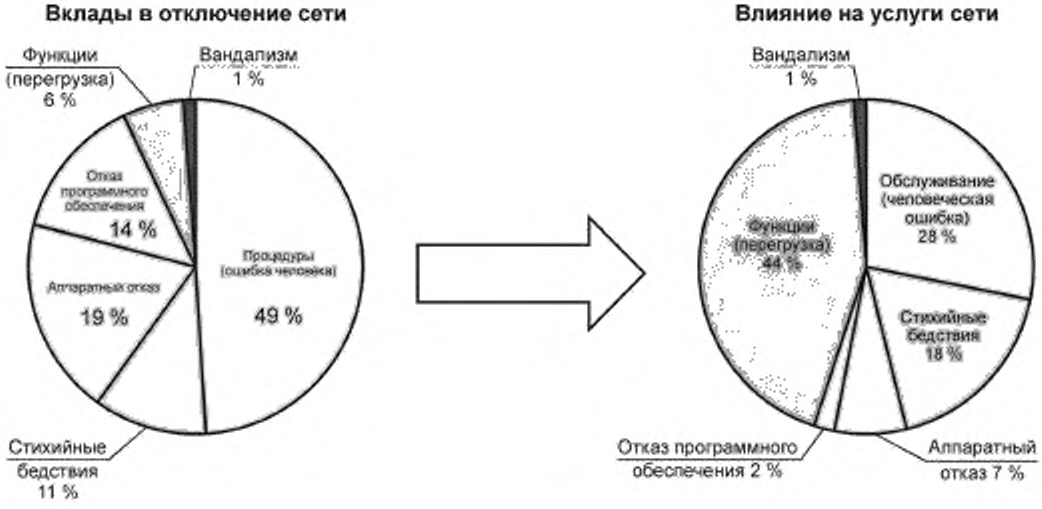


Рисунок С.1 — Вклады в отключение сети и результирующее влияние на услуги сети

С.3 Оценка характеристик надежности работы сети

Показатели готовности можно определить по совокупной (3196,5 мин) продолжительности прерываний работы сети за два года (2 × 365 × 24 × 60 = 1051200 мин) эксплуатации сети служб. Средняя продолжительность неработоспособного состояния сети составляет 1598 мин в год.

Коэффициент готовности сети в целом = (1051200 – 3196,5) / 1051200 = 99,696 %.

Работа услуг сети показывает 44 % влияния на функции (перегрузку), что проявляется в 6 % общего количества прерываний работы сети. Это наблюдение указывает на недостаточные возможности работы сети, что является основной причиной необходимого повышения надежности сети. Вклад процедур (человеческая ошибка) 49 % предполагает необходимость улучшения процедур OAMP.

Оператор сети оценивает состояние надежности работы сети в целом в соответствии с информацией о прерываниях работы сети, фиксируемой вместе с поставщиками услуг сети. Отдельные поставщики услуг несут ответственность за свои сегменты сети, свой повседневный вклад в работу услуги. Тенденции отказов и ухудшение работы определенных сегментов сети требуются для анализа данных о работе с привязкой ко времени от отдельных поставщиков услуг. Для определения времени обнаружения неисправности, времени до восстановления и интенсивности FRU требуется дополнительная информация о записях технического обслуживания сегментов сети от поставщиков услуг.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного национального стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р 27.015—2019 (МЭК 60300-3-15:2009)	MOD	IEC 60300-3-15:2009 «Менеджмент надежности. Часть 3-15. Руководство по применению. Проектирование надежности системы»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- MOD — модифицированный стандарт..

Библиография

[1] МЭК 61907:2009 Разработка функциональной надежности коммуникационных сетей (Communication network dependability engineering)

[2] МЭК 60050-191:1990* Международный электротехнический словарь. Глава 191: Надежность и качество услуг [International Electrotechnical Vocabulary (IEV) — Chapter 191: Dependability and quality of service]

[3] ITU-T Recommendation I.350:1988. General aspects of quality of service and network performance in digital networks, including ISDN

[4] ITU-T Recommendation G.1000, Communications quality of service: a framework and definitions

[5] ITU-T Recommendation E.800, Definitions of terms related to quality of service

[6] МЭК 61078:2006 Методы анализа надежности систем. Структурная схема надежности и булевы методы (Analysis techniques for dependability — Reliability block diagram and Boolean methods)

[7] МЭК 62198:2013 Управление риском в проектах. Указания по применению (Project risk management — Application guidelines)

[8] МЭК 31010: 2019 Менеджмент риска. Методы оценки риска (Risk management — Risk management techniques)

[9] МЭК 60812:2018 Анализ видов и последствий отказов (FMEA и FMECA) [Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)]

[10] МЭК 60300-3-11:2009 Управление общей надежностью. Часть 3-11. Руководство по применению. Техническое обслуживание, направленное на обеспечение надежности (Dependability management — Part 3-11: Application guide — Reliability centred maintenance)

[11] МЭК 61882:2016 Исследования опасности и работоспособности (HAZOP). Руководство по применению [Hazard and operability studies (HAZOP studies) — Application guide]

[12] МЭК 60300-3-1:2003 Управление общей надежностью. Часть 3-1. Руководство по применению. Методы анализа для определения общей надежности. Руководство по методологии (Dependability management — Part 3-1: Application guide — Analysis techniques for dependability — Guide on methodology)

[13] МЭК 61165:2019 Применение марковских методов (Application of Markov techniques)

[14] Lyu, M. R. (Ed.): The Handbook of Software Reliability Engineering, IEEE Computer Society Press and McGraw-Hill Book Company, 1996

[15] ИСО/МЭК 7498-1:1994 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель (Information technology — Open Systems Interconnection — Part 1: Basic Reference Model: The Basic Model)

[16] TL 9000, Quality Management System — Requirements Handbook 3.0, March 2001, Quality Excellence for Suppliers of Telecommunications Forum (QuEST Forum)

[17] TL 9000, Quality Management System — Measurements Handbook 3.5, March 2003, Quality Excellence for Suppliers of Telecommunications Forum (QuEST Forum)

[18] KUHN D.R., Sources of Failure in the Public Switched Telephone Network, IEEE Computer, Vol.30, No.4 (April 1997), National Institute of Standards and Technology, Gaithersburg, Maryland 20899 USA

* МЭК 60050-191:1990 заменен на МЭК 60050-192:2015.

УДК 62-192:658.51.011:658.562:623:006.354 ОКС 03.120.01

Ключевые слова: надежность в технике, коммуникационная сеть, надежность работы сети, надежность услуги сети, обеспечение надежности, узел, соединение, трафик, перегрузка, причины отказа, путь выполнения услуги

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 12.10.2021. Подписано в печать 28.10.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,76

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «РСТ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва. Нахимовский пр-т. д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru