Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
Пермский национальный исследовательский политехнический университет (ПНИПУ)

Факультет: электротехнический (ЭТФ)
Направление: 09.03.01 – Информатика и вычислительная техника (ИВТ)
Профиль: Компьютерные системы (КС)
Кафедра информационных технологий и автоматизированных систем (ИТАС)

Зав. кафедрой: д-р экон. наук, проф.
Файзрахманов Р.А._____
«_____»_____ 2026 г.

КУРСОВОЙ ПРОЕКТ

по дисциплине

«Проектирование информационных технологий и компьютерных сетей»

на тему

«Сетевое резервирование в дата-центрах»

Студент: 21.05.2026 Зайцева Карина Владимировна
(подпись, дата)

Группа: КС-23-1бзу

Состав курсовой работы:
1. Пояснительная записка на ____ стр.
2. Графический материал.
3. Электронный носитель с материалами курсовой работы.

Руководитель курсовой работы: 21.05.26 Доцент, канд. тех. наук Масич Г.Ф.
(подпись, дата)

(оценка)

Консультант по предметной области: Доцент, канд. тех. наук Масич Г.Ф.
(подпись, дата)

Пермь 2026

РЕФЕРАТ

Курсовая работа 57 с., 18 рис., 11 табл., 40 источн.

СЕТЕВОЕ РЕЗЕРВИРОВАНИЕ, ДАТА-ЦЕНТР, ОТКАЗОУСТОЙЧИВОСТЬ, L2-РЕЗЕРВИРОВАНИЕ, L3-РЕЗЕРВИРОВАНИЕ, MLAG, VRRP, BGP, ECMP, BFD, VXLAN, EVPN.

Объектом исследования является сетевая инфраструктура дата-центра.

Цель работы — обзор и систематизация подходов к сетевому резервированию в дата-центрах.

В процессе работы использованы методы анализа технических источников, сравнения сетевых технологий, классификации подходов к резервированию и обобщения практических решений. Рассмотрены горячее и холодное резервирование, физическое резервирование, L2- и L3-резервирование, межплощадочное резервирование, а также ограничения, которые невозможно устранить только сетевыми средствами.

В результате работы систематизированы основные уровни сетевого резервирования: физический, канальный, сетевой, overlay-уровень и межплощадочный уровень. Практическая значимость работы заключается в возможности применения результатов при проектировании и модернизации сетевой инфраструктуры дата-центров, корпоративных серверных помещений и облачных платформ.

Рекомендации по внедрению включают использование независимых физических трасс, резервных сетевых устройств, MLAG/MC-LAG, EVPN Multihoming, VRRP, BGP, ECMP и BFD. Экономическая значимость работы состоит в снижении риска простоев информационных систем и сокращении времени восстановления после аварий.

Развитие сетевого резервирования связано с распространением leaf-spine-архитектур, VXLAN EVPN-фабрик, автоматизации сетевых конфигураций, предиктивного мониторинга и самовосстанавливающихся сетевых решений.

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем проекте применяют следующие термины с соответствующими определениями.

Дата-центр — специализированная инженерная и информационно-технологическая площадка, предназначенная для размещения серверного, сетевого, телекоммуникационного и инженерного оборудования.

Сетевое резервирование — совокупность технических и организационных решений, направленных на сохранение сетевой связности при отказе отдельных компонентов сети.

Отказоустойчивость — способность системы сохранять работоспособность при отказе одного или нескольких компонентов.

Единая точка отказа — элемент системы, отказ которого приводит к нарушению работы всей системы или значительной её части.

Горячее резервирование — способ резервирования, при котором резервный элемент постоянно находится в рабочем состоянии и готов автоматически принять нагрузку при отказе основного элемента.

Холодное резервирование — способ резервирования, при котором резервный элемент заранее подготовлен, но не находится в активной работе и требует ручного ввода в эксплуатацию при отказе основного элемента.

Физическое резервирование — резервирование физических компонентов сети: кабелей, портов, сетевых карт, коммутаторов, маршрутизаторов, блоков питания, стоек, PDU и внешних каналов связи.

L2-резервирование — резервирование на канальном уровне модели OSI, связанное с обеспечением отказоустойчивости Ethernet-сегментов, VLAN, агрегированных каналов и подключений серверов.

L3-резервирование — резервирование на сетевом уровне модели OSI, связанное с обеспечением отказоустойчивости маршрутизации, шлюзов, IP-связности и внешних подключений.

Leaf-spine-архитектура — архитектура сети дата-центра, в которой серверы подключаются к leaf-коммутаторам, а leaf-коммутаторы соединяются со spine-коммутаторами для обеспечения масштабируемой связности.

Overlay-сеть — логическая сеть, построенная поверх существующей физической или маршрутизируемой сети.

Underlay-сеть — базовая физическая или маршрутизируемая сеть, поверх которой строятся overlay-сети.

Multihoming — подключение одного сетевого устройства, сервера или сегмента к нескольким сетевым устройствам или каналам связи для повышения отказоустойчивости.

Split-brain — аварийная ситуация, при которой два резервируемых устройства одновременно считают себя активными, что может привести к нарушению работы сети.

Межплощадочное резервирование — резервирование сетевой и сервисной инфраструктуры между двумя или более дата-центрами.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящем проекте применяют следующие сокращения и обозначения.

ACL — Access Control List, список контроля доступа.

BFD — Bidirectional Forwarding Detection, протокол быстрого обнаружения отказов сетевого пути.

BGP — Border Gateway Protocol, протокол внешней динамической маршрутизации.

DCI — Data Center Interconnect, технология или комплекс решений для соединения дата-центров между собой.

DWDM — Dense Wavelength Division Multiplexing, плотное спектральное мультиплексирование.

ECMP — Equal-Cost Multi-Path, механизм использования нескольких равнозначных маршрутов.

EVPN — Ethernet VPN, технология построения виртуальных Ethernet-сетей с использованием BGP control plane.

IP — Internet Protocol, сетевой протокол межсетевого взаимодействия.

L2 — Layer 2, канальный уровень модели OSI.

L3 — Layer 3, сетевой уровень модели OSI.

LACP — Link Aggregation Control Protocol, протокол управления агрегированием каналов.

MLAG — Multi-Chassis Link Aggregation, агрегирование каналов между несколькими физическими коммутаторами.

MC-LAG — Multi-Chassis Link Aggregation, технология агрегирования каналов с использованием нескольких коммутаторов.

NIC — Network Interface Card, сетевая карта.

OSI — Open Systems Interconnection, эталонная модель взаимодействия открытых систем.

OTN — Optical Transport Network, оптическая транспортная сеть.

PDU — Power Distribution Unit, блок распределения питания.

RSTP — Rapid Spanning Tree Protocol, ускоренная версия протокола STP.

SFP — Small Form-factor Pluggable, сменный оптический или медный трансивер.

STP — Spanning Tree Protocol, протокол предотвращения петель в Ethernet-сети.

ToR — Top of Rack, коммутатор верхнего уровня стойки.

VLAN — Virtual Local Area Network, виртуальная локальная сеть.

vPC — Virtual Port Channel, технология Cisco для подключения устройства к двум коммутаторам как к одному логическому узлу.

VRRP — Virtual Router Redundancy Protocol, протокол резервирования виртуального маршрутизатора.

VXLAN — Virtual Extensible LAN, технология построения overlay-сетей поверх L3-инфраструктуры.

ЦОД — центр обработки данных.

ВВЕДЕНИЕ

Современный дата-центр представляет собой сложную инженерную и сетевую инфраструктуру, в которой отказ одного элемента не должен приводить к полной потере доступности сервисов. Поэтому при проектировании сетей ЦОД применяются различные механизмы резервирования: дублирование физических каналов, коммутаторов, маршрутизаторов, внешних подключений, шлюзов и логических сетевых сервисов.

Актуальность темы обусловлена тем, что информационные системы организаций всё чаще размещаются в дата-центрах и облачных инфраструктурах. Для таких систем важна непрерывность работы, так как сбой сетевой инфраструктуры может привести к недоступности приложений, баз данных, систем хранения, пользовательских сервисов и корпоративных информационных систем. При этом простое добавление второго коммутатора или второго канала связи не всегда обеспечивает реальную отказоустойчивость. Если резервные элементы зависят от одной точки питания, одной кабельной трассы, одного оператора связи или одной ошибки конфигурации, то такая схема сохраняет скрытые единые точки отказа.

В качестве отправной точки в работе используется материал Selectel, посвящённый сетевому резервированию в дата-центрах. В нём рассматриваются физическое резервирование, L2- и L3-подходы, а также практические схемы подключения оборудования в ЦОД. Дополнительно используются материалы по MLAG, BGP, VRRP, VXLAN, EVPN, BFD и межплощадочному резервированию, так как эти технологии широко применяются в современных сетях дата-центров.

Цель курсовой работы — выполнить обзор, сравнение и систематизацию подходов к сетевому резервированию в дата-центрах, а также определить особенности применения физических, L2-, L3- и межплощадочных механизмов резервирования при проектировании отказоустойчивой сетевой инфраструктуры.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Рассмотреть сущность сетевого резервирования и его роль в обеспечении отказоустойчивости дата-центров.

2. Изучить особенности горячего и холодного резервирования сетевой инфраструктуры.

3. Описать физическое резервирование оборудования, каналов связи, uplink-подключений и внешних сетевых подключений дата-центра.

4. Проанализировать технологии L2-резервирования, включая LACP, MLAG, MC-LAG, vPC, VXLAN и EVPN Multihoming.

5. Проанализировать технологии L3-резервирования, включая VRRP, BGP, ECMP и BFD.

6. Рассмотреть особенности межплощадочного резервирования дата-центров и применения DCI, DWDM, OTN, BGP и VXLAN EVPN Multi-Site.

7. Определить элементы и факторы, которые невозможно полностью зарезервировать только сетевыми средствами.

8. Систематизировать отечественные и зарубежные источники по теме сетевого резервирования и сформировать рекомендации по применению рассмотренных подходов.

Объект исследования — процессы проектирования отказоустойчивой сетевой инфраструктуры дата-центра.

Предмет исследования — технологии физического, канального, сетевого и межплощадочного резервирования, применяемые при построении сетей дата-центров.

1 Общие принципы сетевого резервирования в дата-центрах

Сетевое резервирование — это совокупность технических и организационных решений, направленных на сохранение сетевой связности при отказе отдельных компонентов. В дата-центре резервируются не только коммутаторы и маршрутизаторы, но и физические линии связи, трансиверы, кабельные трассы, блоки питания, вентиляторы, uplink-порты, внешние каналы связи, IP-шлюзы, маршруты и сервисы управления [1, 5, 13].

Главная задача резервирования заключается в устранении единой точки отказа. Единой точкой отказа может быть один физический кабель, один коммутатор доступа, один маршрутизатор, один uplink-канал, один оператор связи, один блок питания или одна кабельная трасса [1, 3, 15]. Если любой из таких элементов выходит из строя и это приводит к потере связности, значит, схема сети не является полноценно отказоустойчивой.

В инженерной практике применяются схемы резервирования N, N+1, 2N и 2(N+1). Схема N означает минимально необходимое количество компонентов без дополнительного резерва. Схема N+1 предполагает наличие одного дополнительного элемента, который может заменить отказавший компонент. Схема 2N означает полное дублирование рабочей системы. Схема 2(N+1) является более устойчивой, так как дублируются две группы компонентов, каждая из которых имеет собственный дополнительный резерв [15, 18, 20].

В сетевой инфраструктуре дата-центра резервирование обычно строится по нескольким уровням. На физическом уровне дублируются кабели, сетевые карты, порты, коммутаторы, блоки питания и трассы. На канальном уровне используются технологии LACP, MLAG, MC-LAG, vPC, STP, VXLAN и EVPN. На сетевом уровне применяются VRRP, BGP, OSPF, ECMP и BFD [1, 8, 21, 22, 23, 24, 27]. Основные уровни сетевого резервирования в дата-центрах представлены в таблице 1.

Таблица 1 — Уровни сетевого резервирования в дата-центрах

Уровень резервирования	**Что резервируется**	**Примеры технологий**
Физический уровень	Коммутаторы, кабели, порты, блоки питания, трассы	Dual-homing, независимые трассы, hot-swap PSU
L2-уровень	Ethernet-сегменты, VLAN, агрегированные каналы	STP, LACP, MLAG, MC-LAG, vPC
L3-уровень	Маршруты, шлюзы, внешние подключения	VRRP, BGP, OSPF, ECMP, BFD
Overlay-уровень	Виртуальные сети поверх IP-фабрики	VXLAN, EVPN
Межплощадочный уровень	Связность между ЦОД	DCI, DWDM, OTN, BGP, VXLAN EVPN Multi-Site

Как видно из таблицы 1, сетевое резервирование в дата-центре не ограничивается только дублированием физических компонентов. Оно включает несколько уровней, каждый из которых решает отдельную задачу отказоустойчивости.

На практике перечисленные уровни не используются изолированно. Например, сервер может быть физически подключён к двум ToR-коммутаторам, на уровне L2 может использоваться MLAG, а на уровне L3 — маршрутизация через BGP и ECMP. Такой комбинированный подход позволяет повысить устойчивость сети и снизить риск простоя [1, 26, 28, 36].

2 Горячее и холодное резервирование

Резервирование сетевой инфраструктуры может быть организовано по разным схемам. Наиболее распространёнными являются горячее и холодное резервирование. Их отличие заключается в состоянии резервного элемента и времени его включения в работу. При горячем резервировании резервный компонент уже находится в рабочем состоянии и может автоматически принять нагрузку. При холодном резервировании запасной компонент заранее подготовлен, но не участвует в работе сети до возникновения аварии.

Общее различие между горячим и холодным резервированием показано на рисунке 1.

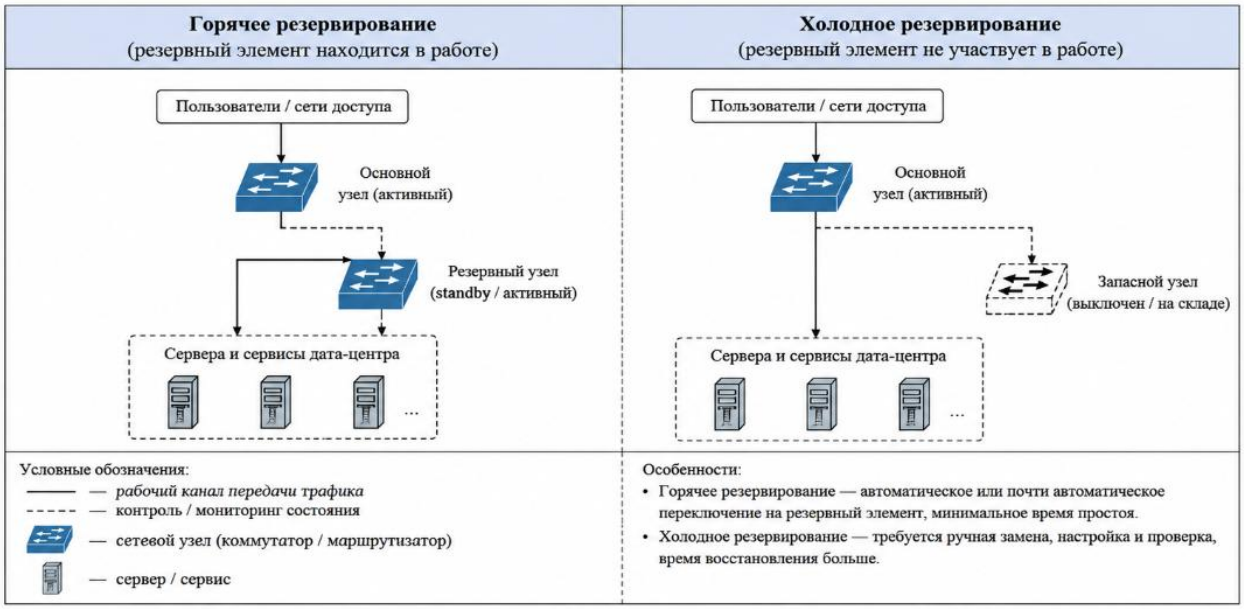

Рисунок 1 — Сравнение горячего и холодного резервирования

Как показано на рисунке 1, горячее резервирование обеспечивает быстрое переключение на резервный элемент, поскольку он уже подключён к рабочей схеме. Холодное резервирование требует больше времени, так как запасной компонент необходимо физически установить, подключить, настроить и проверить.

2.1 Горячее резервирование

Горячее резервирование — это схема, при которой резервный элемент постоянно находится в рабочем состоянии и готов принять нагрузку автоматически или почти автоматически. В сетях дата-центров горячее

резервирование применяется для шлюзов, маршрутизаторов, коммутаторов, физических линков, BGP-сессий, виртуальных IP-адресов и каналов между сетевыми устройствами [13, 14, 21].

Одним из примеров горячего резервирования является использование VRRP. Протокол VRRP позволяет нескольким маршрутизаторам использовать один виртуальный IP-адрес, который применяется хостами как шлюз по умолчанию. Если активный маршрутизатор становится недоступен, резервный маршрутизатор принимает его роль и продолжает обслуживать трафик [21]. Такой подход позволяет уменьшить время простоя при отказе шлюза.

Пример горячего резервирования шлюза с использованием VRRP представлен на рисунке 2.

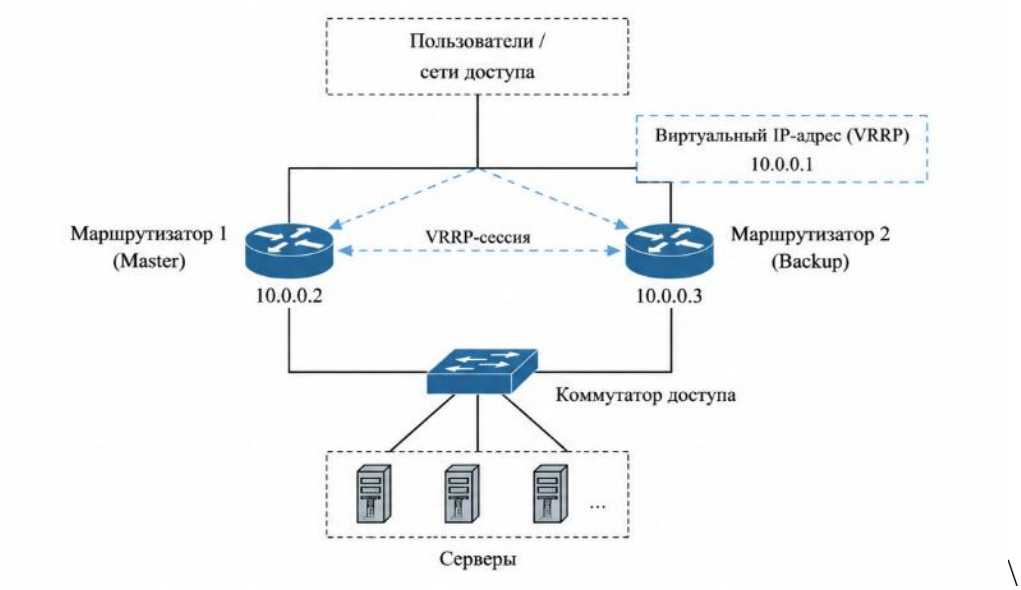

Рисунок 2 — Горячее резервирование шлюза с использованием VRRP

На рисунке 2 показано, что пользователи и серверы используют виртуальный IP-адрес 10.0.0.1 в качестве шлюза по умолчанию. В нормальном режиме активным является Маршрутизатор 1 (Master), а Маршрутизатор 2 находится в состоянии резервного (Backup).

Если активный маршрутизатор становится недоступным, резервный маршрутизатор автоматически принимает роль Master и продолжает обслуживать трафик на том же виртуальном IP-адресе, что обеспечивает минимальное время простоя для пользователей и сервисов.

Другим примером горячего резервирования является MLAG или MC-LAG. В такой схеме сервер подключается к двум разным физическим коммутаторам, но логически видит их как один агрегированный канал. При отказе одного коммутатора или одного физического линка сервер сохраняет сетевую доступность через оставшийся путь [8, 36]. Подобные механизмы часто применяются на уровне подключения серверов к ToR-коммутаторам.

Горячее резервирование может работать по модели active-standby или active-active. В active-standby-схеме один элемент является основным, а второй ожидает отказа. В active-active-схеме оба элемента одновременно участвуют в передаче трафика. Active-active-подход эффективнее использует ресурсы, однако требует более сложной настройки и контроля состояния [30, 33, 36]. Основные преимущества и недостатки горячего резервирования приведены в таблице 2.

Таблица 2 — Преимущества и недостатки горячего резервирования

Преимущества	**Недостатки**
Минимальное время восстановления после отказа	Более высокая стоимость оборудования
Возможность автоматического переключения	Сложность настройки и диагностики
Поддержка критичных сервисов	Риск некорректного переключения или split-brain-сценария

Из таблицы 2 следует, что горячее резервирование обеспечивает минимальное время восстановления, но требует дополнительных затрат на оборудование, настройку и сопровождение.

Таким образом, горячее резервирование целесообразно применять для критичных компонентов сетевой инфраструктуры, где даже кратковременная недоступность может привести к серьёзным последствиям [13, 14].

2.2 Холодное резервирование

Холодное резервирование — это схема, при которой резервный элемент заранее подготовлен, но не находится в активной работе. Например, в дата-центре может храниться запасной коммутатор, маршрутизатор, блок питания, трансивер, патч-корд или сервер, который будет установлен и настроен только

после отказа основного оборудования [13, 15]. Пример холодного резервирования сетевого оборудования представлен на рисунке 3.

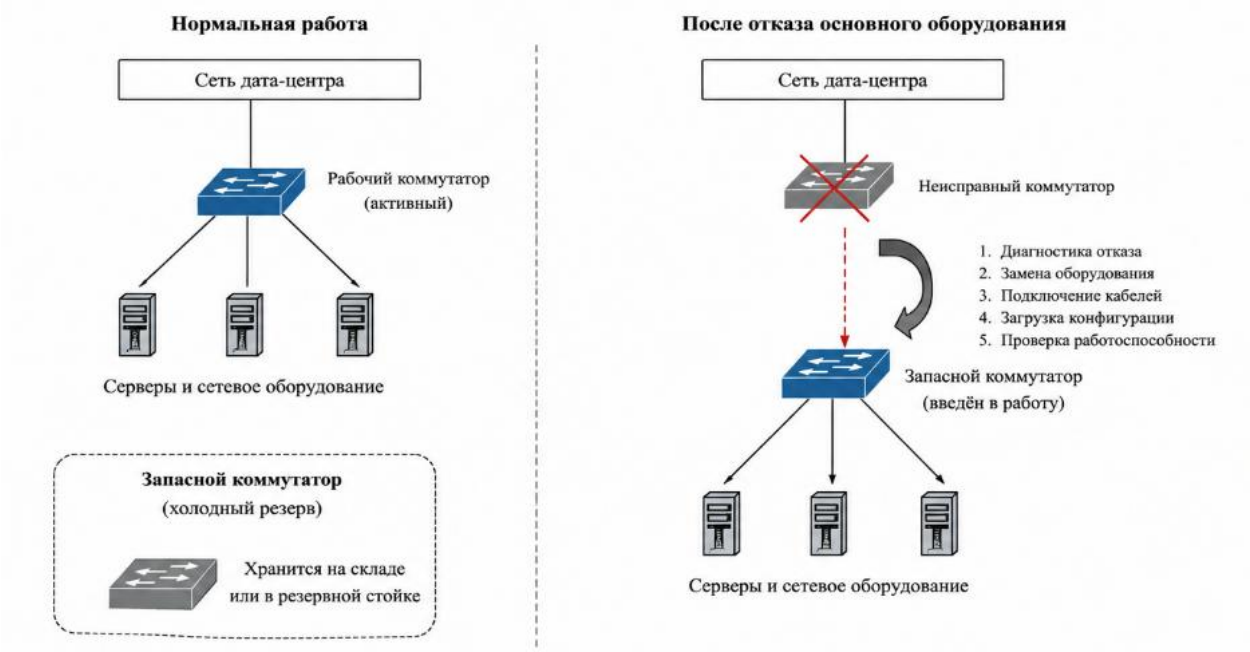

Рисунок 3 - Пример холодного резервирования сетевого оборудования

Как показано на рисунке 3, в нормальном режиме работает основной коммутатор, а запасной коммутатор находится в резерве и не участвует в передаче трафика. При отказе основного оборудования выполняются диагностика, замена устройства, подключение кабелей, загрузка конфигурации и проверка работоспособности. Такой подход позволяет восстановить работу сетевой инфраструктуры, однако требует значительно большего времени по сравнению с горячим резервированием.

Холодное резервирование дешевле горячего, так как резервный элемент не обязательно постоянно включён в рабочую схему. Однако время восстановления при такой модели значительно выше. Для восстановления может потребоваться диагностика, физическая замена оборудования, подключение кабелей, загрузка конфигурации и проверка работоспособности [14, 15]. Сравнение горячего и холодного резервирования представлено в таблице 3.

Таблица 3 — Сравнение горячего и холодного резервирования

Критерий	**Горячее резервирование**	**Холодное резервирование**
Состояние резерва	Постоянно работает	Отключён или не введён в эксплуатацию
Время восстановления	Секунды или минуты	Минуты, часы или больше
Стоимость	Выше	Ниже
Автоматизация	Обычно есть	Обычно отсутствует
Применение	Критичные сервисы	Запасные компоненты, некритичные системы

Как видно из таблицы 3, горячее резервирование целесообразно применять для критичных сервисов, а холодное — для запасных компонентов и менее критичных участков инфраструктуры.

Для дата-центров наиболее рациональным является комбинированный подход. Критичные сетевые узлы, такие как border-маршрутизаторы, ToR-коммутаторы, шлюзы и uplink-каналы, резервируются горячим способом. При этом отдельные запасные компоненты, например трансиверы, кабели и блоки питания, могут храниться как холодный резерв [5, 13, 15].

3 Физическое резервирование

Физическое резервирование является базовым уровнем отказоустойчивости. Оно включает дублирование физических компонентов сети и инженерной инфраструктуры. Если физический уровень построен неправильно, то L2- и L3-протоколы не смогут обеспечить полноценную отказоустойчивость [1, 3, 15].

К основным элементам физического резервирования относятся сетевые карты серверов, коммутаторы доступа, кабельные линии, трансиверы, uplink-подключения, блоки питания, PDU, стойки и внешние каналы связи [1, 5, 12]. Основные элементы физического резервирования и способы их дублирования приведены в таблице 4.

Таблица 4 — Элементы физического резервирования

Элемент	**Способ резервирования**
Серверные сетевые карты	Использование двух и более NIC
Коммутаторы доступа	Подключение сервера к двум ToR-коммутаторам
Кабели	Прокладка по разным физическим трассам
Трансиверы	Использование независимых SFP/QSFP-модулей
Блоки питания	Подключение к разным PDU
Uplink-каналы	Подключение к разным spine/aggregation-узлам
Внешние операторы	Подключение к разным провайдерам связи

Данные таблицы 4 показывают, что физическое резервирование должно охватывать не только сетевые устройства, но и кабельную, энергетическую и внешнюю телекоммуникационную инфраструктуру.

3.1 Резервирование сетевых карт сервера и коммутаторов доступа

Одним из основных способов физического резервирования является дублирование сетевых интерфейсов сервера и подключение к двум разным коммутаторам доступа. Такая схема позволяет сохранить связность при отказе одного сетевого адаптера, одного кабеля или одного ToR-коммутатора [1, 5, 8]. Пример резервирования сетевых карт сервера и коммутаторов доступа представлен на рисунке 4.

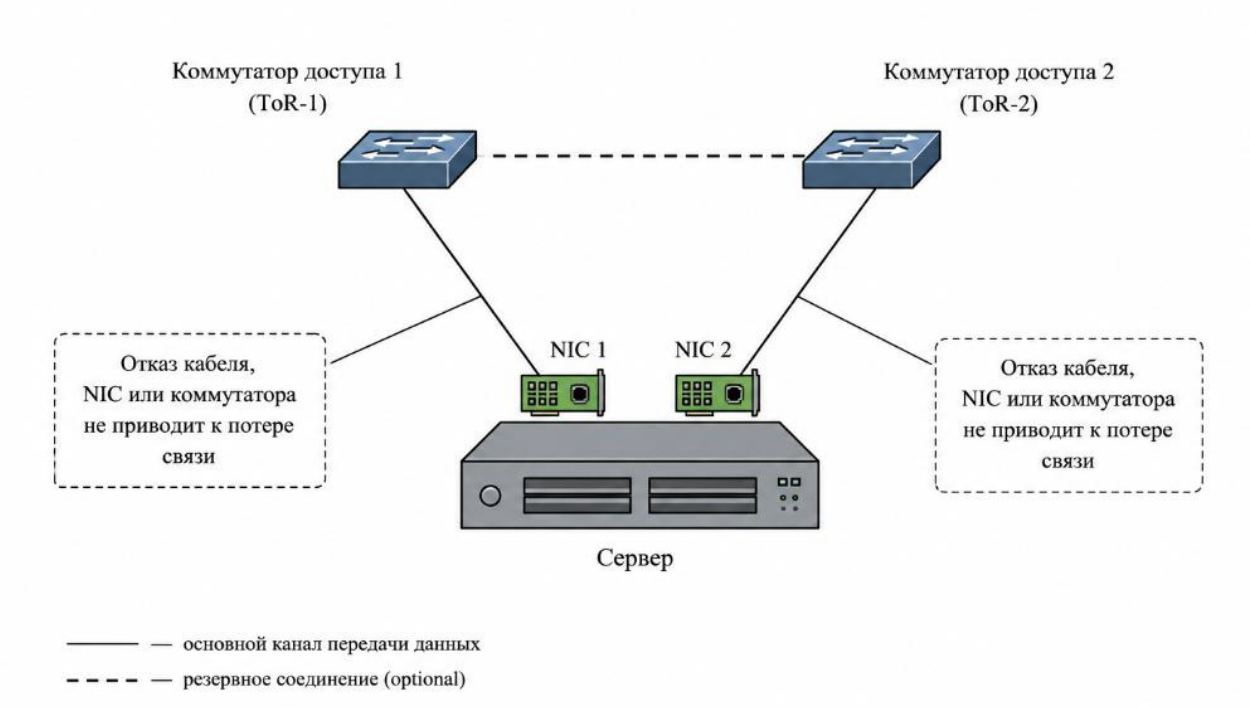

Рисунок 4 — Резервирование сетевых карт сервера и коммутаторов доступа

Как показано на рисунке 4, сервер оснащён двумя сетевыми интерфейсами, каждый из которых подключён к отдельному коммутатору доступа. При отказе одного интерфейса, одного кабеля или одного ToR-коммутатора трафик продолжает передаваться через второй путь. Такая схема устраняет одну из основных единых точек отказа на уровне подключения сервера [1, 8].

3.2 Резервирование питания: блоки питания и PDU

Для физического резервирования недостаточно дублировать только сетевые соединения. Не менее важным является резервирование электропитания, поскольку отказ одного блока питания, одной PDU или одной линии питания может привести к отключению оборудования [13, 15]. Пример резервирования питания оборудования дата-центра показан на рисунке 5.

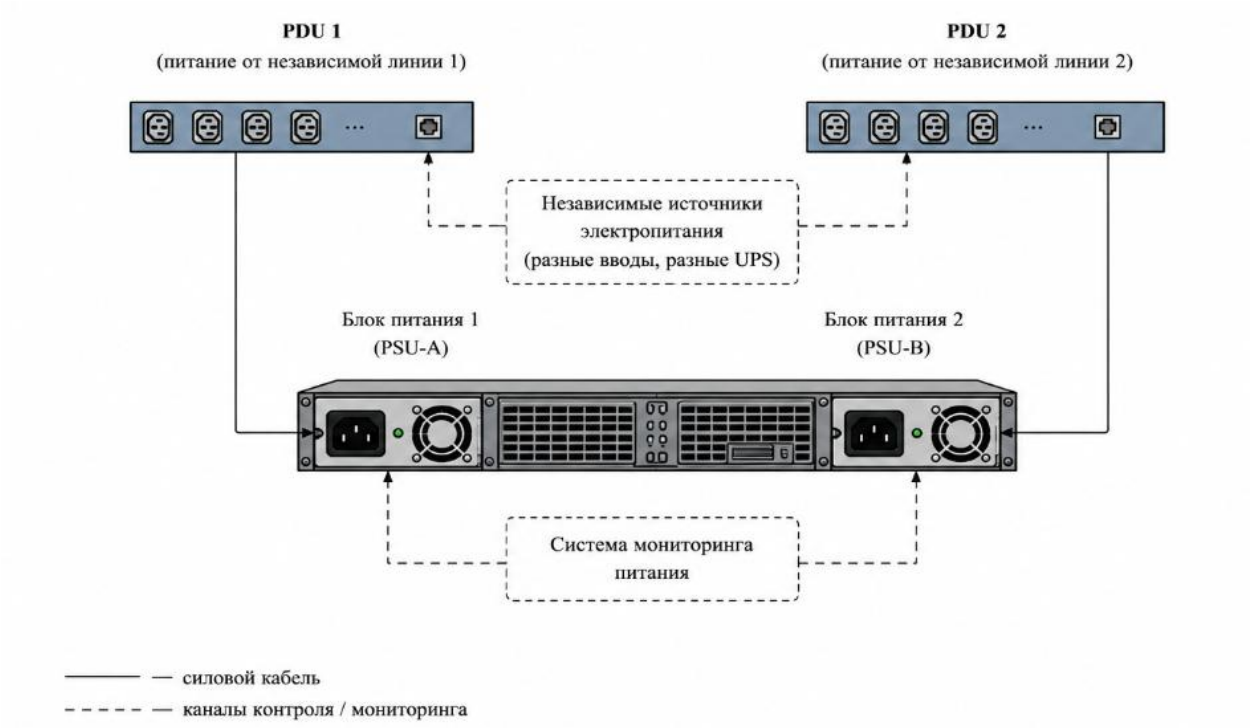

Рисунок 5 — Резервирование питания оборудования с использованием двух блоков питания и двух PDU

Из рисунка 5 видно, что сервер или коммутатор оснащён двумя блоками питания, которые подключаются к разным PDU. Такое решение позволяет сохранить работоспособность оборудования при отказе одного блока питания, одной PDU или одной линии электропитания. В дата-центрах подобная схема является обязательным элементом физической отказоустойчивости [13, 15, 18].

3.3 Резервирование кабельных трасс и uplink-подключений

Физическое резервирование включает не только наличие двух кабелей, но и их прокладку по разным трассам. Если оба кабеля проходят через один кабельный канал, повреждение этой трассы приведёт к одновременному отказу обоих соединений [3, 15]. Пример резервирования кабельных линий и uplink-подключений представлен на рисунке 6.

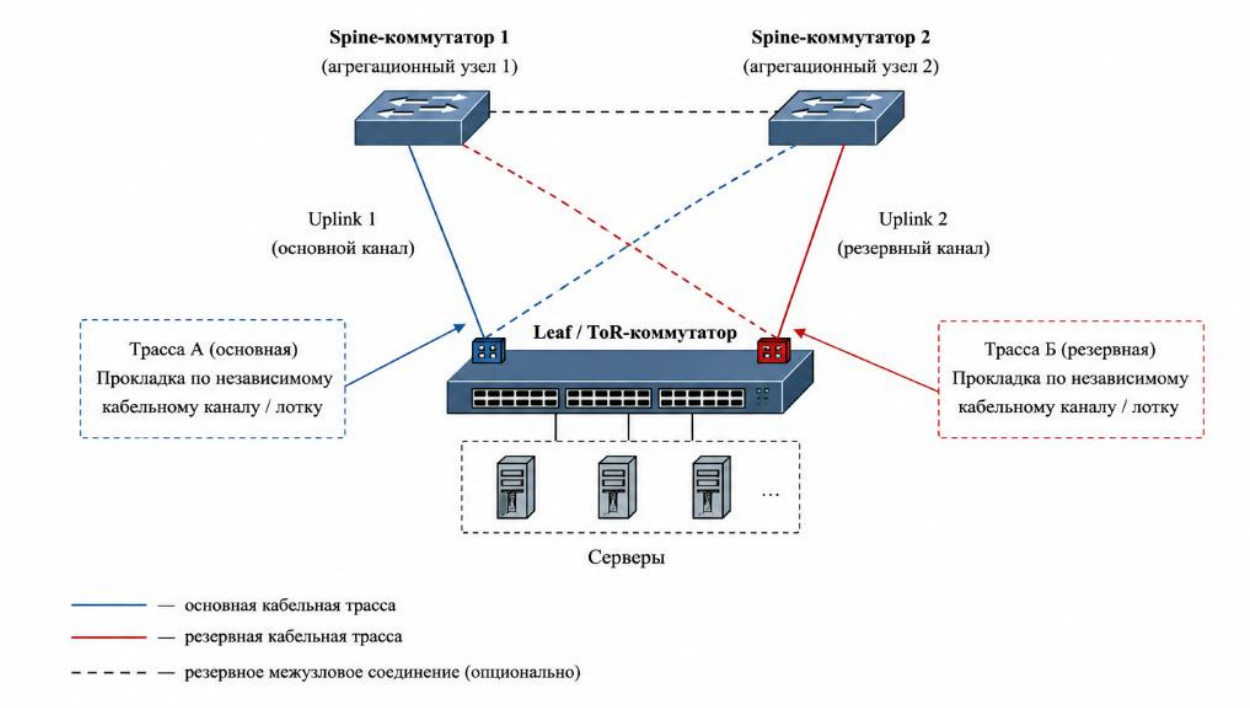

Рисунок 6 — Резервирование кабельных трасс и uplink-подключений

Как показано на рисунке 6, два uplink-канала прокладываются по независимым физическим маршрутам и подключаются к разным коммутаторам или узлам агрегации. При повреждении одной кабельной трассы трафик продолжает передаваться по второй. Это повышает устойчивость сети к механическим повреждениям, ошибкам монтажа и авариям на трассе [3, 15].

3.4 Резервирование внешних каналов связи

Для полноценной отказоустойчивости дата-центра необходимо резервировать не только внутреннюю сеть, но и внешние подключения. При использовании одного провайдера или одного физического ввода внешней линии связи сохраняется риск полной потери внешней доступности [3, 7, 15]. Пример резервирования внешних каналов связи представлен на рисунке 7.

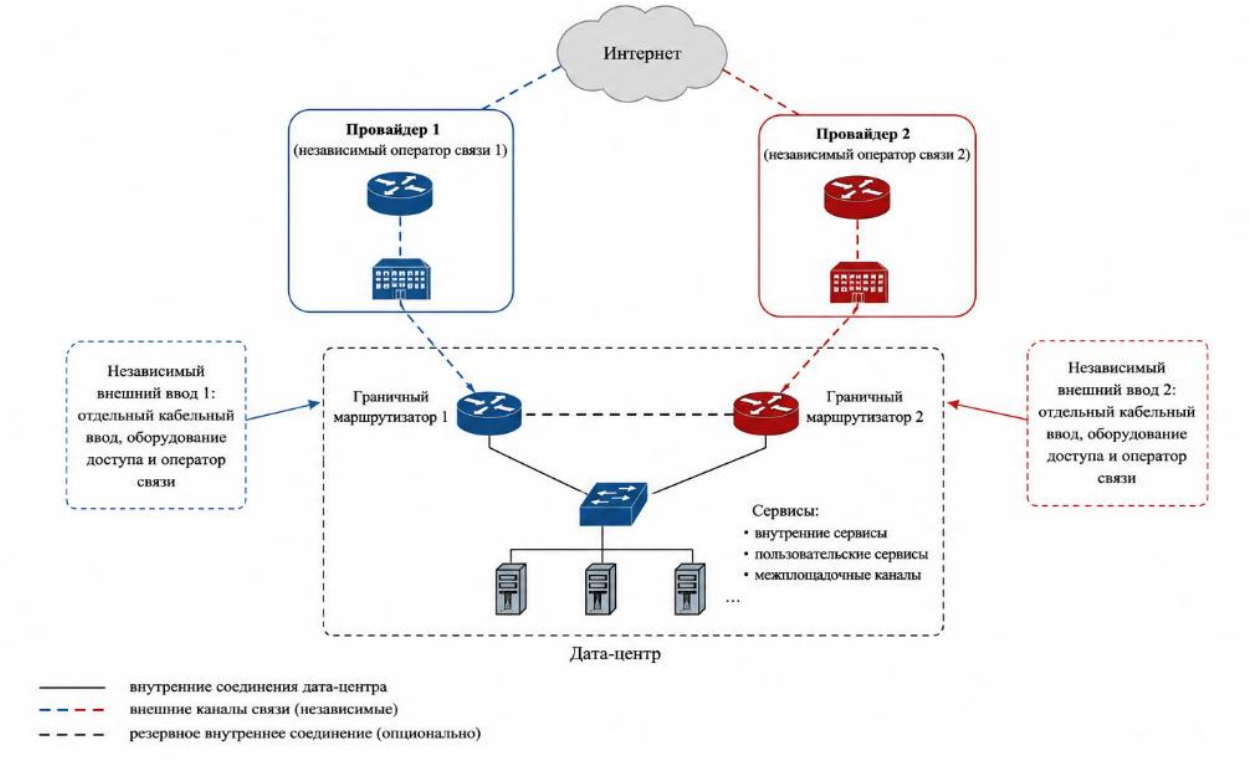

Рисунок 7 — Резервирование внешних каналов связи дата-центра

На рисунке 7 показано, что дата-центр подключается к двум независимым операторам связи через разные внешние вводы. При отказе одного провайдера или одного канала доступ к внешним сетям сохраняется через второго оператора. Такая схема применяется для повышения надёжности интернет-доступа, межплощадочного взаимодействия и клиентских сервисов [3, 7, 24].

3.5 Обобщающая схема физического резервирования сервера в дата-центре

Важным условием является не только наличие второго элемента, но и его независимость. Если два канала проходят через одну кабельную трассу, то физическое повреждение этой трассы приведёт к отказу обоих каналов. Если два коммутатора подключены к одной PDU, то отказ питания также может вывести из строя оба устройства [3, 15]. Поэтому при проектировании нужно учитывать не только логическую схему, но и фактическое размещение оборудования.

Типовая схема физического резервирования сервера в дата-центре представлена на рисунке 8.

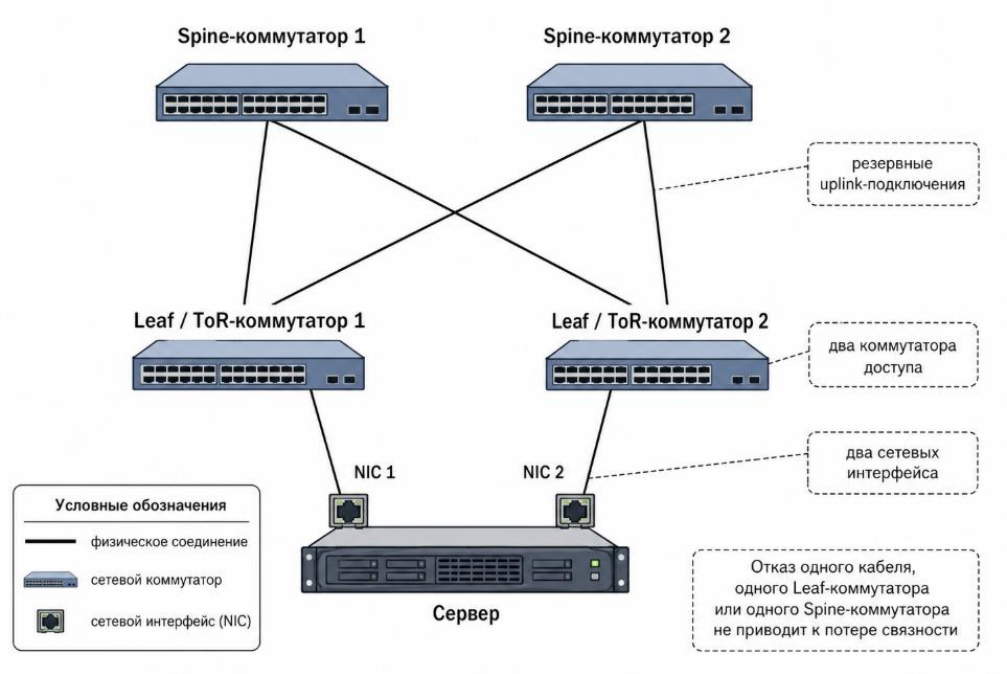

Рисунок 8 — Типовая схема физического резервирования сервера в дата-центре

Как показано на рисунке 8, сервер подключается к двум разным коммутаторам доступа, а каждый leaf-коммутатор имеет резервные uplink-подключения к spine-уровню. Такая схема позволяет сохранить сетевую связность при отказе одного кабеля, одного leaf-коммутатора или одного spine-коммутатора [26, 28, 37].

Для физического резервирования также важно учитывать требования к оборудованию. В дата-центрах часто применяются коммутаторы с поддержкой hot-swap-блоков питания, резервируемых вентиляторов, нескольких uplink-портов и поддержки технологий MLAG или EVPN Multihoming [8, 12, 36]. Это позволяет не только повысить доступность, но и выполнять часть технических работ без полной остановки сетевого узла.

4 L2-резервирование

L2-резервирование относится к канальному уровню модели OSI. Оно применяется там, где необходимо обеспечить отказоустойчивость Ethernet-сегментов, VLAN, физических линков между сервером и коммутаторами, а также связность внутри одной широковещательной доменной области [1, 8, 36].

К основным технологиям L2-резервирования относятся STP, RSTP, LACP, MLAG, MC-LAG, vPC, VXLAN и EVPN Multihoming [8, 22, 23, 25, 30, 33, 36].

Суть L2-резервирования заключается в том, что сервер или сетевое устройство подключается к сети не через один физический канал, а через несколько независимых подключений. При этом важно учитывать, что два кабеля не подключаются в один физический порт сетевой карты. Для резервирования используются два сетевых порта: это могут быть две отдельные сетевые карты или одна сетевая карта с двумя портами. Каждый порт подключается к отдельному коммутатору доступа.

На практике для такой схемы могут использоваться LACP и MLAG/MC-LAG. LACP объединяет несколько физических портов сервера в один логический агрегированный канал. MLAG позволяет подключить этот агрегированный канал не к одному физическому коммутатору, а к двум разным ToR-коммутаторам, которые для сервера выглядят как одно логическое устройство [8, 36]. В результате отказ одного кабеля, одного сетевого порта или одного коммутатора доступа не приводит к полной потере сетевой связности.

Пример организации L2-резервирования с использованием LACP и MLAG представлен на рисунке 9.

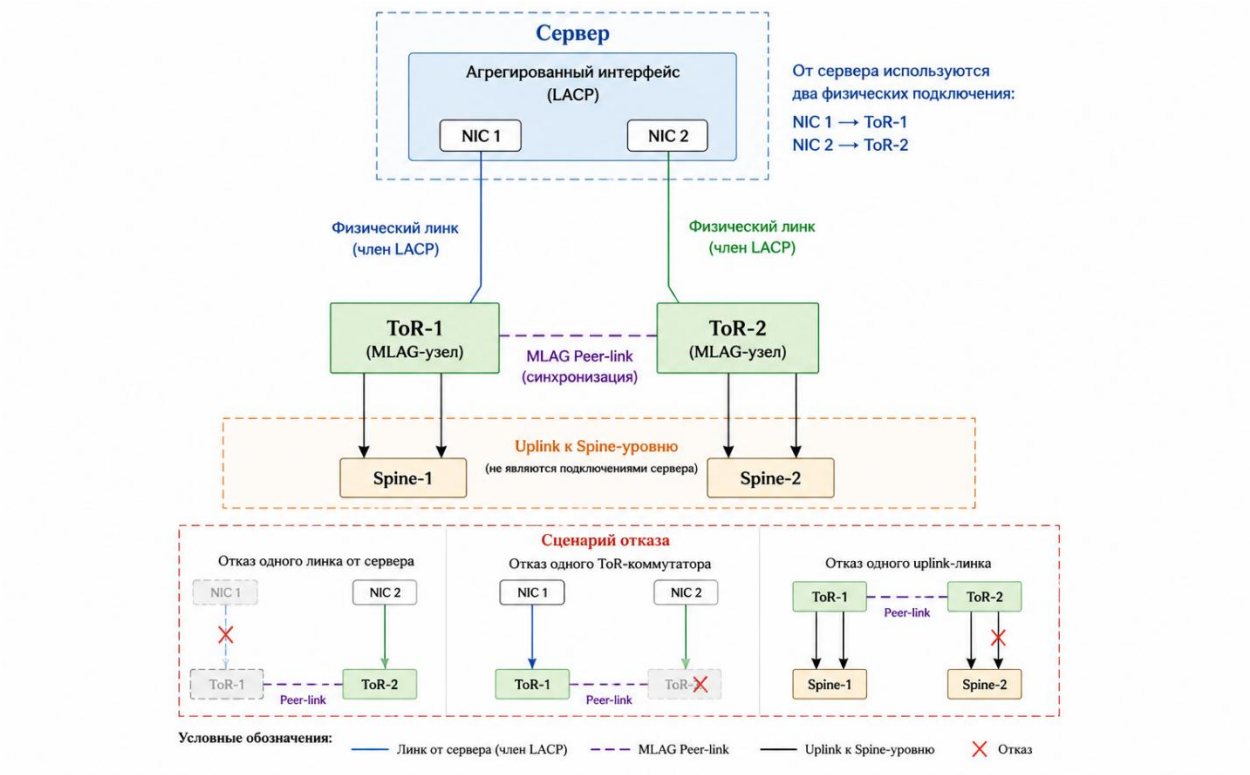

Рисунок 9 — Схема L2-резервирования с использованием LACP и MLAG

На рисунке 9 представлена схема L2-резервирования подключения сервера с использованием LACP и MLAG. Сервер подключается к сети двумя физическими интерфейсами: NIC 1 подключается к ToR-1, а NIC 2 — к ToR-2. Эти два физических линка являются участниками одного агрегированного интерфейса LACP, поэтому для сервера они работают как единый логический канал [8, 36].

Коммутаторы ToR-1 и ToR-2 образуют MLAG-пару и для подключенного сервера воспринимаются как единый логический узел. Между ними используется MLAG Peer-link, предназначенный для синхронизации служебной информации и состояния агрегированного соединения. В отдельных реализациях MLAG также может применяться keepalive-канал для контроля состояния соседнего коммутатора и снижения риска split-brain-ситуаций [4, 8, 36].

Отдельно на рисунке показаны uplink-подключения ToR-коммутаторов к Spine-уровню. Эти линии не являются подключениями сервера, а относятся к связям между уровнем доступа и уровнем ядра сетевой фабрики дата-центра [26, 28].

В нижней части рисунка приведены возможные сценарии отказа: отказ одного линка от сервера, отказ одного ToR-коммутатора и отказ одного uplink-линка. Во всех случаях сетевое подключение сервера сохраняется за счёт оставшегося доступного пути. Такая схема позволяет устранить единую точку отказа на уровне подключения сервера к сети и повысить отказоустойчивость L2-сегмента [8, 30, 36].

4.1 STP и его ограничения

Классическим способом защиты Ethernet-сети от петель является STP. Протокол блокирует избыточные пути, чтобы в сети не возникали широковещательные штормы. Однако в дата-центрах STP имеет серьёзные ограничения, так как часть физических линков находится в заблокированном состоянии и не используется для передачи полезного трафика [1, 36].

Для небольших сетей STP может быть приемлемым решением, но в современных дата-центрах он считается недостаточно эффективным. Это связано с ограниченной масштабируемостью, риском ошибок при изменении топологии и неэффективным использованием резервных каналов [1, 36]. Поэтому в ЦОД чаще применяются технологии, позволяющие использовать несколько каналов одновременно.

4.2 LACP и агрегирование каналов

LACP используется для объединения нескольких физических каналов в один логический. Это повышает пропускную способность и позволяет пережить отказ одного физического линка [8, 36]. Например, если сервер подключён к коммутатору двумя или четырьмя кабелями, LACP может объединить эти соединения в один агрегированный интерфейс.

Однако обычный LAG имеет ограничение: все физические порты должны завершаться на одном коммутаторе. Если этот коммутатор откажет, весь агрегированный канал станет недоступен [8]. Поэтому для дата-центров более полезным является расширенный вариант — MLAG или MC-LAG.

4.3 MLAG, MC-LAG и vPC

MLAG/MC-LAG позволяют подключать один сервер или сетевое устройство к двум разным физическим коммутаторам так, чтобы для подключенного оборудования это выглядело как один логический агрегированный канал [8, 36]. У разных производителей технология может называться по-разному: MLAG, MC-LAG, vPC, M-LAG и т.д. Например, Cisco использует термин vPC, Arista — MLAG, Juniper — EVPN LAG Multihoming или MC-LAG в зависимости от платформы и сценария [30, 35, 36].

MLAG/MC-LAG широко применяются в сетях дата-центров для подключения серверов, систем хранения, гипервизоров и сетевых сервисов. Однако такие схемы требуют аккуратной настройки peer-link, keepalive-соединений и правил отказа, так как неправильная конфигурация может привести к петлям или раздвоению активной роли [30, 36]. Основные преимущества и недостатки MLAG/MC-LAG представлены в таблице 5.

Таблица 5 — Преимущества и недостатки MLAG/MC-LAG

Преимущество или недостаток	**Описание**
Преимущество	Сервер сохраняет связь при отказе одного ToR-коммутатора
Преимущество	Оба канала могут использоваться одновременно
Преимущество	Для сервера схема выглядит как обычный LACP-канал
Недостаток	Требуется служебная связь между коммутаторами
Недостаток	Возможны split-brain-сценарии
Недостаток	Реализация зависит от конкретного производителя

Из таблицы 5 видно, что MLAG/MC-LAG позволяют повысить отказоустойчивость подключения серверов, но требуют более сложной настройки и контроля состояния между коммутаторами.

MLAG/MC-LAG широко применяются в сетях дата-центров для подключения серверов, систем хранения, гипервизоров и сетевых сервисов.

Однако такие схемы требуют аккуратной настройки peer-link, keepalive-соединений и правил отказа, так как неправильная конфигурация может привести к петлям или раздвоению активной роли [30, 36].

4.4 VXLAN и EVPN

В современных дата-центрах всё чаще используется модель IP-fabric и overlay-сетей. В такой архитектуре underlay-сеть строится на L3-маршрутизации, а L2-сегменты создаются поверх неё с помощью VXLAN [23, 28, 37]. Общая схема построения VXLAN overlay поверх L3 underlay представлена на рисунке 10.

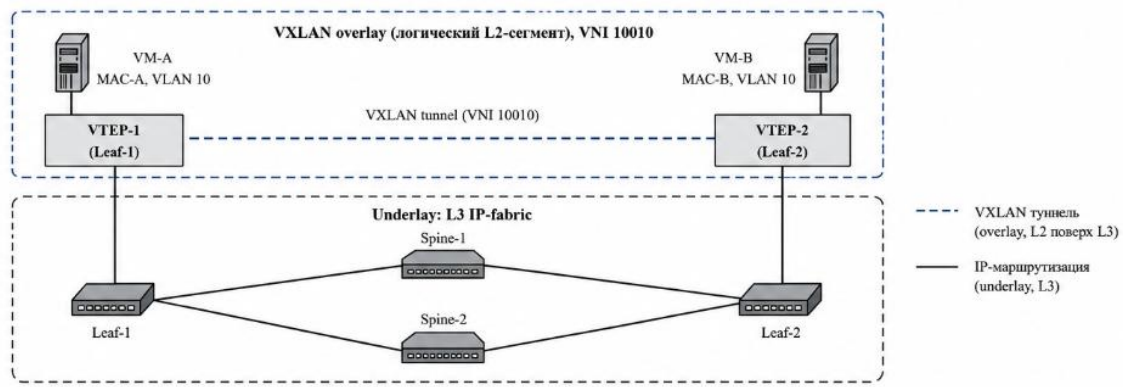

Рисунок 10 — Схема VXLAN overlay поверх L3 underlay

Как показано на рисунке 10, виртуальные машины VM-A и VM-B могут находиться на разных физических серверах или в разных стойках, но относиться к одному логическому L2-сегменту VXLAN. Передача кадров между ними выполняется через VXLAN-туннель между VTEP-устройствами. При этом базовая сеть underlay остаётся маршрутизируемой L3-сетью и может использовать BGP, OSPF, IS-IS и ECMP для выбора путей передачи трафика [23, 26, 28].

VXLAN предназначен для создания виртуальных L2-сетей поверх L3-инфраструктуры. Это особенно важно для виртуализированных дата-центров, где требуется большое количество изолированных сетевых сегментов, а классического VLAN-пространства может быть недостаточно [23]. RFC 7348 указывает, что ограничение VLAN в 4094 идентификатора становится недостаточным для многопользовательских и виртуализированных сред, а

VXLAN использует 24-битный VNI, что позволяет создавать значительно больше логических сегментов.

EVPN используется как control plane для распространения информации о MAC- и IP-адресах. EVPN позволяет строить более управляемую overlay-сеть и поддерживает сценарии multihoming, при которых один Ethernet-сегмент может быть подключён к нескольким сетевым устройствам [22, 25, 33]. Принцип работы EVPN как control plane для VXLAN показан на рисунке 11.

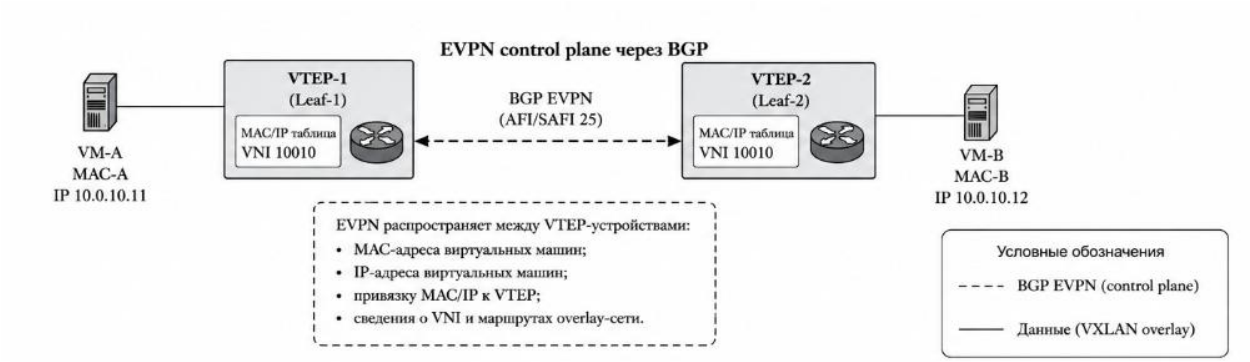

Рисунок 11 — Схема EVPN как control plane для VXLAN

Как видно из рисунка 11, EVPN передаёт между VTEP-устройствами служебную информацию о MAC- и IP-адресах, VNI и расположении конечных узлов. Благодаря этому VTEP-устройство может заранее знать, через какой удалённый VTEP доступна нужная виртуальная машина или сервер. Такой подход снижает объём flood-трафика по сравнению с классическим L2-подходом и делает overlay-сеть более управляемой [22, 25, 28].

В отличие от классического L2-подхода, VXLAN EVPN позволяет масштабировать сеть поверх маршрутизируемой IP-фабрики. Это снижает зависимость от больших широковещательных доменов и позволяет использовать преимущества L3-маршрутизации, включая ECMP и BGP [25, 26, 28]. В практических руководствах Cisco VXLAN BGP EVPN рассматривается именно как дата-центровая fabric-архитектура, где BGP EVPN выполняет роль control plane для VXLAN-сегментов.

5 L3-резервирование

L3-резервирование относится к сетевому уровню модели OSI. Оно связано с отказоустойчивостью маршрутов, шлюзов, внешних подключений,

динамической маршрутизации и распределением трафика между несколькими путями [7, 21, 24, 26, 27].

Если L2-резервирование решает задачу сохранения Ethernet-сегмента, то L3-резервирование обеспечивает устойчивую маршрутизацию между сетями. В дата-центрах L3-подход особенно важен для leaf-spine-архитектуры, внешних подключений, межплощадочной связности и связи с операторами [26, 28, 32].

L3-резервирование применяется для обеспечения отказоустойчивости маршрутизации, внешних подключений и шлюза по умолчанию. В такой схеме могут использоваться VRRP для резервирования виртуального шлюза, BGP для обмена маршрутами с внешними сетями и ECMP для распределения трафика между равнозначными маршрутами. Общая схема L3-резервирования показана на рисунке 12.

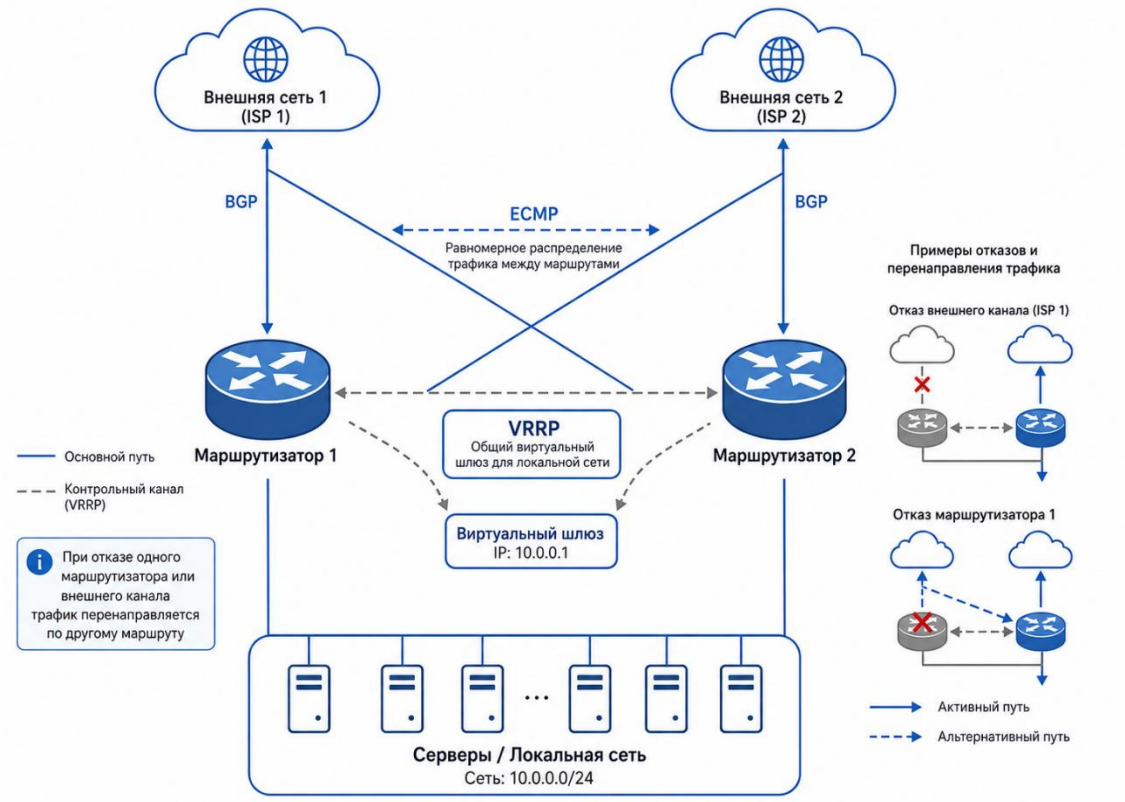

Рисунок 12 — Схема L3-резервирования с использованием VRRP, BGP и ECMP

На рисунке 12 показано, что локальная сеть дата-центра использует общий виртуальный шлюз, реализованный с помощью VRRP. Внешняя связность обеспечивается через два маршрутизатора и два независимых

внешних подключения. При отказе одного маршрутизатора или одного внешнего канала трафик может быть перенаправлен через оставшийся доступный маршрут [21, 24, 26, 27].

5.1 VRRP

VRRP применяется для резервирования шлюза по умолчанию. Несколько маршрутизаторов образуют виртуальный маршрутизатор с одним виртуальным IP-адресом. Хосты используют этот IP-адрес как default gateway. Если активный маршрутизатор выходит из строя, резервный маршрутизатор принимает его роль [21].

Преимущество VRRP заключается в простоте и понятности. Серверы и другие хосты не должны знать о наличии нескольких физических маршрутизаторов, так как для них существует один виртуальный шлюз [21]. Это удобно для сетей, где не требуется сложная динамическая маршрутизация на стороне конечных устройств.

Однако VRRP не решает всех задач. Обычно он работает по модели active-standby, где один маршрутизатор активен, а второй находится в резерве. Кроме того, VRRP резервирует шлюз, но не гарантирует доступность всего последующего маршрута до внешней сети [21, 24].

5.2 BGP

BGP является основным протоколом маршрутизации между автономными системами. В дата-центрах BGP применяется не только для внешнего подключения к интернету, но и для построения внутренней маршрутизации в leaf-spine-фабриках [24, 26].

Использование BGP внутри дата-центра позволяет строить масштабируемую и предсказуемую L3-сеть. Каждый leaf-коммутатор может иметь несколько uplink-подключений к spine-коммутаторам, а маршруты между ними распространяются через BGP [26, 28]. В случае отказа одного пути трафик может быть перенаправлен через другие доступные маршруты.

Пример L3-резервирования дата-центра с использованием нескольких пограничных маршрутизаторов и внешних операторов связи показан на рисунке 13.

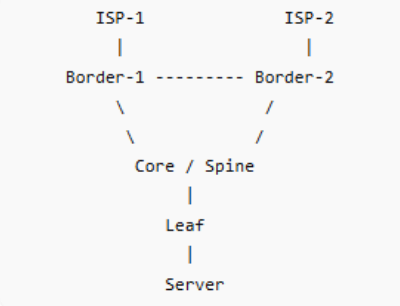

Рисунок 13 — Пример L3-резервирования через BGP

Как показано на рисунке 13, дата-центр может иметь несколько пограничных маршрутизаторов и несколько внешних операторов связи. При отказе одного оператора или одного border-маршрутизатора маршруты перестраиваются через оставшийся путь [7, 24, 26].

BGP также применяется в VXLAN EVPN-сетях, где он используется как control plane для распространения информации о виртуальных сетях, MAC-адресах и IP-префиксах [22, 25, 28].

5.3 ECMP

ECMP позволяет использовать несколько равнозначных маршрутов одновременно. В leaf-spine-сетях это особенно важно, так как каждый leaf-коммутатор может иметь несколько uplink-подключений к разным spine-коммутаторам [26, 28, 37].

При нормальной работе трафик распределяется между несколькими путями. Если один путь становится недоступен, он исключается из таблицы маршрутизации или из балансировки, а трафик продолжает идти через оставшиеся пути [26]. Такой подход повышает отказоустойчивость и позволяет эффективнее использовать сетевую инфраструктуру.

Принцип работы ECMP в leaf-spine-сети дата-центра представлен на рисунке 14.

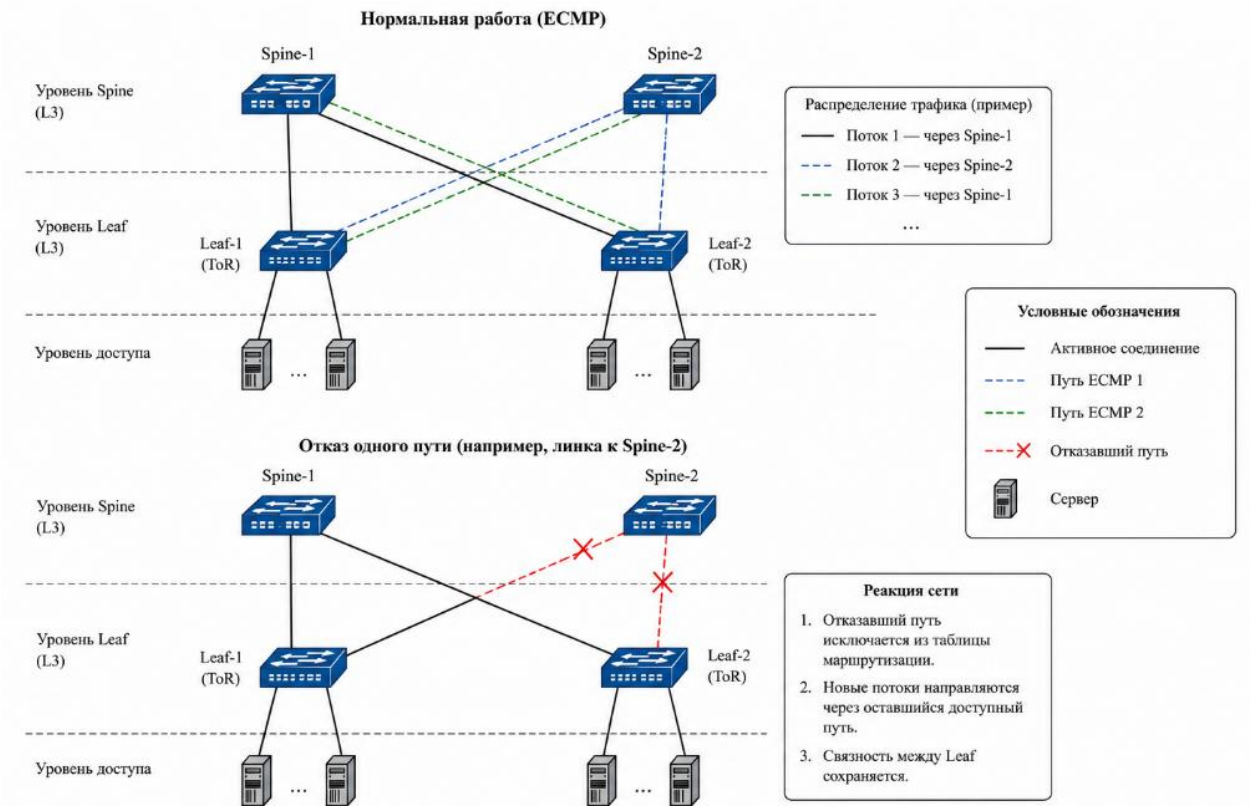

Рисунок 14 — Схема распределения трафика по равнозначным маршрутам ECMP

Как показано на рисунке 14, каждый leaf-коммутатор имеет несколько L3-подключений к spine-коммутаторам. При наличии нескольких равнозначных маршрутов механизм ECMP позволяет распределять трафик между ними. Обычно распределение выполняется не произвольно, а на основе хэширования параметров потока, например IP-адресов источника и назначения, портов TCP/UDP и протокола. Поэтому разные сетевые потоки могут передаваться через разные uplink-каналы, что позволяет эффективнее использовать пропускную способность сети [26, 28].

При отказе одного uplink-канала или одного spine-коммутатора соответствующий маршрут исключается из набора доступных равнозначных путей. После этого новые потоки направляются через оставшиеся активные соединения. Благодаря этому ECMP повышает отказоустойчивость L3-фабрики дата-центра и снижает риск полной потери связности между leaf-коммутаторами [26, 28, 37].

Для более быстрого исключения отказавшего пути из маршрутизации ECMP часто используется совместно с протоколами динамической

маршрутизации и механизмом BFD. Протокол маршрутизации определяет доступные пути, ECMP распределяет трафик между ними, а BFD ускоряет обнаружение отказов физических каналов или соседних устройств [26, 27, 40].

5.4 BFD

BFD применяется для быстрого обнаружения отказов сетевого пути. Без BFD протокол маршрутизации может обнаружить отказ только после истечения стандартных таймеров. Это может занимать слишком много времени для критичных сервисов [27, 40].

BFD позволяет быстрее определить недоступность соседнего устройства или сетевого пути. Поэтому он часто используется вместе с BGP, OSPF, IS-IS и EVPN [27, 40]. В дата-центрах BFD особенно полезен на border-маршрутизаторах и в leaf-spine-фабриках, где важно быстро перестраивать маршруты при отказе оборудования или канала.

Принцип работы BFD при обнаружении отказа сетевого пути представлен на рисунке 15.

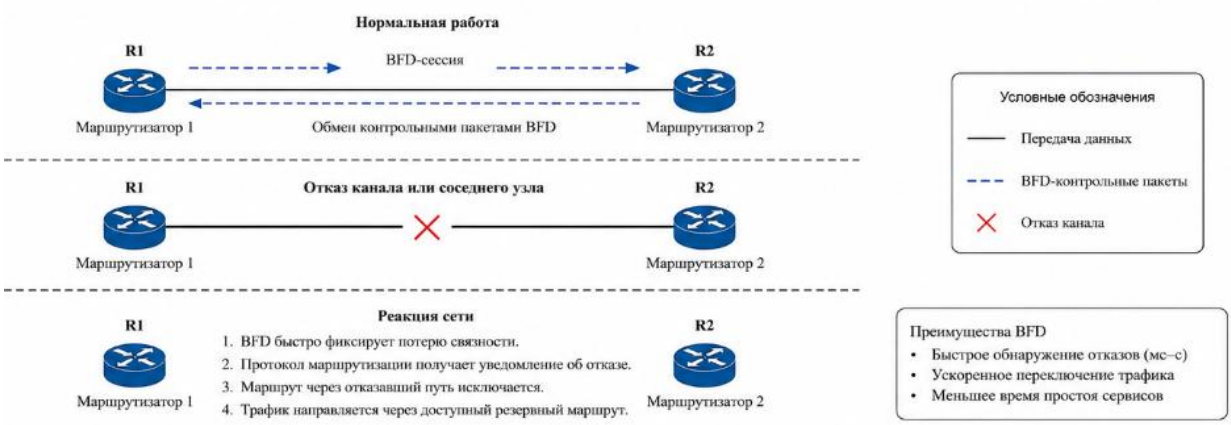

Рисунок 15 — Схема обнаружения отказа сетевого пути с использованием BFD

Как показано на рисунке 15, BFD организует отдельную контрольную сессию между соседними маршрутизаторами или коммутаторами. Пока канал доступен, устройства регулярно обмениваются BFD-пакетами. При прекращении обмена BFD быстро фиксирует отказ и передаёт информацию протоколу маршрутизации. После этого BGP, OSPF, IS-IS или другой протокол исключает недоступный путь из таблицы маршрутизации, а трафик перенаправляется через оставшийся доступный маршрут [27, 40].

Такой механизм особенно важен в сетях дата-центров, где задержка при обнаружении отказа может привести к кратковременной недоступности сервисов. Использование BFD позволяет сократить время реакции сети и ускорить переключение трафика при отказе оборудования или физического канала [27, 40].

5.5 L3-фабрика дата-центр

Современные дата-центры часто строятся по leaf-spine-архитектуре. В такой модели leaf-коммутаторы подключают серверы, системы хранения и гипервизоры, а spine-коммутаторы обеспечивают связность между leaf-уровнем [26, 28, 37].

Leaf-spine-архитектура хорошо сочетается с L3-маршрутизацией, BGP и ECMP. Она позволяет уменьшить количество уровней в сети, сделать задержку более предсказуемой и обеспечить наличие нескольких равнозначных путей между узлами [26, 28]. При этом L2-сегменты могут быть реализованы поверх L3-фабрики с помощью VXLAN EVPN [23, 25, 28].

Общая схема L3-фабрики дата-центра на основе leaf-spine-архитектуры представлена на рисунке 16.

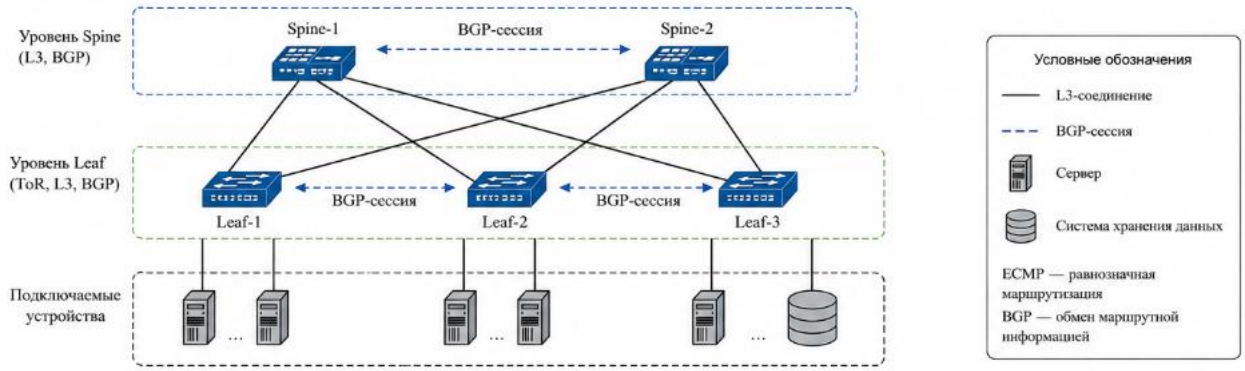

Рисунок 16 — Схема L3-фабрики дата-центра на основе leaf-spine-архитектуры

Как видно из рисунка 16, каждый leaf-коммутатор имеет несколько uplink-подключений к spine-коммутаторам. Благодаря этому между leaf-уровнем и spine-уровнем формируется несколько равнозначных маршрутов. При нормальной работе трафик может распределяться между несколькими путями с помощью ECMP. При отказе одного spine-коммутатора или одного

uplink-канала трафик продолжает передаваться через оставшиеся доступные соединения [26, 28, 37].

В такой архитектуре L3-маршрутизация используется уже на уровне фабрики дата-центра. Это снижает зависимость от больших L2-доменов и делает сеть более масштабируемой. Для обмена маршрутной информацией может применяться BGP, а для быстрого обнаружения отказов — BFD. При необходимости L2-сегменты могут быть построены поверх L3-фабрики с помощью VXLAN EVPN [23, 25, 26, 28].

6 Сравнение L2- и L3-резервирования

L2- и L3-резервирование решают разные задачи. L2-подход применяется там, где требуется сохранить Ethernet-сегмент, VLAN или L2-доступ сервера. L3-подход применяется для маршрутизации между сетями, внешней связности и построения масштабируемой фабрики дата-центра [1, 21, 22, 23, 24, 26]. Сравнение L2- и L3-резервирования приведено в таблице 6.

Таблица 6 — Сравнение L2- и L3-резервирования

Критерий	**L2-резервирование**	**L3-резервирование**
Уровень OSI	Канальный	Сетевой
Основная задача	Сохранить Ethernet-сегмент или VLAN	Сохранить маршрутизацию
Типовые технологии	STP, LACP, MLAG, MC-LAG, vPC, EVPN Multihoming	VRRP, BGP, OSPF, ECMP, BFD
Масштабируемость	Ограничена широковещательными доменами	Выше, особенно в leaf-spine
Основной риск	Петли, broadcast storm, split-brain	Ошибки маршрутизации, route leak
Где применяется	Доступ серверов, VLAN, L2-сервисы	Fabric, border, DCI, интернет
Современный подход	VXLAN EVPN поверх L3	BGP, ECMP, BFD

Как видно из таблицы 6, L2-резервирование удобно применять на уровне доступа и Ethernet-сегментов, тогда как L3-резервирование лучше подходит для масштабируемой маршрутизации, внешней связности и построения leaf-spine-фабрик.

Основной вывод заключается в том, что L2-резервирование удобно на уровне подключения серверов и сервисов, которым нужен общий Ethernet-сегмент. L3-резервирование лучше подходит для масштабируемой фабрики дата-центра, внешней связности и распределения трафика между несколькими маршрутами [26, 28, 37]. На практике эти подходы применяются совместно.

Например, сервер может подключаться к двум ToR-коммутаторам через MLAG, а сами ToR-коммутаторы могут подключаться к spine-уровню через L3-маршрутизацию и ECMP [8, 26, 36]. При этом overlay-сеть VXLAN EVPN может обеспечивать нужные L2-сегменты поверх маршрутизируемой инфраструктуры [22, 23, 25, 28].

7 Межплощадочное резервирование

Межплощадочное резервирование применяется, когда необходимо обеспечить доступность сервисов не только внутри одного дата-центра, но и между несколькими площадками. Такой подход особенно важен для критичных информационных систем, облачных платформ, банковских сервисов, телеком-инфраструктуры и корпоративных приложений [3, 32, 34, 38].

Для межплощадочной связности могут использоваться DCI, DWDM, OTN, IP/MPLS, BGP, VXLAN EVPN Multi-Site и другие технологии [3, 32, 34, 38, 39]. Выбор конкретного решения зависит от требований к задержке, пропускной способности, отказоустойчивости, стоимости и модели размещения данных.

Резервирование между дата-центрами должно учитывать физическую независимость маршрутов. Даже если организация арендует два канала связи, они могут проходить через одну магистраль или одну точку агрегации оператора. В таком случае авария на общей трассе приведёт к потере обоих каналов [3, 15].

Для повышения отказоустойчивости желательно использовать разные физические вводы, разных операторов связи, разные трассы и независимые точки подключения [3, 7]. На сетевом уровне для этого часто применяется BGP, так как он позволяет управлять маршрутизацией между автономными системами и несколькими внешними подключениями [7, 24].

Межплощадочное резервирование используется для повышения устойчивости сервисов за пределами одной физической площадки. В этом случае резервируются не только сетевые каналы, но и вычислительные ресурсы, системы хранения данных и внешняя доступность сервисов. Пример межплощадочного резервирования двух дата-центров представлен на рисунке 17.

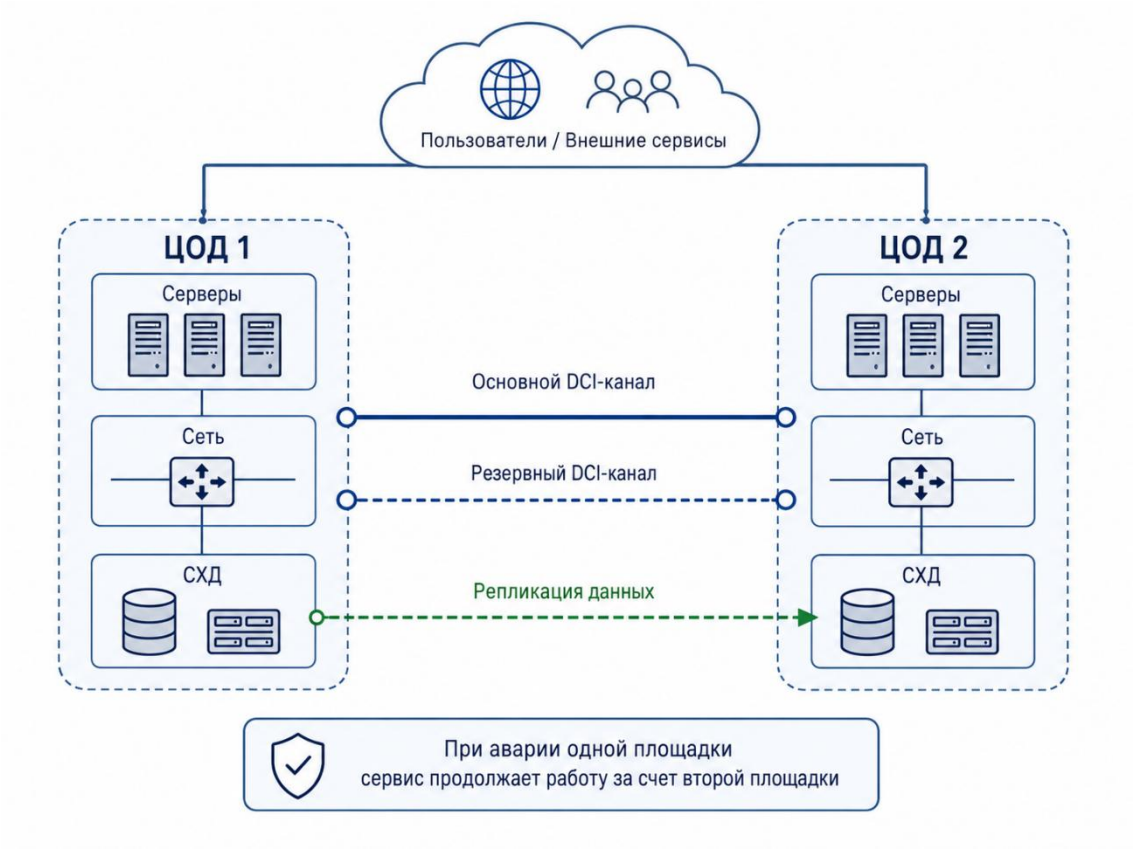

Рисунок 17 — Схема межплощадочного резервирования дата-центров

Как показано на рисунке 17, пользователи и внешние сервисы могут обращаться к двум площадкам, между которыми организованы основной и резервный DCI-каналы. Дополнительно между площадками выполняется репликация данных. При аварии одного дата-центра сервис может продолжить работу за счёт второй площадки, если заранее настроены маршрутизация, репликация и сценарии аварийного восстановления [3, 32, 34, 38].

Для реализации межплощадочного резервирования используется не одна отдельная технология, а совокупность сетевых, транспортных и сервисных механизмов. Их задача заключается в обеспечении связности между дата-центрами, резервировании маршрутов, переключении внешнего трафика и поддержании актуальности данных на второй площадке. Основные технологии, поддерживающие межплощадочное резервирование, представлены в таблице 7.

Таблица 7 — Технологии межплощадочного резервирования дата-центров

Технология	**Назначение при межплощадочном резервировании**
DCI	Общее название решений для соединения дата-центров между собой. Используется для передачи трафика между площадками и организации резервной связности.
DWDM	Позволяет передавать несколько оптических каналов по одной волоконно-оптической линии. Применяется для высокоскоростной связи между ЦОД.
OTN	Используется для построения отказоустойчивой оптической транспортной сети между площадками.
IP/MPLS	Позволяет организовать управляемую маршрутизацию и передачу трафика между дата-центрами через операторскую или корпоративную сеть.
BGP	Используется для резервирования внешних маршрутов, выбора доступного пути и переключения трафика между площадками.
Anycast	Позволяет объявлять один и тот же IP-адрес с нескольких площадок, чтобы пользовательский трафик направлялся к доступному или ближайшему ЦОД.
VXLAN EVPN Multi-Site	Позволяет строить overlay-сети между несколькими дата-центрами и расширять сетевые сегменты между площадками.
GSLB / DNS-балансировка	Используется для перенаправления пользователей на доступную площадку при отказе основного дата-центра.
Репликация данных	Обеспечивает актуальность данных на резервной площадке. Может быть синхронной или асинхронной.
Мониторинг и автоматизация переключения	Используются для обнаружения аварии и запуска сценариев failover или disaster recovery.

Из таблицы 7 видно, что межплощадочное резервирование включает несколько уровней. На физическом и транспортном уровне применяются DCI, DWDM и OTN. На сетевом уровне используются IP/MPLS, BGP, Anycast и VXLAN EVPN Multi-Site. На уровне сервисов применяются GSLB, DNS-балансировка и механизмы репликации данных. Поэтому схема,

представленная на рисунке 17, должна рассматриваться не только как резервирование каналов связи, но и как комплексная архитектура обеспечения доступности сервисов между двумя дата-центрами [3, 24, 32, 34, 38, 39].

На практике выбор технологий зависит от режима работы площадок. При схеме active-passive основная нагрузка обслуживается первым дата-центром, а второй используется как резервный. При схеме **active-active** обе площадки одновременно принимают пользовательский трафик и обслуживают сервисы. Для active-active обычно требуются более сложные механизмы маршрутизации, балансировки и синхронизации данных, например BGP, Anycast, GSLB и VXLAN EVPN Multi-Site [24, 32, 34, 38].

8 Что нельзя полностью зарезервировать

Несмотря на наличие большого количества сетевых технологий, не всё можно полностью зарезервировать. Резервирование снижает вероятность простоя, но не устраняет все возможные риски [13, 14, 15].

8.1 Ошибки конфигурации

Если администратор ошибочно применил неправильную конфигурацию сразу на оба резервных устройства, отказоустойчивость не поможет. Например, можно одновременно удалить BGP-соседей, неправильно настроить VLAN, ошибиться в route-map, применить некорректный ACL или нарушить работу MLAG [24, 30, 36].

Поэтому резервирование должно дополняться процедурами управления изменениями, проверкой конфигураций, staged rollout, тестированием и возможностью быстрого rollback [13, 14].

8.2 Человеческий фактор

Даже самая надёжная архитектура зависит от эксплуатации. Ошибки при коммутации, замене оборудования, обновлении прошивок и изменении маршрутизации могут привести к аварии [13, 15]. Поэтому важны регламенты, документация, мониторинг, обучение персонала и проведение работ в технологические окна.

8.3 Единая физическая зона отказа

Если два резервных канала проходят через одну трассу, резервирование является формальным. При повреждении трассы оба канала выйдут из строя. Аналогично, если резервные устройства используют одну систему питания или одну точку агрегации оператора связи, такая схема сохраняет скрытую единую точку отказа [3, 15].

8.4 Ошибки программного обеспечения

Сетевые устройства могут иметь одинаковую версию программного обеспечения с одинаковым дефектом. При определённых условиях оба резервных устройства могут отказать одновременно. Поэтому в критичных

системах необходимо внимательно подходить к обновлениям, тестировать новые версии ПО и выполнять staged upgrade [13, 14].

8.5 Зависимость от одного провайдера

Два внешних канала от одного оператора не всегда означают настоящую независимость. Они могут проходить через одну магистраль, одну точку агрегации или один узел связи. Для реальной отказоустойчивости желательно использовать разных операторов, разные физические вводы и независимые трассы [3, 7, 15].

8.6 Архитектурные ошибки приложения

Сеть может быть полностью зарезервирована, но приложение всё равно может быть недоступно. Например, если база данных находится в единственном экземпляре, если DNS указывает только на один узел, если балансировщик не имеет резерва или если приложение не умеет работать в active-active-схеме [13, 14].

8.7 Массовые аварии и внешние факторы

Не всегда можно защититься только сетевыми средствами от массовых внешних факторов: крупной аварии электропитания, пожара, DDoS-атаки, ошибки глобальной маршрутизации, повреждения нескольких магистралей или сбоя у внешнего провайдера [15, 18, 20]. Для таких случаев требуется не только сетевое резервирование, но и георезервирование, резервные площадки, резервное копирование, план аварийного восстановления и регулярные учения.

9 Практическая систематизация подходов

Для проектирования отказоустойчивой сети дата-центра можно использовать несколько уровней зрелости. Они отличаются стоимостью, сложностью и степенью защищённости от отказов [1, 13, 15].

9.1 Минимальный уровень

Минимальный уровень подходит для некритичных сервисов. В такой схеме сервер может иметь один сетевой интерфейс, один коммутатор доступа, один uplink и один шлюз. Резервирование в основном реализуется за счёт холодного резерва оборудования [13, 15]. Основные характеристики минимального уровня резервирования представлены в таблице 8.

Таблица 8 — Минимальный уровень резервирования

Компонент	**Решение**
Сервер	Один сетевой интерфейс
Коммутатор	Один ToR
Uplink	Один канал
Шлюз	Один маршрутизатор
Резерв	Холодный

Из таблицы 8 видно, что минимальный уровень резервирования содержит большое количество единых точек отказа, поэтому он не подходит для критичных сервисов.

Недостаток такого подхода заключается в большом количестве единых точек отказа. Он не подходит для критичных сервисов и систем, где требуется высокая доступность [13, 14].

9.2 Базовый отказоустойчивый уровень

Базовый отказоустойчивый уровень подходит для корпоративных сервисов средней критичности. В такой схеме сервер имеет две сетевые карты, подключается к двум коммутаторам, а на уровне шлюза используется VRRP [8, 21, 36]. Состав базового отказоустойчивого уровня представлен в таблице 9.

Таблица 9 — Базовый отказоустойчивый уровень

Компонент	**Решение**
Сервер	Две NIC
Доступ	Два ToR
L2	LACP/MLAG
Шлюз	VRRP
Uplink	Два канала
Мониторинг	SNMP/Zabbix/Prometheus

Как видно из таблицы 9, базовый отказоустойчивый уровень позволяет устранить часть единых точек отказа за счёт дублирования сетевых карт, коммутаторов, uplink-каналов и шлюза.

Такой вариант позволяет устранить часть единых точек отказа и обеспечить автоматическое переключение при отказе одного канала, коммутатора или шлюза [21, 36].

Базовый отказоустойчивый уровень сети дата-центра включает дублирование ключевых компонентов доступа: двух сетевых интерфейсов сервера, двух ToR-коммутаторов, резервного шлюза и двух uplink-каналов. Такая схема подходит для корпоративных сервисов средней критичности и позволяет устранить основные единые точки отказа. Структура базового отказоустойчивого уровня представлена на рисунке 18.

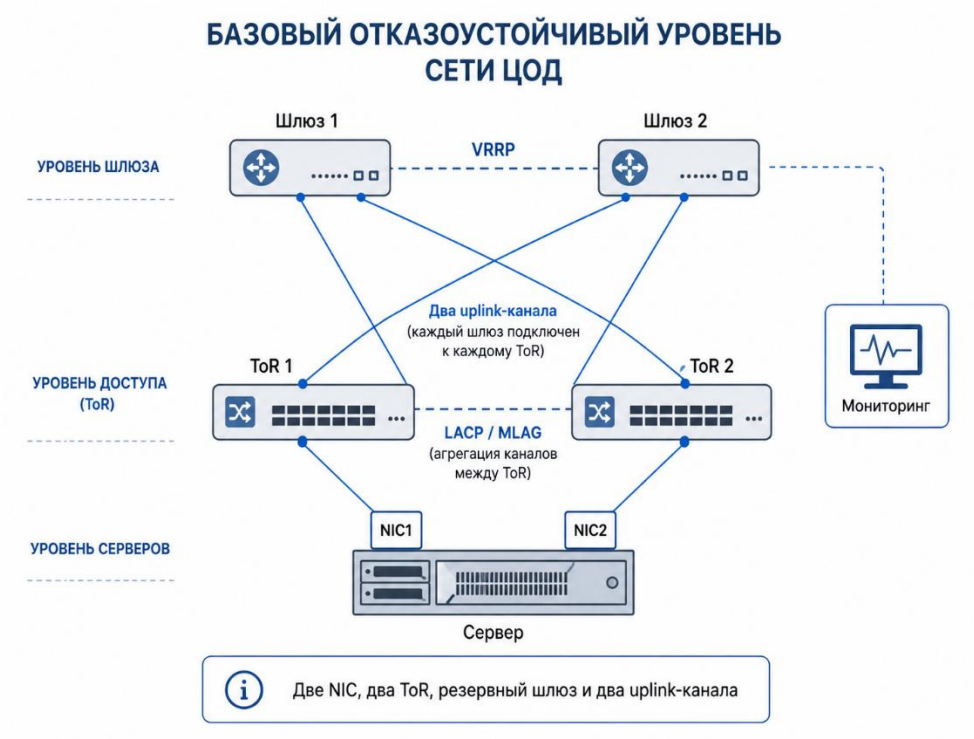

Рисунок 18 — Базовый отказоустойчивый уровень сети дата-центра

Из рисунка 18 видно, что сервер подключается к двум ToR-коммутаторам через два сетевых интерфейса, а уровень шлюза резервируется с помощью VRRP. Наличие двух uplink-каналов и мониторинга позволяет своевременно обнаруживать отказы и переключать трафик на доступный путь. Такая схема является более надёжной по сравнению с минимальным уровнем резервирования, так как исключает отказ одного сетевого интерфейса, одного коммутатора доступа или одного шлюза как единственную причину потери связности [8, 21, 36].

9.3 Современная дата-центровая фабрика

Современная дата-центровая фабрика подходит для облачной инфраструктуры и высоконагруженных сервисов. Она строится по leaf-spine-архитектуре, использует L3-маршрутизацию, BGP, ECMP, BFD и overlay-технологии VXLAN EVPN [23, 25, 26, 28, 37]. Основные компоненты современной дата-центровой фабрики представлены в таблице 10.

Таблица 10 — Современная дата-центровая фабрика

Компонент	**Решение**
Архитектура	Leaf-spine
Underlay	L3 BGP/OSPF/IS-IS
Overlay	VXLAN EVPN
Резервирование доступа	MLAG или EVPN Multihoming
Балансировка маршрутов	ECMP
Быстрое обнаружение отказов	BFD
Внешняя связность	Два и более border-узла, BGP с несколькими операторами

Из таблицы 10 следует, что современная дата-центровая фабрика объединяет физическое резервирование, L3-маршрутизацию, overlay-сети и механизмы быстрого обнаружения отказов.

Такой подход является более сложным, но он лучше масштабируется и позволяет строить отказоустойчивые сети для крупных дата-центров [26, 28, 37].

9.4 Георезервирование

Георезервирование применяется для наиболее критичных сервисов. Оно предполагает использование двух и более дата-центров, независимых каналов связи, резервных внешних подключений, репликации данных и плана аварийного восстановления [3, 32, 34, 38]. Основные элементы георезервирования представлены в таблице 11.

Таблица 11 — Георезервирование

Компонент	**Решение**
Площадки	Два и более ЦОД
Каналы между ЦОД	DCI, DWDM, OTN, IP/MPLS
Адресация	BGP, Anycast, GSLB
Данные	Репликация
Восстановление	DR-план
Тестирование	Регулярные аварийные учения

Как видно из таблицы 11, георезервирование выходит за пределы одной площадки и требует не только сетевого резервирования, но и репликации данных, резервных каналов и плана аварийного восстановления.

Георезервирование не заменяет локальное резервирование внутри дата-центра. Оно дополняет его и позволяет сохранить доступность сервисов даже при серьёзной аварии на одной площадке [3, 15, 18].

10 Рекомендации по проектированию сетевого резервирования

При проектировании сетевого резервирования в дата-центре необходимо придерживаться комплексного подхода. Недостаточно зарезервировать только коммутаторы или только внешние каналы связи. Нужно учитывать физический, канальный, сетевой и эксплуатационный уровни [1, 13, 15].

Основные рекомендации:

1. Исключать единые точки отказа на каждом уровне: питание, кабели, коммутаторы, маршрутизаторы, uplink-каналы и провайдеры [1, 3, 15].
2. Использовать физически независимые трассы, а не просто два кабеля, проложенных рядом [3, 15].
3. Разделять L2- и L3-задачи: не растягивать L2-сегменты там, где задачу можно решить маршрутизацией [23, 26, 28].
4. Использовать MLAG/MC-LAG или EVPN Multihoming для отказоустойчивого подключения серверов [8, 33, 36].
5. Использовать BGP, ECMP и BFD для масштабируемой L3-фабрики [24, 26, 27].
6. Документировать все резервные связи и проверять их фактическую независимость [13, 14].
7. Регулярно тестировать отказоустойчивость, а не считать её существующей только по схеме [13, 15].
8. Внедрять мониторинг, логирование и автоматическую проверку конфигураций [13, 14].
9. Разделять production, management и storage-трафик, чтобы отказ одного сегмента не приводил к полной потере управляемости инфраструктуры [28, 29].
10. Для критичных сервисов применять георезервирование, резервные площадки и план аварийного восстановления [3, 18, 20, 32].

Таким образом, проектирование резервирования должно рассматриваться не как разовая настройка протоколов, а как постоянный

процесс, включающий архитектуру, эксплуатацию, мониторинг, документацию и регулярную проверку отказоустойчивости [13, 14, 15].

ЗАКЛЮЧЕНИЕ

В ходе курсового проекта были рассмотрены основные подходы к сетевому резервированию в дата-центрах. Установлено, что отказоустойчивость сети должна строиться на нескольких уровнях: физическом, L2, L3, overlay и межплощадочном.

Физическое резервирование включает дублирование сетевых карт, кабелей, коммутаторов, блоков питания, uplink-каналов и внешних подключений. Горячее резервирование подходит для критичных сервисов и обеспечивает быстрое переключение, а холодное используется для запасных компонентов и требует большего времени восстановления.

В работе проанализированы технологии L2-резервирования: STP, LACP, MLAG, MC-LAG, vPC, VXLAN и EVPN Multihoming, а также технологии L3-резервирования: VRRP, BGP, ECMP и BFD. Показано, что современные сети дата-центров всё чаще строятся на leaf-spine-архитектуре, BGP, ECMP, BFD и VXLAN EVPN.

Отдельно рассмотрено межплощадочное резервирование, для которого применяются DCI, DWDM, OTN, BGP, VXLAN EVPN Multi-Site, Anycast, GSLB и репликация данных. Такое резервирование повышает устойчивость сервисов при аварии на одной из площадок.

Цель курсового проекта достигнута: выполнены обзор и систематизация подходов к сетевому резервированию. Практическая значимость работы заключается в возможности использования результатов при проектировании и модернизации сетей дата-центров. Экономическая значимость состоит в снижении риска простоев, уменьшении потерь от недоступности сервисов и сокращении времени восстановления после аварий.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Сетевое резервирование в дата-центрах [Электронный ресурс] // Selectel. — URL: https://selectel.ru/blog/network-reservation/ (дата обращения: 20.04.2026).

2. Сетевое резервирование в дата-центрах: решаем задачку про двух велосипедистов [Электронный ресурс] // Habr. — URL: https://habr.com/ru/companies/selectel/articles/675168/ (дата обращения: 20.04.2026).

3. ЦОД под защитой: резервирование DWDM и OTN в действии [Электронный ресурс] // Selectel. — URL: https://selectel.ru/blog/about-the-reservation/ (дата обращения: 20.04.2026).

4. Технологии физического резервирования коммутаторов [Электронный ресурс] // Selectel. — URL: https://selectel.ru/blog/stack_and_mlag/ (дата обращения: 20.04.2026).

5. Дополнительные услуги для размещенного оборудования [Электронный ресурс] // Selectel Docs. — URL: https://docs.selectel.ru/server-colocation/about/additional-services/ (дата обращения: 20.04.2026).

6. Публичные сети и подсети выделенного сервера [Электронный ресурс] // Selectel Docs. — URL: https://docs.selectel.ru/dedicated/networks/public-networks-and-subnets/ (дата обращения: 20.04.2026).

7. Как настроить резервированную схему сети с использованием протокола BGP [Электронный ресурс] // Selectel. — URL: https://selectel.ru/blog/tutorials/how-to-set-up-a-redundant-network-scheme-with-bgp-protocol/ (дата обращения: 20.04.2026).

8. Настройка технологии Multi-Switch Link Aggregation Group MLAG [Электронный ресурс] // Eltex. — URL: https://eltexcm.ru/baza-znanij/ethernet-kommutatory-mes/mes2300-xx3300-xx3500-xx531253xxa53xx-xx54xx-xx5500-32/lag/nastrojka-tehnologii-multi-switch-link-aggregation-group-mlag/ (дата обращения: 20.04.2026).

9. Сети для самых матёрых. Микровыпуск №7. MPLS EVPN [Электронный ресурс] // Linkmeup. — URL: https://linkmeup.ru/blog/1221/ (дата обращения: 20.04.2026).

10. Сети для самых матёрых. Микровыпуск №7. EVPN [Электронный ресурс] // Habr. — URL: https://habr.com/ru/articles/316792/ (дата обращения: 20.04.2026).

11. Первый сетевой коммутатор 25GbE для ЦОД от YADRO [Электронный ресурс] // Habr. — URL: https://habr.com/ru/companies/mclouds/articles/829442/ (дата обращения: 20.04.2026).

12. KORNFELD D1156/D2132 Datasheet [Электронный ресурс] // YADRO. — URL: https://st.yadro.com/docs/KORNFELD/KORNFELD_Datasheet.pdf (дата обращения: 20.04.2026).

13. Как повысить отказоустойчивость ИТ-оборудования [Электронный ресурс] // ITGLOBAL.COM. — URL: https://itglobal.com/ru-ru/company/blog/kak-povysit-otkazoustojchivost-it-oborudovaniya/ (дата обращения: 20.04.2026).

14. Отказоустойчивость [Электронный ресурс] // ITGLOBAL.COM. — URL: https://itglobal.com/ru-ru/company/glossary/otkazoustojchivost/ (дата обращения: 20.04.2026).

15. Объясняю резервирование в дата-центре на пиве [Электронный ресурс] // Habr. — URL: https://habr.com/ru/companies/rt-dc/articles/501848/ (дата обращения: 20.04.2026).

16. ГОСТ Р 70139-2022. Центры обработки данных. Термины и определения [Электронный ресурс]. — URL: https://allgosts.ru/01/040/gost_r_70139-2022 (дата обращения: 20.04.2026).

17. Нормативные базы для создания ЦОД в России и за рубежом [Электронный ресурс] // Secuteck. — URL:

https://www.secuteck.ru/articles/normativnye-bazy-dlya-sozdaniya-cod-v-rossii-i-za-rubezhom (дата обращения: 20.04.2026).

18. Классификация уровней надежности ЦОД [Электронный ресурс] // MWS. — URL: https://mws.ru/blog/klassifikaciya-tier-cod/ (дата обращения: 20.04.2026).

19. Что такое ЦОД Tier и зачем он нужен [Электронный ресурс] // Uptime. — URL: https://uptime.ru/chto-takoye-tsod-tier-i-zachem-on-nuzhen (дата обращения: 20.04.2026).

20. Уровни надежности ЦОД [Электронный ресурс] // Edgecenter. — URL: https://edgecenter.ru/blog/urovni-nadezhnosti-tsod (дата обращения: 20.04.2026).

21. RFC 5798. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6 [Электронный ресурс] // IETF Datatracker. — URL: https://datatracker.ietf.org/doc/html/rfc5798 (дата обращения: 20.04.2026).

22. RFC 7432. BGP MPLS-Based Ethernet VPN [Электронный ресурс] // IETF Datatracker. — URL: https://datatracker.ietf.org/doc/html/rfc7432 (дата обращения: 20.04.2026).

23. RFC 7348. Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks [Электронный ресурс] // IETF Datatracker. — URL: https://datatracker.ietf.org/doc/html/rfc7348 (дата обращения: 20.04.2026).

24. RFC 4271. A Border Gateway Protocol 4 (BGP-4) [Электронный ресурс] // RFC Editor. — URL: https://www.rfc-editor.org/rfc/rfc4271.html (дата обращения: 20.04.2026).

25. RFC 8365. A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN) [Электронный ресурс] // IETF Datatracker. — URL: https://datatracker.ietf.org/doc/html/rfc8365 (дата обращения: 20.04.2026).

26. RFC 7938. Use of BGP for Routing in Large-Scale Data Centers [Электронный ресурс] // IETF Datatracker. — URL: https://datatracker.ietf.org/doc/html/rfc7938 (дата обращения: 20.04.2026).

27. RFC 5880. Bidirectional Forwarding Detection (BFD) [Электронный ресурс] // RFC Editor. — URL: https://www.rfc-editor.org/rfc/rfc5880.html (дата обращения: 20.04.2026).

28. VXLAN BGP EVPN Data Center Fabrics Design and Implementation Guide [Электронный ресурс] // Cisco. — URL: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-vxlan-bgp-evpn-design-and-implementation-guide.html (дата обращения: 20.04.2026).

29. Securing Network Infrastructure in VXLAN BGP EVPN Data Centers [Электронный ресурс] // Cisco. — URL: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/securing-network-infrastructure-in-vxlan-bgp-evpn-data-centers.html (дата обращения: 20.04.2026).

30. Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide. Configuring vPC Multihoming [Электронный ресурс] // Cisco. — URL: https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/104x/configuration/vxlan/cisco-nexus-9000-series-nx-os-vxlan-configuration-guide-release-104x/m_configuring_vpc_multihoming.html (дата обращения: 20.04.2026).

31. EVPN Multihoming Configuration Guide [Электронный ресурс] // Cisco. — URL: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/mpls/b-mpls/m-ce-evpn-multihoming.html (дата обращения: 20.04.2026).

32. NextGen DCI with VXLAN EVPN Multi-Site Using vPC BGW [Электронный ресурс] // Cisco. — URL: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/whitepaper-c11-742114.html (дата обращения: 20.04.2026).

33. EVPN Multihoming Overview [Электронный ресурс] // Juniper Networks. — URL: https://www.juniper.net/documentation/us/en/software/junos/evpn/topics/concept/evpn-bgp-multihoming-overview.html (дата обращения: 20.04.2026).

34. VXLAN Data Center Interconnect Using EVPN Overview [Электронный ресурс] // Juniper Networks. — URL:

https://www.juniper.net/documentation/us/en/software/junos/evpn/topics/concept/vxlan-evpn-integration-overview.html (дата обращения: 20.04.2026).

35. Introduction to EVPN LAG Multihoming [Электронный ресурс] // Juniper Networks. — URL: https://www.juniper.net/documentation/us/en/software/nce/evpn-lag-multihoming-guide/topics/concept/evpn-lag-guide-introduction.html (дата обращения: 20.04.2026).

36. EOS Multi-Chassis Link Aggregation [Электронный ресурс] // Arista Networks. — URL: https://www.arista.com/en/um-eos/eos-multi-chassis-link-aggregation (дата обращения: 20.04.2026).

37. VXLAN for Data Center Fabric [Электронный ресурс] // Arista Networks. — URL: https://www.arista.com/en/solutions/vxlan (дата обращения: 20.04.2026).

38. Data Center Interconnection with VXLAN Design Guide [Электронный ресурс] // Arista Networks. — URL: https://www.arista.com/assets/data/pdf/Whitepapers/Arista_Design_Guide_DCI_with_VXLAN.pdf (дата обращения: 20.04.2026).

39. EVPN-MPLS with Multihoming [Электронный ресурс] // Nokia Documentation. — URL: https://documentation.nokia.com/sr/25-10/7750-sr/books/services-configuration-reference/evpn-mpls-with-multihoming.html (дата обращения: 20.04.2026).

40. What Is BFD? How Does It Work? [Электронный ресурс] // Huawei. — URL: https://info.support.huawei.com/info-finder/encyclopedia/en/BFD.html (дата обращения: 20.04.2026).