Приложение №15

к протоколу МГС №46-2014



Межгосударственный совет по стандартизации,

метрологии и сертификации

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ**

к Системе информационного обеспечения

деятельности Межгосударственного совета

по стандартизации, метрологии и сертификации

2014 г.

**Содержание**

1. Основание для выполнения работ…………………………………………...3
2. Исполнитель работ и сроки выполнения……………………………………3
3. Цель и назначение разработки………………………….……………………3
4. Термины и определения...………….………………………………………...4
5. Общие технические требования…………………………………………......9

Приложение №1 Общая схема сетевой топологии элементов

инфраструктуры кластера высокой доступности………..................….......11

Приложение №2 Технические требования к серверам ...........….…........12

Приложение №3 Схема подключения кабелей питания .........13

Приложение №4 Перечень программных продуктов,

используемый в гостевых системах………….………………..………........14

Приложение №5 Схема организации доступа

гостевых систем СИО МГС в сеть Интернет…………………….………...15

Приложение №6 Перечень оборудования и платного   
программного обеспечения необходимого для построения кластера высокой доступности .......16

1. **Основание для выполнения работ.**

Решение Межгосударственного совета по стандартизации, метрологии и сертификации (Протокол МГС № 45-2014 п. 24.7, г. Сочи, Российская Федерация), рекомендации Рабочей группы по применению информационных технологий в сфере стандартизации, метрологии и сертификации (протокол РГ по ИТ МГС № 31-2014 п. 4.3, г. Витебск, Республика Беларусь).

**2. Исполнитель работ и сроки выполнения.**

Исполнитель работ:

Комитет технического регулирования и метрологии Министерства по инвестициям и развитию Республики Казахстан (Госстандарт Республики Казахстан)

010000, Республика Казахстан, г. Астана,

ул. Орынбор, 11, здание "Эталонный центр"

Сроки выполнения работ:

начало - 01.07.2014

окончание - 01.04.2015.

**3. Цель и назначение разработки.**

Целью выполняемых работ является описание общих технических требований к системе информационного обеспечения деятельности МГС, а также описание инфраструктуры и схемы, перечней программных продуктов.

Данные технические требования являются основанием для разработки следующих документов:

* Техническое задание на разработку системы информационного обеспечения деятельности Межгосударственного совета по стандартизации, метрологии и сертификации (далее - СИО МГС);
* Техническая спецификация на оборудование и программное обеспечение СИО МГС;
* Правила информационного взаимодействия СИО МГС;
* Политика информационной безопасности СИО МГС;
* Правила, инструкции и рекомендации по информационной безопасности СИО МГС;
* Программы и методики испытания.

**4. Термины и определения**

* **Веб–интерфейс** - это совокупность средств, при помощи которых пользователь взаимодействует с веб-сайтом или любым другим приложением через браузер;
* **Виртуализация** - предоставление набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации, и обеспечивающее при этом логическую изоляцию вычислительных процессов, выполняемых на одном физическом ресурсе;
* **Инфраструктура -** комплекс взаимосвязанных обслуживающих структур или объектов, составляющих и/или обеспечивающих основу функционирования системы;
* **Масштабирование -** увеличение производительности каждого компонента системы с целью повышения общей производительности;
* **Мониторинг** - непрерывный процесс наблюдения и регистрации параметров объекта, в сравнении с заданными критериями;
* **Консоль** - совокупность устройств (в том числе устройств ввода-вывода), обеспечивающая взаимодействие человека-оператора с компьютером.
* **Высокая доступность** – метод проектирования, позволяющий обеспечивать непрерывный доступ к системе в течение какого-либо промежутка времени. Доступность означает возможность группе пользователей использовать систему. Если у них нет такой возможности, система считается недоступной. Термин время недоступности обозначает период времени, в течение которого система была недоступна.

Для проектируемых систем высокая доступность (99%) подразумевает создание избыточности в критических точках системы. Тогда отказ одного компонента, будь то отказ сетевого коммутатора или сетевой карты, не будет вызывать сбой приложения. Стандартные методы высокой доступности включают развертывание избыточных аппаратных средств и использование множественных сетевых связей.

* **Кластер высокой доступности** – это группа серверов (минимум три), работающих как единая система для предоставления высокой доступности сервисов и приложений для клиентов.

Кластерная система характеризуется высокой надежностью, производительностью, гибким масштабированием и легкостью в управлении. Высокая надежность достигается путем дублирования всех критически важных для работы компонентов. Высокая производительность и масштабируемость – за счет распределения нагрузки между узлами (серверами) кластера. Легкость управления подразумевает собой возможность управлять как централизованно всем кластером, так и отдельными серверами, входящими в его состав. Существует множество программных решений для построения такого рода кластеров. Одним из них является построение кластера высокой доступности на базе системы виртуализации с открытым исходным кодом Proxmox VE.

Система виртуализации Proxmox VE позволяет решать широкий спектр задач, таких как:

– поддержка оборудования различных производителей;

– простое управление через веб–интерфейс;

– мониторинг нагрузки в реальном времени;

– подключение к «физической» консоли гостевых систем непосредственно из браузера (гостевая система – это операционная система, устанавливаемая на виртуальную машину);

– объединение серверов в кластер с возможностью живой миграции гостевых систем (без остановки гостевой системы, а также в автоматическом режиме);

– быстрое развертывание гостевых систем из шаблонов. Доступно только для OpenVZ. OpenVZ – технология виртуализации на уровне операционной системы, которая базируется на ядре Linux. OpenVZ позволяет на одном физическом сервере запускать множество изолированных копий операционной системы, называемых «виртуальные среды»;

– автоматическое резервное копирование гостевых систем на системы хранения данных (СХД).

* **Каналы связи.** Каналы связи включают в себя локальную сеть и каналы доступа в сеть Интернет с использованием оптоволоконных линии связи и гарантированной полосой пропускания не менее 20 Мб/с. Для повышения надежности предоставления сервисов СИО МГС в сети Интернет необходимо иметь минимум два независимых подключения к сети Интернет. Данный способ обеспечит доступность СИО МГС в случае выхода из строя одного из каналов связи;
* **Сетевое оборудование** (сетевые коммутаторы)−устройства, необходимые для работы компьютерной сети. Для нормального функционирования кластера высокой доступности необходимо использовать 2 сетевых коммутатора имеющих не менее 48 портов каждый и шириной пропускания не менее 1ГБ/с (например HP 2530–48G Switch). В случае выхода из строя одного из коммутаторов функционирование кластера поддерживается через второй коммутатор. Сетевые коммутаторы должны поддерживать технологию VLAN (Vlan0, Vlan1, Vlan2, Vlan3, Vlan4 Приложение 1). **VLAN** – логическая («виртуальная») локальная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимого от их физического местонахождения. VLAN имеет те же свойства, что и физическая сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети;
* **Серверы.** Серверы – аппаратное обеспечение, выделенное и/или специализированное для выполнения на нем сервисного программного обеспечения. Технические требования к серверам приведены в   
  Приложении 2;
* **СХД.** СХД – комплексное программно–аппаратное решение по организации надежного хранения информационных ресурсов и предоставления гарантированного доступа к ним. Для нормального функционирования виртуальных машин в кластере необходимо две отказоустойчивые СХД: основная и резервная. На основной СХД запускаются гостевые системы, работающие в кластере. Соединение основной СХД с кластером осуществляется по протоколам ISCSI или NFS посредством локальной сети. СХД должна иметь быстрые жесткие диски SAS общей ёмкостью не менее 24ТБ с возможностью настройки массивов из нескольких дисков (RAID 5, RAID 6) (например HP P2000 G3 iSCSI MSA). На резервной СХД хранятся резервные копии виртуальных машин основной СХД. Соединение резервной СХД с кластером происходит по протоколу NFS через локальную сеть. СХД должна иметь жесткие диски не ниже класса SATA Revision 3.0 общей ёмкостью не менее 24ТБ с возможностью настройки массивов из нескольких дисков (RAID 5, RAID 6) (например QNAP TS–869U). В случае выхода из строя основной СХД, гостевые системы будут запущены на резервной СХД с минимальным временем простоя сервисов;
* **Устройство распределения питания (RackPDU)** предназначено для распределения электрической энергии и должно иметь не менее 8 интерфейсов подключения (например APC AP7921). Схема подключения кабелей питания приведена в Приложении 3;
* **Источники бесперебойного питания (ИБП).** ИБП – источник вторичного электропитания, автоматическое устройство, назначение которого – обеспечить подключенное к нему электрооборудование бесперебойным снабжением электрической энергией в пределах нормы (Приложение 3). Выходная мощность ИБП должна быть не менее 3000 ВА (например Smart–UPS 3000VA);
* **Система комплексной сетевой защиты.** Система комплексной сетевой защиты – программно–аппаратный комплекс, предназначенный для защиты периметра локальной сети и предоставляемых сервисов от внутренних и внешних угроз (атаки хакеров, хищение, уничтожение, модификация информации и др.). Система комплексной сетевой защиты также должна позволять создать демилитаризованные зоны (dmz1, dmz2, dmz3). Демилитаризованная зона – технология обеспечения защиты информационного периметра, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана, с целью минимизировать ущерб при взломе одного из общедоступных сервисов, находящихся в зоне. Система комплексной сетевой защиты должна иметь функцию балансировки нагрузки по протоколам tcp, udp, ip, ssl, http, https, а также не менее 10 ethernet–портов с шириной пропускания не менее 1 Гб/с (например, на базе оборудования предоставления сетевых сервисов FortiGate–100D).
* **системы авторизации и аутентификации** - основой защиты информационных систем являются идентификация и аутентификация, так как все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами. В качестве субъектов могут выступать как пользователи, так и процессы, а в качестве объектов – информация и другие информационные ресурсы системы;
* **системы разграничения доступа к информации** - после выполнения авторизации и аутентификации необходимо установить полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования;
* **средства межсетевого экранирования** - комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами;
* **системы аварийного восстановления и резервного копирования** - процесс создания копии данных, предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения;
* **системы антивирусной защиты** - программа для обнаружения компьютерных вирусов, а также нежелательных, вредоносных программ и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения файлов или системы вредоносным кодом;
* **системы контроля электронной почты и web-трафика** - контроль действий должен быть комплексным и масштабируемым, чтобы у пользователей не было возможности даже случайным образом нанести какой-то вред информационной среде, будь это сообщение по электронной почте или какой-то другой способ передачи информации в сети Интернет;
* **системы сегментирования локальной вычислительной сети**- повышение безопасности сети путем разделения её на множество зон;
* **системы мониторинга и обнаружения и предотвращения вторжений** - программное или аппаратное средство, предназначенное для выявления и предотвращения фактов неавторизованного доступа (вторжения или сетевой атаки) в систему или сеть;
* **средства криптографической защиты информации -**методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней.

**5.Общие технические требования**

Для организации доступа пользователей к Системе информационного обеспечения деятельности Межгосударственного совета по стандартизации, метрологии и сертификации необходимо построить отказоустойчивую систему с минимальным временем простоя, с возможностью масштабирования, интеграции различных модулей, решений и систем, создать современную платформу и обеспечить бесперебойную работу обмена данных и самой инфраструктуры СИО МГС.

Минимальное время простоя обеспечивается системами класса «Высокой доступности». Одним из решений для построения систем класса «Высокой доступности» является объединение программных и аппаратных ресурсов в кластер высокой доступности.

Для обеспечения доступности в 99% предоставления сервисов СИО МГС необходимо реализовать кластер высокой доступности на базе Proxmox VE, а также создать необходимую инфраструктуру.

Общая схема сетевой топологии элементов инфраструктуры кластера высокой доступности приведена в Приложении 1.

После включения описанных выше аппаратных ресурсов в кластер высокой доступности, необходимо запустить следующие гостевые системы для обеспечения работы СИО МГС:

– веб–сервера (srvweb1, srvweb2, srvweb3, srvweb4);

– DNS–сервера (srvdns1, srvdns2);

– сервер баз данных (srvsql1);

– почтовый сервер(srvpost);

– прокси–сервер (srvproxy);

– сервер мониторинга (monitoring).

Перечень программных продуктов, используемый в гостевых системах, приведен в Приложении 4.

Предлагаемые программно–аппаратные решения должны обеспечивать возможность гибкой модификации структуры и масштабирования ресурсов СИО МГС. Программное обеспечение (далее - ПО), предлагаемое к использованию в системе, должно соответствовать современным мировым требованиям по функциональному назначению, поддерживать основные протоколы совместимости и обмена. ПО должно быть создано на модульной основе, позволяющей легко добавлять, изменять функциональные возможности системы.

Для предоставления сервисов СИО МГС в сеть Интернет необходимо обеспечить выход гостевых систем в сеть Интернет. Схема организации доступа гостевых систем СИО МГС в сеть Интернет приведена в Приложении 5.

Общий перечень оборудования и платного программного обеспечения, необходимого для построения кластера высокой доступности, приведен в Приложении 6.

Реализация кластера высокой доступности для предоставления сервисов СИО МГС позволит обеспечить:

– доступность сервисов СИО МГС в 99%;

– высокую надежность за счет дублирования всех критически важных для работы СИО МГС компонентов;

– гибкое масштабирование и легкость в управлении за счет распределения нагрузки между серверами кластера и виртуализации.

Обеспечение информационной безопасности СИО МГС необходимо выполнять на основе стандарта ISO 27001, представляющее собой ряд мероприятий, направленных на предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию, а также её утечки:

* системы авторизации и аутентификации;
* системы разграничения доступа к информации;
* средства межсетевого экранирования;
* системы аварийного восстановления и резервного копирования;
* системы антивирусной защиты;
* системы контроля электронной почты и web-трафика;
* системы сегментирования локальной вычислительной сети;
* системы мониторинга и обнаружения и предотвращения вторжений;
* средства криптографической защиты информации.

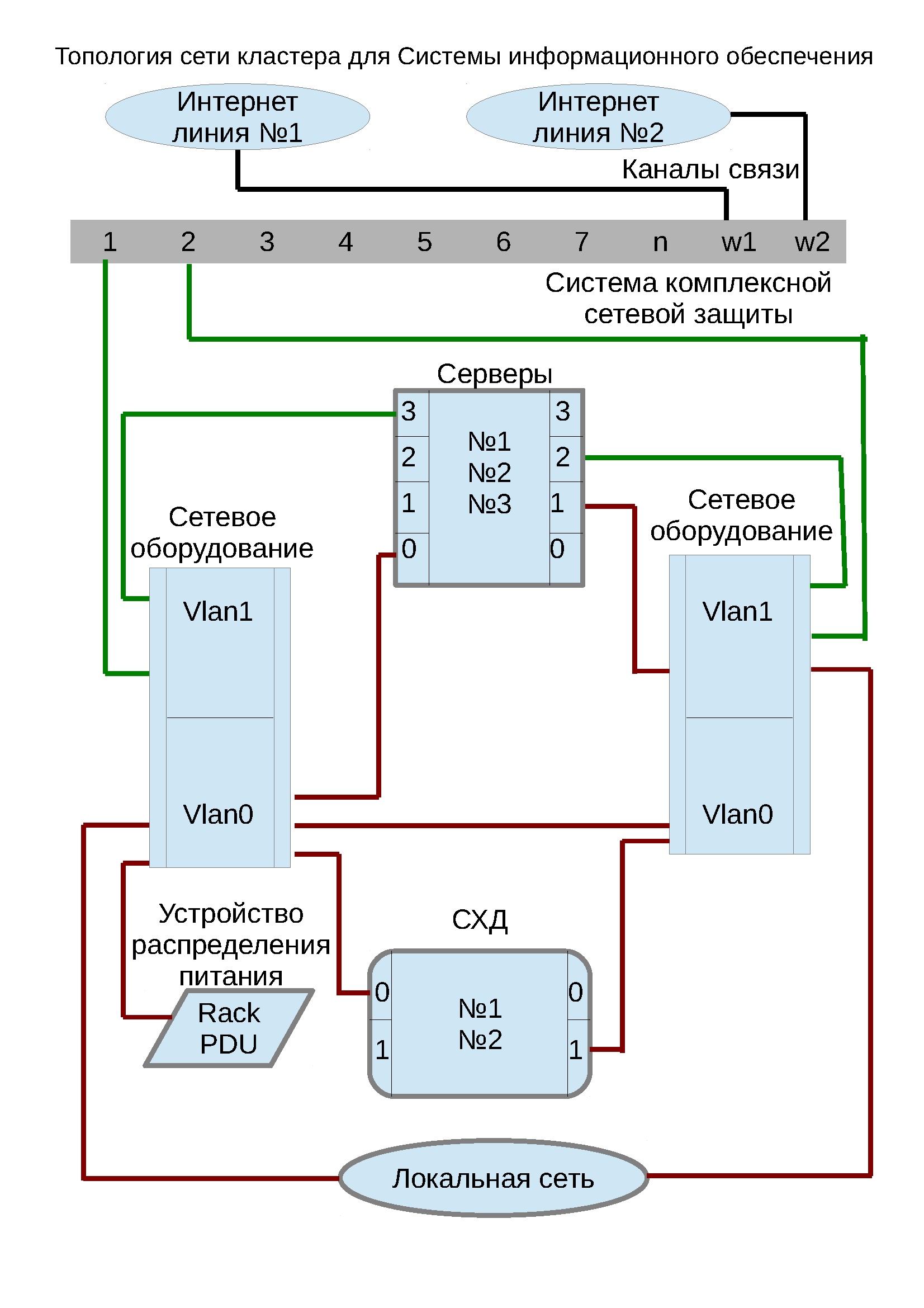
Для выявления возможных сбоев в процессе обмена данными между компонентами и модулями необходимо проводить тестирование:

* функциональное тестирование – тестирование ПО на соответствие функциональным спецификациям;
* стресс-тестирование на устойчивость – программная эмуляция нагрузки на ПО с целью проверки работоспособности в реальных условиях;
* тестирование производительности оборудования – анализ пиковой производительности оборудования на предмет соответствия требованиям.

Приложение 1

**Общая схема сетевой топологии элементов**

**инфраструктуры кластера высокой доступности**



Приложение 2

**Технические требования к серверам**

Сокет: Dual/QuadSocketServer (Quad/Six/HexaCoreCPUs´);

Процессор: CPU: 64bit (IntelEMT64 or AMD64);

Материнская плата: Intel VT/AMD–V capable CPU/Mainboard (for KVM Full Virtualization support);

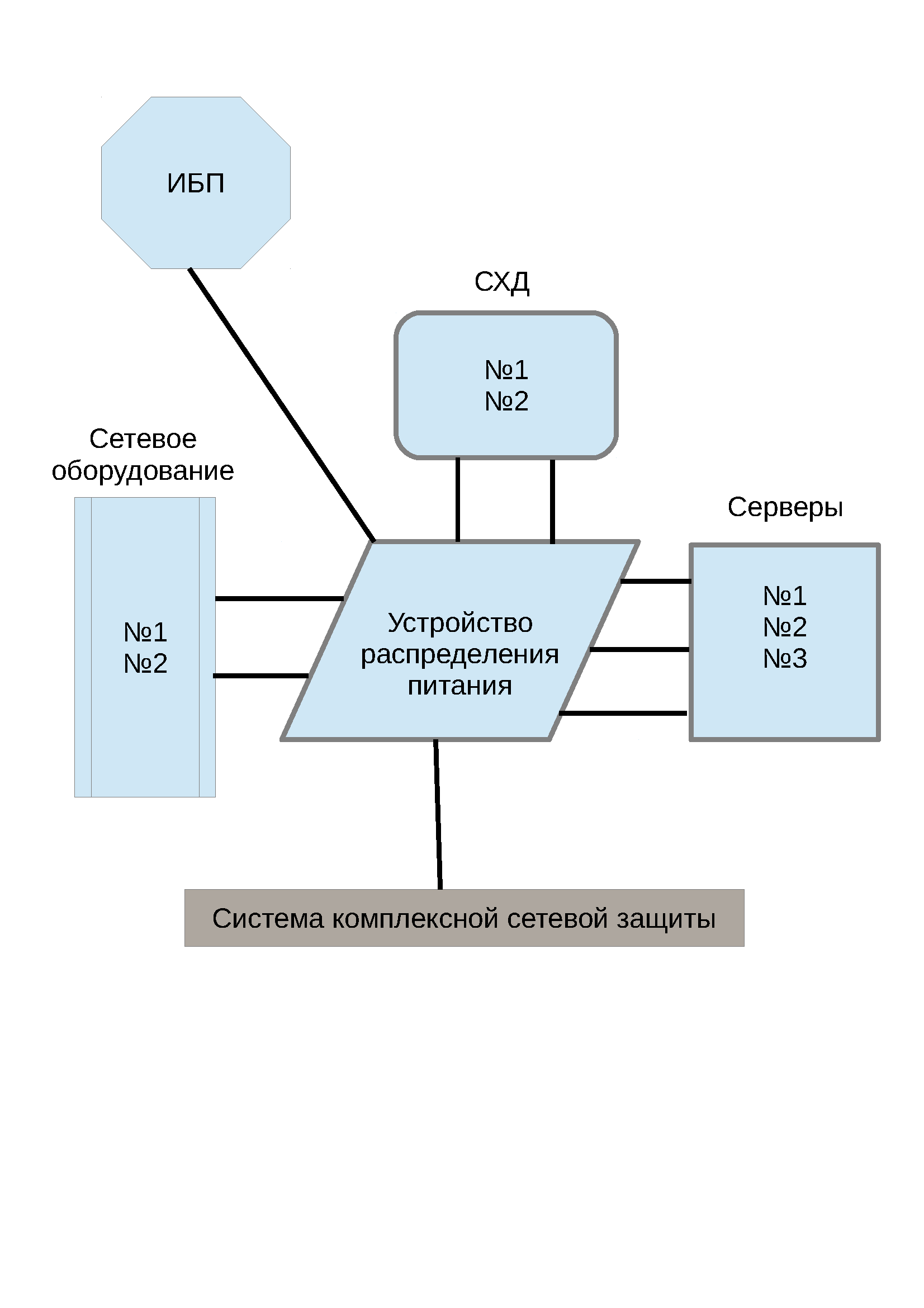
Оперативная память: 128 ГБ;

Жесткие диски: 15krpmSAS, hardware RAID with batteries protected write cache (BBU) or flash protection, Raid1 0;

Сетевые адаптеры: не менее 4 штук, 1Гб/с.

Приложение 3

**Схема подключения кабелей питания**



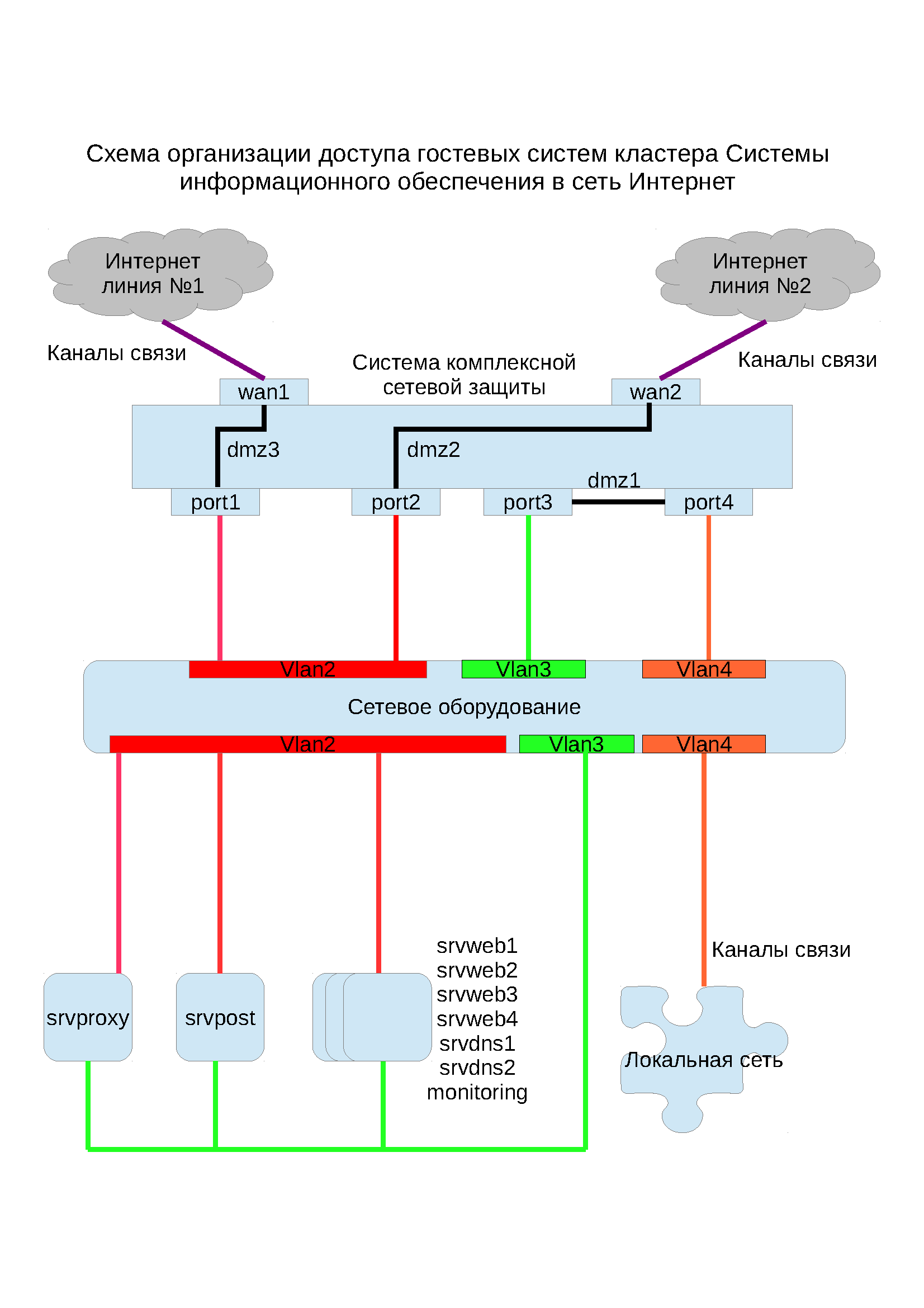
Приложение 4

**Перечень программных продуктов, используемый в гостевых системах**

|  |  |
| --- | --- |
| **Веб–сервера (srvweb1, srvweb2, srvweb3, srvweb4)** | |
| Ubuntu | операционная система |
| Nginx | frotend HTTP–сервер |
| Apache | backend HTTP–сервер |
| PHP | скриптовый язык программирования общего назначения |
| ClamAntiVirus | пакет антивирусного программного обеспечения |
| ProFTPd | FTP–сервер |
| **DNS–сервера (srvdns1, srvdns2)** | |
| Ubuntu | операционная система |
| Bind | открытая реализация DNS–сервера, обеспечивающая выполнение преобразования DNS–имени в IP–адрес и наоборот |
| Bindgraph | утилита для построения графиков количества запросов к DNS– серверу BIND |
| **Сервер баз данных (srvsql1)** | |
| Ubuntu | операционная система |
| MySQL | Система управления базами данных |
| **Почтовый сервер (srvpost)** | |
| Ubuntu | операционная система |
| Apache | backend HTTP–сервер |
| PHP | скриптовый язык программирования общего назначения |
| ClamAntiVirus | пакет антивирусного программного обеспечения |
| ProFTPd | FTP–сервер |
| Dovecot | свободный IMAP и POP3–сервер |
| Qmail | MTA (агент доставки почты) |
| SpamAssassin | средство для фильтрации спама |
| **Прокси–сервер (srvproxy)** | |
| Ubuntu | операционная система |
| Apache | backend HTTP–сервер |
| PHP | скриптовый язык программирования общего назначения |
| ClamAntiVirus | пакет антивирусного программного обеспечения |
| ProFTPd | FTP–сервер |
| MySQL | Система управления базами данных |
| Squid | программный пакет, реализующий функцию кэширующего прокси–сервера |
| Lightsquid | учет статистики прокси–сервера Squid |
| **Сервер мониторинга (monitoring)** | |
| Ubuntu | операционная система |
| MySQL | Система управления базами данных |
| Zabbix–Server | свободная система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования |
| Graylog2 | система централизованного сбора, хранения и анализа информации, которая пишется в syslog |

Приложение 5

**Схема организации доступа гостевых систем СИО МГС в сеть Интернет**



Приложение 6

**Перечень оборудования и платного программного обеспечения, необходимого для построения кластера высокой доступности**

|  |  |  |
| --- | --- | --- |
| № | Наименование | Количество |
| 1 | Сервер HP Proliant DL360pG8 E5–2620 p420i/512Mb 8x16Gb RAM 2x300Gb SAS HDD | 3 |
| 2 | Сетевой коммутатор (J9775A) HP 2530–48G Switch | 2 |
| 3 | Система хранения данных (BK830B) HP P2000 G3 iSCSI MSA 2–cntrl LFF Array с жесткими дисками (AW555A) HP P2000 2TB 6G SAS 7.2K 3.5in MDL HDD | 1 |
|  | Устройство распределения питания APC AP7921 | 1 |
| 5 | Источник бесперебойного питания APC SUA3000RMI2U | 2 |
| 6 | Оборудование предоставления сетевых сервисов FortiGate–100D 20 x GE RJ45 ports (including 1 x DMZ port, 1 x Mgmtport, 2 x HA port, 16 x internalswitchports), 2 x sharedmediapairs (including 2 x GE RJ45, 2 x GE SFP slots), 32GB onboardstorage, HardwareReplacement, обновление ПО и сигнатур для IPS, AV, AS, Webfiltering (2 Yr.) \* | 1 |
| 7 | Система хранения данных QNAP TS–869U–RP/8 с жесткими дисками Seagate 2000 Gb (ST2000VN000) | 1 |
| 8 | SSL Certificates: True BusinessID Wildcard | 1 |
| 9 | Годовая техническая поддержка системы виртуализации ProxmoxSubscriptionPlans "STANDARD" | 1 |
| 10 | Доменное имя | 1 |
| 11 | Оптоволоконная линия для подключения к сети интернет на скорости не менее 20 Мбит/с | 2 |
| 12 | Оптические конверторы | 2 |

\*Данная конфигурация включает двухгодичную лицензию на использование сетевых сервисов. По окончании срока использования лицензию необходимо продлять.