УТВЕРЖДЕНО
приказом автономного учреждения Чувашской Республики «Центр информационных технологий» Министерства цифрового развития, информационной политики Чувашской Республики
от 02.11.2023 № 185

Единые технические и технологические требования к элементам инфраструктуры и требования к информационной безопасности электронного правительства Чувашской Республики

Оглавление

1. Общие положения 7
1.1. Цели и задачи технических и технологических требований к элементам инфраструктуры электронного правительства в Чувашской Республике 7
1.2. Нормативно-техническое обеспечение ИТ-деятельности 7
2. Современные тенденции в области ИТ 10
2.1. Консолидация ресурсов 100
2.2. Виртуализация ресурсов 100
2.2.1. Логическое деление вычислительных комплексов 11
2.3. Современная архитектура приложений 122
2.3.1. Сервис-ориентированная архитектура – SOA 122
2.3.2. Многоуровневая архитектура клиент-сервер 122
2.4. Модель SaaS 133
2.5. Средства интеграции приложений (middleware) 133
2.6. Современная коммуникационная инфраструктура 133
3. Рекомендации по управлению ИТ инфраструктурой 144
3.1. Необходимость изменений в ИТ-инфраструктуре 144
3.2. Рекомендации по проведению изменений в ИТ инфраструктуре 144
3.2.1. Общие требования к тестированию и приемке изменений 144
3.2.2. Требования «разумного консерватизма» 144
3.2.3. Автоматизация тиражирования обновлений ПО 155
3.3. Рекомендации по планированию ИТ-инфраструктуры 155
3.3.1. Рекомендации по выбору горизонтов планирования для ИТ-приложений 166
3.3.2.Рекомендации по расчету производительности и объема хранимой информации для ИТ-систем (масштабирование ИТ-систем) 166
4. Каталогизация и классификация элементов ИТ-инфраструктуры 17
4.1. Типизация элементов ИТ-инфраструктуры 17
4.2. Классификация государственных информационных систем 18
4.3. Классификация по уровню требуемой непрерывности обслуживания 19
4.4. Принципы создания КРК 200
5.Технические требования к элементам ИТ-инфраструктуры 222
5.1.Требования к наименованиям элементов 222
5.1.1. Требования к наименованиям доменов 222
5.1.2. Требования к наименованию участников домена 222
5.1.3. Требования к адресам электронной почты 22
5.2. Требования к рабочим местам пользователей 233
5.2.1. Требования к персональным компьютерам 233
5.2.2.Требования к системному ПО рабочих мест пользователей 24
5.2.3.Требования к периферийным устройствам 25
5.3.Требования к мультисервисной сети 26
5.3.1.Требования к распределенной мультисервисной сети 2626
5.3.2.Требования к внешним каналам связи 31
5.4. Прикладное программное обеспечение (ПО) 32
5.4.1. Общие требования к прикладному ПО 33
5.4.2.Общие требования к универсальному прикладному ПО 34
5.4.3. Общие требования к заказному прикладному ПО 34
5.5. Требования к инфраструктуре центров обработки данных 34
5.5.1. Требования к системам обработки и хранения данных 34
5.5.2. Требования к помещениям и инженерным системам 400
5.6. Требования к обеспечению информационной безопасности 44
5.7. Требования к обеспечению непрерывности предоставления услуг 45

5.7.1. План обеспечения непрерывности предоставления услуг и восстановления после аварии 45
5.8. Требования к системе управления и мониторинга....46
5.8.1. Общие требования....4746
5.8.2. Требования к структуре СУМ ЦОД I и II уровней....47
5.8.3. Требования к функциональности СУМ ЦОД I и II уровней....47
5.8.4.Требования к управлению и мониторингу мультисервисной сети....4847
5.9. Требования к созданию и вводу в действие систем. Требования к документации....48
5.9.1. Требования к техническому заданию....49
5.9.2. Требования к технорабочему проекту....49
5.9.3. Требования к программам и методикам испытаний....50
5.9.4. Требования к эксплуатационной документации....50
5.9.5. Требования к поставке оборудования и ПО....50
5.9.6. Требования к вводу в действие....50
6. Минимальные требования к характеристикам типовой электронно-вычислительной техники, офисного оборудования, общесистемного и офисного программного обеспечения для нужд государственных учреждений Чувашской Республики, находящихся в ведении исполнительных органов Чувашской Республики....52
6.1. Типовая электронно-вычислительная техника....52
6.2. Типовое офисное оборудование....53
6.3. Типовое общесистемное программное обеспечение....54
6.4. Типовое офисное программное обеспечение....55
7. Минимальные требования к мультисервисной сети....5656
7.1. Минимальные требования к корпоративной распределенной мультисервисной сети....56
8. Минимальные требования к инфраструктуре центров обработки данных....64
8.1. Минимальные требования к системам обработки и хранения данных....64
8.2. Минимальные требования к системному ПО....64
8.3. Минимальные требования к помещениям и инженерным системам....64
9. Минимальные требования к системе управления и мониторинга....67
9.1. Требования к размещению системы управления и мониторинга ЦОД I и II уровней....67
9.2. Требования к системам управления и мониторинга ЦОД I и II уровней....67
9.3.Требования к рабочим станциям операторов системы управления и мониторинга....67
9.4. Требования к KVM системам....67
10. Минимальные требования к документации....68
11. Требования к средствам обеспечения безопасности....69
12. Таблица именования официальных адресов электронной почты и доменов для государственных учреждений Чувашской Республики....72

Используемые термины и сокращения

Термин	Описание
АВР	Автомат выбора резерва
ДМЗ	Демилитаризованная зона
ДЭС	Дизель-генераторные электростанции
ИБП	Источник бесперебойного питания
ИТ	Информационные технологии
ИС	Информационная система
КРК	Каталог рекомендованных конфигураций
ЛВС (LAN)	Локальная вычислительная сеть
МСЭ (firewall)	Межсетевой экран
МФУ	Многофункциональное периферийное устройство
ОИВ	Органы исполнительной власти
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
РФ	Российская Федерация
СКС	Структурированная кабельная система
СПД	Система передачи данных
СУБД	Система управления базами данных
СУМ	Система управления и мониторинга
СХД	Система хранения данных
ТЗ	Техническое задание
ЦИТ	АУ «Центр информационных технологий» Министерства цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики
ЦОД	Центр обработки данных
ЭП	Электронное правительство
API	Application programming interface, интерфейс прикладного программирования
COBIT	Control Objectives for Information and Related Technology («Задачи информационных и смежных технологий»), результат обобщения мирового опыта, международных и национальных стандартов и руководств в области управления ИТ, аудита и информационной безопасности
D2D	Disk-to-Disk, технология резервного копирования, когда резервное копирование выполняется с диска хост системы на диск системы резервного копирования. Служит для сокращения времени, необходимого для резервного копирования.
D2D2T	Disk-to-Disk-to-Tape, технология резервного копирования, когда резервное копирование выполняется с диска хост системы на диск системы резервного копирования, откуда переносится на ленту. Служит для сокращения времени, необходимого для резервного копирования

	ввиду медленного ввода/вывода с ленточных носителей.
DRP	Disaster Recovery Plan, план аварийного восстановления
DRS	Disaster Recovery System, система аварийного восстановления
EIGPR	Enhanced Interior Gateway Routing Protocol, протокол маршрутизации, использующий механизм DUAL для выбора наиболее короткого маршрута.
ERP	Enterprise Resource Planning system, автоматизированная система управления предприятием
IPMA	International Project Management Association, Международная ассоциация по управлению проектами
ITIL	Information Technology Infrastructure Library, библиотека инфраструктуры информационных технологий. Свод правил и рекомендаций, описывающий лучшие из применяемых на практике способов организации работы ИТ подразделений или ИТ компаний
LCR	Least Cost Routing («маршрутизация по критерию наименьшей стоимости»), технология, обеспечивающая прохождение телефонного вызова от одного абонента к другому по маршруту, обеспечивающему наименьшую стоимость телефонного соединения (наименьшую стоимость минуты разговора).
Middleware	Программная среда интеграции приложений
MPLS	Multiprotocol Label Switching, новый стандарт передачи данных в мультисервисных коммуникационных сетях
MTBF	Mean Time Between Failures, среднее время безотказной работы
NAS	Network Attached Storage, сетевая система хранения данных, сетевое хранилище.
NGN	Next Generation Network, сеть следующего поколения
OSI	Open Systems Interconnection, модель взаимодействия открытых систем
OSPF	Open Shortest Path First, протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала
PMI	Project Management Institute, институт управления проектами
QoS	Quality of Service («качество сервиса»), способность коммуникационной системы обеспечивать то или иное качество услуг в зависимости от вида передаваемых данных
RPO	Recovery Point Objective, целевая точка восстановления, т.е. момент, до которого необходимо восстановить данные или, другими словами, это фактически допустимый объем потерянных данных
RTO	Recovery Time Objective, целевое времени восстановления, т.е. время, необходимое на восстановление данных
SaaS	Software as a service («Программное обеспечение как услуга»), модель продажи программного обеспечения, при которой поставщик разрабатывает веб-приложение и самостоятельно управляет им, предоставляя заказчикам доступ к программному обеспечению через Интернет.
SAN	Storage Area Network, сеть хранения данных
SIP	Session Initiation Protocol, протокол установления сеанса. Стандарт на способ установления и завершения пользовательского интернет-сеанса, включающего обмен мультимедийным содержимым (видео- и аудиоконференция)
SNMP	Simple Network Management Protocol, протокол управления сетевыми устройствами
SOA	Service-Oriented Architecture, сервис-ориентированная архитектура.

	Модульный подход к разработке программного обеспечения, основанный на использовании сервисов со стандартизированными интерфейсами.
TCO	Total Cost of Ownership, совокупная стоимость владения
VLAN	Virtual Local Area Network, виртуальная локальная сеть
WAFS	Wide-Area File Services, файловые службы для глобальных сетей
Wi-Fi	Wireless Fidelity, технология беспроводных сетей
xWDM	Серия технологий передачи данных по оптическим каналам с уплотнением по длине волны

1. Общие положения

Внедрение элементов электронного правительства (ЭП) требует оптимальной адаптации ИТ-инфраструктуры органов исполнительной власти к реализации целей и задач, предъявляемых в рамках ЭП. Оптимальная адаптация ИТ-инфраструктуры к построению ЭП подразумевает реализацию синтеза методологических и идеологических основ, заложенных в документе ITIL, современных направлений развития и реализация эффективной ИТ-инфраструктуры в ОИВ и иных субъектах, использующих ИТ для повышения эффективности в своей деятельности. Результатом обозначенного синтеза выступает документ «Единые технические и технологические требования к элементам инфраструктуры электронного правительства в Чувашской Республике», определяющий конкретизированные базисные подходы к построению, развитию и интеграции ИТ-инфраструктур различных ОИВ в рамках ЭП.

1.1 Цели и задачи технических и технологических требований к элементам инфраструктуры электронного правительства в Чувашской Республике

Целью настоящего документа является описание базисных технических и технологических принципов построения ИТ-инфраструктуры ОИВ в рамках системы ЭП.

Задачи:

Описание системы категорий и понятий, используемых в рамках ИТ-инфраструктуры ЭП. Определение принципов экономической эффективности создания, функционирования и динамического изменения ИТ-инфраструктуры ЭП.

Обозначение технологических требований и технологий, используемых для построения, развития и интеграции ИТ-инфраструктуры органов исполнительной власти в рамках ЭП. Выделение формальных механизмов технологического взаимодействия уровней ИТ-инфраструктуры, а также функционального уровня, необходимых для эффективной реализации ЭП.

Унификации однородных составляющих различных уровней ИТ-инфраструктуры.

1.2 Нормативно-техническое обеспечение ИТ-деятельности

Технические и технологические требования к элементам инфраструктуры ЭП в Чувашской Республике созданы в соответствии с законодательством Российской Федерации, законодательством Чувашской Республики, с учетом международных и национальных стандартов в области информационных технологий.

Нормативные правовые акты Российской Федерации:

- Федеральный закон от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
- Федеральный закон от 9 февраля 2009 года № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;
- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;
- Национальная программа «Цифровая экономика Российской Федерации»;
- Типовая программа развития и использования информационных и телекоммуникационных технологий субъекта Российской Федерации утверждена распоряжением Правительства Российской Федерации от 3 июля 2007 года № 871-р;
- Постановление Правительства Российской Федерации от 15 апреля 2014 г. № 313 "Об утверждении государственной программы Российской Федерации "Информационное общество (2011 - 2020 годы)"
- Постановление Правительства Российской Федерации от 10 октября 2020 г. № 1646 «О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной

власти и органов управления государственными внебюджетными фондами» (вместе с «Положением о ведомственных программах цифровой трансформации»);

- Постановление Правительства Российской Федерации от 28 сентября 2010 г. № 764 «Об утверждении Правил осуществления контроля за соблюдением субъектами естественных монополий стандартов раскрытия информации»;
- Постановление Правительства Российской Федерации от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия»;
- Постановление Правительства от 25 декабря 2009 г. № 1088 «О государственной автоматизированной информационной системе «Управление»;
- Постановление Правительства Российской Федерации от 6 ноября 2007 г. № 758 «О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий»;
- Постановление Правительства Российской Федерации от 29 декабря 2007 года № 947 «Об утверждении Правил разработки, апробации, доработки и реализации типовых программно-технических решений в сфере региональной информатизации»;
- Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации»;
- Распоряжение Правительства Российской Федерации от 17 декабря 2009 года № 1993-р «Об утверждении сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых в электронном виде учреждениями субъектов Российской Федерации и муниципальными учреждениями»;

Нормативные правовые акты Чувашской Республики:

- Постановление Кабинета Министров Чувашской Республики от 10 октября 2018 г. № 402 «О государственной программе Чувашской Республики «Цифровое общество Чувашии»;
- Постановление Кабинета Министров Чувашской Республики от 1 февраля 2021 г. № 28 «О внесении изменений в государственную программу Чувашской Республики «Цифровое общество Чувашии»;
- Распоряжение Кабинета Министров Чувашской Республики от 10 марта 2005 г. № 65-р «О порядке представления сведений об основных показателях деятельности организаций для проведения систематического анализа финансового состояния и учета платежеспособности крупных, экономически или социально значимых организаций в Чувашской Республике»;
- Распоряжение Кабинета Министров Чувашской Республики от 15 апреля 2020 г. № 328-р «О составе Комиссии по цифровому развитию и использованию информационных технологий в Чувашской Республике по должностям и признании утратившими силу некоторых решений Кабинета Министров Чувашской Республики»;
- Постановление Кабинета Министров Чувашской Республики от 09 октября 2019 г. № 410 «Об утверждении Положения о государственной информационной системе «Автоматизированная информационная система многофункциональных центров предоставления государственных и муниципальных услуг»;
- Распоряжение Кабинета Министров Чувашской Республики от 17 ноября 2016 г. № 823-р о перечне государственных и муниципальных услуг, предоставляемых в электронном виде органами исполнительной власти Чувашской Республики, органами местного самоуправления, государственными учреждениями Чувашской Республики, муниципальными учреждениями и другими организациями, в которых размещается государственное задание (заказ) или муниципальное задание (заказ);

- Постановление Кабинета Министров ЧР от 13 декабря 2017 г. № 499 (ред. от 26.08.2020) «О Республиканском центре обработки данных» (вместе с «Положением о Республиканском центре обработки данных»).
- Постановление Кабинета Министров ЧР от 20 июля 2021 г. № 317 «О едином региональном операторе инфраструктуры и операторе информационной безопасности электронного правительства Чувашской Республики».

Технические и технологические требования к элементам инфраструктуры ЭП в Чувашские Республики развивают положения вышеуказанных нормативных документов по следующим направлениям:

- рекомендации по вопросам развития ИТ-инфраструктуры; требования к типизации и унификации ИТ-инфраструктуры;
- требования к поставщикам ИТ продукции и услуг; требования к элементам ИТ-инфраструктуры и их размещению;
- требования к внедрению и вводу в эксплуатацию государственных информационных систем;
- перечень рекомендуемых технических параметров оборудования и конфигурационных решений (Приложения к настоящему документу).

2. Современные тенденции в области ИТ

Современные технические сервисные подходы к построению и управлению информационно-вычислительными средами предполагают отказ от понятий «отдельный компьютер», «программа» или «программно-аппаратный комплекс». Вместо этого современный подход оперирует понятиями «ИТ-сервис» (информационная система) и «ИТ-ресурсы». С точки зрения данного подхода, основные задачи, стоящие перед современными ИТ-подразделениями - это:

- построение ИТ-инфраструктуры, ориентируясь на требования функциональных заказчиков; сохранение и повышение качества предоставляемых ИТ-сервисов; обеспечение безопасности функционирования ИТ-сервисов; обеспечение непрерывности функционирования ИТ-сервисов;
- сокращение общей стоимости владения ИТ (далее ТСО).

При построении ИТ-инфраструктуры рекомендуется использовать следующие современные подходы и технологии:

- консолидацию ресурсов; виртуализацию ресурсов; современную архитектуру приложений; модель SaaS;
- средства интеграции приложений; современную коммуникационную инфраструктуру.

2.1. Консолидация ресурсов

Современная ИТ-инфраструктура и, прежде всего, коммуникационная среда создают предпосылки для консолидации приложений и данных в современных центрах обработки данных (ЦОД). Данная модель построения ИТ-инфраструктуры обеспечивает более высокую:

- эффективность за счет снижения ТСО (прежде всего затрат на обслуживание и сопровождение ИТ систем и снижения капитальных затрат на обеспечивающую инфраструктуру);
- непрерывность (доступность) приложений за счет более высокой степени резервирования и отказоустойчивости программно-аппаратных средств, применяемых в ЦОД.

При построении и модернизации ИТ-инфраструктуры рекомендуется рассматривать четыре вида консолидации ресурсов:

1. Централизация — консолидация географически распределенных серверов в одном или нескольких ЦОД.
2. Консолидация данных — консолидация баз данных и/или устройств хранения для достижения более высокой доступности и управляемости данными.
3. Физическая консолидация — объединение серверов под управлением одной и той же ОС и с подобными приложениями, на более мощных системах.
4. Консолидация приложений и хранилищ данных — размещение различных приложений на мощных серверах с разделяемыми разделами, либо на системах виртуализации.

Практика показывает, что ТСО консолидированных решений значительно ниже, чем стоимость владения его различными компонентами в случае их раздельной эксплуатации.

2.2 Виртуализация ресурсов

Виртуализация — процесс представления набора вычислительных ресурсов, или их логического объединения, который дает преимущества перед оригинальной конфигурацией. Это новый, «виртуальный» взгляд на ресурсы, не ограниченных реализацией, географическим положением или физической конфигурацией составных частей. Обычно виртуализированные ресурсы включают в себя вычислительные мощности и хранилище данных.

Виртуализация — это общий термин, охватывающий абстракцию ресурсов для многих аспектов вычислений. Типы виртуализации:

- Программная виртуализация предполагает функционирование виртуальных сред поверх программной прослойки, обеспечивающей доступ изолированных виртуальных машин к общему пулу аппаратных ресурсов; Аппаратная виртуализация позволяет выделить виртуальной машине нужные аппаратные ресурсы и обеспечить распределение аппаратных мощностей на уровне устройств.

Области применения виртуализации:

- Виртуализация на уровне ОС: виртуализирует физический сервер на уровне ОС, позволяя запускать изолированные и безопасные виртуальные серверы на одном физическом сервере. Эта технология не позволяет запускать ОС с ядрами, отличными от типа ядра базовой ОС. При виртуализации на уровне ОС не существует отдельного слоя гипервизора. Вместо этого сама хостовая ОС отвечает за разделение аппаратных ресурсов между несколькими виртуальными серверами и поддержку их независимости друг от друга;
- Виртуальные машины: окружение, которое представляется для «гостевой» ОС, как аппаратное. Однако на самом деле это программное окружение, которое эмулируется программным обеспечением хостовой системы. Эта эмуляция должна быть достаточно надежной, чтобы драйверы гостевой системы могли стабильно работать. При использовании паравиртуализации, виртуальная машина не эмулирует аппаратное обеспечение, а, вместо этого, предлагает использовать специальный интерфейс прикладного программирования (API);
- Виртуализация ресурсов: разделение одного физического сервера на несколько частей, каждая из которых видна для владельца в качестве отдельного сервера. Не является технологией виртуальных машин, осуществляется на уровне ядра ОС;
- Виртуализация приложений: процесс использования приложения преобразованного из требующего установки в ОС в не требующий этого. Для виртуализации приложений программное обеспечение виртуализатора определяет при установке виртуализуемого приложения, какие требуются компоненты ОС и их эмулирует, таким образом, создается необходимая специализированная среда для конкретно этого виртуализируемого приложения и, тем самым, обеспечивается изолированность работы этого приложения.

Понятие «виртуальные машины» предполагает разделение на:

- Виртуализацию серверов: размещение нескольких логических серверов в рамках одного физического (консолидация); объединение нескольких физических серверов в один логический для решения определенной задачи;
- Виртуализацию рабочих станций: использование на рабочем месте «тонких» клиентов, позволяющих выполнять все необходимые пользователю задачи на сервере в отдельной для каждого клиента виртуализированной ОС.

Основные предпосылки применения технологий серверной виртуализации следующие:

- неуклонное повышение мощности единичного сервера, зачастую превышающее потребности конкретного приложения; аппаратная поддержка виртуализации в современных процессорах;
- большое число наследуемых приложений на устаревающих ОС и аппаратных платформах; тенденции к консолидации ИТ-инфраструктуры.

Рекомендуется использовать технологии и средства виртуализации ИТ-ресурсов при построении ИТ-инфраструктуры.

2.2.1 Логическое деление вычислительных комплексов

Технология аппаратных и программных разделов (partitioning)– это архитектурный подход к ИТ-инфраструктуре, позволяющий виртуализировать аппаратные ресурсы и сделать их доступными для множества независимых операционных сред. Изначально разработанная для mainframe, технология позволяет разделить один сервер на несколько

полностью независимых аппаратных или программных виртуальных серверов или логических разделов. Технология с небольшими различиями поддерживается ведущими производителями ИТ-оборудования. Технология логического деления вычислительных комплексов в сочетании с планами восстановления после сбоев и восстановления после катастроф (DRS и DRP) и с использованием двух разнесенных ЦОД (основного и резервного), создают основу катастрофоустойчивой инфраструктуры таким образом, что приложение и разделы с критическими приложениями, выполняемые в основном ЦОД, могут переключаться на резервный ЦОД с минимальными потерями.

Современные системы виртуализации позволяют создание кластеров высокой готовности, позволяющие перемещать сервисы (виртуальные машины) между узлами (аппаратными серверами) для распределения нагрузки единичного узла и для обеспечения функционирования сервиса при аппаратном сбое единичного узла. Рекомендуется использовать такие конфигурации, с целью обеспечения высокой доступности сервисов.

2.3 Современная архитектура приложений

Рекомендуется отдавать предпочтение ИТ-решениям, имеющим современную, сервис-ориентированную многоуровневую архитектуру.

2.3.1 Сервис-ориентированная архитектура – SOA

Наиболее перспективная архитектура построения приложений на настоящее время – Service Oriented Architecture (SOA – сервис-ориентированная архитектура). Основная задача SOA облегчить интеграцию приложений - как новых программных решений, так и систем предыдущих поколений. Архитектура SOA независима от языков программирования, платформ или протокольных спецификаций, с помощью которых сервисы разрабатываются, а также от того, где и с помощью чего они развернуты. Практически архитектура SOA требует наличия не только сервисов, но и средств, с помощью которых эти сервисы могут быть обнаружены и подключены, а также множества компонентов, таких, как: серверы приложений, связующее ПО, репозиторий и даже специализированные пакеты централизованного управления SOA.

2.3.2. Многоуровневая архитектура клиент-сервер

Клиент-сервер — вычислительная или сетевая архитектура, в которой задания или сетевая нагрузка распределены между поставщиками услуг (сервисов), называемыми серверами, и заказчиками услуг, называемыми клиентами. Нередко клиенты и серверы взаимодействуют через компьютерную сеть и могут быть как различными физическими устройствами, так и программным обеспечением.

В настоящее время большинство ИС проектируются с использованием трехуровневой архитектуры «клиент-сервер», представляющей ИС в виде совокупности трех компонент: сервера баз данных, сервера приложений, отвечающего за выполнение логики приложения, и клиентского приложения или клиентского интерфейса («тонкий клиент»). Основными преимуществами выделения логики приложения в отдельную составляющую являются возможность повторного использования кода, легкость модификации централизованно развернутых компонентов, повышение производительности используемого сервера базы данных, возможность масштабирования системы в целом и независимость системы от физического расположения базы данных. Кроме того, системы, построенные в трехуровневой архитектуре, существенно проще и дешевле в эксплуатации, т.к. все исправления и конфигурационные настройки вносятся централизованно.

Составляющие трехуровневой архитектуры:

- уровень представления (реализующий функции ввода и отображения данных); прикладной уровень (реализующий универсальные сервисы, а также функции, специфичные для определенной предметной области);
- уровень доступа к информационным ресурсам (реализующий фундаментальные функции хранения и управления информационно-вычислительными ресурсами).

2.4. Модель SaaS

Программное обеспечение как услуга (software as a service, сокр. SaaS) - модель использования программного обеспечения, при которой поставщик разрабатывает веб-приложение и самостоятельно управляет им, предоставляя пользователям доступ к ПО через сеть. Основное преимущество модели SaaS для пользователя состоит в отсутствии затрат, связанных с установкой, обновлением и поддержкой работоспособности оборудования и работающего на нѐм ПО. Использование SaaS предпочтительней как более дешевая и простая альтернатива внутренним информационным ресурсам.

2.5. Средства интеграции приложений (middleware)

Для построения интегрированной ИТ инфраструктуры, особенно при использовании различных программно-аппаратных сред, рекомендуется использовать специализированные программные средства – Интеграционные платформы. Интеграционная платформа должна обеспечивать доступ в реальном масштабе времени к различным информационным ресурсам, обмен и синхронизацию данных между ними, автоматически, по заданным правилам и расписанию - поддержку единого стандарта обмена информацией между приложениями, независимо от платформ, на которых они существуют.

Базовые функциональные возможности должны включать в себя средства проверки корректности, очистки, объединения структурированных и неструктурированных данных, репликации данных и публикации информации о событиях, а также средства корпоративного поиска.

Продукты такого типа, как правило, строятся на принципах сервис-ориентированной архитектуры и предназначены для решения задач обеспечения достоверности информации в масштабе организации, контроля качества данных, их преобразования, перемещения и объединения, а также управления метаданными.

Применение данных технологий позволяет, с помощью соответствующих сервисов, предоставляемых приложениям, процессам и отдельным пользователям, быстро сопоставить, согласовать и объединить разрозненные данные, поступающие из различных источников.

2.6. Современная коммуникационная инфраструктура

Для построения сетей передачи данных рекомендуется применять технологии построения виртуальной частной сети на базе MPLS/VPN, с использованием услуг, предоставляемых крупными телекоммуникационными операторами национального масштаба. При необходимости, резервирование каналов осуществляется телекоммуникационными операторами, в том числе, с использованием мобильной связи. При невозможности резервирования канала средствами телекоммуникационного оператора необходимо предусмотреть наличие резервного канала с возможностью переключения на него в случае недоступности основного.

Построение внутренней сетевой инфраструктуры рекомендуется производить на базе современных принципов построения сети, обеспечивающих гарантированное качество сетевых услуг (QoS).

Архитектура таких сетей состоит из четырех основных компонентов, а именно:

1. Интеллектуальная сетевая инфраструктура на базе протокола IP;
2. Интеллектуальные клиентские места с поддержкой протокола IP;
3. Служебные серверные приложения;
4. Современные пользовательские приложения.

Основа архитектуры - ее распределенная природа, благодаря которой система легко масштабируется. За счет этого, сетью на базе данной архитектуры можно охватить одно здание или несколько стоящих рядом зданий, объединенных высокоскоростной локальной сетью, предоставить в сети сервисы телефонии и данных для пользователей удаленных офисов и подразделений, объединенных IP сетью.

Защита информации ограниченного доступа при её передаче с использованием информационно-телекоммуникационных сетей должна обеспечиваться в соответствии с требованиями нормативных правовых актов Российской Федерации в области защиты информации, в том числе в соответствии Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17, Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 № 152.

3. Рекомендации по управлению ИТ инфраструктурой

3.1. Необходимость изменений в ИТ-инфраструктуре

При решении задач управления ИТ-инфраструктурой существенное значение имеют процессы, связанные с изменениями ИТ-инфраструктуры. Технические решения, связанные с изменениями ИТ-инфраструктуры, должны быть обоснованы, в том числе, с учетом оценки их влияния на стоимость и качество услуг, оказываемых ИТ-службой, и реализованы с учетом следующих рекомендаций по внесению изменений и планированию ИТ-инфраструктуры.

3.2. Рекомендации по проведению изменений в ИТ инфраструктуре

Процесс по проведению изменений в ИТ-инфраструктуре – это процесс использования стандартизированных методов и процедур для эффективного и своевременного проведения изменений в ИТ-инфраструктуре с минимальными негативными последствиями для деловых процессов.

При изменении ИТ-инфраструктуры необходимо учитывать следующие требования:

- Общие требования к тестированию и приемке изменений;
- Требований «разумного консерватизма» при внедрении новых версий ИТ-компонентов;
- Требований автоматизации тиражирования обновлений ПО; Обязательное документирование вносимых изменений.

3.2.1. Общие требования к тестированию и приемке изменений

Процесс тестирования и приемки изменений ИТ-инфраструктуры должен удовлетворять следующим общим требованиям:

- Решение о проведении изменений должны приниматься Службой заказчика по согласованию с функциональными заказчиками. Служба заказчика вправе разработать упрощенный порядок принятия решений о проведении некритичных для деловых процессов изменений;
- Перед вводом изменений в эксплуатацию необходимо разработать и протестировать план
- Внесения изменений с обязательным указанием контрольных точек принятия решения об отказе от внесенных изменений и возврате системы в предыдущее состояние;
- Тестирование плана внесения изменений необходимо производить в среде, аналогичной производственной; Тестирование и приемку изменений необходимо производить в среде, аналогичной производственной;
- Ввод изменений в эксплуатацию предваряется резервным копированием всех элементов системы, подвергшихся изменению.

3.2.2. Требования «разумного консерватизма»

При внедрении, модернизации, обновлении ИТ-компонентов должны быть соблюдены следующие общие требования «разумного консерватизма»:

- внедрение новых версий ПО должно иметь обоснованные преимущества перед используемыми версиями ПО и не должно ухудшать текущего состояния дел;
- для критически важных деловых процессов недопустимо внедрение последних версий
- промышленного ПО и/или его компонентов, за исключением используемых в схожей промышленной среде более 2 лет и имеющих при этом не менее 2 корректирующих обновлений от производителя (релизов, патчей, сервис-паков, обновлений ПО и т.п.);
- недопустимо использование тестовых версий ИТ-компонентов (альфа, бета версии ПО и т.п.) в режиме промышленной эксплуатации; при планировании внедрения новых версий ПО рекомендуется учитывать долгосрочные
- планы производителя по выпуску новых версий/релизов; перед внедрением новых версий ПО в промышленную эксплуатацию обязательно
- тщательное тестирование функционирования соответствующей системы, с заключениями соответствующих ключевых специалистов.

3.2.3. Автоматизация тиражирования обновлений ПО

Автоматизация тиражирования обновлений ПО должна выполняться с учетом следующих общих требований и рекомендаций:

- при выборе ПО, при прочих равных функциональных характеристиках, преимущество следует отдавать системам, имеющим службы централизованного управления и обновления;
- создание и внедрение решения по автоматизации тиражирования обновлений ПО должно производиться в рамках отдельных проектов ИТ-службы и с использованием собственной серверной системы тиражирования обновлений. Обновление ПО непосредственно с Интернет-портала производителя не допускается;
- функциональные возможности автоматизированной системы тиражирования обновлений должны позволять реализацию полного и упрощенного циклов управления изменениями, проводить автоматическую проверку (аудит) тиражирования обновлений; тиражирование обновлений в области безопасности критичных для предприятия систем (обновления ОС, ПО с непосредственным доступом во внешние сети/Интернет, антивирусные системы и т.п.) подлежит обязательной автоматизации; тиражирование обновлений в области безопасности на рабочие станции и инфраструктурные ИТ-компоненты (домен-контроллеры, DNS/DHCP/mail-сервера и т.п.) в части системного и офисного ПО подлежит обязательной автоматизации;
- обновление инфраструктурного ПО (домен-контроллеры, DNS/DHCP/mail-сервера), включающего смену функциональности, смену версии используемого ПО, за исключением обновлений в области безопасности, необходимо проводить под контролем соответствующего специалиста, предварительно проведя тестирование в тестовой среде, аналогичной производственной;
- рекомендуется автоматизация тиражирования обновлений клиентской части программных приложений;
- перед масштабным тиражированием обновлений необходимо провести тестирование в локальной тестовой среде.

3.3. Рекомендации по планированию ИТ-инфраструктуры

При планировании ИТ-инфраструктуры должен быть обеспечен экономически обоснованный уровень соответствия ресурсов ИТ-инфраструктуры текущим и будущим потребностям потребителей. Для эффективного планирования ИТ-инфраструктуры необходимо учитывать прогноз развития основной деятельности потребителя и технического развития ИТ. Поэтому для каждого потребителя важное значение имеет выбор горизонтов планирования для различных ИТ-приложений и определение базовой методики расчета производительности и объема хранимой информации для ИТ-систем.

3.3.1. Рекомендации по выбору горизонтов планирования для ИТ-приложений

Выбор горизонтов планирования ИТ-приложений должен определяться горизонтом планирования потребителя. При этом горизонт планирования ИТ-инфраструктуры должен быть меньше, чем горизонт планирования ИТ-приложений.

Рекомендуется исходить из следующих горизонтов планирования ИТ-приложений:

- 8-9 лет для приложений класса ERP и приложений управления ИТ, критичных для деловых процессов;
- 5-6 лет для деловых приложений и систем операционного управления ИТ;
- 3-5 лет для офисных и системных приложений.

При этом для соответствующих элементов ИТ инфраструктуры рекомендуется установить следующие горизонты планирования:

- 5-6 лет для приложений класса ERP и приложений управления ИТ, критичных для деловых процессов; 3-4 года для деловых приложений и систем операционного управления ИТ;
- 2-3 года для офисных и системных приложений.

3.3.2. Рекомендации по расчету производительности и объема хранимой информации для ИТ-систем (масштабирование ИТ-систем)

Расчет производительности ИТ-систем должен производиться в терминах ИТ-услуг, исходя из планируемых сроков использования (горизонта планирования), объемов, значений показателей уровня предоставления и производительности услуг.

При расчете производительности подлежат учету нагрузочные возможности всех задействованных в предоставлении ИТ-услуг компонентов: ИТ-услуг, ИТ-систем, компонентов инфраструктуры и систем информационной безопасности, включая клиентские рабочие станции.

При растете производительности ИТ-систем обязателен учет как средних, так и пиковых показателей нагрузки. Рекомендуется для расчета производительности использовать предоставляемый производителем инструментарий - нагрузочные кривые и разработанные лучшие методики (bestpractices).

В общем случае, в ходе расчета рекомендуется проводить оценку загрузки по следующим компонентам:

- сервер приложений; сервер баз данных;
- серверные средства информационной безопасности (антивирусное обеспечение, программный МСЭ, криптографические системы и т.п.);
- компоненты мониторинга (агенты и т.п.); системное ПО;
- аппаратная платформа (процессоры, оперативная память, дисковая подсистема, сетевой интерфейс);
- сети хранения данных (SAN, NAS);
- сети передачи данных, включая активные устройства (МСЭ, маршрутизаторы и т.п.); сетевые сервисы (сервисы каталога, DNS, DHCP и т.п.);
- клиентские рабочие станции в аппаратной и программной части.

Для оценки объема хранимой информации рекомендуется использовать собственные статистические данные по объемам и динамике изменения данных за длительные (от 1 месяца) периоды и максимальные значения в пиковые периоды. При отсутствии собственных данных допустимо использование статистики схожих предприятий или экспертных оценок. При внедрении новых сервисов следует придерживаться информации, указываемой производителем, как в области начальных требований, так и в прогнозируемых объемах увеличения информации. Последний показатель следует корректировать в ходе последующей эксплуатации систем.

При оценке объема хранимой информации обязателен учет не только полезного объема, но и объемов системной и служебной информации (системы шифрования, файлы логирования, файлы журналов транзакций и т.п.).

4. Каталогизация и классификация элементов ИТ-инфраструктуры

4.1 Типизация элементов ИТ-инфраструктуры

Унификация и типизация элементов ИТ-инфраструктуры способна значительно снизить расходы и облегчить внедрение новых ИТ-решений, снизить затраты на подготовку ИТ- персонала, упростить сопровождение и обслуживание этих решений в будущем и, в конечном итоге, значительно снизить общую стоимость владения ИТ- инфраструктурой в целом.

Под типизацией понимается снижение номенклатуры и повышение качества ИТ-элементов и конфигураций, внедряемых в органах государственной власти Чувашской Республики.

Данные Технические требования в области ИТ выдвигают требования к следующим категориям ИТ инфраструктуры:

- рабочим местам пользователей (ПК, периферийное оборудование);
- мультисервисной сети (корпоративная сеть, внешние каналы связи); прикладному ПО;
- инфраструктуре центров обработки данных (системы хранения и резервирования, серверы);

Общие требования к указанным категориям и их отдельным элементам приведены в главе 6 настоящего документа. При разработке технических политик и других нормативных документов в области ИТ необходимо учитывать указанные требования.

В приложениях к данному документу приведены рекомендуемые минимально допустимые технические требования к соответствующим категориям. При развитии ИТ-инфраструктуры органов государственной власти Чувашской Республики, государственных учреждений Чувашской Республики необходимо учитывать данные рекомендации. Также данные рекомендации необходимо учитывать при разработке и внедрении Каталогов Рекомендованных Конфигураций в ЦИТ.

При построении современной ИТ-инфраструктуры для определения места установки (размещения) ИТ-решения необходимо провести классификацию данного решения в зависимости от совокупности следующих параметров: состава пользователей данной системы, степени агрегации информации, хранения и обработки данных; решаемых задач; уровня сложности и т.д.

С точки зрения данной классификации рекомендуется выделить следующие классы или уровни инфраструктуры для размещения ИТ-систем:

- Центр обработки данных - ЦОД I уровня, (уровень Правительства Чувашской Республики, ЦИТ) – обеспечивает централизованное хранение и обработку данных на уровне Правительства Чувашской Республики. Ресурсы данного ЦОД используются для консолидации информации с нижележащих уровней, обеспечения информационного взаимодействия органов государственной власти Чувашской Республики и оказания ИТ-сервисов всем организациям, финансируемым из республиканского бюджета Чувашской Республики.
- Центр обработки данных - ЦОД II уровня, основной центр хранения и обработки данных в рамках одного органа государственной власти Чувашской Республики. Услугами данного ЦОД пользуется большинство сотрудников данного ОГВ и государственных учреждений.

В разделе «5.5. Требования к инфраструктуре центров обработки данных (системы хранения и резервирования, серверы)» содержатся общие требования к оборудованию ЦОД различного уровня. Кроме того, в приложениях к данному документу приведены текущие рекомендованные минимальные требования к ИТ-конфигурациям и их элементам (программно-аппаратным средствам, системам связи и коммуникаций). ИТ-конфигурации с заявленными характеристиками ниже приведенных минимальных значений не

рекомендуется закупать и вводить в эксплуатацию в органах государственной власти Чувашской Республики, государственных учреждений Чувашской Республики.

4.2. Классификация государственных информационных систем

К основным направлениям информатизации в Чувашской Республике относятся следующие группы ИС:

1. Информационные системы предоставления государственных услуг и инфраструктуры электронного правительства

Такие информационные системы обеспечивают переход к новой форме организации деятельности органов государственной власти и органов местного самоуправления, качественно новый уровень оперативности и удобства получения организациями и гражданами государственных и муниципальных услуг, а также информации о результатах деятельности органов власти.

К ним относятся Региональная система межведомственного взаимодействия Чувашской Республики, Региональный агрегатор государственной информационной системы о государственных и муниципальных платежах, Официальный портал органов власти Чувашской Республики, Автоматизированная информационная система многофункциональных центров предоставления государственных и муниципальных услуг, Система электронного документооборота органов власти Чувашской Республики, Региональный сегмент Единой государственной информационной системы социального обеспечения и другие.

2. Информационные системы обеспечения специальной деятельности

К ним относятся информационные системы, предназначенные для автоматизации либо информационной поддержки исполнения государственных функций, предусмотренных нормативно-правовыми актами Чувашской Республики, - информационные системы органов исполнительной власти Чувашской Республики по отраслевой принадлежности.

3. Информационные системы обеспечения типовой деятельности

Это информационные системы, предназначенные для автоматизации обеспечивающей деятельности государственных органов в рамках исполнения ими типовых полномочий, предусмотренных нормативными правовыми актами Чувашской Республики. Например, системы бухгалтерского учета, справочно-правовые системы и другие.

4. Информационные системы управления социальной сферой

Информатизация процессов управления в социальной сфере ориентирована, прежде всего, на внедрение экономических механизмов и ИТ, направленных на:

- смягчение негативных последствий бедности, снижение социального неравенства и предотвращение социального иждивенчества;
- расширение рынка и повышение качества предоставляемых социальных услуг.

5. Информатизация деятельности органов исполнительной власти Чувашской Республики.

Анализ основных направлений деятельности органов исполнительной власти Чувашской Республики позволяет выделить следующие направления информатизации:

- Информационные системы предоставления государственных услуг. Информационные системы предоставления государственных услуг предназначены для повышения качества и доступности предоставляемых государственных услуг, упрощения процедур и сокращения сроков их оказания, повышения открытости информации о деятельности органов государственной власти и органов местного самоуправления.
- Информационные системы электронного правительства. ИС ЭП обеспечивают переход к новой форме организации деятельности органов государственной власти и органов местного самоуправления, качественно новый уровень оперативности и удобства получения организациями и гражданами государственных и муниципальных услуг, а также информации о результатах деятельности органов власти.
- Информатизация учрежденческой деятельности органов исполнительной власти;

- Информационная поддержка деятельности по вопросам управления государственной собственностью;
- Информатизация экономической деятельности и финансово-кредитного комплекса Чувашской Республики;
- Информатизация международных связей и внешнеэкономической деятельности Правительства Чувашской Республики;
- Информатизация процессов управления по предотвращению и ликвидации чрезвычайных ситуаций.

4. Информатизация органов законодательной и представительной власти Чувашской Республики.

Информатизация законодательной и представительной власти Чувашской Республики проводится в следующих направлениях:

- информационная поддержка проведения заседаний Государственного Совета Чувашской Республики, информационная поддержка законотворческой деятельности депутатов и депутатских комиссий; информационная поддержка текущей деятельности депутатов;
- информационная поддержка геополитического и социально-экономического мониторинга Чувашской Республики.

6. Информационные системы природопользования и охраны окружающей среды.

Информатизация процессов эффективного использования природных ресурсов (природопользования) и охраны окружающей среды направлена на создание необходимых условий, обеспечивающих сбалансированное развитие природно-сырьевой базы для удовлетворения потребностей в топливно-энергетических, минеральных, водных и лесных ресурсах, обеспечение конституционных прав граждан на благоприятную окружающую среду.

Направлениями информатизации процессов управления природопользованием и охраной окружающей среды являются:

- информатизация процессов управления использованием минерально-сырьевых ресурсов; информатизация процессов управления использованием лесных ресурсов;
- информатизация процессов управления использованием водных ресурсов; информатизация процессов управления охраной окружающей среды; информатизация процессов регулирования в области обращения с отходами.

6. Информационные системы органов местного самоуправления

Можно выделить следующие основные типовые направления информатизации органов местного самоуправления:

- информатизация финансово-кредитной деятельности;
- информационная поддержка управления имуществом;
- информационная поддержка управления потребительским рынком;
- информатизация процессов социального развития территории;
- информатизация процессов градостроительства;
- информационная поддержка управления коммунальным хозяйством;
- информатизация учрежденческой деятельности органов местного самоуправления;
- создание инфраструктуры информатизации местного самоуправления

4.3. Классификация по уровню требуемой непрерывности обслуживания

Многие критические управленческие и технологические процессы опираются на компьютерные системы обработки и хранения данных и не могут функционировать без их использования. Поэтому, обеспечение непрерывности обслуживания и доступности ИТ-решений является важнейшим показателем непрерывности государственного управления в целом, и важным классифицирующим фактором для элементов ИТ-инфраструктуры. Исходя из предъявляемых требований к надежности отдельных элементов и конфигураций ИТ-

систем в целом и их восстановлению после сбоев и отказа оборудования, ПО или инфраструктурных элементов, современные ИТ-технологии предоставляют различные архитектурные и конфигурационные решения, обеспечивающие данные требования. С точки зрения обеспечения непрерывности обслуживания управленческих и технологических пользователей и процессов, а также требований к отказоустойчивости, можно предложить следующую классификацию ИТ-решений:

- Mission Critical – системы, работающие в режиме «боевого дежурства». К таким системам относятся: остро критические с точки зрения государственного управления или внешних факторов – например экологии, приложения, а также технологические приложения, работающие в режиме реального времени. Выход из строя этих систем влечет за собой невосполнимые потери для управления, в т.ч. угрозу жизни и здоровью персонала и населения. Рекомендованное время восстановления подобных систем после отказа менее 10 минут. Для таких систем должны использоваться специализированные серверные платформы и инфраструктурные уровни с полным многократным резервированием всех компонентов, в том числе с использованием резервных удаленных ЦОД;
- Business Critical – системы, критические для управления, с режимом работы 24x7x365. Выход из строя этих систем влечет за собой значительные потери для управления. Рекомендованное время восстановления подобных систем после отказа менее 2 часов. Для таких систем должны использоваться кластерные решения и инфраструктурные уровни с частичным резервированием используемых инфраструктурных компонентов;
- Business Operational – обычные деловые приложения - системы, не требующие работы в реальном времени, с режимом работы 8x5. Рекомендованное время восстановления подобных систем после отказа 4-6 часа. Для таких систем рекомендуется использовать резервирование хранения данных и электропитания;
- Office Production – не критические для управления приложения, персональные данные. Рекомендованное время восстановления подобных систем после отказа 1-2 рабочих дня.

Необходимо учитывать, что общая непрерывность и отказоустойчивость ИТ-конфигураций определяется соответствующей непрерывностью и отказоустойчивостью ее отдельных элементов: аппаратных, программных средств и инфраструктуры, необходимой для ее успешного функционирования – каналов связи, системы электропитания и т.д. и, в конечном итоге, зависит от уровня непрерывности и отказоустойчивости его слабейшего компонента (принцип «слабого звена»). Классификация систем с точки зрения обеспечения непрерывности и отказоустойчивости должна быть одним из решающих факторов при выборе уровня инфраструктуры (ЦОД) для размещения ИТ-систем. В разделе «6.5. Требования к инфраструктуре центров обработки данных (системы хранения и резервирования, серверы)» содержатся общие требования к таким конфигурациям в разрезе ЦОД различного уровня.

4.4. Принципы создания КРК

Основная цель создания КРК – провести унификацию используемого оборудования и ПО, и обеспечить целостность и управляемость ИТ-инфраструктуры органов государственной власти Чувашской Республики, государственных учреждений Чувашской Республики.

При построении и развитии своей ИТ-инфраструктуры все органы государственной власти Чувашской Республики, государственные учреждения Чувашской Республики должны закупать и внедрять только внесенные в каталог ИТ-конфигурации. Закупка конфигураций, которые не входят в данный список, возможна в только виде исключения.

Унификация ИТ-решений, используемых в рамках конкретного органа государственной власти позволит добиться снижения общего ТСО, что подразумевает снижение расходов на закупки, внедрение и эксплуатацию элементов ИТ- инфраструктуры.

Каталог может создаваться в каждом органе государственной власти Чувашской Республики и должен содержать следующий минимальный набор данных о рекомендованной конфигурации:

- название конфигурации; класс объекта (функциональный раздел каталога) в соответствии с приложением - «7.6. Приложение 6. Классификатор объектов ИКТ-инфраструктуры»;
- класс конфигурации по уровню использования;
- класс конфигурации по уровню непрерывности;
- рекомендуемый набор аппаратных средств, для данной конфигурации; рекомендуемый набор программных средств, для данной конфигурации.

Для каждой позиции данного каталога необходимо выбрать конкретных производителей и конкретный перечень моделей их оборудования (или эквивалент) или ПО, принимая во внимание рекомендации к требованиям к элементам ИТ-инфраструктуры, приведенные в главе 6 и Приложениях к данному документу.

В качестве рекомендованных минимальных значений технических и функциональных параметров конфигураций необходимо использовать данные Приложений 2-6 к настоящему документу.

При создании каталога рекомендованных конфигураций необходимо руководствоваться следующими основными принципами:

- Все конфигурации, включаемые в каталог, должны соответствовать общим требованиям к оборудованию и ПО, изложенным в главе 6 настоящего документа;
- В качестве рекомендованных минимальных значений технических и функциональных параметров конфигураций необходимо использовать данные Приложений 2-6 к настоящему документу;
- Количество унифицированного оборудования и ПО в каждом функциональном разделе каталога должно быть минимально;
- Рекомендуется использовать стандартное оборудование и ПО зарекомендовавшего себя на рынке производителя в данной области, который постоянно развивает и совершенствует свой модельный ряд;
- Каталог должен регулярно (не реже чем раз в год) пересматриваться и обновляться;
- Рекомендуется использовать сложное аппаратно–программное обеспечение разного назначения одного и того же производителя. Такое решение упрощает управление ИТ-инфраструктурой, позволяет снизить эксплуатационные затраты, а также стоимость вновь приобретаемого аппаратно–программного обеспечения;

5. Технические требования к элементам ИТ-инфраструктуры

Данные технические требования рассматриваются в разрезе лучших мировых практик по созданию ИТ-инфраструктуры для современных корпораций. Отдельные требования предъявляются к следующим категориям инфраструктурных элементов:

- Элементы инфраструктуры ЭП в Чувашской Республике:
  - Домены;
  - Участники доменов;
  - Электронная почта;
- Рабочие места пользователей:
  - Персональные компьютеры;
  - Системное ПО рабочих мест пользователей;
  - Периферийные устройства;
- Прикладное ПО;
- Мультисервисная сеть:
  - Корпоративная распределенная мультисервисная сеть;
  - Внешние каналы связи;
- Инфраструктура центров обработки данных:
  - Системы обработки и хранения данных;
  - Помещения и инженерные системы;
  - Информационная безопасность;
  - Непрерывность предоставления ИТ-услуг;
  - Системы управления и мониторинга;

5.1. Требования к наименованиям элементов

Инфраструктура ЭП складывается из ряда элементов, в число которых входит и доменная структура, и электронная почта. В данном разделе перечислены требования к наименованиям доменов, участников доменов и адресов электронной почты.

5.1.1. Требования к наименованиям доменов

Доменное имя организации формируется с использованием символов, входящие в стандартный набор символов, разрешенных для использования в именах DNS узлов Интернета. Допустимые знаки определены в документе RFC 1123.

Для доменов третьего уровня и ниже (поддоменов) корпоративных доменов инфраструктуры ЭП (в том числе домена cap.ru) допустимо использовать: английские строчные буквы (a-z), цифры (0-9) и дефис (-). Имя поддомена не должно превышать 12 символов.

5.1.2. Требования к наименованию участников домена

Шаблон: Т-Ф, где:

1. Т — тип сервиса либо название ведомства (delo- система электронного документооборота, ag-Администрация Главы Чувашской Республики, agro- Министерство сельского хозяйства Чувашской Республики, и так далее)
2. Ф — функция в сети либо порядковый номер (DC, DNS, DHCP, WEB, DB, … — для серверов; 01, 02, 03 … — для рабочих станций).

5.1.3. Требования к адресам электронной почты

Электронная почта государственных органов Чувашской Республики и государственных учреждений Чувашской Республики используется для служебных целей.

Лица, замещающие государственные должности Чувашской Республики, государственные гражданские служащие Чувашской Республики для официальной электронной переписки используют почтовые адреса в домене cap.ru. Использование для официальной электронной переписки почтовых адресов в публичных сервисах

предоставления адресов электронной почты (в том числе gmail.com, mail.ru, rambler.ru и др.) и поддоменах, не относящихся к домену cap.ru, запрещается.

В адресное пространство электронной почты государственных органов Чувашской Республики и государственных учреждений Чувашской Республики входят:

1. официальные адреса органов государственных органов Чувашской Республики и государственных учреждений Чувашской Республики (далее – официальные адреса);
2. служебные адреса структурных подразделений государственных органов Чувашской Республики и государственных учреждений Чувашской Республики (далее - служебные адреса);
3. персональные адреса работников государственных органов Чувашской Республики и государственных учреждений Чувашской Республики (далее - персональные адреса).

Официальные адреса органов государственной власти Чувашской Республики устанавливаются, в соответствии с приложением 9 настоящего документа. Официальные адреса эксплуатируются работниками, ответственными за ведение делопроизводства в государственном органе Чувашской Республики и государственном учреждении Чувашской Республики.

Служебные и персональные адреса назначаются и ликвидируются по заявкам руководителей органов государственных органов Чувашской Республики. Служебные адреса эксплуатируются работниками, ответственными за ведение делопроизводства в структурном подразделении. Персональный адрес электронной почты эксплуатируется лично владельцем, либо, по его поручению, другим лицом.

Персональный адрес электронной почты является деперсонифицированным и складывается из транслитерации краткого наименования органа власти и последовательной нумерации сотрудников. Пример корректного адреса электронной почты: agro10@cap.ru. Порядок составления имени пользователя является строгим и не допускает изменений в порядке символов, изменении знаков пунктуации. Символы указываются строго на латинице, строчными буквами.

При необходимости использования обезличенного (общего) почтового ящика, например, для общих вопросов или как почтовый ящик группы пользователей, допускается до знака "@" вместо номера указывать обобщенное ключевое слово, например, info. Указанный адрес должен являться псевдонимом для существующего (существующих) адреса (адресов) электронной почты конкретного пользователя (пользователей).

Структура именования домена является трехуровневой. При необходимости допускается использование более глубокой вложенности доменов.

5.2. Требования к рабочим местам пользователей

5.2.1. Требования к персональным компьютерам

Данный раздел рассматривает общие технические требования к парку персональных компьютеров, эксплуатируемых в органах государственной власти Чувашской Республики, а также Государственных учреждений Чувашской Республики.

Конкретные минимальные технические требования изложены в приложении – «7.1.1 Минимальные требования к характеристикам ПК». Рекомендованные технические требования указаны в КРК.

При несоответствии компьютерного парка конфигурациям, указанным в КРК (устаревание компьютерного парка), и при условии, что минимальные технические требования общесистемного ПО превышают используемые технические конфигурации, рекомендуется обновление компьютерного парка до актуального состояния, указанного в КРК из расчета 20% от общего числа АРМ в год.

5.2.1.1. Общие требования

При развитии парка персональных компьютеров и выборе закупаемых моделей ПК ИТ-службы ЦИТ и Государственных учреждений Чувашской Республики должны руководствоваться следующими положениями:

- Аппаратная платформа и ПО персональных компьютеров должны быть стандартизованы и сертифицированы, иметь гибкую и масштабируемую архитектуру;
- Аппаратные характеристики ПК должны соответствовать, либо превосходить минимальные системные требования используемого ПО. В случае, когда аппаратные характеристики превосходят минимальные системные требования используемого ПО, конфигурация должны быть адекватной выполняемым задачам, не должна сильно превышать минимальные требования;
- Для обеспечения общего уровня услуг, управление данными всех ПК должно быть унифицировано, т.е. для ПК должно быть организовано централизованное распространение ПО с помощью единого инструмента распространения обновлений ПО;
- ПК с установленным системным и прикладным ПО (рабочая станция) должен иметь аппаратную либо программную систему удаленного управления;
- Для повышения качества и скорости администрирования количество различных программно–аппаратных конфигураций персональных компьютеров должно быть ограничено. Рекомендуется использование не более 4 типовых конфигураций.

Для спецификации технических требований выделяются следующие ключевые параметры ПК:

- Производительность. Производительность персональных компьютеров должна обеспечиваться за счет:
  - Параметров быстродействия процессора;
  - Необходимого и достаточного объема оперативной памяти;
  - Скорости внутренних шин передачи данных;
  - Качества и быстродействия графической подсистемы;
  - Устройств ввода/вывода;
- Надежность. Надежность должна обеспечиваться за счет аппаратных средств и ПО и определяться исходя из среднего времени безотказной работы (MTBF). Масштабируемость. Масштабируемость должна обеспечиваться архитектурой и конструкцией персонального компьютера за счет возможности наращивания:
  - Числа и мощности процессоров;
  - Объемов оперативной и внешней памяти.

5.2.1.2. Требования к типизации конфигураций

Весь парк ПК в органах государственной власти Чувашской Республики, государственных учреждениях Чувашской Республики предлагается разделить на следующие типовые конфигурации АРМ:

АРМ Типа 1. Персональный компьютер для работы со специализированным прикладным ПО (офисные системы, финансовые системы, СЭД и т.п.);

АРМ Типа 2. Персональный компьютер повышенной мощности для работы с графическими пакетами, пакетами ПО моделирования, САПР, АСУЭИ, АСУТП и пр. Используется для приложений с развитой графикой, высокими требованиями к производительности процессора и объемам оперативной памяти;

АРМ Типа 3. Тонкий клиент. Маломощный персональный компьютер для работы с приложениями в терминальной среде, либо с программами - тонкими клиентами в клиент-серверной архитектуре. При такой работе основные ресурсоемкие операции производятся на сервере.

Мобильное АРМ. Ноутбук для работы мобильных пользователей.

Каждое АРМ состоит из системного блока, монитора (допускается объединение системного блока и монитора в моноблок), клавиатуры, манипулятора «мышь» (при необходимости) с установленным и настроенным общесистемным ПО.

5.2.2. Требования к системному ПО рабочих мест пользователей

Конкретные минимальные технические требования изложены в приложении – «6.1.2. Минимальные требования к системному ПО рабочих мест пользователей».

ОС офисного назначения должны:

- Соответствовать по типу клиентским ОС;
- Поддерживать все сетевые сервисы, обеспечивающие функционирование корпоративной сети;
- Обеспечивать необходимый уровень информационной безопасности;
- Быть совместимыми с корпоративным стандартом используемого офисного ПО.

5.2.3. Требования к периферийным устройствам

Настоящий раздел излагает основные технические требования к применяемым и закупаемым для органов государственной власти Чувашской Республики, государственных учреждений Чувашской Республики периферийным устройствам, входящим в ИТ инфраструктуру.

Конкретные минимальные технические требования изложены в приложении – «6.1.3. Минимальные требования к периферийным устройствам».

Рассматриваются требования к следующим классам периферийных устройств:

- Устройства печати (принтеры);
- Многофункциональные устройства;

Требования к специализированным устройствам, имеющим узкое технологическое применение (термопринтеры, принтеры штрих-кодов, наклеек, типографии и т.д.), не рассматриваются. Использование специализированного оборудования принимается на основе конкретных технических требований технологического процесса.

Для описания минимальных требований к периферийному оборудованию используется следующая классификация устройств:

- Персональное устройство – находится в постоянном использовании одним сотрудником;
- Групповое устройство – используется в режиме разделения ресурсов группой сотрудников;
- Корпоративное устройство – используется в задачах, подразумевающих использование высокопроизводительных устройств (графика, большие форматы вывода данных (A1,A2,A3) и т.д.

5.2.3.1. Общие требования

В данном разделе излагаются общие требования, которые необходимо применять при выборе и закупке нового периферийного оборудования в целях развития ИТ в органах государственной власти Чувашской Республики, государственных учреждениях Чувашской Республики. Периферийное оборудование должно отвечать следующим основным требованиям:

- Производительность. Периферийное оборудование должно обеспечивать потребности деловых процессов и удовлетворять требованиям, определенным в количественных показателях (например, количество копий в минуту, разрешение сканируемого изображения и т.д.).
- Надежность. Периферийное оборудование должно позволять обеспечивать непрерывность деловых процессов и удовлетворять требованиям, определенным в количественных показателях (MTBF).

- Функциональность. В том случае, если рабочее место сотрудника должно быть оборудовано несколькими видами периферийного оборудования, следует отдавать предпочтение при закупке МФУ, которое должно поддерживать все или частично все следующие функции:
  - печатного устройства;
  - сканирующего устройства;
  - копировального устройства;
- Совместимость. Периферийное оборудование должно технически и программно сопрягаться с персональными компьютерами (в случае использования группового или корпоративного устройства – с серверами) независимо от типа процессора и ОС.
- Безопасность. Выход из строя какого-либо периферийного устройства не должен влиять на устойчивую работу персональных компьютеров (в случае использования группового или корпоративного устройства – серверов) с другим периферийным оборудованием.
- Управляемость. Подключение и управление персональным периферийным оборудованием по возможности должны быть простыми и не требовать оперативного использования инструкций и описаний работы устройств.
- Низкая ТСО. Запчасти и расходные материалы для периферийного оборудования должны быть легко доступны и обладать невысокой стоимостью.
- Низкий уровень создаваемого акустического шума. Периферийным оборудование в процессе работы не должно создавать помех окружающим. Для эксплуатации шумного оборудования должны быть предусмотрены специально выделенные помещения.
- Низкое энергопотребление. Рекомендуется приобретение оборудование, имеющее режим пониженного энергопотребления (режим ожидания).
- Следует отдавать предпочтение тем периферийным устройствам, которые в штатном режиме имеют возможность обмена информацией через локальную сеть.
- Те периферийные устройства, которые имеют возможность подключаться как к ПК, так и к локальной сети следует подключать к локальной сети.

5.2.3.2. Требования к групповым и корпоративным устройствам

Для групповых и корпоративных устройств должны применяться более жесткие требования, нежели к персональным устройствам. При выборе групповых и корпоративных устройств необходимо исходить из оценки количества пользователей, которые будут эксплуатировать данные устройства.

МФУ должны проходить периодическое техническое обслуживание, которое будет способствовать более высокой доступности устройства и снизит ТСО. Периодичность данного обслуживания необходимо определять из технических требований по эксплуатации каждого конкретного устройства.

См. «7.8 Приложение 8. Каталог рекомендованных конфигураций».

5.3. Требования к мультисервисной сети

5.3.1. Требования к распределенной мультисервисной сети

Данный раздел рассматривает технические требования к распределенной мультисервисной сети. Приводятся требования к архитектуре, протоколам и оборудованию.

Конкретные минимальные технические требования изложены в приложении – «6.2.1. Минимальные требования к корпоративной распределенной мультисервисной сети».

5.3.1.1. Общие требования

Основные стратегические положения и подходы к организации корпоративной распределенной мультисервисной сети: ориентация на архитектуру сетей следующего поколения (NGN).

Телефония, аудиоконференцсвязь, видеоконференцсвязь и передача данных должны основываться на единой конвергентной мультисервисной сети, которая позволяет предоставлять указанные сервисы, обеспечивая необходимый и достаточный уровень QoS.

Сеть построена на следующих принципах:

- Распределенная корпоративная архитектура, обеспечивающая QoS;
- Высокая доступность и надежность сети;
- Производительность, управляемость и масштабируемость сети;
- Мультисервисная сеть должна проектироваться с учетом требований информационной безопасности.

Весь трафик должен быть классифицирован на следующие классы, определяющие приоритет обслуживания:

- Трафик реального времени (телефонный, аудио и видео);
- Трафик передачи пользовательских данных;
- Технологический трафик.

Если технологическое оборудование требует наивысшего класса обслуживания, то его трафику должен быть отдан наивысший приоритет. После этого должен идти трафик реального времени, после которого следует трафик пользовательских приложений. Причем пропускная способность сети и активное сетевое оборудование должны всегда обеспечивать качество для трафика реального времени.

При аварийных ситуациях ресурсы сети должны отдаваться технологическому трафику и части трафика реального времени и пользовательского трафика в том объеме, в котором это необходимо для обеспечения бесперебойной работы основного технологического оборудования и обслуживающего его персонала. Данные правила должны быть реализованы в настройках оборудования и вступать в силу автоматически при наступлении аварийной ситуации.

5.3.1.2. Требования к архитектуре сети

Архитектура мультисервисной сети должна быть основана на следующих принципах:

Строиться на трехуровневой модели; Иметь резервирование по оборудованию и каналам; Поддерживать VLAN;

Архитектурно разбиваться на демилитаризованные зоны (ДМЗ); Сеть должна обеспечивать необходимую для решения задач производительность; Сеть должна обеспечивать QoS для разных классов трафика.

Мультисервисная сеть для ЦОД должна проектироваться, исходя из трехуровневой модели коммутации:

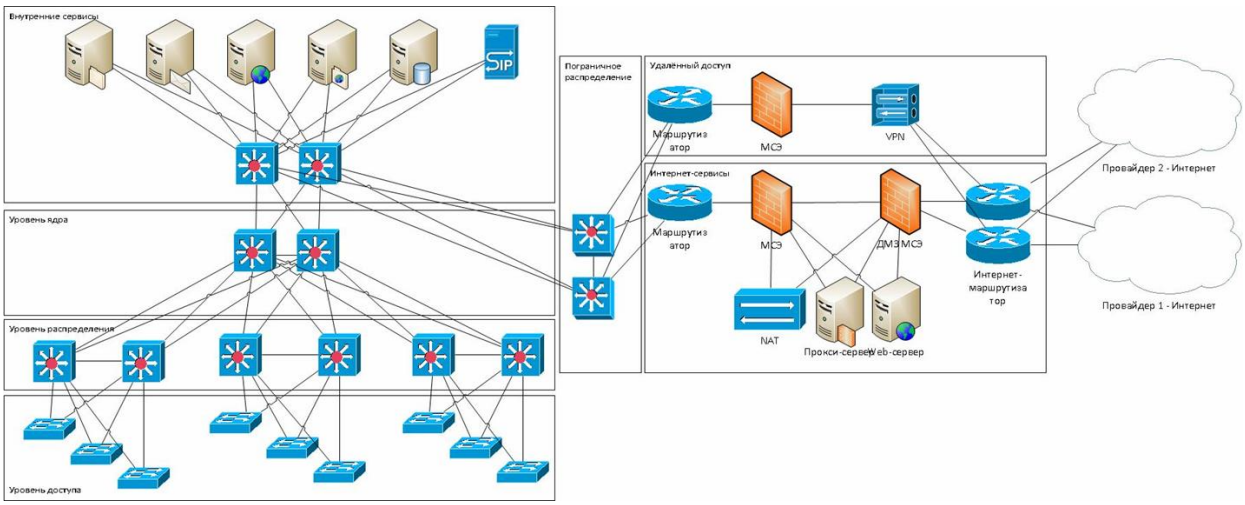
Уровень доступа (Access Layer) – коммутаторы 2-го уровня модели OSI с интеллектуальностью 3–4-го уровней модели OSI (с целью обеспечения требований к сетевой безопасности, QoS и т. д.).

Уровень распределения (Distribution Layer) – коммутаторы 3–4-го уровней модели OSI.

Магистральный уровень / уровень ядра (Core Layer) – коммутаторы 3–4-го уровней модели OSI.

В случаях, когда использование выделенных коммутаторов уровня распределения в каком-либо сегменте сети нецелесообразно по причине снижения производительности сетевой инфраструктуры, снижения надежности или в силу иных причин, допускается переносить функции коммутаторов уровня распределения на коммутаторы уровня ядра.

Принципиальная схема указанной трехуровневой модели приведена на следующем рисунке:



Выбранная архитектура сети должна позволять наращивать сеть путем добавления новых блоков, обеспечивать высокий детерминизм поведения сети, требовать минимальных усилий и средств для поиска и устранения неисправностей. Интеллектуальные сервисы 3-го уровня модели OSI (в том числе протоколы маршрутизации) должны обеспечивать сокращение области, затрагиваемой при возникновении разнообразных проблем с неисправным или неверно настроенным оборудованием, а также балансировку нагрузки между/внутри уровнями иерархии и быструю сходимость.

Должны быть соблюдены общие правила проектирования трехуровневой структуры:

- Любые проблемы с оборудованием и каналами связи на нижележащих уровнях не должны сказываться на верхних уровнях;
- Транзитные резервные маршруты определенного уровня не должны проходить через нижележащие уровни;
- Классификация трафика должны происходить только на уровне доступа. Приоритизация трафика должна поддерживаться всеми уровнями сети. Уровень распределения должен только агрегировать трафик. Ядро сети должно только осуществлять быструю коммутацию и маршрутизацию пакетов;
- Время сходимости таблиц маршрутизации и их объем должны быть оптимизированы для каждого уровня посредством выбора оптимальной схемы резервирования;
- Удаленные пользователи и внешние каналы связи не должны подсоединяться напрямую к ядру сети. Необходимо использовать коммутаторы доступа для предотвращения лавинообразных перестроек таблиц маршрутизации всей сети;
- Запрещается использование неуправляемых коммутаторов. Минимально допустимый коммутатор в сети - управляемый коммутатор уровня 2.

Резервирование для ЦОД I уровня должно, а для ЦОД II уровня рекомендуется организовывать следующим образом:

- В сети должно быть не менее двух коммутаторов уровня ядра, связанных между собой по 10 (либо выше) GigabitEthernet, либо объединенных в отказоустойчивый стек с эквивалентной пропускной способностью;
- Каждый коммутатор уровня доступа должен иметь соединения каналами Gigabit Ethernet с двумя коммутаторами уровня распределения;
- Каждый коммутатор уровня распределения должен иметь соединения каналами Gigabit Ethernet (либо выше) с двумя коммутаторами уровня ядра;
- Для обеспечения отказоустойчивости в сети должно быть два пограничных маршрутизатора. Маршрутизаторы подключаются каждый к не менее чем двум различным интернет-провайдерам и осуществляют маршрутизацию пакетов по протоколу BGP. Каждый пограничный маршрутизатор должен быть связан с двумя устройствами, обеспечивающими функциональность МСЭ или IDS/IPS;

- Для обеспечения независимости от интернет-провайдеров должна использоваться автономная системы (AS) с собственным пулом ip-адресов (не менее /23).

Производительность сети должна быть обеспечена следующим образом:

- Поэтажные коммутаторы (коммутаторы доступа) должны соединяться с коммутаторами уровня распределения по GigabitEthernet или 10 GigabitEthernet;
- Серверы должны соединяться с коммутаторами уровня распределения по GigabitEthernet или 10 GigabitEthernet. При необходимости допускается подключение серверов к коммутаторам уровня ядра; Коммутаторы уровня распределения и ядра должны быть выбраны соответствующей производительности. При выборе уровня производительности, необходимо учитывать требование поддержки всех требуемых протоколов с требуемым уровнем QoS.
- Между двумя зданиями рекомендуется прокладывать оптические каналы. При больших расстояниях, необходимости пропуска большого объема трафика и больших скоростей передачи данных рекомендуется организовывать каналы связи на основе технологии оптического уплотнения (xWDM) и агрегации каналов.

Надежность сети должна быть обеспечена при помощи выполнения следующих правил:

- Оборудование магистрального уровня должно иметь резервирование всех компонентов; Сеть должна быть спроектирована в соответствии с требованиями по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования, утвержденными приказом Минкомсвязи России от 25.08.2009 № 104, требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17;
- В сети должны использоваться VLAN. VLAN должны в обязательном порядке защищаться все ресурсы сети и пользователей, с использованием которых осуществляется обработка защищаемой информации.

Поддержка масштабируемости сети должна быть обеспечена следующим образом:

- За счет правильного внедрения трехуровневой модели коммутации.
- За счет масштабируемости коммутаторов, которая должна достигаться за счет объединения коммутаторов в группы (стеки). Причем каждый коммутатор в стеке должен работать в двух режимах – как главный коммутатор стека и как процессор коммутации пакетов. Должна обеспечиваться отказоустойчивость системы по схеме 1:N (при выходе из строя одного из коммутаторов стека, независимо от выполняемой им функции, остальные будут продолжать выполнение своих функций без остановки работы всей сети);
- Рекомендуется использовать динамический протоколы внутренней маршрутизации OSPF либо EIGRP как обладающие хорошей масштабируемостью, быстрой сходимостью, учитывающие качество каналов связи и занимающие минимальную полосу канала.

Система IP-адресации сети должна обеспечивать:

- Разделение адресного пространства на служебный блок (сети, связывающие маршрутизаторы, виртуальные интерфейсы и т.п.) и блок адресов локальной сети. Такое разделение позволяет эффективно строить правила доступа к сетевым устройствам;
- Распределение адресного пространства локальной сети блоками в соответствии с территориальным расположением. Такое разделение позволяет производить агрегирование адресов, что приводит к уменьшению таблиц маршрутизации и упрощает управление сетью.

Для осуществления аутентификации на уровне доступа для всех устройств, обеспечивающих функционирование сети, и при доступе к консоли управления всеми устройствами, сеть должна обладать следующими возможностями:

- Безопасность портов, т.е. должна быть возможность использования порта коммутатора с предварительно заданными физическими адресами пользовательских ПК (MAC-адреса). При попытке подключения неавторизованного устройства должно производиться отключение этого порта и уведомление системы управления сетью; Автоматическое конфигурирование портов коммутаторов, т.е. должна быть автоматизация;

- изменения конфигурации порта на основе логического подключения пользователя к сети; Аутентификация административного доступа на Radius сервере, т.е. должна быть идентификация, авторизация и учет при доступе к командной строке устройства; Ограничение доступа по IP адресам, с учетом ограничения на доступ к командной строке устройства и системной консоли, а также SNMP трафика;
- Должна быть автоматическая фильтрация трафика неиспользуемых протоколов на портах коммутаторов.

Для обеспечения высокой доступности сети рекомендуется использовать следующую функциональность:

- Поддержка протокола RSTP/MSTP или иных протоколов резервирования второго уровня; Поддержка возможности объединять в единый логический канал несколько физических соединений между коммутаторами; Функции автоматического переключения с основного маршрутизатора на резервный в случае отказа основного;
- Балансировка нагрузки между резервируемыми маршрутизаторами; Функции внутреннего ПО для улучшения времени сходимости протоколов маршрутизации и балансировки нагрузки через равноценные маршруты.

Для поддержки приложений, основанных на технологии многоадресной рассылки IP Multicast, от сетей требуется наличие следующих возможностей:

- На уровне доступа/распределения – передача пакетов IP Multicast на канальном уровне на скорости физического канала, динамическая регистрация посредством протоколов IGMP и PIM.
- Магистральный уровень – передача пакетов IP Multicast на канальном и сетевом уровнях на скорости физического канала, масштабируемые протоколы маршрутизации трафика IP Multicast.

5.3.1.3. Требования к телефонии, аудио- и видео-конференцсвязи

Основной протокол передачи аудио- и видеоинформации – IP. Допускается использование традиционной аналоговой телефонии в следующих случаях:

- Унаследованные существующие телефонные станции;
- Экономическая целесообразность. Данное исключение действует до момента, когда стоимость VoIP телефонов станет сопоставима с ценой аналогового телефона.

VoIP преимущественно должна внедряться по технологии SIP, т.к. данная технология, по сравнению с H.323, используется в сетях следующего поколения и имеет большую функциональность. При этом необходимо обращать внимание на совместимость реализации протокола SIP между оконечными устройствами и программно-аппаратным комплексом, обеспечивающим функциональность учрежденческой телефонной станции. Данная совместимость должна выражаться в поддержке основного функционала по обработке поступающих звонков с оконечных устройств. В целях недопущения проблем, связанных с несовместимостью реализации протокола SIP, рекомендуется устанавливать оконечные устройства (телефоны) и программно-аппаратные комплексы, обеспечивающие функциональность учрежденческой телефонной станции, одного производителя, либо проводить тщательное лабораторное тестирование совместимости аппаратуры разных производителей.

Системы видеоконференцсвязи должны поддерживать Web-конференции и интегрироваться с офисными приложениями.

Сервера аудиоконференцсвязи должны поддерживать или иметь возможность расширения для поддержки видеоконференцсвязи.

Видеоконференцсвязь должна организовываться на технологии IP с использованием стандартов H.323/H.264.

При пакетной передачи за эталон качества речи должен быть принят уровень качества, равный 4 баллам по шкале MOS/PAMS (Mean Opinion Score, субъективный метод оценки согласно рекомендации P.800). Рекомендуется использовать кодек G.729 (MOS = 4.07).

Требования к параметрам качества пакетной передачи: задержка пакетов – до 150 мс, джиттер – до 50 мс.

При наличии двух и более провайдеров, включая традиционную телефонию и VoIP, рекомендуется использовать LCR. При этом оборудование VoIP должно обеспечивать мониторинг качества канала связи.

5.3.1.4. Требования к оборудованию

Оборудование уровня доступа должно обладать возможностью классификации трафика (Traffic Classification), т.е. должна быть обеспечена возможность классифицировать трафик по типам приложений, физическим и сетевым адресам источников и получателей, портам коммутаторов. Классифицированный трафик должен получать метку, обозначающую назначенный пакетам уровень приоритета, тем самым давая возможность устройствам сети соответствующим образом обслуживать этот трафик. Должна быть обеспечена реклассификация пакетов на основе заданной администратором политики качества обслуживания. Например, пользователь назначает высокий приоритет своему трафику и передает его в сеть. Этот приоритет может затем быть понижен в соответствии с сетевой политикой, а не на основе требований пользователя. Данный механизм должен быть ключевым в обеспечении качества обслуживания в рамках всей сети.

Оборудование магистрального уровня должно обладать следующей функциональностью:

- Предотвращение и управление перегрузками, т.е. должна быть обеспечена возможность управлять поведением сети при перегрузках, отбрасывая определенные пакеты на основе классификации или политики в моменты перегрузки сети и множества очередей на интерфейсах. Администратор должен устанавливать пороговые значения для различных уровней приоритета.
- Планирование, т.е. должна быть обеспечена возможность осуществлять приоритетную передачу пакетов, основанную на классификации или политике качества обслуживания, при помощи нескольких очередей.
- Резервирование основных узлов, к которым может относиться: блок питания, блок вентиляторов, процессорный модуль.
- Предоставлять возможность углубленного анализа потоков сетевого и транспортного уровней при помощи протокола IPFIX (RFC 3917), Netflow, J-Flow или другого протокола предоставления агрегированной статистики по ip-потокам.

В ЦОД I и II уровня помимо обеспечения резервирования основных узлов оборудования магистрального уровня, рекомендуется обеспечить такое же резервирование для оборудования уровня распределения.

Во всем активном сетевом оборудовании должны быть средства мониторинга политики качества обслуживания и безопасности, планирования сети и сервисов:

- Должна быть обеспечена возможность сбора статистики с точностью до порта сети для анализа производительности и выявления узких мест сети.
- Должна быть обеспечена возможность перенаправлять трафик отдельных портов, групп портов и виртуальных портов на анализатор протоколов для детального анализа.
- Должна быть обеспечена возможность расширенного мониторинга событий в реальном времени для расширения возможностей диагностики, помимо внешних анализаторов. Должна быть обеспечена возможность сбора и сохранения информации о существенных сетевых событиях, включая изменения конфигураций устройств, изменения топологии, программные и аппаратные ошибки по технологии syslog.
- Должна быть обеспечена возможность доступа к интерфейсу управления устройством и отчетам через стандартный WEB–браузер с использованием протокола HTTPS.
- Должна быть возможность подключения к устройству для его настройки с использованием протокола ssh.

- Должна быть обеспечена возможность автоматической конфигурации Fast/Gigabit Ethernet портов, виртуальных сетей, транков VLAN.
- Должна быть обеспечена возможность автоматического распознавания топологии сети посредством агентов распознавания топологии.
- В целях обеспечения производительности локальной сети, ее масштабируемости, удовлетворения требованиям информационной безопасности и обеспечения качества обслуживания мультисервисного трафика, запрещается использовать концентраторы (hub). Вместо них должны использовать только коммутаторы (switch).

Все активное оборудование должно иметь конструктивное 19” стоечное исполнение.

5.3.2. Требования к внешним каналам связи

Данный раздел рассматривает технические требования к внешним каналам связи**,** которые предоставляются сторонними операторами связи.

5.3.2.1. Общие положения

В целях унификации необходимо выделить следующие используемые виды каналов связи:

- Телефонные цифровые потоки E1 PRI.
- Выделенные каналы передачи данных.
- Арендуемые каналы сети передачи данных.

При выборе вида канала связи преимущество необходимо отдавать каналам связи, которые подключаются к сети MPLS оператора, т.к. только сети MPLS в настоящее время эффективно обеспечивают QoS для мультисервисного трафика при приемлемой стоимости услуги. Рекомендуемый интерфейс подключения – Ethernet, точка-точка.

Каналы связи для соединений точка–точка или точка–многоточка между ЦОД I и II уровней должны организовываться посредством технологии MPLS или иной технологии, обеспечивающей выполнение необходимых требований по пропускной способности канала и качеству предоставления услуги, которую поддерживает оператор связи. При этом должен быть заключен договор, который предусматривает обеспечение QoS для аудио- и видеоданных, если таковые имеются. Требования должны быть указаны в соответствующем SLA.

С целью резервирования коммуникаций для ЦОД I уровня обязательно, а для ЦОД II уровня желательно наличие подключения к двум независимым операторам. Способ подключения описан в главе 4.3.1.2 «Требования к архитектуре сети».

При подключении ЦОД I и II уровней оператор связи должен обеспечить круглосуточную службу технической поддержки, которая в любое время суток не только принимает заявки, но и устраняет инциденты.

5.3.2.2. Цифровые проводные каналы связи

Качество цифровых каналов связи и телематических служб должно соответствовать требованиям, утвержденным в Российской Федерации и содержащимся в следующих документах:

- Приказ Минсвязи России от 10.08.96 №92 «Нормы на электрические параметры цифровых каналов и трактов магистральных и внутризоновых первичных сетей».
- РД 45.128–2000 «Сети и службы передачи данных».
- РД 45.129–2000 «Телематические службы».

5.4 Прикладное программное обеспечение (ПО)

Прикладное программное обеспечение (прикладное ПО) является одной из основных компонент современной ИТ-инфраструктуры. С точки зрения конечного пользователя, именно прикладное ПО помогает решать те или иные деловые задачи.

В рамках данного документа мы будем рассматривать следующие основные характеристики прикладного ПО:

- Функциональность – способность ПО максимально эффективно выполнять заявленные функции, с требуемыми характеристиками; Функциональная полнота – полный набор функций, которые способно выполнять данное ПО;
- Платформонезависимость – способность ПО функционировать в разных программно-аппаратных средах, под управлением разных ОС; Производительность – способность ПО обеспечивать сбор, обработку и хранение
- определенных объемов информации при заданной конфигурации аппаратной платформы конкретной архитектуры.
- Масштабируемость – способность ПО корректно работать на малых и на больших системах с производительностью, которая в целом последовательно увеличивается в соответствии с увеличением вычислительной мощности системы (количества процессоров и их ядре, размера доступной оперативной памяти, быстродействия дисковых массивов, количества серверов и т.д.), используемых для эксплуатации данного ПО;
- Способность к интеграции – способность ПО к интеграции и взаимодействию с другими
- системами, в том числе с унаследованным ПО и с системами сторонних производителей, и эксплуатируемыми на других платформах;
- Зрелость – наличие истории развития данного ПО (присутствие данного ПО на рынке в течение определенного промежутка времени, регулярный выпуск производителем новых версий, релизов и обновлений) и объявленных производителем планов по его развитию. Наличие «экосистемы» - количество организаций, эксплуатирующих ПО, количество разработчиков и специалистов, умеющих внедрять и разворачивать ПО, доступность обучения (учебные центры, обучающая литература и т.п.);
- Надежность и отказоустойчивость – способность ПО и систем, построенных на его базе, к бесперебойной, непрерывной работе, а в случае возникновения программно-аппаратных сбоев - способность к быстрому восстановлению работоспособности системы.

Общая стоимость владения (ТСО) ПО – складывается из затрат на начальное приобретение аппаратной составляющей и приобретение (разработку) ПО, ввод его в эксплуатацию и расходов на его эксплуатацию и сопровождение в течение нормативного срока жизни данного программно-аппаратного комплекса. Общая стоимость владения включает затраты: на обновление ПО и оборудования; на обучение, обслуживание, администрирование и техническую поддержку.

С точки зрения процессов разработки, поставки и сопровождения всю совокупность прикладного ПО можно разделить на две группы:

- Универсальное (тиражируемое) ПО – ПО, доступное на рынке и служащее для решения универсальных задач.
- Заказное ПО – ПО, разработанное по заказу ИТ-подразделением или сторонней организацией.

При наличии на рынке ПО с открытым кодом с функциональностью, надежностью и удобством использования сопоставимыми или превосходящими по аналогичным показателям ПО с закрытым кодом предпочтение в использовании должно отдаваться ПО с открытым кодом.

5.4.1 Общие требования к прикладному ПО

При выборе и внедрении нового прикладного ПО должны соблюдаться следующие требования:

- Все используемое прикладное ПО должно быть унифицировано и каталогизировано в рамках КРК в виде списка ПО, допустимого к использованию;

- ПО клиентских ПК должно быть функционально полным и обеспечивать выполнение как стандартных деловых процессов, так и специфических деловых задач данного пользователя;
- ПО должно быть зрелым: производитель (поставщик) должен гарантировать поддержку, сопровождение данного ПО в течение всего нормативного срока жизни данного ПО;
- Рекомендуется использовать платформонезависимое ПО, обеспечивающее свободу выбора программно-аппаратных средств для его эксплуатации и, в конечном счете, снижение общей стоимости владения системой;
- Рекомендуется использовать производительное, масштабируемое ПО, обеспечивающее гарантии непрерывности деловых процессов при росте объемов обрабатываемой и хранимой информации. Желательно, чтобы производитель ПО регулярно проводил объемное и нагрузочное тестирование своего ПО и предоставлял данные о результатах данного тестирования;
- Рекомендуется использовать только ПО, обладающее способностью к интеграции с другими системами, и обладающее открытой архитектурой. При выборе ПО необходимо учитывать возможности его интеграции в существующую ИТ инфраструктуру предприятия;
- При выборе ПО преимущества должны получать системы с подтвержденным положительным опытом использования в государственных учреждениях;
- Для обеспечения критических деловых процессов и услуг рекомендуется использовать отказоустойчивое ПО;
- Общая стоимость владения ПО, рассчитанная на весь нормативный срок эксплуатации данного ПО, должна служить важнейшим критерием при выборе того или иного поставщика и ПО;
- ПО, предназначенное для обеспечения защиты информации, должно иметь сертификаты соответствия требованиям по безопасности информации;
- ПО должно быть надлежащим образом документировано. Минимальные требования к документации – наличие документов «Руководства пользователя» и «Руководство администратора».

5.4.2. Общие требования к универсальному прикладному ПО

При закупке нового универсального прикладного ПО должны соблюдаться следующие требования:

- Рекомендуется закупать ПО в рамках специальных моделей лицензирования, обеспечивающих снижение стоимости закупки;
- При использовании лицензируемого ПО на него должны быть обязательно получены и надлежащим образом зарегистрированы соответствующие лицензии; Рекомендовано к использованию ПО производителей, зарекомендовавших себя на рынке в данной области. Желательно, чтобы данный производитель присутствовал на рынке с данным или аналогичным ПО не менее трех лет. Не рекомендуется использование устаревших версий ПО, а также слишком новых, «незрелых» версий ПО;
- Должно быть запрещено к использованию ПО, не имеющее как лицензий, так и поддержки (сопровождения) со стороны производителя;
- При выборе универсального ПО необходимо руководствоваться общим требованиями к прикладному ПО, а также рекомендациями главы 2 «Современные тенденции в области ИТ» данного документа.

5.4.3 Общие требования к заказному прикладному ПО

При разработке нового прикладного ПО должны соблюдаться следующие требования:

- Процесс проектирования, разработки и внедрения заказного ПО должен соответствовать требованиям раздела 5.9. «Требования к созданию и вводу в действие систем. Требования к документации» настоящего документа.
- необходимости технико-экономического обоснования разработки и внедрения данного ПО. Заказчик ПО должен представить технико-экономического обоснования разработки и внедрения данного ПО, с учетом требований и принципов минимизации ТСО для данного решения.
- При выборе разработчика ПО основное внимание должно уделяться опыту предыдущей работы данного разработчика по созданию (проектированию, реализации и внедрению) подобных систем. Желательно требование реализации не менее трех аналогичных по функционалу и функциональной полноте проектов в течение последних двух лет.
- При выборе разработчика ПО необходимо сформулировать требования к применяемым системам управления качеством.
- Рекомендуется включать в процедуры приемки ПО передачу разработчиком исходных текстов программ и других объектов, необходимых для создания ПО. Процедура приемки должна обязательно включать в себя контрольную компиляцию переданных исходных текстов, с созданием полностью работоспособной версии ПО, и выполнение контрольного примера на данной версии; В договоре на разработку ПО необходимо отражать распределение авторских и смежных прав на конечный продукт, а также ограничения на его дальнейшее использование сторонами.

5.5. Требования к инфраструктуре центров обработки данных

5.5.1. Требования к системам обработки и хранения данных

Данный раздел рассматривает технические требования к системам хранения и резервного копирования данных.

Конкретные минимальные технические требования изложены в приложении – «6.3.1 Минимальные требования к системам обработки и хранения данных».

5.5.1.1. Общие требования

Общие требования к системам обработки, хранения и резервного копирования данных для всех ЦОД:

- Производительность.
  - Производительность оборудования должна складываться из производительности основных подсистем. Необходимо отслеживать нагрузку основных подсистем, выявлять узкие места и наращивать, по мере необходимости, производительность путем оптимизации конфигурации, установки дополнительных модулей либо замены текущих модулей на более производительные.
  - В рабочем режиме сервер должен иметь загрузку основных ресурсов не более чем на 75%, чтобы выдерживать пиковую нагрузку в случае необходимости.
- Виртуализация. Рекомендуется использовать оборудование, поддерживающие виртуализации как при обработке информации (поддержка виртуализации на аппаратном уровне используемых серверов), так и при хранении (виртуальные диски на системе хранения данных) и резервном копировании информации (виртуальные ленты, использование технологий D2D, либо D2D2T).
- Масштабируемость. Необходимо использовать оборудование, имеющего, в случае необходимости, возможность наращивания Готовность. Степень готовности оборудования должна обеспечиваться за счет:
  - уменьшения единичных точек отказа;

- технологии объединения нескольких серверов в кластер;
- использование систем высокой готовности от ведущих производителей.

5.5.1.2. Серверы

Выбор серверного оборудования должен зависеть от тех задач (приложений), которые они будут решать. Учитывая, что разброс задач огромен и, при возрастании количества пользователей и объемов данных, требования к вычислительным ресурсам резко повышаются, то рекомендуется:

- Выбирать серверы, позволяющие постепенно масштабировать ресурсы и увеличивать производительность.
- Использовать технологию виртуализации, которая позволяет разделять ресурсы высокопроизводительного сервера между приложениями, которые требуют не очень больших ресурсов для своей реализации, на аппаратном и программных уровнях.

Данных подход, который сочетает в себе установку масштабируемых серверов и технологию виртуализации, позволит уменьшить ТСО и увеличить прозрачность и управляемость всей вычислительной инфраструктурой за счет динамического перераспределения ресурсов.

Серверы должны обеспечивать:

- Высокую скорость обработки данных при сниженных затратах на обслуживание; Простоту управления для быстрого изменения и перераспределения ресурсов в зависимости от потребностей; Высокую надежность и непрерывность обработки и доступа к информации;
- Интеграцию их в существующую инфраструктуру и совместную работу с уже использующимися системами обработки данных; Быть энергоэффективными.

При выборе серверов рекомендуется отдавать предпочтение платформам, поддерживающим многоядерные конфигурации.

Высокопроизводительные серверные платформы должны иметь ряд встроенных систем высокой доступности, таких как: резервные вентиляторы и блоки питания горячей замены; диски и адаптеры I/O горячего подключения; динамическая очистка и перераспределение страниц памяти; динамическое перераспределение процессоров и способность к восстановлению; интегрированная служба оповещения о событиях, работающая в режиме реального времени; встроенная расширенная система обнаружения неисправностей с выделенным сервисным процессором и шиной; наличие удаленной консоли.

Во всех серверных решениях должно быть уделено большое внимание предотвращению возможных сбоев. Для ЦОД I и II уровней должны быть реализованы соответствующие функции, при помощи которых осуществляется непрерывный контроль состояния всех компонентов сервера и анализ тенденций изменения контролируемых показателей. При обнаружении какой-либо потенциальной проблемы, например, возможного перегрева процессора, специальные функции динамического перераспределения ресурсов должны обеспечить перенос процессов с потенциально–сбойного компонента на исправный без прерывания выполнения приложений. При этом администратор системы и/или служба технической поддержки должны получить уведомление и подробный отчет о происшедшем событии.

ПО, реализующее технологию виртуализации серверов, должно давать возможность быстро и просто разделять вычислительные ресурсы в зависимости от требований приложений, а также уменьшать общее число серверов, позволяя нескольким виртуальным серверам размещаться на одном физическом, рационально используя его вычислительные ресурсы и память.

ПО, реализующее технологию виртуализации серверов, должно реализовывать следующую функциональность:

- Функция декомпозиции:
  - компьютерные ресурсы должны рассматриваться как единый однородный пул, распределяемый между виртуальными машинами;

- множество приложений и ОС должны сосуществовать на одной физической компьютерной системе;

- Функция изоляции:
  - виртуальные машины должны быть полностью изолированы друг от друга. Аварийный отказ одной из них не должен оказывать никакого влияния на остальные;
  - данные не должны передаваться между виртуальными машинами и приложениями, за исключением случая использования общих сетевых соединений со стандартной конфигурацией;
- Совместимость:
  - Совместимость должна гарантироваться посредством представления виртуальной аппаратуры приложениям и ОС как стандартной.

В ЦОД I уровня обязательно, а в ЦОД II уровня рекомендуется использовать дисковый массив для хранения основных прикладных данных и функцию хранения данных передавать сети хранения данных (SAN) с последующей виртуализацией SAN. Встроенные диски серверов использовать только для системных целей, используя технологию избыточности RAID.

Если для ЦОД II уровня не используются сети SAN, то должны быть использованы устройства NAS с функциональностью виртуализации.

Таким образом, для ЦОД I и II уровней должна быть внедрена технология виртуализации на всех уровнях ИТ-инфраструктуры:

- Локальная сеть – технология VLAN.
- Сервера – технология виртуализации серверов.
- Сети и системы хранения данных – технология виртуализации SAN или NAS.

ОС для обслуживания серверных приложений и промышленных систем должны:

- Быть высоконадежными и защищенными.
- Обеспечивать высокий уровень быстродействия приложений.
- Обладать встроенными возможностями для организации удаленного мониторинга всех основных сервисов ОС.

5.5.1.3. Сети и системы хранения данных

Главными приоритетами в развитии систем хранения данных должны быть:

- наращивание емкости систем хранения данных; концентрирование систем хранения данных в едином месте, причем количество территориально-удаленных мест должно быть ограничено; расширение возможностей восстановления после аварий; уменьшение времени восстановления;
- уменьшение окон резервного копирования (интервалов времени, отведенных для подготовки резервной копии) для критически важных приложений.

Должны быть выделены следующие уровни системы хранения данных:

- Сверхоперативный уровень; Оперативный уровень; Уровень долгосрочного хранения данных; Электронный архив;
- Резервного копирования данных.

Сверхоперативный уровень – данные этого уровня используются высоконагруженными СУБД, сервисами. Оборудование должно иметь максимальное быстродействие, поддерживать большой объем кэш-памяти, использовать твердотельные накопители с максимальным быстродействием: AllFlash системы хранения с подключением по протоколу iSCSI .

Оперативный уровень – данные с этого уровня достаточно часто используются пользователями. Соответственно оборудование должно быть достаточно быстродействующим и иметь высокую степень доступности. Рекомендуется использовать быстрые диски SCSI со скоростью вращения 15k или 10k.

Уровень долгосрочного хранения данных – постоянное место хранения данных, которое помимо производительности должно обладать надежностью. Рекомендуется использовать диски SAS/SATA.

Электронный архив – хранилище данных, которое обеспечивает физическую сохранность данных вне зависимости от действий пользователей. Данные, помещенные в электронный архив, нельзя стереть или изменить. При изменении данных в электронном архиве должна храниться как исходная копия, так и все ее модификации. Электронных архив должен создаваться на неперезаписываемых оптических носителях информации. Данное устройство должно иметь интерфейс iSCSI и подсоединяться к сети SAN.

Резервное копирование данных - объемное хранилище данных для возможности быстрого и недорогого восстановления информации (документов, программ, настроек и т. д.) в случае утери рабочей копии информации по какой-либо причине. Основное требование к системе резервного копирования - надежность хранения информации. Она обеспечивается применением отказоустойчивого оборудования систем хранения, дублированием информации и заменой утерянной копии другой в случае уничтожения одной из копий (в том числе как часть отказоустойчивости).

Рекомендуется внедрить ПО для управления жизненным циклом информации (ILM), которое, согласно настроенным правилам, должно автоматически перемещать данные между разными уровнями хранения в зависимости от их востребованности.

Кроме этого, ПО управления контентом должно перемещать данные в единую систему хранения по заранее настроенным правилам, в зависимости от критичности деловой информации, непосредственно с рабочих ПК пользователей.

Система хранения данных должна иметь:

единые средства для репликации данных, которые должны перемещать данные между уровнями систем хранения данных, приводя в соответствие ценность данных и этап их жизненного цикла с показателями доступности, производительности, безопасности и стоимости уровня хранения; масштабируемую виртуализацию, позволяющую управлять ресурсами многоуровневой

системы хранения данных как одним пулом, который необходимо разделять между пользователями и обслуживать как единое целое.

СХД должна иметь способность управлять логическими разделами внешней памяти. Логические разделы должны распределять ресурсы одного физического устройства хранения данных на несколько виртуальных устройств, каждое из которых должно независимо настраиваться для отдельных приложений и/или групп пользователей. Эта стратегия эффективно работает при хранении значительных объемов разнотипных данных, поэтому логические разделы должны стать частью многоуровневой инфраструктуры хранения данных.

Система управления СХД должна быть интегрирована в саму СХД, без использования дополнительного серверного оборудования.

В настоящее время существуют следующие концепции хранения данных:

- концепция NAS представляет собой сетевую архитектуру, оптимизированную для обеспечения сетевого файлового сервиса. NAS используется для хранения информации на файловом уровне и обычно поддерживают доступ к файлам по протоколам NFS, CIFS/SMB, FTP, HTTP;
- концепция SAN, ориентированная на хранение информации на блочном уровне. SAN может использовать в качестве среды передачи данных как технологию FibreChannel, так и технологию Ethernet с использованием протокола iSCSI.

Все эти решения объединяет одна характеристика – попытка снизить TCO системы хранения, внедряя эффективное управление централизованной информацией, изолированно располагающимися в гетерогенной среде, включающей различные ОС, форматы данных и пользовательские интерфейсы.

В ЦОД I уровня должна быть внедрена технология SAN, как удовлетворяющая всем необходимым требованиям. Для ЦОД II уровня также рекомендуется технология SAN, но допускается возможность развертывания устройств NAS для организации файловых сервисов. При этом должна быть стратегически выбрана одна технология или продуман и обоснован подход одновременного использования и SAN и NAS без взаимных конфликтов, обеспечивающий виртуализацию для серверных систем и общее управление единым пулом СХД.

Целью внедрения и использования технологии SAN должно стать обеспечение реальной консолидации ресурсов хранения и их совместного использования, т.к. емкость хранения должна подключаться ко многим серверам, в том числе и удаленным, а машины, обрабатывающие данные, должны освобождаться от задач управления ресурсами и их хранения.

При внедрении технологии SAN должно быть обеспечено:

- независимость топологии SAN от storage–систем и серверов; удобное централизованное управление;
- удобное резервирование данных без перегрузки локальной сети и серверов; высокое быстродействие; высокая масштабируемость; высокая гибкость; высокая готовность.

При выборе и внедрении конкретного оборудования и ПО для реализации SAN необходимо соблюдать следующее требование: система хранения данных должна поддерживать уровни логической абстракции (виртуализации) между физическими портами на данном дисковом массиве, блоками данных на конкретных дисковых группах и логическими томами или файлами, к которым серверы или приложения должны иметь доступ.

В частности, должны быть реализованы следующие сервисы виртуализации:

Виртуализация подключения к SAN. К дисковому массиву через SAN должны получать доступ несколько серверов и распределение физических портов массива между ними не должно являться управленческой проблемой и не должно стать препятствием для полного использования возможностей СХД.

Виртуализация логических дисков и томов:

- Любая модификация приложения (например, добавление новых серверов, устройств хранения данных или функций) требует выполнения сложного комплекса
- действий по изменению настроек, как на серверах, так и на дисковых массивах. Эти действия не должны быть причиной ошибок и простоев, и не должны увеличивать время, необходимое на развертывание и модификацию приложения.
- СХД должна обеспечивать надежные сервисы управления логическими дисками и томами для распространения расширенных сервисов управления информацией и хранением данных на модульные системы хранения данных, поддерживающие различные типы дисков.
- Необходимо иметь соответствующее аппаратное обеспечение с производительностью, достаточной для значительного повышения масштабируемости и гибкости решений по виртуализации без ущерба для
- доступности данных или без увеличения расходов на управление системой хранения данными.

При построении SAN в ЦОД I уровня на коммутаторах рекомендуется создавать две независимые Fabric (Dual fabric). Dual fabric позволяет избежать единой точки отказа в SAN, обеспечивая высокий уровень надежности и отказоустойчивости. Кроме того, изменения конфигурации, регламентные работы (например, установка нового firmware) на коммутаторах одной из Fabric не сказываются на работе другой. Применение Dual fabric совместно с ПО, реализующим поддержку альтернативных путей доступа и распределение нагрузки, для соединения серверов и устройств хранения (пути должны быть распределены между разными Fabric) позволяет создать надежную SAN. Также необходимо

предусматривать наличие на серверах ПО Dynamic multipathing для обеспечения непрерывной работы приложений с двумя фабриками.

Рекомендуется выбирать оборудование, поддерживающее Fibre Channel iSCSI с пропускной способностью не менее 10 Гбит/с. В случае необходимости обеспечения более высокой скорости передачи данных по магистральным каналам необходимо использование транкинга (trunking) - объединения нескольких каналов передачи данных в один канал.

5.5.1.4. Обеспечение высокой доступности приложений

В тех случаях, когда требуется обеспечить высокую надежность и доступность приложений и ИС для пользователей, необходимо использовать технологии кластеризации приложений. В зависимости от требуемой величины надежности и доступности системы, которую необходимо обеспечить, целесообразно применять либо кластеры, работающие в режиме активный/резервный (high-availability clusters), либо параллельные кластеры (parallel clusters), обеспечивающие более высокий уровень доступности. При выборе прикладного ПО необходимо учитывать возможности систем по работе в кластерных конфигурациях.

5.5.1.5. Резервное копирование данных

Резервное копирование данных ИС для всех ЦОД должно осуществляться в соответствии с «Политикой резервного копирования», которая должна содержать общее описание процессов резервного копирования. Дополнения к «Политике резервного копирования» содержат процессы резервного копирования для различных ИС и регламенты их выполнения.

5.5.1.6. Обеспечение катастрофоустойчивости

Катастрофоустойчивость – способность компьютерного комплекса, состоящего из нескольких систем, сохранить критически важные данные и продолжить выполнять свои функции после массового (возможно, целенаправленного) уничтожения его компонентов в результате различных катаклизмов как природного характера, так и инспирированных человеком.

Катастрофоустойчивость предполагает в первую очередь обеспечение сохранности данных, а также возможность восстановления работы после крупной локальной аварии или глобального катаклизма, причем теми же средствами обеспечивается и должная степень надежности всех или критически важных подсистем. Поскольку компоненты распределены, то в случае массовых отказов на одной площадке основную работу можно перенести на другую площадку.

Сохранение данных можно обеспечить как средствами СХД (синхронное/асинхронное зеркалирование данных на резервный ЦОД), так и средствами приложений. Например, при работе с СУБД настраивается пересылка в удаленный ЦОД журналов изменений, которые ведут большинство СУБД. Резервный центр при этом не обслуживает пользователей, однако обязан иметь комплект оборудования и ПО для поддержки соответствующей базы данных нужного объема, способный успевать вносить в нее изменения по мере поступления журналов из основного центра.

Также для обеспечения катастрофоустойчивости критических систем в резервном ЦОДе необходимо иметь вычислительные мощности не ниже используемых на резервируемом ЦОДе.

5.5.2. Требования к помещениям и инженерным системам

Данный раздел рассматривает требования к помещениям, в которых располагается серверное и сетевое оборудование, а также к инженерным системам, которые поддерживают данные помещения.

Конкретные минимальные технические требования изложены в приложении – «6.3.3 Минимальные требования к помещениям и инженерным системам».

5.5.2.1. Общие требования к помещениям

Серверные помещения всех ЦОД должны удовлетворять следующим общим требованиям:

- Запрещается размещать серверные помещения в помещениях, оснащенных большим количеством инженерных сооружений, которые представляют потенциальную опасность для оборудования.
- Запрещается размещать серверные помещения под помещениями столовой, туалетов и других помещений, связанных с потреблением воды.
- Во избежание протечек воды с крыши запрещается размещать серверные помещения на последнем этаже здания.
- Серверная комната должна представлять собой помещение с ограниченным доступом, предназначенное для размещения серверного оборудования.
- Конструкция серверной комнаты должна соответствовать следующим требованиям:
  - Поддерживать требуемую непрерывность рабочих процессов.
  - Поддерживать требуемый вес оборудования серверной комнаты.
  - Защищать ценное оборудование и данные.
- Физический доступ к серверной комнате должны иметь только уполномоченные сотрудники ИТ-подразделений и обслуживающих организаций.
- Для ограничения физического доступа к серверной комнате должны использоваться автоматизированные системы контроля доступа.
- В зависимости от уровня ЦОД, серверная комната должна быть оснащена:
  - источником бесперебойного питания;
  - системой кондиционирования;
  - дизель – генератором;
  - системой регулирования чистоты и влажности воздуха;
  - серверными и телекоммуникационными шкафами, стойками. Рекомендуемая высота шкафа 42U;
  - системами контроля состояния внутренней среды:
    - системой раннего дымообнаружения;
    - датчиками доступа;
    - датчиками физического состояния оборудования. Разрешается использовать встроенные в оборудование датчики физического состояния;
    - датчиками температуры/влажности;
  - системой видеонаблюдения.

Обязательным требованием к серверному помещению является наличие фальшпола, выдерживающего нагрузку от устанавливаемого оборудования и работающих с ним людей. При необходимости под фальшполом располагаются кабели электроснабжения и слаботочная инфраструктура. Рекомендуется фальшпол из МДФ– плиток на металлической основе с ламинированным покрытием или съемный фальшпол с покрытием «керамогранит» размером 600 х 600 мм. Высота над уровнем пола – от 100 до 800 мм, для серверных помещений наиболее оптимально 350 – 500 мм. Для распределения потоков холодного воздуха от системы кондиционирования рекомендуется использовать перфорированные панели.

Рекомендуется при расчете площади помещений исходить из расчета 2 кв. м на один 19– дюймовый шкаф, если иного не предусмотрено техническим проектом или рабочей документацией.

5.5.2.2. Структурированные кабельные системы

Структурированная кабельная система (СКС) — физическая основа информационной инфраструктуры предприятия, позволяющая свести в единую систему множество информационных сервисов разного назначения.

СКС представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы. Она состоит из набора медных и оптических кабелей, кросс-панелей, соединительных шнуров, кабельных разъемов, модульных гнезд, информационных розеток и вспомогательного оборудования. Все перечисленные элементы интегрируются в единую систему и эксплуатируются согласно определенным правилам.

Кабельная система — это система, элементами которой являются кабели и компоненты, которые связаны с кабелем. К кабельным компонентам относится все пассивное коммутационное оборудование, служащее для соединения или физического окончания (терминирования) кабеля — телекоммуникационные розетки на рабочих местах, кроссовые и коммутационные панели в телекоммуникационных помещениях, муфты и сплайсы.

Общие требования к СКС следующие:

- СКС должна быть спроектирована с избыточностью по количеству подключений.
- Рабочее место должно иметь, как минимум, один разъем для подключения к ЛВС и один разъем для подключения к телефонной сети.
- Максимальное расстояние горизонтальной проводки не должно превышать 90м.
- СКС должна соответствовать ГОСТ Р 53246-2008 и ГОСТ Р 53245-2008, которые определяют общие требования к основным узлам СКС и методику испытания, соответственно.
- Кабельные компоненты должны быть не менее категории 5е для подключения АРМ, либо оборудования на коммутаторы уровня доступа и не менее категории 6 либо оптических подключений для подключения коммутаторов уровня доступа к коммутаторам уровня распределения и далее.
- Во всех типах ЦОД также должны использоваться кабельные компоненты не менее категории 6.
- Прокладку кабелей в коридорах должна осуществляться за фальшпотолком, если таковой имеется, а при его отсутствии - в специализированных кабель-каналах (коробах) или в существующих закладных;
- в рабочих помещениях подвод кабеля к рабочим местам производится в кабель-каналах.
- СКС должна быть документирована.
- На СКС должна предоставляться гарантия производителя на работоспособность на срок не менее 25 лет. Подрядчик должен быть сертифицирован производителем и иметь проверенное измерительное оборудование. При проведении приемочных испытаний подрядчик должен предоставить протоколы тестирования СКС на соответствие установленным нормам.

5.5.2.3. Электроснабжение

Общие требования к системе электроснабжения всех ЦОД следующие:

- В серверное помещение электропитание должно подаваться от главного щита здания, где бы данное помещение не находилось. Также от главной шины заземления здания проводится кабель заземления до контура заземления серверного помещения. Все провода должны иметь соответствующее сечение согласно техническому проекту и цвет, согласно нормативным документам.
- Питание ПК, периферийных устройств, офисной техники, серверов, систем хранения и активного сетевого оборудования должно быть отделено от питания промышленных установок. Питание должно осуществляться от отдельных поэтажных автоматов, а те, в свою очередь, отдельно должны подсоединяться к главному щиту здания через отдельную систему автоматов.

- При организации питания ПК, периферийных устройств и офисной техники рекомендуется после автоматов в поэтажных щитах устанавливать устройство защитного отключения согласно действующим нормам.
- Систему электроснабжения для ЦОД рекомендуется организовывать от двух территориально разнесенных трансформаторных подстанций. Кабельные линии должны идти независимыми маршрутами. Рекомендуется использовать автоматы выбора резерва (АВР), осуществляющие выбор и переключение между основными и резервными линиями.
- Для ЦОД I уровня необходимо, а для ЦОД II уровня рекомендуется использовать дизель–генераторные электростанции (ДЭС). В схеме электроснабжения они должны располагаться параллельно вводам кабелей электропитания в здание. Для правильной работы ДЭС и двух независимых вводов должен быть предусмотрено устройство автоматического включения резервного питания. В случае полного пропадания электропитания, либо несоответствия его требуемым параметрам (напряжение, частота, «чистота») должен осуществляться автоматический запуск ДЭС, и нагрузка переводится на нее. ДЭС должна иметь запас топлива, рассчитанный не менее чем на 8 часов непрерывной работы и возможность пополнения топливом без остановки генератора. ДЭС должны иметь возможность непрерывной работы до 3 месяцев при условии налаженной поставки топлива.
- Для ЦОД I и II уровней после ввода кабелей электропитания в здание или после ДЭС, при ее наличии, должны быть установлены централизованные ИБП двойного преобразования.

Требования к электроснабжению шкафов для ЦОД всех уровней:

- К каждому шкафу должно быть подведено питающее напряжение 220 В переменного тока от двух независимых источников через индивидуальные автоматические выключатели. Подключение оборудования, имеющего два блока питания, осуществлять к двум независимым источникам. Подключение оборудования, имеющего один блок питания, осуществлять к одному из источников питания, равномерно распределяя нагрузку в соответствии с энергопотреблением, указанным в паспорте оборудования.
- Потребляемая мощность должна быть рассчитана в техническом проекте. Если устанавливаются пустые шкафы и на размещение оборудования в них еще нет проекта, то рекомендуется оценивать энергопотребление в среднем 7 кВт на шкаф. Если в шкафах предполагается устанавливать blade-серверы или иное оборудование, имеющее повышенное энергопотребление, то потребляемая мощность должна быть не менее 15 кВт на шкаф.

5.5.2.4. Кондиционирование и система холодоснабжения

Требования к системам кондиционирования и холодоснабжения для всех ЦОД:

- Серверные помещения должны быть оборудованы промышленной прецизионной системой кондиционирования и вентиляции (системы холодоснабжения) согласно СП 60.13330.2016. В задачи системы холодоснабжения должно входить поддержание внутри помещения рабочей температуры в пределах от 19 до 24 °С и влажности от 40 до 80%. Резервирование системы холодоснабжения ЦОД I уровня обязательно, а для ЦОД II уровня рекомендуется осуществлять по схеме с N+1 (с одним запасным кондиционером). Все кондиционеры должны быть подключены к единой системе управления. Программное обеспечение должно позволять осуществлять ротацию запасного кондиционера, что позволяет более эффективно расходовать ресурс системы холодоснабжения в целом.
- Для ЦОД I уровня необходимо, а для ЦОД II уровня рекомендуется организовывать приток свежего воздуха. Приток рекомендуется осуществлять через специальную установку, подготавливающую уличный воздух. Кроме того, она должна создавать внутри помещения дополнительное давление, что препятствует проникновению внутрь пыли.
- Для увлажнения воздуха в ЦОД I и II уровней рекомендуется использовать парогенераторы. Сухой воздух малоэффективен для охлаждения системой хладоснабжения в силу физических принципов кондиционирования. При понижении влажности

электростатический потенциал увеличивается, что может быть причиной вывода оборудования из строя.

- Рекомендуется вывод горячего воздуха из шкафов в воздуховод и его транспортировку к кондиционеру, либо рассмотреть возможность организации холодных и горячих коридоров, либо предусмотреть использование кондиционеров, размещаемых между стоек.
- При использовании системы кондиционирования с воздуховодами и забором горячего воздуха сверху шкафа необходимо наличие системы принудительной вентиляции в верхней части шкафа.
- При использовании системы кондиционирования без воздуховодов необходимо использовать стойки с перфорированными передними и задними дверьми для лучшего охлаждения от системы кондиционирования.

5.5.2.5. Системы раннего обнаружения пожара и пожаротушения

Требования к системе раннего обнаружения пожара и газового пожаротушения для всех ЦОД:

- ЦОД должны быть оборудованы системой автоматического пожаротушения (ГОСТ 12.1.004–91.ССБТ). Система пожаротушения не должна наносить вред оборудованию. Система газового пожаротушения должна сработать в зачаточной фазе развития пожара, т. е. когда происходит тление нагревающихся элементов или начальное воспламенение, и за время менее одной минуты потушить очаги возгорания.
- Комплекс предупреждения о пожаре и пожаротушения должен сообщить о потенциальной возможности возгорания намного раньше, чем придется задействовать систему тушения. Это должно быть достигнуто установкой большого количества высокочувствительных дымовых, оптических, химических, спектральных и прочих пожарных извещателей, увязанных в единую интеллектуальную систему оповещения о пожаре и пожаротушения, а также комплексом организационных мероприятий. В него должен входить постоянный визуальный осмотр оборудования, соблюдение пожарных норм и правил, а также правил эксплуатации электроустановок.
- Рекомендуется использовать огнетушащие смеси на основе хладонов либо инертных газов, т.к. они наносят наименьший ущерб оборудованию.
- Требуется предусмотреть систему удаления газа из помещения после срабатывания системы пожаротушения.
- При срабатывании системы газового пожаротушения должны отключаться все системы, нагнетающие воздух в помещение ЦОД.

5.5.2.6. Комплексные системы безопасности

Комплексные системы безопасности должны состоять из:

- системы видеонаблюдения;
- системы разграничения физического доступа;

Требования к системе видеонаблюдения:

- Система видеонаблюдения должна собирать и передавать видеоинформацию в режиме реального времени; Система видеонаблюдения должна записывать и воспроизводить цветное изображение;
- Все входы в аппаратный зал должны находиться под видеонаблюдением; Должен храниться как минимум недельный архив информации системы доступа в помещения для расследования возможных инцидентов.

Требования к системе разграничения физического доступа:

- Должна быть использована система разграничения доступа на основе бесконтактных ключей, которая состоит из сервера управления, системы контроллеров и считывателей, а также индивидуальных карт (ключей).

- Данные системы (архив информации) должны храниться минимум три месяца.

5.6. Требования к обеспечению информационной безопасности

Целью обеспечения информационной безопасности инфраструктуры электронного правительства является защита компонентов инфраструктуры электронного правительства от внутренних и внешних угроз информационной безопасности.

Принимаемые меры по обеспечению информационной безопасности информационных систем и компонент информационно-телекоммуникационной инфраструктуры электронного правительства должны соответствовать требованиям, установленными федеральными законами «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О безопасности критической информационной инфраструктуры Российской Федерации», принимаемыми в соответствии с ними нормативными правовыми актами, в том числе:

- требованиям к порядку реализации мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем, утвержденными постановлением Правительства Российской Федерации от 06.07.2015 № 676;
- требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17;
- требованиям к составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18.02.2013 № 21;
- требованиям к составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденными приказом ФСБ России от 10 июля 2014 года № 378
- требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25.12.2017 № 239;
- требованиям иных руководящих и методических документов ФСТЭК России и ФСБ России, государственных стандартов в области защиты информации.

Задачами обеспечения информационной безопасности инфраструктуры электронного правительства являются:

- предотвращение неправомерного доступа к информации, обрабатываемой в компонентах инфраструктуры электронного правительства, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
- недопущение информационного воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование компонентов инфраструктуры электронного правительства;
- обеспечение функционирования компонентов инфраструктуры электронного правительства в условиях воздействия угроз безопасности информации;
- обеспечение возможности восстановления функционирования компонентов инфраструктуры электронного правительства.

Основные направления обеспечения информационной безопасности инфраструктуры электронного правительства:

- разработка и внедрение политик информационной безопасности и иных организационно-распорядительных документов по обеспечению информационной безопасности инфраструктуры электронного правительства;
- проектирование систем защиты информации информационных систем инфраструктуры электронного правительства;
- реализация требований по обеспечению защиты информации при её обработке в информационных системах инфраструктуры электронного правительства;
- проведение мероприятий по аттестации объектов информатизации инфраструктуры электронного правительства по требованиям безопасности информации;
- организация обработки и хранения государственных информационных ресурсов органов исполнительной власти Чувашской Республики в центрах обработки данных в соответствии с требованиями информационной безопасности;
- внедрение и сопровождение программно-аппаратных средств и комплексов, предназначенных для защиты информации при её обработке в информационных системах органов исполнительной власти Чувашской Республики;
- внедрение в органах исполнительной власти Чувашской Республики сертифицированных средств защиты информации;
- контроль и анализ эффективности принятых мер защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в органах исполнительной власти Чувашской Республики;
- выявление и анализ компьютерных атак на компоненты инфраструктуры электронного правительства, реагирование на них и принятие мер по их предотвращению;
- проведение аудита информационной безопасности, выявление и анализ уязвимостей информационных систем и компонент информационно-телекоммуникационной инфраструктуры электронного правительства, принятие мер по их устранению;
- мониторинг, выявление и расследование инцидентов информационной безопасности, реагирование на них и принятие мер по их предотвращению;
- консультационная и информационная поддержка участников электронного правительства по вопросам обеспечения защиты информации, повышение осведомленности участников электронного правительства в области информационной безопасности;
- обучение и повышение квалификации специалистов, работающих в сфере информационных технологий и защиты информации.

5.7. Требования к обеспечению непрерывности предоставления услуг

5.7.1. План обеспечения непрерывности предоставления услуг и восстановления после аварии

Необходимо иметь план обеспечения непрерывности предоставления услуг и восстановления после аварии. Данный план должен включать в себя следующее пункты, которые необходимы для регламентации работ в области ИТ:

- Перечень внешних и внутренних угроз для деловых процессов органов государственной власти. К внешним угрозам необходимо отнести техногенные, природные, человеческие и прочие угрозы;
- План обеспечения бесперебойного функционирования организации в случае нештатной ситуации – детальный перечень мероприятий, которые должны быть выполнены до, вовремя и после чрезвычайного происшествия или бедствия. Этот план должен быть документирован и регулярно испытываться для того, чтобы убедиться, что в случае нештатной ситуации он обеспечит продолжение деятельности организации и наличие резерва критически важных ресурсов;
- План должен учитывать определенное целевое время восстановления данных (RTO), которое определяется с точки зрения требований непрерывности к деловым

процессам. В зависимости от RTO план должен ранжировать все ресурсы и задачи компании на 3 приоритета:

- Приоритет 1 – задания, которые должны выполняться в соответствии с установленным графиком.
- Приоритет 2 – задания, которые могут выполняться при наличии времени и ресурсов.
- Приоритет 3 – задания, которые не должны выполняться в случае бедствия. План должен содержать процедуры выполнения следующих функций:
- Ввод в действие процедур для чрезвычайных ситуаций. о Уведомление сотрудников, поставщиков и заказчиков. о Формирование группы (групп) восстановления.
- Оценка последствий бедствия.
- Переезд в альтернативное рабочее помещение (помещения).
- Восстановление функционирования критически важных приложений.
- Восстановление основного рабочего помещения.
- Информирование персонала компании о временных способах доступа к информационным ресурсам: телефония, передача данных, местонахождение общих информационных ресурсов компании.

- Резервному копированию подлежат все программы и данные (включая их настройки), обеспечивающие работоспособность системы и выполнение ею своих задач (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.
- Резервному копированию подлежат все настройки активного сетевого оборудования. Резервному копированию подлежит вся проектная документация (технический проект, рабочая документация, эксплуатационная документация).
- Все программные средства, используемые в системе должны иметь эталонные (дистрибутивные) копии. Их местонахождение и сведения о лицах, ответственных за их создание, хранение и использование должно быть указано явно в соответствующих документах. Там же должны быть указаны перечни наборов данных, подлежащих резервному копированию, периодичность копирования, место хранения и ответственные за создание, хранение и использование резервных копий данных.
- Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала.

5.8. Требования к системе управления и мониторинга

Данный раздел рассматривает требования к системе управления и мониторинга.

Конкретные минимальные технические требования изложены в приложении – «6.4 Приложение 4. Минимальные требования к системе управления и мониторинга».

5.8.1. Общие требования

Задачи системы управления и мониторинга:

- Повышение эффективности использования ИТ–инфраструктуры;
- Поддержание высокого уровня обслуживания прикладных систем; Превентивное решение потенциальных проблем;
- Сокращение потерь из–за простоев при восстановлении данных.

Система управления и мониторинга (СУМ) ИТ инфраструктуры ЦОД должна удовлетворять следующим общим требованиям:

- СУМ должна быть масштабируема в рамках ИТ структуры; СУМ должна обеспечивать мониторинг объектов управления различных типов и производителей в гетерогенной сети;

- СУМ должна обеспечивать возможность включения в контур мониторинга существующих и проектируемых объектов управления; Режим работы СУМ должен совпадать с режимом функционирования объектов управления.

5.8.2. Требования к структуре СУМ ЦОД I и II уровней

СУМ должна состоять из следующих основных подсистем:

- Подсистема мониторинга и управления распределенной сетью передачи данных и периферийного оборудования;
- Подсистема мониторинга и управления серверными комплексами, ОС и приложениями;
- Подсистема мониторинга и администрирования ПК;
- Подсистема мониторинга и администрирования оборудования и процессов резервного копирования.

5.8.3. Требования к функциональности СУМ ЦОД I и II уровней

СУМ должна обеспечивать выполнение следующих функций:

- Удаленный доступ к серверу управления через активные консоли; Поддержка параллельной работы нескольких операторов (со своими полномочиями и зоной ответственности) с сервером управления;
- Защита доступа к серверу управления по любым вариантам входа в систему со стороны неуполномоченных лиц; Разграничение на области компетенции по решению возникающих проблем;
- Различный уровень графического представления информации для различного эксплуатационного персонала, в зависимости от его роли в эксплуатационном процессе;
- Удаленный мониторинг объектов управления; Мониторинг контролируемых объектов при помощи агентов;
- Выбор параметров мониторинга и настройка порогов срабатывания агентов, для оценки текущего состояния систем; Централизованная регистрация событий, происходящих в контролируемых объектах СПД,
- ОС, СУБД, приложениях, информационных сервисах; Расширение списка регистрируемых событий и адаптация к используемым приложениям и существующим технологиям; Централизованная обработка всех регистрируемых событий;
- Оповещение операторов системы о работе информационных ресурсов посредством выдачи информационного сообщения на консоль оператора; Оповещать операторов системы о возникших проблемах посредством выдачи звукового сигнала; Анализ производительности работы объектов управления;
- Автоматическая обработка и графическое представление оперативной информации по состоянию информационных сервисов; Сбор, хранение и анализ параметров функционирования объектов управления.

5.8.4. Требования к управлению и мониторингу мультисервисной сети

Мониторинг IP–сетей, управления конфигурациями, сбоями, производительностью, а также методы и средства инвентаризации IP–сетей должны быть строго регламентированы и автоматизированы.

Соответствующая база данных для ЦОД I и II уровней должна содержать полную и достоверную информацию обо всех элементах сети в иерархическом виде с учетом географической иерархии с одной стороны и функциональной иерархии (приложения, IP–сети, базовые сети) с другой.

Функционально база данных может быть представлена как две взаимодействующие базы данных: инвентаризационная и системы управления событиями в сети.

Инвентаризационная база данных должна объединять информацию от различных источников и предоставлять ее в удобной форме. Рекомендованный набор информации для включения в инвентаризационную базу данных:

- О топологии сети и установленном оборудовании в управляемых сетях.
- Подробную информацию об используемых каналах связи (в случае арендованных каналов – информацию об организации, предоставившей канал, контактные данные специалистов и службы технической поддержки, способах связи).
- Полную спецификацию оборудования: текущую версию ПО, заводские и инвентаризационные номера, текущие и предыдущие файлы конфигурации, версию ПО, контактную информацию обслуживающей организации, место установки и ответственные лица.
- Для сетевого оборудования – подробное описание интерфейсов в табличном виде с указанием IP–адресов, VLAN, подключенных сетей или серверов приложений для LAN–интерфейсов, или используемых каналов связи (физических и виртуальных), протоколов маршрутизации и подключенного удаленного оборудования для WAN–интерфейсов.

Автоматизированная система обработки событий для ЦОД I и II уровней должна обеспечивать:

- Автоматизированный сбор в режиме реального времени и хранение информации о сбоях, неисправностях, превышении критических порогов и т.п. активного оборудования и каналов связи.
- Уведомление обслуживающего персонала о возникающих проблемах и передачу этой информации по иерархической структуре (административной, топологической, системной) в соответствии с установленными административными правилами.
- Отображение истории обработки события (кем, когда, какие действия были предприняты). Сохранение истории событий по каждому объекту управления.
- Привязку события к объекту, т.е. в инвентаризационной составляющей должна быть ссылка на историю событий объекта и наоборот.

Кроме этого, система обработки событий должна предоставлять аналитическую информацию в соответствии с заданными административными требованиями (например, выборку по объектам, на которых не были своевременно проведены профилактические работы, выборку по событиям, которые не были закрыты в течение месяца и т.п.)

5.9. Требования к созданию и вводу в действие систем. Требования к документации

Данный раздел описывает минимальные требования к созданию и вводу в действие ИС и элементов ИТ-инфраструктуры, а также требования к документации, которая сопровождает создание и ввод в действие и на основе которой осуществляется дальнейшее сопровождение ИС и ИТ- инфраструктуры.

Конкретные требования к документации с точки зрения удовлетворения действующим нормативным документам изложены в приложении – «7.5 Приложение 5. Минимальные требования к документации».

При создании и вводе в действие систем и элементов ИТ-инфраструктуры должны быть соблюдены следующие стадии:

1. Стадия создания «Технического задания».
2. Стадия создания «Технорабочего проекта» - для объектов ИТ- инфраструктуры.
3. Стадия создания «Программ и методик испытаний».
4. Стадия создания «Эксплуатационной документации».
5. Стадия поставки оборудования и ПО.
6. Стадия монтажа, пусконаладочных работ, предварительных (автономных и комплексных) испытаний.
7. Стадия опытной эксплуатации.
8. Стадии приемочных испытаний в промышленную эксплуатацию.

Окончательным вводом ИС в эксплуатацию считается утверждение ответственным органом исполнительной власти Чувашской Республики правового акта о вводе ИС в эксплуатацию, определяющего перечень мероприятий по обеспечению ввода системы в эксплуатацию и устанавливающего срок начала эксплуатации.

5.9.1. Требования к техническому заданию

Должно быть выделено два вида задания: задание на проектирование и техническое задание (ГОСТ 34.602–89).

Задание на проектирование – приложение к договору, в котором должны быть перечислены все документы, которые должны быть разработаны, в том числе техническое задание. Задание на проектирование может быть опущено, если к договору сразу прилагается техническое задание на создание системы.

Техническое задание (ТЗ) является основным документом, определяющим требования и порядок создания (развития или модернизации) ИС или элементов ИТ инфраструктуры, в соответствии с которым проводится их разработка и приемка при вводе в действие.

ТЗ должно быть составлено с учетом рекомендаций ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы».

Включаемые в ТЗ требования должны ясно и четко описывать функциональность будущей системы и соответствовать современному уровню развития технологий и не уступать аналогичным требованиям, предъявляемым к лучшим современным аналогам.

ТЗ должно обязательно содержать следующие разделы согласно ГОСТу, которые могут быть разделены на подразделы:

- общие сведения; назначение и цели создания (развития) системы;
- характеристика объектов автоматизации; требования к системе;
- состав и содержание работ по созданию системы;
- порядок контроля и приемки системы; требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие;
- требования к документированию;
- источники разработки.

5.9.2. Требования к технорабочему проекту

Данной стадии может предшествовать разработка Эскизного проекта, в котором должны быть описаны все основные технические решения и проведен их сравнительный анализ с другими возможными решениями.

Технорабочий проект должен состоять из технического проекта и рабочей документации.

Технический проект должен содержать как минимум следующие документы:

- Пояснительная записка.
- Схема связи или блок-схема.
- Спецификация оборудования.
- Сводный сметный расчет и Локальный сметный расчет.

Пояснительная записка должна содержать:

- Описание предлагаемого технического решения.
- Обоснование предлагаемого технического решения, сравнивая его с другими возможными решениями, а также проводя анализ современных технологий и подходов к решению поставленной задачи.

Рабочая документация должна содержать как минимум альбом на каждую площадку (серверное помещение).

Вместо технического проекта может быть разработан Рабочий проект, если отсутствует создание нового технического решения, которое было создано ранее и имеется технический проект, который описывает и обосновывает данное техническое решение.

В этом случае рабочий проект должен содержать как минимум следующие документы:

- Пояснительная записка.
- Рабочая документация.
- Сводный сметный расчет и Локальный сметный расчет.

5.9.3. Требования к программам и методикам испытаний

Программы и методики испытаний должны быть разработаны и утверждены до проведения соответствующих работ. Должны быть разработаны следующие программы и методики:

- Программа и методика предварительных испытаний, которая должна включать автономные и комплексные испытания.
- Программа опытной эксплуатации.
- Программа и методика приемочных испытаний.

Виды испытаний и общие требования к их проведению определены ГОСТ 34.603-92 «Виды испытаний автоматизированных систем».

5.9.4. Требования к эксплуатационной документации

Эксплуатационная документация для оборудования должна содержать следующие разделы:

- Руководство по эксплуатации.
- Схема электрическая функциональная.
- Формуляр (на каждый узел связи).
- Схема электрических соединений (перечень элементов и таблица соединений).
- Ведомость эксплуатационных документов.
- Ведомость ЗИП.

Руководство по эксплуатации должно подробно описывать порядок работы с оборудованием вплоть до перечня команд. Назначение руководства по эксплуатации – уменьшение влияния человеческого фактора за счет документирования всей работы с оборудованием и ПО.

Эксплуатационная документация для ПО должна содержать следующие документы:

- «Руководство оператора»;
- «Руководство администратора».

5.9.5. Требования к поставке оборудования и ПО

Требования по поставке и сопровождению изложены в разделе «Требования к поставщикам, и производителям оборудования» данного документа.

5.9.6. Требования к вводу в действие

Рекомендуется осуществлять все этапы испытаний системы перед ее вводом в действие, т.е.:

- Предварительные (автономные и комплексные) испытания. Опытная эксплуатация.
- Приемочные испытания для приема системы в промышленную эксплуатацию.

Рекомендуется на этапе предварительных испытаний предусматривать тестирование программных систем при помощи компаний, специализирующихся в данной области.

Все оборудование, вводимое в промышленную эксплуатацию, должно иметь соответствующие сертификаты соответствия, если это предусмотрено законодательством. В частности, необходимо иметь следующие сертификаты:

- сертификат соответствия в системе «Связь», если оборудование подсоединяется к сети общего пользования;
- сертификат соответствия в соответствии с Положением о системе сертификации, утвержденным постановлением Правительства Российской Федерации от 26.06.1995 № 608, если оборудование или программное обеспечение используется в качестве средства защиты

информации или криптографического (шифровального) средства (средства криптографической защиты информации), реализующего отечественные криптографические алгоритмы на основе государственных стандартов.

Ввод в эксплуатацию государственных информационных систем должен осуществляться в соответствии с Требованиям к порядку реализации мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем, утвержденными постановлением Правительства Российской Федерации от 06.07.2015 № 676

Окончательным вводом ИС в эксплуатацию считается утверждение ответственным органом исполнительной власти Чувашской Республики правового акта о вводе ИС в эксплуатацию, определяющего перечень мероприятий по обеспечению ввода системы в эксплуатацию и устанавливающего срок начала эксплуатации.

6. Минимальные требования к характеристикам типовой электронно-вычислительной техники, офисного оборудования, общесистемного и офисного программного обеспечения для нужд государственных учреждений Чувашской Республики, находящихся в ведении исполнительных органов Чувашской Республики

6.1. Типовая электронно-вычислительная техника

Технические характеристики	АРМ1	АРМ2	АРМ3	АРМ4
Процессор	x86-совместимый, не менее серии i3-12xxx или аналогичный, базовая частота от 3,3 ГГц	x86-совместимый, не менее серии i5-12xxx или аналогичный, базовая частота от 2,5 ГГц	x86-совместимый, не менее серии i3-12xxx или аналогичный, базовая частота от 1,2 ГГц	x86-совместимый, не менее серии i5-12xxx или аналогичный, базовая частота от 1,3 ГГц
Оперативная память	16 Гб	32 Гб	8 Гб	16 Гб
Жесткий диск	256 Гб SSD	500 Гб SSD	256 Гб SSD	500 Гб SSD
Внешние порты ввода/вывода	USB 3.2 x 4, HDMI, аудио вход/выход, разъѐм для микрофона, RJ– 45	USB 3.2 x 4, HDMI, аудио вход/выход, разъѐм для микрофона, RJ– 45	USB 3.2 x 3, Bluetooth, Wi-Fi, HDMI, аудио вход/выход, разъѐм для микрофона, RJ– 45	USB 3.2 x 3, Bluetooth, Wi-Fi, HDMI, аудио вход/выход, разъѐм для микрофона, RJ– 45
Видео	интегрировано	Дискретная видеокарта с объемом оперативной памяти не менее 8 Гб	интегрировано	Дискретная видеокарта с объемом оперативной памяти не менее 8 Гб
Монитор (соотношение сторон 16/9)*	LCD (TFT) 23,8" цветной, Яркость – не ниже 250 д/м2; Контрастность – не ниже чем 600:1 Время отклика пикселя – не менее 5 мс; Цветовая палитра – макс. 24–бит. (16777216 цветов); Интерфейс цифровой HDMI или Display Port	LCD (TFT) 23,8", цветной, Яркость – не ниже 250 кд/м2; Контрастность – не ниже чем 600:1 Время отклика пикселя – не менее 5 мс; Цветовая палитра – макс. 24–бит. (16777216 цветов); Интерфейс цифровой HDMI или Display Port	LCD (TFT) 14" цветной, Яркость – не ниже 250 кд/м2; Контрастность – не ниже чем 600:1 Время отклика пикселя – не менее 5 мс; Цветовая палитра – макс. 24–бит. (16777216 цветов); Интерфейс цифровой HDMI или Display Port	LCD (TFT) 15" цветной, Яркость – не ниже 250 кд/м2; Контрастность – не ниже чем 600:1 Время отклика пикселя – не менее 5 мс; Цветовая палитра – макс. 24–бит. (16777216 цветов); Интерфейс цифровой HDMI или Display Port
Сетевой	Ethernet	Ethernet	Ethernet	Ethernet

адаптер	100/1000	100/1000	100/1000	100/1000
Устройства ввода/вывода	Оптическая мышь, клавиатура	Оптическая мышь, клавиатура	Тач-пад, клавиатура	Тач-пад, клавиатура
Система мониторинга	Наличие контроля температуры процессора и оборотов вентилятора	Наличие контроля температуры процессора и оборотов вентилятора	Наличие контроля температуры процессора и оборотов вентилятора	Наличие контроля температуры процессора и оборотов вентилятора
Гарантия	12 месяцев	12 месяцев	12 месяцев	12 месяцев

АРМ1 – предназначены для выполнения типовых задач (делопроизводство, работа с документами, подготовка писем, аналитических материалов и типовых документов);
АРМ2 - предназначены для выполнения задач, связанных с работой в графических и видеоредакторах;
АРМ3 – предназначены для выполнения типовых задач (делопроизводство, работа с документами, подготовка писем, аналитических материалов и типовых документов) при проведении выездных мероприятий;
АРМ4 - предназначены для выполнения задач, связанных с работой в графических и видеоредакторах, при проведении выездных мероприятий.

6.2. Типовое офисное оборудование

Технические характеристики	МФУ1	МФУ2	МФУ3	МФУ4
Категория	Персональный	Персональный	Групповой	Групповой
Функции	печать, сканирование и копирование			
Формат	А4	А4	А3	А3
Тип печати	Лазерный	Лазерный	Лазерный	Лазерный
Цвет	Ч/б	Цветной	Ч/б	Цветной
Скорость печати	Не менее 17 стр. в мин.	Не менее 17 стр. в мин.	Не менее 17 стр. в мин.	Не менее 17 стр. в мин.
Разрешение при печати	Не менее 600x600 dpi	Не менее 600x600 dpi	Не менее 600x600 dpi	Не менее 600x600 dpi
Разрешение при сканировании	Не менее 600x600 dpi	Не менее 600x600 dpi	Не менее 600x600 dpi	Не менее 600x600 dpi
Автоподача при сканировании	Да	Да	Да	Да
Скорость копирования	Не менее 20 копий/мин	Не менее 20 копий/мин	Не менее 20 копий/мин	Не менее 20 копий/мин
Интерфейс с ПК	Ethernet	Ethernet	Ethernet	Ethernet
Гарантия	12 месяцев	12 месяцев	12 месяцев	12 месяцев

6.3. Типовое общесистемное программное обеспечение

Технические характеристики	ОС1	ОС2	ОС3
Нахождение в Едином реестре российских	Программное обеспечение включено в Единый реестр российских программ для ЭВМ и БД		

программ для ЭВМ и БД			
Требования по информационной безопасности	«Базовый»: для типовой работы, не связанной с обработкой персональных данных и конфиденциальной информации в государственных информационных системах (ГИС)	«Усиленный»: для обработки конфиденциальной информации в ГИС, в информационных системах персональных данных, а также в составе значимых объектов критической информационной инфраструктуры (КИИ) любого класса (уровня, категории) защищённости. Дополнительно используется в других информационных (автоматизированных) системах для обработки информации ограниченного доступа без содержания сведений, составляющих гостайну)	«Максимальный»: для обработки информации любой категории доступа в ГИС, в информационных системах персональных данных, в составе значимых объектов КИИ, иных информационных (автоматизированных) системах, обрабатывающих информацию ограниченного доступа, в т.ч. содержащую сведения, составляющие гостайну до степени «особой важности» включительно
Совместимость	Совместим с архитектурами x86, AMD64 и EM64T		
Обновление	Имеет штатные средства получения и установки обновлений безопасности, выпускаемых разработчиком дистрибутива для содержащихся в нем приложений. Срок, в течение которого для дистрибутива выпускаются обновления безопасности, должен истекать не ранее двух лет с момента приобретения дистрибутива. По истечение этого срока должна иметься штатная возможность обновления версии дистрибутива до следующей поддерживаемой		
Техническая поддержка	Имеет возможность получения технической поддержки от производителя дистрибутива или уполномоченных им организаций		

6.4. Типовое офисное программное обеспечение

Технические характеристики	Офисное ПО1	Офисное ПО2
Нахождение в Едином реестре российских программ для ЭВМ и БД	Программное обеспечение включено в Единый реестр российских программ для ЭВМ и БД	
Требования к доступности	Декстопное решение	Облачное решение

Наличие модулей	Текстовый редактор, табличный редактор, редактор презентаций, почтовый клиент (при наличии в составе офисного пакета)
Обновление	Имеет штатные средства получения и установки обновлений, выпускаемых разработчиком дистрибутива для содержащихся в нем приложений. Срок, в течение которого для дистрибутива выпускаются обновления, должен истекать не ранее двух лет с момента приобретения дистрибутива. По истечение этого срока должна иметься штатная возможность обновления версии дистрибутива до следующей поддерживаемой
Техническая поддержка	Имеет возможность получения технической поддержки от производителя дистрибутива или уполномоченных им организаций

7. Минимальные требования к мультисервисной сети

7.1. Минимальные требования к корпоративной распределенной мультисервисной сети.

7.1.1. Общие требования

Рекомендуется закупать сетевое оборудование, которое поддерживает следующие протоколы:

Основные протоколы	Протоколы управления, мониторинга и сбора статистики	Протоколы безопасности
IP (RFC 791) ICMP (RFC 792,1256) TCP (RFC 793) UDP (RFC 768) TELNET (RFC 854) BootP (RFC 951, 1542) Telnet Client/Server FTP и/или TFTP	SNMP v1/v2/v3 DHCP Client/Server/Relay Syslog NTP Client RMON 1(4 groups) Policy MIB	DoS Prevention ACLs AAA RADIUS (RFC 2138) SSHv2 Secure Copy v2 802.1x Client

7.1.2. Требования к коммутаторам

Рекомендуется закупать коммутаторы, которые обладают следующими минимальными техническими характеристиками:

Параметр	Уровень		
	Доступа	Агрегации	Ядра
Общие характеристики			
Тип устройства	Коммутация пакетов на основе неблокируемой коммутационной матрицы с промежуточным хранением пакетов		
Характеристики физического уровня			
Протоколы физического и канального уровня	Ethernet 100, 1000, 10000 Мбит/сек (на основе медной витой пары категории 5 и одномодового оптоволокна)		
Порты 10/100/1000 BASE-T(RJ-45)	Не менее 24	Не менее 12	Не менее 24
Гигабитные порты для подключения SFP- модулей (оптоволокно)	Не менее 2	Не менее 2	Не менее 4
Порты 10 GigabitEthernet(SFP+, XFP, XENPAK) или	Опционально	Не менее 16	Не менее 8

слоты для их установки			
Характеристики второго уровня			
Количество запоминаемых MAC-адресов	Не менее 8000	Не менее 16000	Не менее 24000
Поддержка Jumbo frames	Не менее 9000 байт	Не менее 9000 байт	Не менее 9000 байт
Поддержка VLAN по протоколу 802.1Q	Не менее 4096	Не менее 4096	Не менее 4096
Поддержка VLAN trunking	Да	Да	Да
ПоддержкаDouble VLAN (Q-in-Q)	Да	Да	Да
Поддержка групповой регистрации VLAN(GVRP)	Да	Да	Да
Поддержка протоколов связующего дерева	STP, RSTP	STP, RSTP, MSTP	STP, RSTP, MSTP
Поддержка агрегации линков по протоколу 802.3ad (LACP)	Да	Да	Да (в т.ч. на портах, расположенных на разных устройствах в стеке или разных модулях в шасси)
Характеристики третьего уровня			
Аппарартная маршрутизация пакетов L3 IPv4	Опционально		не менее 12000 маршрутов
Аппарартная маршрутизация пакетов L3 IPv6	Опционально		не менее 4000 маршрутов
Количество физических и виртуальных маршрутизируемых интерфейсов	Опционально		Не менее 1000
Поддержка статической маршрутизации	Опционально		Да
Поддержка протоколов динамической маршрутизации	Опционально		RIP v1, RIP v2, OSPF, EIGPR
Поддержка протокола MPLS	Опционально		Да
Поддержка многоадресной рассылки(multicast)	IGMP v1/v2/v3 Snooping (неменее256 групп), Multicast VLAN registration (MVR)		IGMP v1/v2/v3 Snooping (неменее256 групп), PIM-DM, PIM-SM, MVR
Поддержка DHCP	Да	Да	Да

relay			
Поддержка DHCP snooping	Да	Опционально	Опционально
Поддержка DHCP option 82	Да	Опционально	Опционально
ARP proxy	Опционально	Опционально	Да
Поддержка протокола резервирования роутера VRRP	Опционально		Да
Характеристики функций сетевой диагностики и мониторинга			
Поддержка функции диагностики кабеля	Да	Да	Опционально
Поддержка протокола определения топологии сети (CDPили LLDP)	Да	Да	Да
Зеркалирование трафика	На основе портов	На основе портов, VLAN и ACL	
Статистика по интерфейсам	Счетчики пакетов, байт, ошибок		
Мониторинг трафика	Опционально		sFlow, Netflow или аналоги
Характеристики QoS			
Поддержка приоретизации трафика по стандарту 802.1p	Да	Да	Да
Количество очередей приоритетов	Не менее 4 на порт	Не менее 8 на порт	Не менее 8 на порт
Классификация трафика на основе:			
Порта коммутатора	Да	Да	Да
VLAN ID	Да	Да	Да
Очередей приоритетов 802.1p	Да	Да	Да
MAC-адреса	Да	Опционально	Опционально
IPv4/v6-адреса	Да	Опционально	Опционально
DSCP	Да	Опционально	Опционально
Типа протокола	Да	Опционально	Опционально
Номера порта TCP/UDP	Да	Опционально	Опционально
Управление полосой пропускания	На основе порта, с дискретностью не более 64 кбит/сек	На основе порта/потока, с дискретностью не более 64 кбит/сек	
Шейпинг трафика	Нет	Нет	Да
Характеристики безопасности			

Поддержка функции защиты от сетевых петель и информирования об их обнаружении	Да	Да	Да
Поддержка функции защиты от широковещательных штормов и информирования об их обнаружении	Да	Да	Да
Защита от ARP-спуфинга	Да	Да	Да
Фильтрация пакетов по MAC-адресам на каждом порту	Да	Да	Да
Привязка MAC-адреса к порту	Да	Да	Да
Привязка IP-адреса к порту	Да	Да	Да
Ограничение количества MAC-адресов на каждом порту	Да	Да	Опционально
Привязка и контроль соответствия IP- и MAC-адресов клиентских устройств	Да	Да	Опционально
Фильтрация пакетов (ACL) на портах по mac-, ip-адресу (отправителя и получателя), номеру протокола второго и третьего уровней, метке vlan, метке приоритета	Да	Да	Да
Защита CPU коммутатора от перегрузки трафиком	Да	Да	Да
Поддержка изоляции портов друг от друга (port based vlan или traffic segmentation)	Да	Опционально	Опционально
Защита от известных сетевых атак	Опционально		Да
Авторизация портов по протоколу IEEE 802.1x	Веб- и мак-авторизация, локальная и Radius-сервере		
Характеристики управления			

Консольный порт RS-232 для управления	Да	Да	Да
Удаленное управление по протоколу ssh	Да	Да	Да
Удаленное управление по протоколу SNMP	Да	Да	Да
Удаленное сохранение и загрузка конфигурации и прошивки по ftp или tftp	Да	Да	Да
Удаленный мониторинг по протоколу snmp	Да	Да	Да
Поддержка ведения логов и отсылки уведомления syslog и snmp trap на удаленный сервер	Да	Да	Да
Поддержка учетных записей с авторизацией на Radius-сервере	Да	Да	Да
Характеристики отказоустойчивости			
Способ обеспечения отказоустойчивости	Нет	Резервирование компонентов с возможностью «горячей» замены	Резервирование компонентов с возможностью «горячей» замены, резервирование коммутаторов посредством объединения в отказоустойчивый стек, применение отказоустойчивого шасси
Резервируемые компоненты с возможностью «горячей» замены	Нет	Блоки питания, вентиляторы	Блоки питания, вентиляторы, управляющие / коммутирующие платы, компоненты стека / шасси
Установочные характеристики			
Типоразмер	Для установки в стойку 19”		
Высота	1U	1-2U	Не ограничивается
Электропитание	от внутреннего источника питания от сети переменного тока 100-240 В, 50/60 Гц		
Прочее			
Наличие сертификатов	Сертификат соответствия, санитарно-эпидемиологическое заключение		

7.1.3. Требования к пограничным маршрутизаторам

Параметр	Значение
Общие характеристики	
Объем установленной оперативной памяти	Не менее 1 Гб (с возможностью расширения не менее чем до 4 Гб)
Установленный жесткий или flash-диск	Не менее 1 Гб
Сетевые характеристики физического уровня	
ПортыEthernet 10/100/1000 BASE-T (RJ-45)	Не менее 4
Возможность установки дополнительных интерфейсов	Не менее 2 слотов с возможность расширения конфигурации до не менее чем 8 портов 10/100/1000 BASE-T(RJ-45) и 4 портов SFPдля установки оптических модулей
Сетевые характеристики канального уровня	
Инкапсуляция	Ethernet, ATM, Frame Relay, HDLC, PPP, PPPoE
Поддержка VLAN (IEEE 802.1q)	Да
Поддержка агрегированных линков 802.3ad/LACP	Да
Поддержка STP/RSTP/MSTP	Да
Производительность	
Маршрутизация трафика	Не менее 1000 Мбит/сек
Коммутация и маршрутизация	Программная или программно-аппаратная
Поддержка протоколов и возможностей маршрутизации	
Статическая маршрутизация	Да
RIP v1, RIP v2	Да
OSPF	Да
BGP	Да (поддержка не менее 1 FullView)
Маршрутизация на основе фильтров (ACL)	Да
Поддержка маршрутизации на основе IP-адреса источника (sourcerouting)	Да
Маршрутизация Multicast	Да (поддержка протоколов IGMPv1/v2/v3, PIM, DVMRP)
Поддержка MPLS	Да(поддержкаMPLS L2 VPN, MPLS L3 VPN, VPLS)
Поддержка протокола балансировки нагрузки ECMP	Да
Поддержка функций трансляции адресов (NAT)	
Поддержка статической трансляции адресов	Да
Поддержка динамической трансляции адресов назначения с трансляцией портов (SNAT)	Да
Поддержка динамической трансляции адресов источника с трансляцией портов (DNAT)	Да
Характеристики функций сетевой диагностики и мониторинга	
Поддержка SNMP	SNMP v2, SNMP v3
Контроль производительности	Да
Счетчики производительности на	Да

физических, виртуальных интерфейсах и фильтрах	
Экспорт информации по трафику	Netflow или аналоги
Поддержка функций сетевого экрана	
Фильтрация трафика по IP-адресам, портам TCP/UDP	Да
Фильтрация с отслеживанием состояния TCP/UDP-соединенй (statefulfirewall)	Да
Определение и защита от известных сетевых атак	Да
Защита от DOS и DDOS	Да
Наличие системы обнаружения вторжений (IPS) собновляемой базой паттернов	Да
Характеристики QoS	
Управление трафиком на физических интерфейсах, виртуальных интерфейсах и потоках	Ограничение пропускной способности, шейпинг, полисинг, маркировка по классам приоритета
Характеристики управления	
Консольный порт RS-232 для CLI-управления	Да
Удаленное CLI-управление по протоколу ssh	Да
Удаленное управление по http(s)	Да
Удаленное сохранение и загрузка конфигурации и прошивки по ftp или tftp	Да
Поддержка учетных записей с авторизацией на Radius-сервере	Да
Поддержка ведения логов и отсылки уведомления syslog и snmp trap на удаленный сервер	Да
Автоматическое резервирование конфигураций	Да
Атомарное применение изменений конфигураций	Да
Возможность автоматического отката изменений конфигураций при потере управления	Да
Характеристики отказоустойчивости	
Резервируемые компоненты с возможностью «горячей» замены	Блоки питания, вентиляторы, в случае модульного исполнения - управляющие и коммутирующие платы
Поддержка протокола резервирования роутера VRRP	Да
Установочные характеристики	
Типоразмер	Для установки в стойку 19”
Электропитание	от внутреннего источника питания от сети переменного тока 100-240 В, 50/60 Гц

Прочее	
Наличие сертификатов	Сертификат соответствия, санитарно-эпидемиологическое заключение

7.1.4. Требования к точке радиодоступа стандарта Wi–Fi

Рекомендованные требования к оборудованию Wi-Fi:

- стандарт IEEE 802.11 (2,4/5,0 ГГц);
- виртуальные локальные сети (VLAN) – до 16 сегментов; приоритезацию трафика;
- роуминг между точками доступа (Proxy Mobile IP);
- протокол 802.1p QoS;
- управление с помощью HTTP интерфейса, командной строки, FTP, TFTP и Telnet. протокол SNMP;
- стандарт 802.1X;
- локальное и удаленное питание по витой паре; иметь встроенную антенну.

7.1.5. Требования к кодеку видеоконференцсвязи

- поддерживать работу в сетях как IP (H.323),SIP, так и ISDN (H.320);
- поддерживаемые протоколы: H.323 v4, H.239, VNC, Telnet, RTP, HTTP, DHCP, SIP.
- обеспечивать соединение точка–точка на скорости не менее 768 Кбит/сек по IP и не менее 384 Кбит/с по ISDN;
- поддерживать режим передачи двух видео потоков в одном канале связи одновременно для передачи и получения как изображения докладчика, так и дополнительного изображения (компьютер, документальная камера, вспомогательная камера);
- поддерживать протоколы кодирования видео потока H.261, H.263, H.263+, H.263++, H.264 с
- разрешениями 4CIF (704x576), CIF (352x288), QC1F (176x144), чересстрочный CIF (352x576) и частотой обновления до 25 кадров/сек;
- поддерживать протоколы кодирования аудио потока G.711, G.729.
- Интерфейс H.323, SIP: RJ45 Ethernet, 10/100/1000 Мбит/cfull/half duplex
- Обеспечивать подключение ПК и других источников сигнала (документкамера, видеокамера и т.д.).

8. Минимальные требования к инфраструктуре центров обработки данных

8.1. Минимальные требования к системам обработки и хранения данных

Рекомендованные требования к серверам:

- CPU - последнего поколения, количество вычислительных ядер, и размеры оперативного кеша разных уровней подбираются под задачу с учетом рекомендаций производителя;
- RAM– минимально 256 Гб с возможностью расширения минимум до 1024 Гб;
- Видеоподсистема – поддерживаемая используемой ОС; Дисковая подсистема:
- SAS контроллер, минимально 2 (два) канала,
- Используются диски только с технологией горячей замены (hot swap);
- Двухканальный RAID контроллер, кэш память контроллера с автономным энергообеспечением, аппаратная поддержка RAID 0, 1. На многодисковых системах

- аппаратная поддержка RAID 5;

- возможность установки двух iSCSI HBA;

- минимум 2 USB 2.0 порта;
- минимум два сетевых адаптера – Ethernet 1000/10000 Мбит/с с автоматическим выбором скорости передачи данных;
- наличие удаленного управления по сети Ethernet - выделенный или разделяемый порт;
- возможность установки избыточного блока питания с горячей заменой,
- возможность установки в шкаф 19”.

8.2. Минимальные требования к системному ПО

ОС для обслуживания серверных приложений и промышленных систем рекомендуется выбирать из Единого реестра российских программ для ЭВМ и БД.

Если какая-либо прикладная информационная требует использовать определенную ОС, не входящую в рекомендованный список, то данное использование возможно, при условии, что производитель системы не допускает использование рекомендованных ОС.

Если приложение требует использования более низших версий ОС, чем рекомендованные, и работает некорректно на рекомендуемых версиях, то такая замена возможна.

Выбранный дистрибутив должен обладать следующими характеристиками:

Совместим с архитектурами x86, AMD64 и EM64T;

- Поддерживать многопроцессорные SMP–архитектуры и технологию многопоточности Hyper–Threading.
- Использовать ядро ветки 2.6 с поддержкой библиотеки Native POSIX Threading Library (NPTL).
- Иметь компилятор GCC версии не ниже 8.0.
- Быть совместимым со стандартом Linux Standard Base (LSB) 3.2.
- Иметь средства виртуализации;
- Иметь средства создания VPN;

8.3. Минимальные требования к помещениям и инженерным системам

8.3.1. Требования к телекоммуникационным шкафам

- Тип – стандартный закрытый шкаф
- 19”; Высота – 42U;
- Глубина шкафа – 1000 мм;
- Ширина шкафа – 600 мм;

- Съѐмные боковые и задняя стенки;
- Передняя дверь с замком;
- Монтажный комплект;

8.3.2. Требования к источникам бесперебойного питания

- Номинальная мощность и время работы от батарей, обеспечивающие функционирование подключенного оборудования не менее 10 мин; Технология – двойное преобразование;
- Коэффициент полезного действия (при электроснабжении поддерживаемых устройств от внешней сети) – 90% и использование активного корректора коэффициента мощности;
- Выходное напряжение:
  - форма – синусоида;
  - номинальное значение – 220/380 В;

Тестирование батареи:

- при включении;
- ручное;
- автоматическое периодическое;

- Аппаратная защита батареи от глубокого разряда;
- Возможность подключения дополнительной батареи;
- Диапазон входных напряжений 220 В ± 20%;
- Звуковая индикация режима работы от батарей с возможностью отключения;
- Возможность мониторинга и управления по локальному порту (USB/RS232);
- Возможность оснащения: порт RJ–45 для подключения к локальной сети для мониторинга и управления ИБП по протоколу SNMP.
- Возможность установки в стандартный шкаф 19”.
- Крепежный комплект для установки в стандартный шкаф 19”.

8.3.3 Требования к помещениям

При проектировании серверных помещений и узлов связи необходимо руководствоваться следующими документами:

- РД 45.120–2000. Нормы технологического проектирования. Городские и сельские телефонные сети.
- ГОСТ 464–79. Заземление для стационарных установок проводной связи, радиорелейных станций, радиотрансляционных узлов и антенн систем коллективного приема телевидения. Нормы сопротивления.
- СНиП 21–01–97. Противопожарная безопасность зданий и сооружен
- ГОСТ Р 58811-2020 Центры обработки данных. Инженерная инфраструктура. Стадии создания.
- ГОСТ Р 58812-2020 Центры обработки данных. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация

Минимальные требования нормативных документов к серверным помещениям и узлам связи:

- Здание должно быть не ниже II степени огнестойкости (допускается III степень).
- Над помещениями, где устанавливается аппаратура связи, не допускается размещать помещения, связанные с потреблением воды.
- Через помещения ввода кабелей не допускается прокладка силовых кабелей и транзитных инженерных коммуникаций.
- Если не используется фальшпол, то чистые полы производственных помещений должны настилаться на несгораемое основание. Покрытие пола – линолеум антистатический специального назначения ТУ 95–25048396–056–94.

- Должно быть исключено попадание солнечных лучей на ИБП и аккумуляторы. Производственные помещения должны отделяться от других помещений несгораемыми стенами или перегородками с пределом огнестойкости не менее 0,75 часа.
- Освещение проектируется с общей нормируемой освещенностью для помещений такого типа не менее 200 лк.
- Каркасы оборудования, аппаратуры и металлические части должны быть заземлены. Линейные сооружения: шкафы, кабельные ящики, металлические оболочки и экраны кабелей должны быть заземлены.
- Каждое заземляющее устройство должно соответствовать требованиям ПУЭ, иметь паспорт, содержащий схему устройства заземления, основные технические данные, а также данные о результатах проверки состояния заземляющего устройства, о характере производственных ремонтов и изменениях, внесенных в конструкцию данного устройства.
- Отверстия в межэтажных или чердачных перекрытиях, через которые проходят телефонные или другие кабели, должны быть плотно закрыты асбестом и герметизированы цементным раствором, алебастром или другими несгораемыми материалами. Если при работах с кабелями отверстия были вскрыты, то по окончании они должны быть вновь заделаны. Для предотвращения распространения пожара из помещения в помещение необходимо предусмотреть заполнение свободного пространства, оставшегося после прокладки кабелей и проводов в проемах или трубах между помещениями, в том числе и между этажами, легко удаляемыми несгораемыми материалами.
- При входе во все производственные помещения должны быть вывешены таблички с указанием категории помещения по степени опасности поражения электрическим током, взрыво- и пожаробезопасности и знаки безопасности по ГОСТ Р 12.4.026-2001 и фамилии ответственного за состояние охраны труда.
- При наличии возможности одновременного прикосновения персонала к металлическим корпусам оборудования и трубопроводам отопления, водопровода и канализации последние следует оградить токонепроводящими решетками.
- Присоединение заземляющих и нулевых проводников к заземлителям, заземляющему контуру и к заземляющим конструкциям должно быть выполнено сваркой, а к корпусам оборудования – сваркой или надежным болтовым соединением.
- Каждая часть оборудования, подлежащая заземлению или занулению, должна быть присоединена к сети заземления или зануления с помощью отдельного проводника. Последовательное включение в заземляющий или нулевой защитный проводник заземляемых или зануляемых частей оборудования запрещается.
- У мест ввода заземляющих проводников в здание должны быть предусмотрены опознавательные знаки в соответствии с ГОСТ 12.04.026.

9. Минимальные требования к системе управления и мониторинга

9.1. Требования к размещению системы управления и мониторинга ЦОД I и II уровней

Системы мониторинга и управления ЦОД II могут располагаться на серверах систем мониторинга и управления ЦОД I. Системы мониторинга и управления ЦОД I могут располагаться на серверах резервного центра ЦОД I.

9.2. Требования к системам управления и мониторинга ЦОД I и II уровней

В состав системы управления и мониторинга ЦОД I необходимо, а ЦОД II рекомендуется включать следующие системы:

- Система управления и мониторинга сетевой инфраструктуры.
- Система управления и мониторинга серверов и приложений.
- Система мониторинга транзакций и доступности служб.
- Система управления и мониторинга ПК пользователей.

9.3. Требования к рабочим станциям операторов системы управления и мониторинга

Как минимум рабочие станции должны удовлетворять типовой конфигурации «Персональный компьютер», см. «7.1. Типовая электронно-вычислительная техника».

9.4. Требования к KVM системам

Состав KVM-системы: монитор, клавиатуру, манипулятор мышь/сенсорная панель. Система обеспечивает одновременное физическое подключение монитора, клавиатуры, мыши к 8, либо более, серверам или системным блокам без переноса соединительных кабелей.

Необходимые требования:

- высота не более 1U;
- возможность установки в стандартный шкаф 19”.

10. Минимальные требования к документации

Вся документация должна удовлетворять следующим ГОСТ-ам:

- Оформление документов – ГОСТ 2.ххх. Эскизный проект – ГОСТ 2.119-2013.
- Проектно–сметная документация – ГОСТ 34.201–89. Техническое задание на создание – ГОСТ 34.602–89. Технорабочий проект – ГОСТ 34.ххх.
- Технический проект ГОСТ 2.120-2013. Спецификация оборудования, изделий и материалов – ГОСТ 21.110-2013 .
- Виды испытаний автоматизированных систем ГОСТ 34.603–92.
- ГОСТ 34.201-89 Виды, комплектность и обозначения документов при создании автоматизированных систем
- ГОСТ 34.602-89 Техническое задание на создание автоматизированной системы
- ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем

11. Требования к средствам обеспечения безопасности

Технические меры защиты информации должны реализовываться посредством применения средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, в том числе программных и (или) программно-аппаратных средств, в которых они реализованы, имеющих необходимые функции безопасности.

В соответствии с требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17, для обеспечения защиты информации в государственных информационных системах должны применяться:

средства защиты информации не ниже 4 класса, соответствующие 4 или более высокому уровню доверия – для информационных систем 1 класса защищенности;

средства защиты информации не ниже 5 класса, соответствующие 5 или более высокому уровню доверия – для информационных систем 2 класса защищенности;

средства защиты информации 6 класса, соответствующие 6 или более высокому уровню доверия – для информационных систем 3 класса защищенности.

1. Перечень рекомендуемых средств защиты информации:

1) Средства антивирусной защиты информации:

- программное изделие «Kaspersky Endpoint Security для Windows» (рекомендуется);
- программное обеспечение «Dr.Web Enterprise Security Suite».

Для операционных систем Linux:

- программное изделие «Kaspersky Endpoint Security для Linux»;
- программное обеспечение «Dr.Web Enterprise Security Suite».

2) Средства защиты информации от несанкционированного доступа:

- средство защиты информации Secret Net Studio (рекомендуется);
- система защиты информации от несанкционированного доступа «Dallas Lock».

Для операционных систем Linux:

- средство защиты информации «Secret Net LSP»;
- система защиты информации от несанкционированного доступа «Dallas Lock Linux».

При выборе средств защиты информации от несанкционированного доступа следует учесть, что функциональные возможности указанных средств защиты информации можно расширить за счет дополнительных модулей (межсетевой экран, антивирус, средство обнаружения вторжений). Приобретение дополнительных модулей не требуется, в случае если функциональные возможности указанных модулей реализованы иными средствами защиты информации (например, если используется иное антивирусное программное обеспечение, межсетевой экран, функционирующий на границе периметра защищаемого сегмента сети, средство обнаружения вторжений).

3) Межсетевые экраны, имеющие программную реализацию (уровня хоста):

- средство защиты информации Secret Net Studio с модулем межсетевого экранирования (рекомендуется);
- система защиты информации от несанкционированного доступа «Dallas Lock» с модулем межсетевого экранирования;
- программный комплекс ViPNet Client;
- программный комплекс ViPNet Personal Firewall

Для операционных систем Linux:

- средство защиты информации «Secret Net LSP»;
- программный комплекс ViPNet Personal Firewall

Указанные межсетевые экраны уровня хоста необходимо использовать в случае, если на границе периметра защищаемой сети (сегмента сети), в которой располагаются технические средства информационных систем (в том числе рабочие станции, сервера), не установлены межсетевые экраны, имеющие программно-аппаратную реализацию (уровня

сети), а также в случае необходимости применения дополнительных мер защиты информации на основании анализа угроз безопасности информации.

В качестве программно-аппаратных межсетевых экранов рекомендуется использовать программно-аппаратный комплекс защиты информации «ViPNet Coordinator HW» или иной сертифицированный межсетевой экран, соответствующий требованиям ФСТЭК России к межсетевым экранам.

4) Средства обнаружения вторжений, имеющие программную реализацию (уровня хоста):

- средство защиты информации Secret Net Studio с модулем обнаружения вторжений (рекомендуется);
- система защиты информации от несанкционированного доступа «Dallas Lock» с модулем обнаружения вторжений;

Указанные средства обнаружения вторжений уровня хоста необходимо использовать в случае, если в сети (сегменте сети), в которой располагаются технические средства информационных систем (в том числе рабочие станции, сервера), не установлены средства обнаружения вторжений, имеющие программно-аппаратную реализацию (уровня сети).

В качестве программно-аппаратных средств обнаружения вторжений рекомендуется использовать систему обнаружения компьютерных атак (вторжений) VIPNet IDS или иное сертифицированное средства обнаружения вторжений, соответствующие требованиям ФСТЭК России к системам обнаружения вторжений.

5) Средства выявления уязвимостей и анализа защищенности:

- программное изделие «Сетевой сканер безопасности XSpider»;
- программный комплекс «Средство анализа защищенности «Сканер-ВС»;
- система анализа защищенности программного и аппаратного обеспечения TCP/IP сетей (сетевой сканер Ревизор Сети);
- система контроля защищенности и соответствия стандартам «MaxPatrol»;
- программное изделие «Система мониторинга событий информационной безопасности MaxPatrol SIEM»;
- программное средство «ScanOVAL» (предназначено для обнаружения уязвимостей в программном обеспечении на рабочих станциях и серверах).

Для операционных систем Linux:

- программный комплекс «Средство анализа защищенности «Сканер-ВС»;
- программное средство «ScanOVAL для Linux».

5) Средства доверенной загрузки:

- программно-аппаратный комплекс «Соболь» (рекомендуется);
- средство доверенной загрузки «Dallas Lock»;
- программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».

2. Перечень рекомендуемых средств криптографической защиты информации (далее – СКЗИ):

1) Перечень СКЗИ, рекомендуемых для использования на рабочих станциях и серверах:

- СКЗИ «КриптоПро CSP»;
- программный комплекс ViPNet Client, либо ViPNet PKI Client, либо СКЗИ «ViPNet CSP»;

Указанные СКЗИ могут использоваться для криптографической защиты каналов связи при обработке информации в информационных системах, а также в качестве средств электронной подписи.

2) Перечень СКЗИ, рекомендуемых для использования на рабочих станциях и серверах при организации защищенного электронного взаимодействия:

- программный комплекс ViPNet Client;

- СКЗИ «Континент TLS VPN Клиент» (при необходимости организации защищенного взаимодействия с применением прикладного программного обеспечения без использования «тонкого» клиента);
- СКЗИ «МагПро КриптоПакет».

3) Перечень рекомендуемых программно-аппаратных шифровальных (криптографических) средств:

- программно-аппаратный комплекс защиты информации «ViPNet Coordinator HW»;
- СКЗИ «Континент TLS-сервер».

12. Таблица именования официальных адресов электронной почты и доменов для государственных учреждений Чувашской Республики

Название организации	Официальный адрес электронной почты	Структура именования домена для служебных адресов
Администрация Главы Чувашской республики	km2@cap.ru	Ag_XXX@cap.ru
Министерство здравоохранения Чувашской Республики	medicin_knc@cap.ru	medicin_XXX@cap.ru
Министерство культуры, по делам национальностей и архивного дела Чувашской Республики	culture@cap.ru	culture_XXX@cap.ru
Министерство образования и молодежной политики Чувашской Республики	minobr@cap.ru	obrazov_XXX@cap.ru
Министерство природных ресурсов и экологии Чувашской Республики	minpriroda@cap.ru	minpriroda_XXX@cap.ru
Министерство промышленности и энергетики Чувашской Республики	minprom@cap.ru	minprom_XXX@cap.ru
Министерство сельского хозяйства Чувашской Республики	mcx@cap.ru	agro_XXX@cap.ru
Министерство строительства, архитектуры и жилищно-коммунального хозяйства Чувашской Республики	construc@cap.ru	construc_XXX@cap.ru
Министерство транспорта и дорожного хозяйства Чувашской Республики	mintrans_info@cap.ru	mintrans_XXX@cap.ru
Министерство труда и социальной защиты Чувашской Республики	mintrud@cap.ru	mintrud_XXX@cap.ru
Министерство физической культуры и спорта Чувашской Республики	minsport@cap.ru	sport_XXX@cap.ru
Министерство финансов Чувашской Республики	finmail@cap.ru	minfin_XXX@cap.ru
Министерство цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики	info100@cap.ru	digital_XXX@cap.ru
Министерство экономического развития и имущественных отношений	mineconom@cap.ru	economy_XXX@cap.ru

Чувашской Республики		
Государственный комитет Чувашской Республики по делам гражданской обороны и чрезвычайным ситуациям	gkchs@cap.ru	gkchs_XXX@cap.ru
Государственная ветеринарная служба Чувашской Республики	vet@cap.ru	vet_XXX@cap.ru
Государственная служба Чувашской Республики по делам юстиции	minust@cap.ru	minust_XXX@cap.ru
Государственная служба Чувашской Республики по конкурентной политике и тарифам	tarif@cap.ru	tarif_XXX@cap.ru
Государственная жилищная инспекция Чувашской Республики	goszhil-mail@cap.ru	goszhil_XXX@cap.ru
Государственная инспекция по надзору за техническим состоянием самоходных машин и других видов техники Чувашской Республики	gtn_info@cap.ru	gtn_XXX@cap.ru
Полномочное представительство Чувашской Республики при Президенте Российской Федерации	polprchuv@cap.ru	polpred_XXX@cap.ru
Государственный совет Чувашской Республики	gs@cap.ru	gs_XXX@cap.ru