



ТЕХНИЧЕСКАЯ ПОЛИТИКА В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГРУППЫ РУСГИДРО

Содержание

Глоссарий. Определения, обозначения и сокращения.....	3
1 Общие положения.....	5
1.1 Цели и задачи Технической политики в области информационных технологий.....	5
1.2 Нормативно-техническое обеспечение ИТ-деятельности.....	5
1.3 Реализация Технической политики по ИТ.....	6
1.4 Цифровая трансформация и импортозамещение.....	7
1.5 Адаптация и развитие Технической политики по ИТ.....	7
2 Требования к ИТ-инфраструктуре Группы РусГидро.....	9
2.1 Основные компоненты ИТ-инфраструктуры.....	9
2.2 Общие требования к ИТ-инфраструктуре.....	10
2.3 Принципы организации ИТ-инфраструктуры.....	10
2.4 Технические требования к ИТ-инфраструктуре.....	11
3 Требования к обеспечению информационной безопасности.....	55
3.1 План обеспечения непрерывности бизнеса и восстановления после аварии (нештатной ситуации и/или компьютерного инцидента).....	58
4 Требования к унифицированной системе мониторинга технического состояния ИТ-инфраструктуры.....	60
4.1 Требования к функциональности.....	60
4.2 Требования к структуре СМТС.....	61
5 Требования к вводу информационных систем в эксплуатацию.....	62
5.1 Требования к вводу в действие.....	62
5.2 Базовые меры защиты при вводе в эксплуатацию.....	63
6 Требования к подключению Филиалов ОБЩЕСТВА и подконтрольных организаций к информационным ресурсам ПАО «РусГидро».....	65
6.1 Требования к подключению Филиалов.....	65
6.2 Требования к подключению подконтрольных организаций.....	65
7 Требования к поставщикам, производителям и проведению конкурсов.....	66
7.1 Общие требования.....	66
7.2 Требования к поставщикам услуг по эксплуатации и сопровождению.....	67
7.3 Особые требования к поставщикам инновационных ИС и услуг.....	69
ПРИЛОЖЕНИЯ.....	70

1 ГЛОССАРИЙ. ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В данной таблице приведены определения, технические термины и сокращения, употребляемые в настоящем документе.

Термин/сокращение	Описание
API	Application programming interface – программный интерфейс приложения, интерфейс прикладного программирования
BGP	Border Gateway Protocol – протокол граничных роутеров
DHCP	Dynamic Host Configuration Protocol – служба распределения адресов сети
IDS/IPS	Intrusion Detection System – система обнаружения / предотвращения вторжений
IS-IS	Протокол внутренней маршрутизации, для использования во внутренних сетях
LAN	Local Area Network – локальная вычислительная сеть
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
OSI	Open Systems Interconnection – модель взаимодействия открытых систем
OSPF	Open Shortest Path First – один из динамических протоколов маршрутизации
RPO	Целевая точка восстановления, т.е. момент, до которого необходимо восстановить данные или, другими словами, это фактически допустимый объем потерянных данных
RTO	Целевое времени восстановления, т.е. время, необходимое на восстановление данных
SAN	Сеть хранения данных
SLA	Service Level agreement – соглашение об уровне услуг
SNMP	Simple Network Management Protocol – протокол управления сетевыми устройствами
TCO	Total Cost Ownership – совокупная стоимость владения
VLAN	Виртуальная локальная сеть
VPN	Виртуальная частная сеть
VoIP	Voice over IP – передача голоса через IP-сети
Wi-Fi	Технология беспроводных сетей
АСТУ	Автоматизированная система технологического управления
АСУТП	Автоматизированная система управления технологическими процессами
БД	Базы данных
ВКС	Системы видеоконференцсвязи
Группа	Группа РусГидро
ДИТ	Департамент информационных технологий и цифрового развития ПАО «РусГидро»
ДМЗ	Демилитаризованные зоны
Заказчик, Функциональный	Лицо или орган, уполномоченный формировать требования к ИТ-услугам

Термин/сокращение	Описание
заказчик	
ИА	Исполнительный аппарат ПАО «РусГидро»
ИБ	Информационная безопасность
ИС	Информационные системы
ИТ	Информационные технологии
ИТ-инфраструктура	Комплекс аппаратных и системных средств обеспечения ИТ в деятельности Группы РусГидро (вычислительная техника, сети, операционные системы)
ИТ-комплекс	Совокупность ИТ-инфраструктуры, ИС, АСТУ, АСУТП и СДТУ, эксплуатируемых в Группе РусГидро
ИТ-подразделения	Структурные подразделения компаний Группы РусГидро, в функции которых входит обеспечение эксплуатации ИТ-комплекса и оказания ИТ-услуг
ИТ-услуга	Общее понятие, охватывающее различные виды результатов функционирования ИТ-инфраструктуры и ИС Группы РусГидро, используемые пользователями или другими компонентами ИТ-инфраструктуры и ИС для получения дополнительных возможностей
ИТКС	Информационно-телекоммуникационные сети
КПЭ	Ключевой показатель эффективности
КСА СПП	Корпоративная система автоматизации СПП
КСПД	Корпоративная сеть передачи данных
ЛНД(А)	Локальный нормативный документ (акт)
МСЭ	Межсетевой экран (firewall)
МФУ	Многофункциональное (периферийное) устройство печати, с поддержкой функций копирования и сканирования
Общество	ПАО «РусГидро» и его филиалы
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
Реестр российского ПО	Единый реестр российских программ для электронных вычислительных машин и баз данных (https://reestr.digital.gov.ru)
РРПП	Реестр российской промышленной продукции (https://gisp.gov.ru)
СДТУ	Средства диспетчерского и технологического управления
СКС	Структурированные кабельные системы
СМТС	Система мониторинга технического состояния
СО	Системный оператор
СПП	Служба поддержки пользователей
СУБД	Системы управления базами данных
СХД	Системы хранения данных
ТСПД	Технологическая сеть передачи данных
ТфОП	Телефонная сеть общего пользования
ЦОД	Центр обработки данных

2 ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Цели и задачи Технической политики в области

информационных технологий

Целью Технической политики в области ИТ Группы РусГидро (далее – Техническая политика по ИТ) является определение основных требований и ограничений, применяемых при построении, развитии (модернизации) и эксплуатации ИТ-комплекса, оказании ИТ-услуг и реализации проектов в области ИТ в целях повышения эффективности и качества производственной деятельности Группы путем эффективного применения ИТ.

Техническая политика по ИТ направлена на решение задач перспективного и технологического развития Группы путем реализации следующих мероприятий:

- автоматизация и цифровизация технологических и бизнес-процессов Группы;
- преимущественное использование отечественного ПО и радиоэлектронной продукции (импортозамещение);
- снижение совокупной стоимости владения (ТСО) элементов ИТ-комплекса Группы за счет их унификации и типизации;
- выполнение требований международных и российских стандартов в области ИТ.

Техническая политика по ИТ основана на следующих основных принципах:

- соответствие стратегическим целям Группы;
- соответствие требованиям Технической политики Группы;
- прозрачность и обоснованность принимаемых управленческих и технических решений;
- развитие собственных компетенций для обслуживания, проектирования, ремонта и эксплуатации объектов ИТ-комплекса Группы;
- обеспечение ИБ на всех стадиях жизненного цикла объектов ИТ-комплекса Группы;
- комплексный подход в управлении состоянием эффективности, надёжности и безопасности объектов ИТ-комплекса Группы.

2.2 Нормативно-техническое обеспечение ИТ-деятельности

Техническая политика по ИТ детализирует положения и адаптирует требования Технической политики Группы¹ по направлению ИТ-деятельности.

Техническая политика по ИТ разработана с учетом требований следующих ЛНД (А):

- Технической политики Группы;

¹ Утверждена решением Совета директоров Общества (протокол от 10.04.2020 № 307).

- Стратегии развития Группы на период до 2050 года (с детализацией до 2030 года), утвержденной решением Совета директоров Общества (протокол от 28.04.2026 № 400);
- Стратегии цифровой трансформации Группы, утвержденной решением Совета директоров Общества (протокол от 31.05.2024 № 374) (далее – Стратегия ЦТ);
- Политики информационной безопасности ПАО «РусГидро», утвержденной приказом Общества от 08.11.2022 № 853 (далее – Политика информационной безопасности);
- Положения о Департаменте информационных технологий и цифрового развития ПАО «РусГидро», утвержденного приказом Общества от 26.12.2023 № 947.

2.3 Реализация Технической политики по ИТ

Техническая политика по ИТ распространяет свое действие на Общество и его подконтрольные организации.

Техническая политика по ИТ применяется в Обществе с даты утверждения ее решением Правления Общества, в подконтрольных организациях – с даты принятия Советом директоров подконтрольной организации решения о присоединении к Технической политике по ИТ.

Техническая политика по ИТ осуществляется согласно:

- требованиям следующих документов:
 - Программы проведения технического аудита ИТ-комплекса Группы²;
 - Планов корректирующих мероприятий, подготовленных по итогам проведения технического аудита ИТ-комплекса Группы;
 - Производственной программы;
 - Программ инновационного развития и НИОКР;
- достижению КПЭ³, установленных для реализации планов импортозамещения.

Техническая политика по ИТ должна реализовываться с учетом конкретных требований преимущественного использования отечественного ПО и российской радиоэлектронной продукции (РЭП), определяемых планами импортозамещения и Стратегией ЦТ. Ведущая роль в реализации технической политики ИТ и в предоставлении ИТ-услуг в Обществе и подконтрольных организациях закрепляется за ООО «РусГидро ИТ сервис» и ООО «РГЦР» (в части АСТУ, АСУТП и СДТУ).

² Формируется согласно действующим регламентам проведения технического аудита объектов Группы.

³ Устанавливаются в Стратегии ЦТ.

Постоянно действующий Координационный комитет по ИТ ПАО «РусГидро»⁴ обеспечивает согласование и утверждение применяемых технических решений, отвечающих требованиям Технической политики по ИТ.

2.4 Цифровая трансформация и импортозамещение

Цифровая трансформация в Группе осуществляется в соответствии со Стратегией ЦТ.

Стратегия ЦТ направлена на повышение эффективности деятельности Группы за счет внедрения российских цифровых решений с обновленными методическими рекомендациями по цифровой трансформации государственных корпораций и компаний с государственным участием.

Ключевой целью ЦТ Группы является повышение эффективности основной деятельности за счет внедрения цифровых технологий при сохранении надежности и безопасности функционирования энергообъектов холдинга.

ЦТ обеспечивает улучшение показателей основной производственной деятельности за счет повышения операционной эффективности и гибкости, оптимизации управления энергоресурсами, позволяет быстро реагировать на внешние изменения, совершенствует принципы кибербезопасности в целях предотвращения возможных внешних угроз.

ЦТ Группы осуществляется по трем ключевым направлениям:

- развитие корпоративных ИС и пользовательских сервисов;
- развитие и совершенствование АСУТП и СДТУ;
- развитие и совершенствование систем ИБ.

Цифровая трансформация в Группе проводится в соответствии со Стратегией ЦТ и Планами мероприятий и перехода на преимущественное использование отечественного ПО и радиоэлектронного оборудования Общества и его подконтрольных организаций.

Приобретение ПО, не включенного в Реестр российского ПО, осуществляется по согласованию с ДИТ.

Приобретение радиоэлектронной продукции, не включенной в РРПП, осуществляется по согласованию с ДИТ.

2.5 Адаптация и развитие Технической политики по ИТ

Техническая политика по ИТ разрабатывается ДИТ и утверждается решением Правления Общества.

Актуализация Технической политики по ИТ производится по необходимости, но не реже 1 раза в 3 года.

Технические требования к элементам ИТ-комплекса и применяемым техническим решениям, изложенные в составе приложений к Технической

⁴ В соответствии с Положением о Координационном комитете по ИТ, утвержденным приказом Общества от 12.11.2019 № 926.

политике по ИТ в форме Перечня используемых / рекомендуемых технических решений информационно-технологической инфраструктуры ПАО «РусГидро» (Приложение 2), могут актуализироваться по необходимости и утверждаются директором ДИТ.

Для контроля за соблюдением требований Технической политики по ИТ проводится технический аудит на соответствие существующего состояния ИТ-комплекса в целом или отдельных его компонентов требованиям настоящей Технической политики по ИТ⁵. По итогам технического аудита утверждается план корректирующих мероприятий по приведению ИТ-комплекса в соответствие с требованиями Технической политики по ИТ.

3 ТРЕБОВАНИЯ К ИТ-ИНФРАСТРУКТУРЕ ГРУППЫ РУСГИДРО

3.1 Основные компоненты ИТ-инфраструктуры

Аппаратное обеспечение:

- Настольные компьютеры и ноутбуки;
- Планшеты, смартфоны и другие мобильные устройства;
- Серверы и СХД;
- Периферийные устройства и МФУ;
- Оборудование ВКС.

Программное обеспечение:

- Бизнес-приложения (корпоративные ИС);
- Офисные приложения;
- Специализированное ПО (поддержка инфраструктуры);
- Системы безопасности;
- СУБД.

Сети и каналы связи:

- Телекоммуникационные и сетевые ПАК;
- Специализированное ПО (телекоммуникации);
- Коммутаторы;
- Маршрутизаторы;
- Межсетевые экраны (МСЭ);
- Пакетные брокеры;
- Каналы передачи данных;
- Средства криптографической защиты каналов связи.

По зонам ответственности ИТ-инфраструктура делится на сегменты:

- сегменты ИА;
- сегменты филиалов;

⁵ Проводится в рамках Программы проведения технического аудита ИТ-комплекса Группы РусГидро

- сегменты подконтрольных организаций.

Положения Технической политики по ИТ отражают:

- общие требования для всех компонент ИТ-инфраструктуры во всех сегментах (ИА, филиалы, подконтрольные организации);
- частные требования, специфичные для каждого компонента;
- требования для стыков между сегментами ИА, филиалов и подконтрольных организаций.

Основные компоненты АСТУ, АСУТП и СДТУ генерирующих и сетевых объектов Группы, а также структура, состав и требования к ним определяются в Технической политике Группы и Приложении 2 «Реестр типовых технических и программных средств, применяемых в ИТ-инфраструктуре Группы РусГидро».

3.2 Общие требования к ИТ-инфраструктуре

К ИТ-инфраструктуре применяются следующие общие требования:

- предоставлять технические ресурсы с согласованным уровнем качества для решения текущих задач;
- быть готовой предоставить в согласованном объеме и в предсказуемые сроки технические ресурсы для решения перспективных задач;
- обеспечивать требуемый уровень операционной непрерывности;
- обеспечивать требуемый уровень ИБ;
- соответствовать законодательным и нормативным требованиям.

Необходимо также учитывать основные ожидания от управления ИТ-инфраструктурой:

- функциональная полнота и достаточность;
- совокупная стоимость владения ИТ-инфраструктурой (ТСО), оптимально отвечающая потребностям Группы;
- прозрачность и экономическая обоснованность управленческих решений в области ИТ-инфраструктуры.

Структура и состав программно-технических комплексов АСУТП ГЭС, ГАЭС, ТЭС и требования к ним определяются в Технической политике Группы.

3.3 Принципы организации ИТ-инфраструктуры

- стремление к централизации управления ИТ-инфраструктурой;
- стремление к предоставлению ресурсов ИТ-инфраструктуры по сервисной модели;
- стандартизация подходов к управлению ИТ-инфраструктурой;
- стандартизация и оптимизация мер по обеспечению отказоустойчивости, непрерывности и доступности ИС Группы;
- приоритетность развития собственных компетенций в ИТ;

- приоритетность развития собственной ИТ-инфраструктуры для решения задач основных направлений бизнеса;
- концентрация вычислительных мощностей в ЦОД;
- виртуализация вычислительных ресурсов там, где это применимо;
- консолидация данных в ЦОД;
- стандартизация компонентов ИТ-инфраструктуры;
- стремление к максимально возможной независимости от производителей и поставщиков;
- стандартизация подходов к развитию ИС Группы;
- следование лучшим российским и международным практикам в области построения ИТ-инфраструктуры и тенденциям ее развития;
- стремление к непрерывному совершенствованию практик управления ИТ-инфраструктурой.

3.4 Технические требования к ИТ-инфраструктуре

Описание требований к технологической части ИТ-инфраструктуры разбито на 7 разделов:

- 1) Приложения:
 - Бизнес-приложения.
 - Инфраструктурные приложения.
 - ITSM приложения (приложения автоматизирующие процессы управления ИТ услугами).
 - Приложения безопасности.
 - MDM приложения, предназначенные для управления нормативно-справочной информацией.
 - ESB приложения⁶;
 - Приложения информационного обмена технологической информацией.
- 2) Системное ПО.
- 3) Организация сетей и каналов связи.
- 4) Инфраструктура ЦОД и серверных площадок.
- 5) Рабочие места пользователей.
- 6) Периферийные устройства печати.
- 7) СУБД.

В разделе «Бизнес-приложения» рассматриваются приложения, с которыми непосредственно контактирует конечный пользователь в ходе своей ежедневной работы. В разделе определяется итоговая схема размещения ПО в разрезе сегментов (ИА / филиал / подконтрольные организации) и общие требования к данному ПО.

⁶ Приложения, обеспечивающие централизованный и унифицированный событийно-ориентированный обмен сообщениями между различными ИС на принципах сервис-ориентированной архитектуры.

В разделе «Инфраструктурных приложений» приводятся требования к организации инфраструктурных сервисов.

В разделе «Системное ПО» приведены требования к ОС и программным платформам, как для серверов, так и для оборудования рабочих мест пользователей.

В разделе «Организация сетей и каналов связи» описываются типовые решения по организации внутренней локальной вычислительной сети для объектов всех сегментов (ИА / филиал / подконтрольные организации) и их взаимодействие, а также стык с сетями внешних операторов связи, связывающим объекты различных сегментов КСПД между собой.

В разделе «Инфраструктура ЦОД и серверных площадок» приведены требования к планированию и организации типовых ЦОД и серверных комнат внутри объектов всех уровней.

Перечень используемых / рекомендуемых технических решений информационно-технологической инфраструктуры ПАО «РусГидро» приведен в Приложении 2.

Перечень подготовлен с целью унификации проектируемых технических решений и в соответствии с требованиями законодательства Российской Федерации, в том числе в части импортозамещения, а также в соответствии со Стратегией ЦТ.

Перечень устанавливает требования для каждого класса ПО (в соответствии с приказом Минцифры России от 22.09.2020 № 486 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных») и для каждого вида радиоэлектронной продукции (оборудование) согласно коду радиоэлектронной продукции по Общероссийскому классификатору продукции по видам экономической деятельности ОК 034-2014 (КПЕС 2008) (ОКПД2).

Схематическое описание ИТ-инфраструктуры представлено на Рисунке 1:

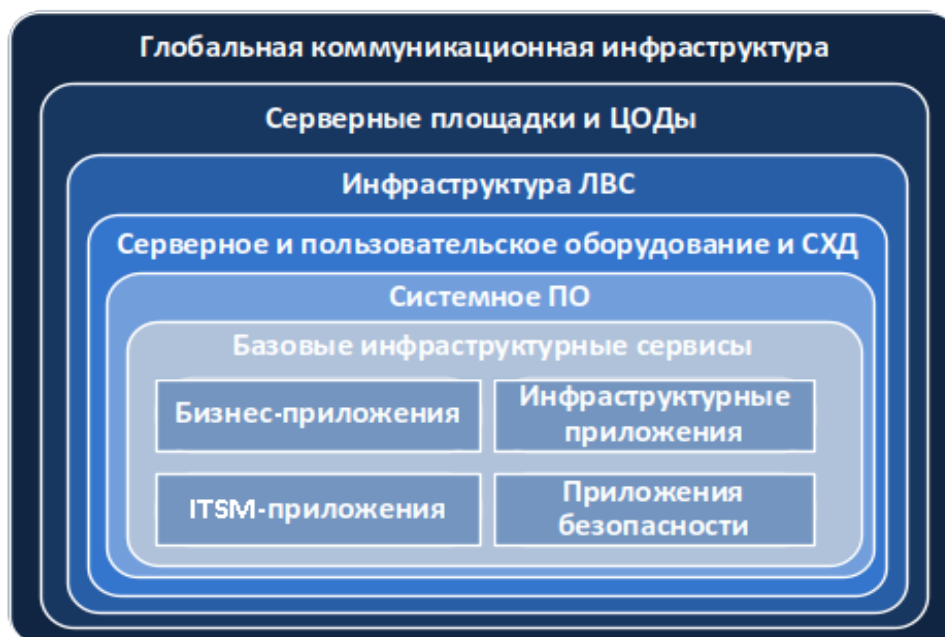


Рисунок 1 – Обобщенная архитектура ИТ-инфраструктуры Группы

3.4.1 Уровень приложений

ИТ-инфраструктура является технической базой, обеспечивающей функционирование приложений.

Приложения могут быть разделены на 7 основных групп:

1. Бизнес-приложения – приложения, автоматизирующие те или иные бизнес задачи. Именно они видны конечным пользователям и используются ими для выполнения их прямых обязанностей.

2. Инфраструктурные приложения – приложения, которые автоматизируют вспомогательные задачи конечных пользователей. В данный класс приложений в первую очередь относятся приложения, связанные с пользовательскими коммуникациями.

3. ITSM приложения – приложения, автоматизирующие внутренние процессы ИТ подразделения.

4. Приложения безопасности – приложения, автоматизирующие задачи, связанные с обеспечением ИБ.

5. MDM Приложения – предназначенные для управления нормативно-справочной информацией.

6. ESB Приложения – связующее ПО, обеспечивающее централизованный и унифицированный событийно-ориентированный обмен сообщениями между различными ИС на принципах сервис-ориентированной архитектуры.

7. Приложения информационного обмена технологической информацией – ПО, обеспечивающее передачу телеметрической информации

(параметры телеизмерений, телесигналы) из систем оперативно-технологического управления на объектах Группы в Ситуационно-аналитический центр Общества.

3.4.1.1 Бизнес-приложения (прикладное ПО)

Прикладное ПО (бизнес-приложения, Business application) является одной из основных компонент современной ИТ-инфраструктуры. С точки зрения конечного пользователя, именно прикладное ПО помогает решать бизнес-задачи.

В рамках Технической политики по ИТ рассматриваются требования к следующим основным характеристикам прикладного ПО:

- Функциональность – способность ПО максимально эффективно выполнять заявленные функции, с требуемыми характеристиками.
- Производительность (performance) – способность ПО обеспечивать сбор, обработку и хранение определенных объемов информации.
- Масштабируемость (scalability) – способность ПО корректно работать на малых и на больших системах с производительностью, которая увеличивается пропорционально вычислительной мощности системы (количества процессоров, дисковых массивов, серверов и т.д.), используемых для эксплуатации данного ПО.
- Способность к интеграции (OSI, Interoperability) – способность ПО к интеграции и взаимодействию с другими системами, в том числе с системами сторонних производителей, и эксплуатируемыми на других платформах.
- Зрелость (maturity) – наличие истории развития данного ПО (присутствие данного ПО на рынке в течение определенного промежутка времени, регулярный выпуск производителем новых версий и релизов) и объявленных производителем планов по его развитию.
- Надежность и отказоустойчивость (reliability and fault-tolerance) – способность ПО и систем, построенных на его базе, к бесперебойной и непрерывной работе, а в случае возникновения программно-аппаратных сбоев – способность к быстрому восстановлению работоспособности систем.
- Общая стоимость владения (ТСО) для ИС – складывается из затрат на начальное приобретение (разработку, доработку) данной ИС, ввод ее в эксплуатацию и расходов на эксплуатацию и сопровождение ИС в течение нормативного срока жизни ИС. Общая стоимость владения включает также затраты на: обновление ПО и оборудования; обучение персонала и обслуживание ИС; администрирование и техническую поддержку ИС.

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 распространенных (типовых) задач.

- Заказное ПО – ПО, разработанное по заказу для специфических задач Группы.

Существуют также гибридные типы ПО, совмещающие признаки обеих этих групп.

Общие требования к прикладному ПО

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

- Все виды приобретаемого ПО должны соответствовать требованиям импортозамещения и требованиям Приложения 2.

- ПО клиентских ПК должно быть функционально полным и обеспечивать выполнение как стандартных бизнес-процессов, так и специфических бизнес-задач данного пользователя. ПО должно иметь полнофункциональный web-интерфейс или «тонкий клиент», поддерживающий корректную работу с ОС и форматами документов, указанными в Приложении 1.

- ПО должно быть зрелым: производитель (поставщик) должен гарантировать поддержку, сопровождение данного ПО в течение всего нормативного срока жизни данного ПО.

- ПО в обязательном порядке должно функционировать в полном объеме на ПК с техническими характеристиками, указанными в Приложении 2 (Раздел 2.1 «Минимальные требования к характеристикам ПК»).

- ПО в обязательном порядке должно функционировать в полном объеме с системным ПО, указанным в Приложении 1 «Требования к типовому рабочему месту пользователя».

- Необходимо использовать производительное масштабируемое прикладное ПО, обеспечивающее гарантии непрерывности бизнес-процессов при росте объемов обрабатываемой и хранимой информации. Желательно, чтобы производитель прикладного ПО регулярно проводил объемное и нагрузочное тестирование своего ПО и предоставлял данные о результатах данного тестирования.

- Необходимо использовать только ПО, обладающее способностью к интеграции с другими системами и обладающее открытой архитектурой, т. е. поддерживающее стандарты OSI. При выборе прикладного ПО необходимо учитывать возможности его интеграции в существующую ИТ-инфраструктуру предприятия. При выборе прикладного ПО предпочтение необходимо отдавать платформам, имеющим открытый API.

- При выборе прикладного ПО преимущества должны получать платформы (системы) с подтвержденным положительным опытом использования в электроэнергетике.

- Для обеспечения критических бизнес-процессов и услуг использовать отказоустойчивое ПО в комбинации с резервированием серверной платформы и инфраструктуры ЦОД.

- Совокупная стоимость владения прикладным ПО в составе ИС, рассчитанная на весь нормативный срок эксплуатации ИС, должна служить основным критерием снижения расходов на эксплуатацию ИС при выборе того или иного поставщика и прикладного ПО.

- ПО должно быть надлежащим образом документировано.

- Использование специализированного ПО допускается только в тех структурных подразделениях, где существует необходимость создания новых документов с использованием данного специализированного ПО. Для просмотра и возможности печати существующих документов, созданных на специализированном ПО, следует использовать бесплатные и менее ресурсоемкие приложения.

- Корпоративным офисным пакетом прикладного ПО является AlterOffice. Требования к форматам электронных офисных документов определены в Приложении 1.

При приобретении и использовании прикладного ПО должны соблюдаться следующие требования:

- Приобретение только ПО из Реестра российского ПО.

- При использовании лицензируемого ПО должны быть получены и надлежащим образом зарегистрированы соответствующие лицензии.

- Приоритет к использованию имеет ПО производителей, зарекомендовавших себя на рынке в данном сегменте.

- Запрещается использование устаревших версий ПО, а также слишком новых, «незрелых» версий ПО.

Общие требования к заказному прикладному ПО

Заказное ПО рассматривается для приобретения только в случае отсутствия ПО в Реестре российского ПО.

При разработке заказного прикладного ПО должны соблюдаться следующие требования:

- Содержание и порядок выполнения работ, связанных с созданием безопасного ПО и устранением выявленных недостатков, в том числе уязвимостей, должны соответствовать требованиям ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

- Процесс проектирования, разработки и внедрения заказного ПО должен соответствовать требованиям Приложения 6.

- При выборе разработчика ПО основное внимание должно уделяться опыту предыдущей работы данного разработчика по созданию (проектированию, реализации и внедрению) подобных систем.

- Рекомендуется включать в процедуры приемки ПО передачу разработчиком исходных текстов программ и других объектов, необходимых для создания ПО, согласно требованиям ГОСТ Р ИСО/МЭК 12.207-99. Процедура приемки должна обязательно включать 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.

- Заказное ПО должно содержать в себе логотипы РусГидро. Использование логотипов разработчика допустимо только после согласования с ДИТ.

Общие требования к ландшафту распределенных ИС бизнес-приложений

- При разработке и внедрении корпоративных ИС предпочтение должно отдаваться системам, построенным по принципу централизованной архитектуры.

- При создании децентрализованных ИС механизм репликации должен использовать штатные средства СУБД, приложения и / или средства системного ПО.

- При создании децентрализованных ИС необходимо предусмотреть возможность восстановления отдельных компонентов систем при помощи репликации с территориально удаленных компонентов системы.

3.4.1.2 Инфраструктурные приложения

В данной части рассматриваются инфраструктурные приложения, а именно приложения, реализующие сервисы:

- электронной почты;
- мгновенных сообщений;
- персональных аудио- и видеокommunikаций;
- офисных приложений.

Общая концепция размещения инфраструктурных сервисов предполагает оптимальный баланс между централизованными и децентрализованными системами.

Основными преимуществами централизованных систем являются:

- Более низкая, по сравнению с децентрализованными системами, совокупная стоимость поддержки сервиса - за счет снижения задействованного персонала и снижения стоимости поддержания его квалификации;

- Более низкая совокупная стоимость построения сервиса – за счет снижения количества задействованного оборудования и лицензий на ПО;
- Более низкая совокупная стоимость модернизации как программной, так и аппаратной конфигурации – за счет снижения количества модернизируемых компонентов.

Основными недостатками централизованных систем являются:

- Более жесткие требования к каналам связи между серверными и клиентскими компонентами системы;
- Более жесткие требования к надежности системы – так как возрастает потенциальное влияние на пользователей в случае недоступности системы.

Исходя из данных предпосылок, требуется реализовывать сервисы централизованно на уровнях ИА и филиалов. В Группе действует Методика использования базовых информационных ресурсов процесса управления информационными технологиями, утвержденная приказом Общества от 11.01.2023 № 9. При этом вопрос администрирования сервиса может решаться отдельно от вопроса размещения компонентов системы. В большинстве случаев целесообразно централизовать администрирование сервиса. Подобная комбинация позволяет совместить преимущества централизованного и децентрализованного подходов.

3.4.1.3 ITSM приложения

Отдельно выделяют приложения, автоматизирующие процессы операционной деятельности ИТ-подразделения, основной задачей которых является совершенствование автоматизации ИТ-процессов, связанных с оказанием услуг, анализ этих процессов, контроль качества услуг и удовлетворенности клиентов. Приложения должны включать следующий функционал:

- управление инцидентами и запросами на обслуживание;
- управление изменениями;
- управление конфигурациями;
- управление проблемами;
- управление уровнем ИТ-услуг.

Данный функционал должен быть реализован в рамках корпоративной системы автоматизации СПП (КСА СПП) и выполнять следующие задачи:

- оперативная диспетчеризация запросов пользователей;
- обеспечение высокой доступности услуг за счет скорейшего устранения инцидентов;
- обеспечение сбора и систематизации данных о причинах возникновения инцидентов, выполненных мероприятиях в ходе устранения

инцидента и категоризации причин и зон ответственности при формировании хронологических отчетов по инцидентам;

- обеспечение высокого качества предоставления услуг за счет обеспечения обработки ЗНО в рамках заданных временных параметров;
- повышение скорости и качества проводимых изменений;
- снижение вероятности возникновения инцидентов, вызванных вносимыми изменениями;
- сбор и актуализация информации о составляющих частях ИТ-инфраструктуры с целью обеспечения данной информацией ИТ-специалистов;
- минимизация негативного влияния на ИТ-услуги инцидентов, вызванных ошибками в ИТ-инфраструктуре, и предотвращение повторения таких Инцидентов путем поиска причин инцидентов и устранения ошибок в ИТ-инфраструктуре;
- предоставление и поддержка единого источника целостной информации об ИТ-услугах в эксплуатации, а также о тех, что готовятся к вводу в эксплуатацию;
- обеспечение гарантий того, что ИТ-услуги предоставлены в соответствии с их целевыми значениями.

Платформа, на которой реализована КСА СПП, должна быть включена в Реестр российского ПО.

3.4.1.4 Приложения безопасности

Приложения безопасности реализуют меры обеспечения ИБ ИТ-инфраструктуры в соответствии с требованиями федерального законодательства и внутренними требованиями, утвержденными в Политике информационной безопасности.

Основные задачи приложений безопасности:

- обеспечение конфиденциальности, доступности и целостности информации, обрабатываемой в ИТ-инфраструктуре;
- выявление и ограничение потенциально опасных действий ПО и пользователей;
- выявление и реагирование на инциденты ИБ;
- централизованное управление средствами защиты информации.

Требования к приложениям безопасности приведены в п. 2.3 «Требования к применяемым техническим решениям» Политики информационной безопасности.

Все применяемые программно-технические решения должны быть включены в Реестр российского ПО.

3.4.1.5 MDM Приложения (НСИ)

В Обществе внедрена и применяется Единая система управления нормативно-справочной информацией (ЕСУ НСИ). При внедрении ИС необходимо использовать ЕСУ НСИ для ведения централизованных классификаторов и справочников (реестров). В общем случае основными критериями включения ресурса (классификатора и справочника) в состав фонда ЕСУ НСИ в качестве централизованного являются:

- ресурс используется двумя и более ИС;
- используется в двух и более бизнес-процессах;
- ресурс имеет высокую стоимость процедуры ведения (для поддержки вовлечено более одного структурного подразделения, процедура растянута во времени);
- ресурс имеет критически важное значение для бизнеса (например, справочник используется как один из основных срезов при подготовке отчетов по деятельности Общества или является основой для формирования ключевых показателей деятельности Общества и т.п.);
- нуждается в профессиональной (экспертной) обработке, ведении и сопровождении.

Использование локальных справочников Системы и требования к интеграции для их централизованного ведения в ЕСУ НСИ Заказчика определяются на этапе проектирования с учетом технической возможности и целесообразности.

3.4.1.6 ESB Приложения

Интеграция Системы с ИС Общества должна быть реализована с использованием интеграционной шины предприятия в соответствии с требованиями к интеграции с ЕИП (актуальную версию документа необходимо запросить у заказчика).

3.4.1.7 Приложения информационного обмена технологической информацией

При внедрении систем оперативно-технологического управления на объектах Группы осуществляется передача телеметрической информации (параметры телеизмерений, телесигналы) в Ситуационно-аналитический центр ПАО «РусГидро». Данная передача должна осуществляться с помощью системы однонаправленной передачи посредством использования информационных диодов. Передача данных осуществляется по протоколу МЭК 60870-5-104 или IEC 60870-6-503 (TASE.2 ICCP).

В качестве метамодели БД об электрической сети, обеспечивающей общую семантику при организации передачи технологической информации, используется объектно-ориентированная Общая Информационная Модель (Common Information Model – CIM) в соответствии с серией ГОСТ Р 58651

«Единая энергетическая система и изолированно работающие энергосистемы. Информационная модель электроэнергетики», которая может быть расширена дополнительными классами. Расширение канонической модели происходит только на уровне ПАО «РусГидро».

3.4.2 Системное ПО

Главным требованием, предъявляемым к системному ПО, является разработка данного ПО преимущественно отечественными разработчиками, выполнение им основных функций эффективного управления ресурсами и обеспечение удобного интерфейса для пользователей и смежных прикладных систем. Системное ПО должно поддерживать мультипрограммную обработку, виртуальную память, свопинг, многооконный графический интерфейс пользователя, достаточную частоту обновлений, а также выполнять другие необходимые функции и услуги. Кроме этих требований функциональной полноты к ОС предъявляются эксплуатационные требования:

- **Расширяемость.** Достигается за счет модульной структуры ОС, при которой программы строятся из набора отдельных модулей, взаимодействующих только через функциональный интерфейс.

- **Переносимость.** Должна обладать переносимостью от одного типа на аппаратную платформу другого типа, такое свойство ОС называют также многоплатформенностью.

- **Надежность и отказоустойчивость.** Система должна быть защищена как от внутренних, так и от внешних ошибок, сбоев и отказов. Ее действия должны быть всегда предсказуемыми, а приложения не должны иметь возможности наносить вред ОС. Надежность и отказоустойчивость ОС прежде всего определяются архитектурными решениями, положенными в ее основу, а также качеством ее реализации (отлаженностью кода).

- **Безопасность.** Современная ОС должна защищать данные и другие ресурсы вычислительной системы от несанкционированного доступа. Чтобы ОС обладала свойством безопасности, она должна как минимум иметь в своем составе средства аутентификации – определения легальности пользователей, авторизации – предоставления легальным пользователям дифференцированных прав доступа к ресурсам, аудита – фиксации всех «подозрительных» для безопасности системы событий. Свойство безопасности особенно важно для сетевых ОС. В таких ОС к задаче контроля доступа добавляется задача защиты данных, передаваемых по сети.

- **Производительность.** ОС должна обладать настолько хорошим быстродействием и временем реакции, насколько это позволяет аппаратная платформа. На производительность ОС влияет много факторов, среди которых основными являются архитектура ОС, многообразие функций, качество

программирования кода, возможность исполнения ОС на высокопроизводительной (многопроцессорной) платформе.

3.4.3 Требования к организации сетей и каналов связи

Конкретные технические требования изложены в Приложении 4 (Раздел 4.1. «Минимальные требования к корпоративной распределенной мультисервисной сети»).

3.4.3.1 Основные положения и подходы к организации мультисервисной сети

Сети передачи данных Группы должны быть построены как мультисервисные (одновременная передача по сети всех видов трафика: телефония, аудиоконференцсвязь, ВКС и передача данных, включая данные систем безопасности), с внедрением механизмов по обеспечению качества обслуживания (IEEE 802.1p/QoS).

Должно быть обеспечено соответствие следующим подходам к организации сетей передачи данных:

- распределенная корпоративная архитектура;
- высокая доступности и надежность сети;
- соответствие требованиям ИБ, принятым в Группе.

Сети передачи данных Группы должны обеспечивать высокую производительность, управляемость и легкое масштабирование сети.

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

- Трафик реального времени (телефонный, аудио и видео).
- Трафик передачи пользовательских данных.
- Технологический трафик (трафик управления оборудованием, трафик АСТУ/АСДУ).

Технологическому трафику должен быть присвоен наивысший приоритет при реализации механизмов по обеспечению качества обслуживания (IEEE 802.1p/QoS).

Трафику реального времени должен быть присвоен приоритет ниже технологического трафика при реализации механизмов по обеспечению качества обслуживания (IEEE 802.1p/QoS). Пропускная способность сети и активное сетевое оборудования должны обеспечивать высокое качество трафика реального времени.

Трафику пользовательских приложений должен быть присвоен приоритет ниже трафика реального времени.

Сетевое оборудование Группы должно быть настроено так, чтобы при возникновении аварийной ситуации ресурсы сети были распределены между технологическим трафиком, частью трафика реального времени и пользовательского трафика в том объеме, в котором это необходимо

для обеспечения бесперебойной работы основного технологического оборудования и обслуживающего его персонала.

3.4.3.2 Требования к архитектуре КСПД объекта

Архитектура КСПД объекта (КСПД ИА, КСПД филиала, КСПД подконтрольной организации) должна быть основана на следующих принципах:

- Трехуровневая иерархическая модель сети.
- Сеть должна строиться с учетом резервирования оборудования и каналов связи на каждом уровне (обладать избыточностью).
- Сеть должна иметь модуль доступа в Интернет (для КСПД ИА, филиалов и подконтрольных организаций).
- Модуль внешних подключений к выделенным каналам связи и VPN (для КСПД ИА, филиалов и подконтрольных организаций).
- Сеть должна иметь возможность разделения КСПД архитектурно на сегменты (поддерживать технологии сегментации, такие как VLAN, VRF и др.)
- Сеть должна архитектурно иметь возможность разделения КСПД разбиваться на ДМЗ.
- Сеть КСПД должна обеспечивать необходимую для бизнеса производительность и масштабируемость.
- Сеть должна обеспечивать качество обслуживания (QoS) для разных классов трафика.

Мультисервисная сеть должна проектироваться для всех офисных площадок Группы (далее – Объектов) исходя из трехуровневой иерархической модели сети, а именно:

- 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.

Архитектура мультисервисной сети также должна:

- поддерживать возможность масштабирования путем добавления новых сетевых модулей;
- обеспечивать высокий уровень надежности;
- минимизировать усилия и средства, необходимые для поиска и устранения неисправностей.

Интеллектуальные сервисы 3-го уровня модели OSI (в том числе протоколы динамической маршрутизации, такие как OSPF, IS-IS, BGP) должны обеспечивать сокращение области влияния на мультисервисную сеть Группы, затрагиваемой при возникновении различных аварийных ситуаций 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 аварийные ситуации с оборудованием и каналами связи на нижележащих уровнях не должны сказываться на функционировании верхних уровней.

- Транзитные резервные маршруты верхних уровней не должны проходить через низлежащие уровни.

- Классификация и приоритезация трафика должна обеспечиваться только на уровне доступа. Уровень распределения должен только агрегировать трафик. Уровень ядра сети должен, преимущественно, обеспечивать быструю коммутацию пакетов между подключенными к нему модулями мультисервисной сети.

- Время сходимости таблиц маршрутизации и их объем должны быть оптимизированы для каждого уровня посредством выбора оптимальной схемы резервирования.

- Устройства пользователей, периферийные устройства и внешние каналы связи не должны подсоединяться, иметь прямого подключения к модулю ядра сети, для этих целей необходимо использовать коммутаторы доступа, устройства МСЭ, дополнительные модули мультисервисной сети, для предотвращения лавинообразных перестроек таблиц маршрутизации, сокращения влияния широковещательного трафика и сокращения области влияния на всю мультисервисную сеть.

При модернизации или создании КСПД объекта (КСПД ИА, КСПД филиала, КСПД подконтрольной организации) архитектура сети передачи данных объекта должна основываться на целевых схемах сегментов сети передачи данных, принятых в Группе.

Надежность мультисервисной сети должна быть обеспечена при помощи выполнения следующих правил:

- Выход из строя любого устройства, входящего в состав любого из модулей мультисервисной сети, не должен приводить к отказу в работоспособности всего модуля.

- Любой модуль, входящий в состав мультисервисной сети, должен быть зарезервирован на уровне оборудования и каналов связи.

- Сеть должна быть спроектирована с учетом требований ИБ.

Отказоустойчивый сегмент сети – это сеть, обеспечивающая наименьшее влияние сбоев на наименьшее количество устройств. Она также построена так, чтобы быстро восстанавливаться при возникновении отказа. Эти сети используют несколько путей передачи данных от источника к месту назначения. Если один путь недоступен, сообщения можно немедленно отправить по другой линии связи. Наличие нескольких путей к месту назначения является резервированием.

Отказоустойчивый сегмент сети должен обеспечивать:

- Уровень доступа из отказоустойчивого сегмента ко всем ресурсам локальной сети должен оставаться неизменным, с точки зрения характеристик и качества;

- Доступ из локальной сети к ресурсам пользователей Отказоустойчивого сегмента может быть ограничен в соответствии с предъявляемыми требованиями к отказоустойчивому сегменту в рамках технического задания и требованиям Политики по информационной безопасности;

- Возможность быстрого отключения (изоляции) от остальной локальной сети при сохранении доступа к основным информационным ресурсам в соответствии с предъявляемыми требованиями специалистов по защите информации (перечень основных ресурсов определяется Соглашениями об уровне услуг).

Поддержка сетевой безопасности для Объектов I уровня обязательно, для Объектов II уровня, в случае, если того требует Политика информационной безопасности, должна быть реализована следующим образом:

- Выделить следующие ДМЗ с целью последующего применения отдельных политик ИБ к каждой зоне:

- для выхода в Интернет – разрешена только исходящая инициализация TCP сессий в сторону узлов сети Интернет.

- для общедоступных серверов и удаленного входа в корпоративную сеть – разрешена только входящая инициализация TCP сессий со стороны сети Интернет, доступ в локальную сеть ограничен.

- для внутренних защищенных серверов.

- Связь ДМЗ между собой должна проходить через оборудование, которое обеспечивает функциональность МСЭ/IDS/IPS на скорости физического канала.

- После пограничных маршрутизаторов сети, которые обеспечивают выход в Интернет и поддержку каналов VPN между ЦОД, должно стоять оборудование, которое обеспечивает функциональность МСЭ/IDS/IPS на скорости физического канала. Причем производитель оборудования / ПО этих МСЭ/IDS/IPS и МСЭ/IDS/IPS, соединяющих ДМЗ, должен быть разным. Данное требование гарантирует то, что при обнаружении уязвимости в оборудовании / ПО одного производителя, сеть останется защищенной оборудованием другого производителя.

- Помимо ДМЗ, на сети должны использоваться виртуальные локальные сети (VLAN).

- Доступ пользователей в интернет возможен только через прокси-сервер, расположенный в DMZ для выхода в интернет.

- Для выхода в интернет специализированных программ, таких как банк-клиент, допускается организация прямого выхода в интернет на фиксированные IP адреса по согласованию с ИБ.

- Все программные продукты, разрабатываемые для Группы, должны иметь механизм доступа к внешним ресурсам через прокси-сервер.

- Безопасность сети должна строиться в соответствии с Политикой информационной безопасности Группы.

Поддержка масштабируемости для всех Объектов должна быть обеспечена следующим образом:

- За счет правильного внедрения трехуровневой иерархической модели сети.

- За счет масштабируемости коммутаторов, которая должна достигаться за счет объединения в группы (стеки). При этом каждый коммутатор в стеке должен работать в двух режимах – как главный коммутатор стека и как процессор коммутации пакетов. Должна обеспечиваться отказоустойчивость системы по схемам N+1 или 2N. То есть, при выходе из строя одного из коммутаторов стека, независимо от выполняемой им функции, остальные будут продолжать выполнение своих функций без остановки работы всей мультисервисной сети.

- Рекомендуются использовать динамический протокол внутренней маршрутизации IS-IS или OSPF как обладающий хорошей масштабируемостью, быстрой сходимостью, учитывающий качество каналов связи и занимающий минимальную полосу канала.

Система IP-адресации сети для всех Объектов 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 иерархической структурой подразделений. Такое разделение позволяет производить агрегирование адресов, что приводит к уменьшению таблиц маршрутизации и упрощает управление сетью.

- Для осуществления аутентификации на уровне доступа для всех Объектов, 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. При попытке подключения неавторизованного устройства должно производиться отключение этого порта и уведомление системы управления сетью.

- Аутентификация административного доступа на Radius или Tacsacs 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.

Для обеспечения высокой доступности сети для Объектов I и Объектов II уровня необходимо обеспечить следующую функциональность:

- Поддержка виртуальных частных сетей (VLAN) на уровне алгоритма «связующего дерева» (Spanning Tree), т.е. должна быть возможность работы отдельного алгоритма Spanning Tree в каждой виртуальной сети для управления путями трафика с точностью до отдельной подсети и обеспечения простого механизма отказоустойчивости на канальном уровне. Также должна быть возможность управления параметром веса порта в алгоритме Spanning Tree для виртуальной сети на транковых портах для загрузки обоих каналов соединения Dual Homing (метод подключения устройств, обеспечивающий основное и резервное соединение).

- Поддержка дополнительных функций в коммутаторах для протокола Spanning Tree:

- поддержка множественных групп Spanning Tree в одной сети;
 - оптимизация алгоритма Spanning Tree для переключения на резервные каналы за время менее 5 секунд;
 - отсутствие задержки алгоритма Spanning Tree при включении пользовательского порта.

- 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 Объектов I и II уровня требуется наличие следующих возможностей:

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

Требования к точкам радиодоступа Wi-Fi:

- Точки радиодоступа Wi-Fi должны поддерживать семейство стандартов IEEE 802.11a/b/g/n/ac/ax Wave 1 и Wave 2.
- Необходимо обеспечить меры по повышению уровня безопасности сети за счет внедрения централизованной системы контроля сетевого доступа, поддерживающей протоколы RADIUS, TACACS+, IEEE 802.1X и технологии WPA/WPA2/WPA3/OWE. Использование конкретных протоколов, обеспечивающих повышение уровня безопасности сети, должно быть определено на этапе проектирования.

3.4.3.3 Требования к системам телефонии, аудио-конференцсвязи и ВКС

Инфраструктура телефонии, аудио-конференцсвязи и ВКС должна соответствовать следующим требованиям:

- Передача сигнального и RTP трафика должна осуществляется по IP-сети.
- Используемая сеть передачи данных должна иметь достаточную для передачи сигнального и медиа трафика пропускную полосу канала.
- Используемая сеть передачи данных должна обеспечивать потерю пакетов (packet loss) не более 1%, задержки (delay) не более 150 мс (от источника до получателя), вариацию задержки (jitter) не более 20 мс.
- Используемая сеть передачи данных должна использовать механизмы обеспечения гарантированного качества обслуживания (QoS) на участках, задействованных для прохождения сигнального и медиа трафика.

- При пакетной передаче за эталон качества речи должен быть принят уровень качества, равный 4 баллам по шкале MOS/PAMS (Mean Opinion Score, субъективный метод оценки согласно рекомендации, Р.800).

- В качестве базового сигнального протокола для межстанционного и терминального взаимодействия должен использоваться Session Initiation Protocol (SIP).

- Для сокращения издержек на обслуживание системы необходимо использовать моновендорное решение телефонии, аудио-конференцсвязи и ВКС.

- Должна быть произведена централизация ресурсов телефонии с выделением центрального кластера обработки вызовов для всей Группы.

- Для телефонии должно быть использовано отказоустойчивое решение, которое бы обеспечивало отказоустойчивое решение как на уровне центрального кластера обработки вызовов, так и на уровне офисов Группы.

- Центральные кластеры обработки вызовов должны размещаться в надежных ЦОД с высоким уровнем доступности.

- Решения телефонии, аудио-конференцсвязи и ВКС должны быть интегрированы в единую систему.

- В рамках Группы должен быть план телефонной нумерации, согласованный с системой ВКС.

- Должна быть обеспечена унификация и централизация стыков с ТфОП с дальнейшей реализацией технологии LCR для сокращения расходов на междугороднюю и международную связь.

- Система должна поддерживать Web-конференции.

- Должна быть обеспечена возможность передачи динамических статусов, текстовых сообщений и мультимедийных файлов между абонентами Системы.

- Система должна обеспечивать возможность мониторинга доступности оборудования.

Допускается использование традиционной аналоговой телефонии в следующих случаях:

- Унаследованные существующие телефонные станции.

Требования к клиентскому обеспечению телефонии, аудио-конференцсвязи и ВКС:

- Каждое рабочее место должно быть обеспечено терминальным устройством, телефонным аппаратом или программным клиентом. В частных случаях работнику Группы может быть дополнительно предоставлен кодек для проведения сеансов ВКС.

- Клиентское обеспечение должно работать по протоколу SIP.

- Программные клиенты должны иметь возможность доступа к сервисам телефонии, аудио-конференцсвязи и ВКС и сервисам унифицированных коммуникаций как в пределах среды передачи данных Группы, так и из публичной сети.

- Клиентское оборудование должно быть совместимо с инфраструктурным оборудованием, что должно быть подтверждено официальными документами от производителя инфраструктурного оборудования.

3.4.3.4 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 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.

Во всем активном оборудовании сети Объектов I и II уровня должны быть средства мониторинга политики качества обслуживания и безопасности, планирования сети и сервисов:

- Обеспечение возможности сбора статистики RMON с точностью до порта сети для анализа производительности сети.
- Обеспечение возможности обнаружения изменения качества обслуживания (QoS).
- Обеспечение возможности перенаправления трафика отдельных портов, групп портов и виртуальных портов на анализатор протоколов для детального анализа.
- Обеспечение возможности углубленного анализа потоков сетевого и транспортного уровней при помощи протокола NetFlow.
- Обеспечение возможности расширенного мониторинга событий в реальном времени для расширения возможностей диагностики, помимо внешних анализаторов.
- Обеспечение возможности сбора и сохранения информации о существенных сетевых событиях, включая изменения конфигураций устройств, изменения топологии, программные и аппаратные ошибки.
- Обеспечение возможности доступа к интерфейсу управления устройством и отчетам через стандартный WEB-браузер, если такая возможность реализована производителем оборудования.
- Обеспечение возможности автоматической конфигурации Fast/Gigabit Ethernet портов, виртуальных сетей, транков VLAN, при условии отсутствия рисков для последующей эксплуатации оборудования и ИБ.
- Обеспечение возможности автоматического распознавания топологии сети посредством агентов распознавания топологии.
- В целях обеспечения производительности локальной сети, ее масштабируемости, удовлетворения требованиям ИБ и обеспечения качества обслуживания мультисервисного трафика запрещается использовать концентраторы (хабы). Вместо них должны использовать только коммутаторы.

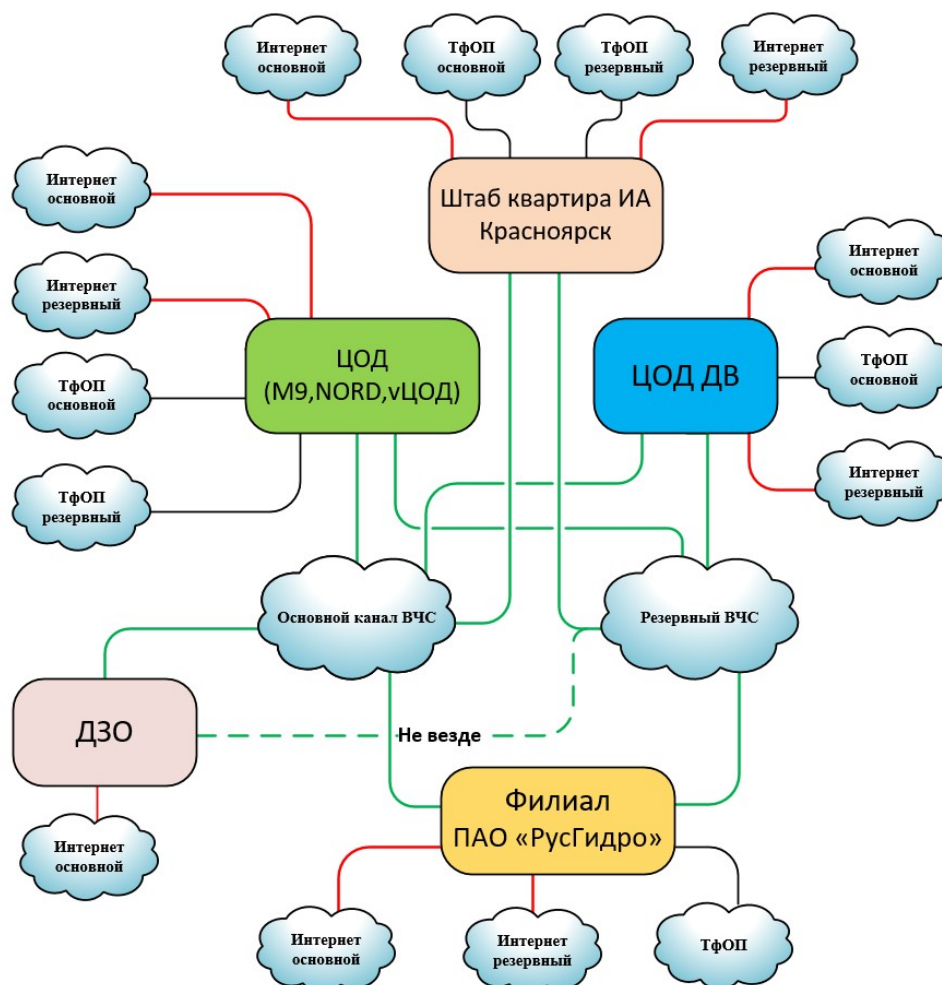
Все активное оборудование должно иметь конструктивное 19” стоечное исполнение.

3.4.3.5 Схема подключения ПАО «РусГидро» к внешним каналам и услугам связи

Структурная схема организации связи ИА и филиалов приведена на Рисунке 2.

2

Рисунок



Структурная схема связи ИА и филиалов ПАО «РусГидро»

Согласно данной схеме:

- Сеть связи ПАО «РусГидро», объединяющая различные сегменты и ЛВС ИА, филиалов и ПО построена на основной и резервной виртуальных частных сетях (L3 IP VPN) на базе MPLS сетей крупнейших магистральных российских операторов;
- Основная ВЧС ПАО «РусГидро» построена на базе MPLS сети крупнейшего российского магистрального оператора связи ПАО «Ростелеком», который обеспечивает наибольший охват территории России собственными оптическими сетями связи и обеспечивает необходимые технические характеристики ВЧС;
- Резервная ВЧС ПАО «РусГидро» построена на базе MPLS сети крупнейшего российского магистрального оператора связи ПАО «Мегафон», который наряду ПАО «Ростелеком» обеспечивает охват территории России собственными оптическими сетями связи и обеспечивает необходимые технические характеристики ВЧС;

- Подключение филиалов осуществляется к основной и резервной ВЧС РусГидро, подключение должно быть организовано по ВОЛС, могут использоваться как собственные ВОЛС, так и арендованные;

- Оказываемая услуга подключения к ВЧС РусГидро должна удовлетворять следующим требованиям:

- Доступность средств связи оператора, задействованных в оказании услуги ВЧС, должна составлять не менее 99,7% в месяц.

- Эксплуатационные характеристики услуги между узлами связи собственной сети оператора (без учета линий доступа), приведены в Таблице 1.

Класс Трафика	Процент потерянных пакетов (PE-to-PE) в среднем за месяц	Односторонние сетевые задержки на наземных каналах (PE-to-PE) в среднем за месяц	Колебания сетевой задержки на наземных каналах (PE-to-PE) (джиттер)
Business Priority	не более 0,25%	не более 75 мсек	не более 50 мсек
Business Critical	не более 0,5%	не более 100 мсек	не нормируется
Normal Priority	не более 1%	не более 150 мсек	не нормируется

Таблица 1 – Эксплуатационные характеристики IP VPN оператора

В Таблице указаны средние за месяц параметры, относящиеся к участку от входящего PE маршрутизатора до исходящего PE маршрутизатора внутри сети MPLS оператора. Данные цифры не учитывают возможных дополнительных задержек, джиттера и потерь пакетов на линии доступа (на участке PE-CE);

- Оператор должен иметь собственную службу поддержки, работающую 24x7, 365/366 дней в году. Прием заявок о неисправностях должен быть организован как по телефону, так и по электронной почте с присвоением номера заявки.

- Доступ корпоративных пользователей ИА в публичную сеть Интернет осуществляется централизованно, используя услугу доступа в Интернет крупнейших магистральных поставщиков услуги (не менее двух федеральных операторов). При этом на подключении должна быть организована защита от DDoS атак.

- Доступ в Интернет организуется на каждом филиале, подключение должно быть организовано к сетям крупнейших магистральных поставщиков услуги (не менее двух федеральных операторов). Среднемесячная доступность опорных сетей и средств связи, находящихся в зоне ответственности исполнителя и

задействованных в оказании услуги, должна быть не ниже 99,7%. Параметры качества передачи данных в зоне ответственности исполнителя по каналу связи между оборудованием ИА (филиала) и ресурсами Интернет, непосредственно подключенными к IP сети оператора, должны соответствовать следующим требованиям:

- процент потерянных пакетов в течение часа – не более 1,0 %;
- среднемесячная задержка передачи пакетов – не более 200 мс.

3.4.3.6 Схема подключения подконтрольных организаций

Подключение сетей подконтрольных организаций должно быть организовано согласно разделу 7.2 Технической политики по ИТ. Подключение Тип 1 должно быть реализовано к основной ВЧС РусГидро.

Подключение должно соответствовать следующим требованиям:

- Доступность средств связи оператора, задействованных в оказании услуги ВЧС, должна составлять не менее 99,7% в месяц.
- Эксплуатационные характеристики услуги между узлами связи собственной сети оператора (без учета линий доступа), приведены в Таблице 1.

В Таблице указаны средние за месяц параметры, относящиеся к участку от входящего PE маршрутизатора до исходящего PE маршрутизатора внутри сети MPLS оператора. Данные цифры не учитывают возможных дополнительных задержек, джиттера и потерь пакетов на линии доступа (на участке PE-CE).

Оператор должен иметь собственную службу поддержки, работающую 24x7, 365/366 дней в году. Прием заявок о неисправностях должен быть организован как по телефону, так и по электронной почте, с присвоением номера заявки.

Схема подключения подконтрольных организаций ПАО «РусГидро» к КСПД ПАО «РусГидро» (тип 1 и 2) приведена на рисунке 3.

Рисунок 3 – Структурная схема организации подключения ПО к КСПД РусГидро

3.4.4 Инфраструктура ЦОД и серверных площадок

Данный раздел рассматривает технические требования к системам хранения и резервного копирования данных. Конкретные технические требования изложены в Приложении 5 «Минимальные требования к инфраструктуре центров обработки данных».

3.4.4.1 Общие требования

Общие требования к системам обработки, хранения и резервного копирования данных для всех ЦОД и технологических (серверных) площадок должны учитывать следующие параметры:

- Производительность: производительность оборудования должна складываться из производительности основных подсистем. Необходимо отслеживать нагрузку основных подсистем, выявлять узкие места и наращивать по мере необходимости производительность путем установки дополнительных модулей. В рабочем режиме сервер должен иметь загрузку основных ресурсов не более чем на 75%, чтобы выдерживать пиковую нагрузку в случае необходимости;

- Виртуализация;
- Масштабируемость;
- Надежность (возможность сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения);

- Ремонтопригодность (время, в течение которого работоспособность может быть восстановлена);

- 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.

В целях обеспечения унифицированной, масштабируемой, отказоустойчивой и экономически эффективной инфраструктуры, соответствующей современным технологическим стандартам и позволяющей обеспечивать растущие потребности Группы в вычислительных мощностях необходимо обеспечить развитие инфраструктуры ключевых ЦОД ПАО «РусГидро» в Москве (ЦОД ПАО «РусГидро» и ООО «РусГидро ИТ сервис»), Красноярском крае (ЦОД ПАО «РусГидро») и Владивостоке (ЦОД ООО «РусГидро ИТ сервис»), реализовать подход к управлению вычислительными ресурсами, предполагающий географическую консолидацию требуемых мощностей в них, а также обеспечивающий возможность финансово эффективной передачи вычислительных мощностей в аренду подконтрольным организациям.

3.4.4.2 Серверы в структуре ЦОД

Выбор серверного оборудования должен зависеть от тех задач (приложений), которые они будут решать:

- Серверы должны позволять постепенно масштабировать ресурсы и увеличивать производительность.

- Серверы должны иметь возможность использования различных ОС (по отдельности или одновременно в составе виртуальных машин).

- Серверы должны иметь встроенные средства удаленного управления.

- При выборе серверов нужно отдавать предпочтение платформам, поддерживающим не менее двух процессоров с многоядерной архитектурой.

- Использовать технологии виртуализации, которые позволяют разделять ресурсы высокопроизводительного сервера между приложениями, которые требуют меньших ресурсов для своей реализации, на аппаратном и программных уровнях.

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

Серверы должны обеспечивать:

- Высокую скорость обработки данных при малых затратах на обслуживание.

- Простоту управления для быстрого изменения и перераспределения ресурсов в зависимости от потребностей.

- Высокую надежность функционирования и непрерывность доступа к информации.

- Интеграцию их в существующую инфраструктуру Группы и совместимую работу с уже использующимися системами.

Высокопроизводительные серверные платформы должны иметь ряд встроенных функций обеспечения 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;

- расширенная система обнаружения неисправностей с выделенным сервисным процессором и шиной при наличии удаленной консоли.

Во всех серверных решениях должно быть уделено большое внимание предотвращению возможных сбоев. Для ЦОД и технологических (серверных) площадок 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 произошедшем 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 сервере, рационально используя его вычислительные ресурсы и память.

ПО, реализующее технологию виртуализации серверов, должно иметь 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.
 - Использовать системы, поддерживающие динамическое выделение ресурсов для приложений в моменты пиковых нагрузок в рамках заданных правил «Capacity-on-demand» (Capacity-on-demand – технология, позволяющая пользоваться масштабируемой надежно защищённой и устойчивой рабочей средой, построенной на принципах «по требованию», а также пользоваться широким спектром технологий для оптимального удовлетворения потребностей разнообразных приложений).
- 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. Должна гарантироваться посредством представления виртуальной аппаратуры приложениям и ОС как стандартной.

В ЦОД и на технологических (серверных) площадках необходимо 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.

Если для технологических площадок не используются сети SAN, то должны быть использованы устройства NAS с функциональностью виртуализации.

Таким образом, для ЦОД и технологических площадок должна быть внедрена технология виртуализации на всех уровнях ИТ-инфраструктуры:

- Локальная сеть – технология VLAN.
- Серверы – технология виртуализации серверов.
- Сети и СХД – технология виртуализации SAN или NAS.

ОС для обслуживания серверных приложений и промышленных систем должны:

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

3.4.4.3 Сети и системы хранения данных (СХД), электронные архивы

Главными приоритетами в развитии СХД должны быть:

- наращивание емкости;
- 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 хранения данных:

1. Оперативный уровень – данные с этого уровня достаточно часто используются пользователями. Соответственно оборудование должно быть достаточно быстродействующим и иметь высокую степень доступности.

2. Уровень долгосрочного хранения данных – постоянное место хранения данных, которое помимо производительности должно обладать надежностью.

3. 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. Электронный архив должен создаваться на не перезаписываемых оптических носителях информации WORM – “Write Once, Read Many”). Данное устройство должно иметь интерфейс Fibre Channel и подсоединяться к сети SAN.

4. Уровень резервного копирования данных.

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 бизнес-критичности информации, непосредственно с рабочих ПК пользователей.

СХД должна иметь:

- единые средства для репликации данных, которые должны перемещать данные между уровнями СХД, 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 СХД 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.

В настоящее время существуют следующие технологии хранения данных:

- концепция NAS-устройства хранения, подключаемого непосредственно к локальной или глобальной сети, ориентированная на файловые сервисы;
- концепция сети хранения данных (SAN), ориентированная на обработку блоков данных, хранящихся в базах данных;
- интерфейс iSCSI, с помощью которого можно создавать сети хранения данных без использования дорогостоящего оптоволоконного оборудования.
- объектное хранилище S3 (Simple Storage Service), при котором данные хранятся в виде объектов (файлов) вместе с метаданными и уникальным идентификатором в контейнерах.

В ЦОД должна быть внедрена технология SAN как наиболее перспективная, развивающаяся и удовлетворяющая всем необходимым

требованиям. Для технологических площадок также требуется технология SAN, но допускается возможность развертывания устройств с использованием технологии iSCSI 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 освободиться от задач управления ресурсами и их хранения.

При внедрении технологии SAN должны быть обеспечены:

- 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: СХД 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. СХД должна позволять создавать несколько виртуальных портов на одном физическом порте Fibre Channel, а также управлять этими портами.
- 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 (LUN) и томами для распространения расширенных сервисов управления информацией и хранением данных на модульные СХД, 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 СХД.

Из всех возможных архитектур построения сети SAN необходимо использовать коммутаторы со способом объединения коммутаторов «Центр-Периферия» (Core-Edge) как наиболее оптимальный с точки зрения производительности, масштабируемости и надежности.

При построении SAN в ЦОД на коммутаторах (за исключением класса Director) требуется создавать две независимые Fabric (такая конструкция называется Dual fabric). Dual fabric позволяет избежать единой точки отказа в SAN, обеспечивая очень высокий уровень надежности и отказоустойчивости. Кроме того, изменения конфигурации, регламентные работы (например, установка нового firmware) на 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.

Требуется выбирать оборудование, поддерживающее Fibre Channel с пропускной способностью 16 Гбит/с. В случае обеспечения более высокой скорости передачи данных по магистральным каналам и при отсутствии возможности ее увеличения за счет использования транкинга (trunking) допускается использовать для этих целей оборудование с пропускной способностью 40 Гбит/с.

В целях обеспечения унифицированной, масштабируемой, отказоустойчивой и экономически эффективной платформы хранения неструктурированных данных, соответствующей современным технологическим стандартам и позволяющей поддерживать текущие и перспективные ИС, сервисы аналитики, резервное копирование и

архивирование в ЦОД ПАО «РусГидро» необходимо обеспечить внедрение S3-совместимого объектного хранилища, как основного компонента платформы хранения неструктурированных данных.

При внедрении S3-совместимого объектного хранилища необходимо:

- стандартизировать использование S3-интерфейса при интеграции новых систем и сервисов для унификации способов доступа к данным и снижения операционных затрат;
- исключить дублирование функциональности и децентрализованное размещение объектных хранилищ путём предоставления единого централизованного S3-сервиса.

Единое объектное хранилище предоставляется как центральный сервис инфраструктуры ИТ, доступный всем подразделениям и проектам. Все потребности в объектном хранении должны удовлетворяться исключительно через данный централизованный сервис, использование локальных или автономных решений, реализующих S3-совместимый интерфейс (например, MinIO, Ceph RGW и другие) вне состава утверждённой ИТ-инфраструктуры запрещено (исключения возможны только по согласованию с Управлением развития инфраструктуры и при наличии технико-экономического обоснования, подтверждающего невозможность использования центрального сервиса).

3.4.4.4 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 требуемых степеней надежности и доступности системы 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.

Для повышения гибкости управления, автоматизации развертывания и масштабирования приложений, рекомендуется рассмотреть использование системы оркестрации контейнеров, такой как Kubernetes, которая обеспечивает автоматическое управление жизненным циклом приложений, мониторинг состояния компонентов, автоматическое восстановление после сбоев, а также интеграцию с различными кластерными конфигурациями для повышения отказоустойчивости и доступности приложений.

Для повышения гибкости управления, автоматизации развертывания и масштабирования приложений, рекомендуется использовать системы оркестрации контейнеров, такие как Kubernetes.

В целях обеспечения технологической независимости, соответствия политике импортозамещения, а также для унификации инфраструктурных решений, повышения безопасности и снижения операционных издержек, запрещается самостоятельное развёртывание, использование сторонних или локальных инсталляций Kubernetes, а также эксплуатация неконтролируемых кластеров. Все ИС и проекты обязаны взаимодействовать с платформой контейнерной оркестрации исключительно через единый интерфейс, предоставляемый ИТ-службой, как сервис и соблюдать установленные стандарты разработки, деплоя и эксплуатации приложений.

3.4.4.5 Резервное копирование данных

Резервное копирование данных ИС для ЦОД и технологических площадок должно осуществляться в соответствии с методикой резервного копирования, которая должна содержать описание процессов резервного копирования различных ИС и регламентов их выполнения.

Для резервного копирования данных должны выполняться процедуры:

- Локальное резервное копирование данных для их быстрого восстановления.
- Удаленное резервное копирование данных для обеспечения катастрофоустойчивости.

3.4.4.6 Локальное резервное копирование данных

Локальное резервное копирование данных должно осуществляться на мобильный носитель с сервера резервного копирования. Сервер резервного копирования должен служить также промежуточным оборудованием, которое должно уменьшать окно резервного копирования посредством предварительного копирования данных на систему быстрых дисков SAS/SATA/FATA, которая должна располагаться в сети SAN.

Также в сети SAN для ЦОД должно быть организовано, автоматическое блочное резервное копирование данных на другое физическое устройство, нежели исходное (data mirroring).

Должен быть принят и утвержден порядок резервного копирования, в котором должны быть регламентированы периоды и окна резервного копирования для полного и инкрементного резервного копирования. Способы резервного копирования следует выбирать в зависимости от следующих параметров:

- RTO – целевое время восстановления, т.е. время, необходимое для восстановления данных.

- RPO – целевая точка восстановления, т.е. момент, до которого необходимо восстановить данные или, другими словами, это фактически допустимый объем потерянных данных.

При планировании процессов резервного копирования следует учесть наличие в инфраструктуре различных ОС и приложений, а также место хранения данных, и выбрать единое ПО для обеспечения резервного копирования. Необходимо также учесть возможности интеграции этого ПО с имеющимися СХД и используемыми приложениями, данные которых подлежат резервному копированию.

Для реализации резервного копирования данных различных ИС требуется составить единый план резервного копирования, в котором отразить виды выполняемого резервного копирования, их периодичность, объем резервируемых данных и продолжительность выполнения резервного копирования, а также хронологическую последовательность выполнения процессов резервного копирования. Также следует предусмотреть осуществление резервного копирования системных данных для восстановления ОС серверов, и, в случае необходимости, клиентских рабочих станций.

3.4.4.7 Обеспечение катастрофоустойчивости

Катастрофоустойчивость должна обеспечиваться за счет копирования данных на территориально-удаленный ЦОД (далее – резервный ЦОД). Степень удаленности резервного ЦОД должна определяться исходя из тех угроз, от которых планируется защитить данные. Данный перечень угроз должен быть сформулирован в Плане обеспечения непрерывности бизнеса, если таковой имеется. Возможны 2 основных стратегии использования распределенных ЦОД – «активный / активный», когда инфраструктурные приложения и сервисы распределены между площадками, и пользователи работают с ближайшим ЦОД, либо «активный / пассивный», при которой приложения централизованы, и пользователи работают с основным узлом. В случае отказа системы, нагрузка автоматически переключается на резервный ЦОД. Возможность применения той или иной стратегии зависит от приложения.

С целью обеспечения катастрофоустойчивости все бизнес-важные данные или их резервные копии (в зависимости от значения параметра точки восстановления данных RPO) требуется с установленной периодичностью копировать (реплицировать) на резервный ЦОД.

Обеспечение катастрофоустойчивости должно осуществляться в соответствии с методикой восстановления ИС, которая должна содержать

описание процессов восстановления различных ИС и регламентов их выполнения.

Вне зависимости от принятой модели удаленной репликации данных должен быть установлен порядок хранения и обращения с резервными копиями данных, где бы они ни находились. Установленный порядок должен гарантировать сохранность резервных копий данных, а также их высокую доступность при возникновении необходимости восстановления данных.

По принципу хранения и использования необходимо выделить два типа данных:

- Неструктурированные данные (файлы).
- Структурированные данные, которые хранятся в СУБД.

Для репликации неструктурированных данных необходимо использовать специализированное ПО – агенты резервного копирования. Для репликации структурированных данных необходимо пользоваться средствами СУБД или ПО, совместимого с данной СУБД.

Вид репликации (полный или инкрементальный) необходимо выбрать в зависимости от объема данных, ширины канала связи (времени репликации), критичности времени восстановления данных при аварии. Рекомендуемый порядок может быть следующим: ежедневное инкрементальное копирование данных и еженедельное полное копирование данных. Указанный порядок должен быть зафиксирован в документах по обеспечению непрерывности бизнеса и восстановлению после аварий.

3.4.4.8 Требования к помещениям и инженерным системам

Серверные помещения ЦОД и технологических площадок должны удовлетворять следующим общим требованиям:

- Запрещается размещать серверные помещения в подвалах и иных помещениях, оснащенных большим количеством инженерных сооружений, которые представляют потенциальную опасность для оборудования.

- 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.
- Защищать ценное оборудование и данные.
- Физический доступ к серверной комнате должны иметь только уполномоченные работники 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;
- системой регулирования чистоты и влажности воздуха;
- серверными и телекоммуникационными шкафами, стойками;
- системами контроля состояния внутренней среды (система раннего дымообнаружения, датчики доступа, датчики физического состояния оборудования, датчики температуры/влажности)
- системой видеонаблюдения;

- В серверной комнате необходимо иметь фальшпол. Фальшпол является необходимым компонентом, т.к. под него нагнетается охлажденный воздух, под ним располагаются кабели электроснабжения и слаботочная инфраструктура. Рекомендуется фальшпол из МДФ-плиток на металлической основе с ламинированным покрытием, размером 600 x 600 мм. Высота над уровнем пола – от 100 до 800 мм, для серверных помещений наиболее оптимально 350 – 500 мм.

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

- При принятии решения по выбору помещения для размещения ЦОД рекомендуется рассматривать возможность аренды площадей на внешних коммерческих технологических площадках, инженерные системы которых удовлетворяют требованиям Технической политики по ИТ.

3.4.4.9 Структурированные кабельные системы (СКС)

СКС всех ЦОД, к которым относится вертикальная и горизонтальная разводка кабелей, шкафы и кроссовое оборудование, должны удовлетворять следующим общим требованиям:

- СКС должна включать в себя горизонтальную и вертикальную разводку. Горизонтальная разводка – кабель 6 категории, вертикальная разводка должна быть оптической и должна позволять состыковывать коммутаторы доступа с коммутаторами уровня распределения (а также, соответственно, коммутаторы уровня распределения с коммутаторами уровня ядра) по 10GigabitEthernet или 40GigabitEthernet.

- На СКС должна предоставляться гарантия производителя на работоспособность на срок не менее 15 лет. Подрядчик должен быть сертифицирован производителем и должен иметь поверенное измерительное оборудование. При проведении приемочных испытаний подрядчик должен предоставить протоколы тестирования СКС на соответствие установленным нормам.

- Необходимо, чтобы каждый шкаф имел высоту не менее 42U (стандартный телекоммуникационный шкаф), а также имел производительную систему вентиляции. При сверхплотном размещении большого количества шкафов с оборудованием, например, необходимо отдельно просчитывать вопросы, связанные с вентиляцией. В частности, необходима организация холодных и горячих коридоров.

3.4.4.10 Электроснабжение

Общие требования к системе электроснабжения ЦОД и технологических площадок:

- В серверное помещение электропитание должно подаваться от главного щита здания, где бы данное помещение ни находилось. Также от главного щита здания проводится кабель заземления. 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 необходимо после автоматов в поэтажных щитах устанавливать устройства защитного отключения (УЗО) согласно действующим нормам.

- Систему электроснабжения для ЦОД следует организовывать от 2-х территориально разнесенных трансформаторных подстанций. Кабельные линии должны идти независимыми маршрутами. Требуется использовать автоматы выбора резерва (ABP), осуществляющие выбор и переключение между основными и резервными линиями.

- Для технологических площадок необходимо использовать дизель-генераторные электростанции (ДЭС). В схеме электроснабжения они должны располагаться после вводов кабелей электропитания в здание. 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.

- Должны быть установлены после ввода кабелей электропитания в здание или после ДЭС, при ее наличии, централизованные источники бесперебойного питания (ИБП) типа online. Это обязательное требование, так как

наиболее опасными являются короткие скачки напряжения, длительностью 2 – 3 секунды. Кроме этого, существуют и такие негативные факторы, наносящие существенный ущерб, как превышение напряжения, изменение частоты, гармоники, нарушение заземления, межфазовый потенциал и т.п. Допускается не устанавливать к ИБП аккумуляторных батарей, если это экономически нецелесообразно и предусмотрены другие ИБП (персональные или групповые) с аккумуляторными батареями, которые обеспечат требуемое время удержания работоспособности системы.

Требования к электроснабжению шкафов:

- К каждому шкафу должно быть подведено питающее напряжение $220 \pm 10\%$ в переменные тока через индивидуальный автоматический выключатель.
- 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 4 кВт на шкаф. Если в шкафах предполагается устанавливать blade-серверы или иное оборудование, имеющее повышенное энергопотребление, то потребляемая мощность должна быть скорректирована согласно документации производителя.

3.4.4.11 Кондиционирование и система холодоснабжения

Требования к системам кондиционирования и холодоснабжения:

- Серверные помещения должны быть оборудованы промышленной системой кондиционирования и вентиляции (системы холодоснабжения) согласно СНИП 41-01-2003.
- 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 обязательно, а для технологических площадок необходимо осуществлять по схеме с N+1 (с одним запасным кондиционером). Все кондиционеры должны быть подключены к единой системе управления. ПО должно позволять осуществлять ротацию запасного кондиционера, что позволяет более эффективно расходовать ресурс системы холодоснабжения в целом.
- Для ЦОД необходимо организовывать приток свежего воздуха с улицы, так как воздух, постоянно циркулирующий через компьютерные шкафы и кондиционеры, «выгорает» и требует обновления. Приток необходимо осуществлять через специальную установку, нагревающую и осушающую уличный воздух. Кроме того, она должна создавать внутри помещения дополнительное давление, что препятствует проникновению внутрь пыли.

- Для увлажнения воздуха 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.

3.4.4.12 Системы раннего обнаружения пожара и пожаротушения

Требования к системе раннего обнаружения пожара и газового пожаротушения:

- 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 нагреваемых 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.

- Необходимо 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.

3.4.4.13 Комплексные системы безопасности

Комплексные системы безопасности должны состоять из:

- системы видеонаблюдения;
- системы разграничения физического доступа;
- технические средства охраны.

Требования к системе видеонаблюдения:

- Система видеонаблюдения должна собирать и передавать видеoinформацию в режиме реального времени.

- Система видеонаблюдения должна записывать и воспроизводить цветное изображение.

- 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 proximity-карт, которая состоит из сервера управления, системы контроллеров

и считывателей, а также индивидуальных карт (ключей).

- Данные системы (архив информации) должны храниться минимум 3 месяца.

Требования к техническим средствам охраны:

- Технические средства охраны не являются элементами ИТ-комплекса, но в случае их пересечения с ИТ-инфраструктурой необходимо руководствоваться положениями Технической политики по ИТ.

3.4.5 Требования к рабочим местам пользователей

Данный раздел рассматривает общие технические требования к рабочим местам пользователей, эксплуатируемых в подразделениях организаций Группы (АРМ). Конкретные требования изложены в Приложении 1, минимальные технические требования к ПК изложены в Приложении 2 (Раздел 2.1. «Минимальные требования к характеристикам ПК»).

3.4.5.1 Общие требования

При развитии парка ПК и выборе закупаемых моделей ПК необходимо руководствоваться следующими положениями:

- Аппаратная платформа и ПО ПК должны быть стандартизованы и сертифицированы, иметь гибкую и масштабируемую архитектуру.

- 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.

- Для повышения качества и скорости администрирования количество различных программно-аппаратных конфигураций ПК должно быть ограничено. Допускается использование не более 5 типовых конфигураций.

Все используемые ПК должны быть собраны из комплектующих на заводах производителей ПК, т.е. запрещено использовать ПК, собранные из отдельных комплектующих силами работников Группы.

Для спецификации технических требований выделяются следующие ключевые параметры ПК:

- Производительность. Должна обеспечиваться за счет:
 - Параметров быстродействия процессора;

- Объем оперативной памяти;
 - Скорости внутренних шин передачи данных;
 - Качества и быстродействия графической подсистемы;
 - Устройств ввода / вывода.
- Надежность. Должна обеспечиваться за счет аппаратных средств и ПО и определяться, исходя из среднего времени безотказной работы (MTBF).
 - Масштабируемость. Должна обеспечиваться архитектурой и конструкцией ПК за счет возможности наращивания объемов оперативной памяти и дискового пространства.
 - Готовность к использованию в корпоративной инфраструктуре. ПК должны обеспечивать возможность работы, как с локальными сервисами, так и с приложениями уровня корпоративной инфраструктуры.

Для рабочих мест определены следующие типы конфигураций:

- Стационарное рабочее место;
- Мобильное рабочее место;
- Высокопроизводительное стационарное рабочее место;
- Мобильное рабочее место руководителя;
- Специализированное рабочее место.

3.4.5.2 Требования к ПО рабочих мест пользователей

Конкретные технические требования к ПО рабочих мест пользователей изложены в Приложении 1 «Требования к типовому рабочему месту пользователя».

ОС офисного назначения должны:

- Соответствовать по типу клиентским ОС;
- Поддерживать все сетевые сервисы, обеспечивающие функционирование корпоративной сети;
- Обеспечивать высокий уровень ИБ;
- Быть совместимыми с корпоративным стандартом используемого офисного ПО;
- Комплектоваться только лицензионным ПО.
- Конечные (пользовательские) настройки системного ПО, также, как и настройки прикладного ПО должны автоматически применяться на клиентских рабочих местах доменными политиками или иными, принятыми в Группе, средствами автоматического распространения настроек. Весь перечень настроек, в обязательном порядке, должен быть отражен в документации к данному ПО.
- Рабочее место необходимо оснастить системным и прикладным ПО с использованием отечественной ОС.

3.4.6 Требования к периферийным устройствам печати

Настоящий раздел описывает основные технические требования к применяемым и закупаемым периферийным устройствам печати, входящим в ИТ-инфраструктуру Группы.

Конкретные минимальные технические требования изложены в Приложении 2 (Раздел 2.3. «Минимальные требования к периферийным устройствам печати»).

Рассматриваются требования к следующим классам периферийных устройств:

- Устройства печати (принтеры):
 - Монохромные принтеры (персональные и группового использования);
 - Цветные принтеры (персональные и группового использования) для офисной и фотографической печати;
- Устройства сканирования:
 - Сканеры персональные;
- Многофункциональные устройства:
 - Персональные МФУ;
 - МФУ группового и корпоративного использования.

Требования к специализированным устройствам, имеющим узкое технологическое применение (термопринтеры, принтеры штрих-кодов, наклеек, типографии, широкоформатные рулонные принтеры, 3D-принтеры), а также ко всем видам технологического периферийного оборудования, используемого в АСУТП, не рассматриваются.

Специализированное оборудование должно быть максимально унифицировано. Использование специализированного оборудования принимается на основе конкретных технических требований технологического процесса под обоснованные потребности владельцев процесса.

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

- Персональное устройство – находится в постоянном использовании одним работником. Устанавливается руководителям или рядовым работникам в случае невозможности использовать «групповые» или «корпоративные» устройства;
- Групповое устройство – используется в режиме разделения ресурсов группой работников (до 20 пользователей);
- Корпоративное устройство – используется большой группой работников (от 20 пользователей).

3.4.6.1 Общие требования

В данном разделе описываются общие требования, которые необходимо применять при выборе и закупке нового периферийного оборудования в целях развития ИТ-инфраструктуры Группы.

Периферийное оборудование должно отвечать следующим основным требованиям:

- Производительность. Периферийное оборудование должно обеспечивать потребности бизнеса 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 бизнес-процессов и удовлетворять требованиям, определенным в количественных показателях (MTBF).

- Функциональность. В том случае, если рабочее место работника 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.

Для периферийных печатных устройств обязательным является наличие возможности подключения по локальной сети.

- Совместимость. Периферийное оборудование должно сопрягаться технически и программно с ПК независимо от типа процессора и ОС. Минимально необходима совместимость с корпоративной ОС.

- Отказоустойчивость. Выход из строя какого-либо периферийного устройства не должен влиять на устойчивую работу ПК с другим периферийным оборудованием.

- Управляемость. Подключение и управление периферийным оборудованием должны быть простыми и не требовать оперативного использования инструкций и описаний работы устройств.

- Низкая стоимость владения. Запчасти и расходные материалы для периферийного оборудования должны быть легко доступны (поставляться официально на территорию РФ) и обладать невысокой стоимостью и высоким качеством, а также как можно больше быть предусмотрены для замены пользователем или специалистом СПП без привлечения специализированной организации.

- Низкий уровень создаваемого акустического шума. Периферийным оборудованием в процессе работы не должно создавать помех окружающим. Уровень

шума не должен превышать 55 дБ[А]. Для эксплуатации шумного оборудования должны быть предусмотрены специально выделенные помещения.

3.4.6.2 Требования к групповым и корпоративным устройствам печати

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.

Помимо указанных выше общих требований для групповых и корпоративных устройств необходимо наличие следующего функционала:

- Поддержка формата А3 для корпоративных, А4 для групповых устройств.

- Потоковое сканирование документов с автоматическим преобразованием в нужный формат с поддержкой сетевого сохранения файлов и возможностью отправки по электронной почте.

- В устройствах формата А3 наличие встроенного считывателя смарткарт / персональных пропусков / прочих устройств для авторизации пользователей (или штатного места под такой считыватель), а также установки ПО / клиента для систем управления доступом и учета печати. Предпочтительны групповые устройства формата А4 с таким же функционалом.

- Наличие возможности централизованного удаленного управления, сбора информации о сбоях, состоянии расходных материалов и об использовании устройств.

- Периферийное оборудование должно иметь периодическое техническое обслуживание, которое будет способствовать более высокой доступности устройств и снизит ТСО. Периодичность данного обслуживания необходимо определять из технических требований по эксплуатации каждого конкретного устройства предпочтительно наличие возможности выполнять обслуживание силами СПП без привлечения специализированной организации.

3.4.7 Требования к СУБД

3.4.7.1.1 В качестве СУБД должна использоваться система, включенная в Реестр российского ПО.

Выбор СУБД должен обеспечивать возможность подключения к централизованной системе управления и администрирования БД (Платформа Tantor) без дополнительного лицензирования.

Использование технологий контейнеризации приложений (chroot, Docker и пр.) для развертывания СУБД возможно только в случае специального решения, закрепленного протоколом, согласованным соответствующим подразделением сопровождающим серверы БД и директором ДИТ.

Использование на серверах СУБД кластерных технологий или технологии репликации возможно только в случае специального решения, закрепленного протоколом, согласованным соответствующим подразделением сопровождающим серверы БД и директором ДИТ.

4 ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные требования по обеспечению ИБ установлены в Политике информационной безопасности, которая описывает правила ИБ, обеспечения защиты информации и информационных ресурсов Группы. Требования по обеспечению ИБ должны выполняться на всех стадиях жизненного цикла (в т.ч. разработка, создание, эксплуатация, вывод из эксплуатации) ИС, автоматизированных систем управления (АСУТП) и ИТКС, функционирующих в любых сегментах инфраструктуры ИТ Группы (в т.ч. в сегментах корпоративных систем, технологических систем и в сегментах КСБ, находящихся в зонах ответственности ПАО «РусГидро», его подконтрольных организаций).

Реализация настоящих требований осуществляется субъектами Группы самостоятельно или с привлечением организаций, соответствующих требованиям законодательства Российской Федерации о лицензировании деятельности в области защиты информации.

Требования по обеспечению ИБ, подлежащие реализации в отношении каждой конкретной системы (ИС/АСУ/ИТКС) должны определяться на основании совокупности категорий информации обрабатываемой системой, в соответствии с требованиями соответствующих нормативных правовых актов Российской Федерации, в том числе:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»;
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;

- иные нормативные правовые акты Российской Федерации, определяющие требования по обеспечению ИБ соответствующих категорий информации.

Требования по обеспечению ИБ должны реализовываться за счет создания и развития комплексных систем обеспечения безопасности информации ИС/АСУ/ИТКС, которые, в т.ч. могут включать и / или агрегировать подсистемы ИБ конкретных ИС/АСУ/ИТКС.

Системы обеспечения безопасности информации должны реализовывать меры необходимые для нейтрализации актуальных угроз безопасности информации в ИС/АСУ/ИТКС в соответствии с соответствующими нормативными правовыми актами Российской Федерации, в т.ч.:

- организационные (регламентация процессов ИБ);
- технические (применение комплексов аппаратных, аппаратно-программных и программных средств защиты информации).

К организационным мерам обеспечения ИБ в первую очередь относится разработка положений, регламентов и процессов взаимодействия. Кроме этого, необходимо произвести:

- документирование и оптимизацию бизнес-процессов;
- установку градации сотрудников и их уровней доступа к информации;
- создание подразделений или назначение лиц, ответственных за обеспечение ИБ;
- информирование и обучение персонала;
- организацию мероприятий по отработке действий персонала (тренировки) при возникновении компьютерных инцидентов и иных нештатных ситуаций;
- обеспечение технической защиты помещений и оборудования;
- организацию пропускной системы для сотрудников, выдача им электронных средств идентификации;
- разработку системы взаимодействия с государственными органами;
- организацию мероприятий по внутреннему контролю состояния защиты информации.

Построение технических систем защиты информации должно осуществляться по принципам:

- система защиты должна быть обоснованной и технически реализуемой;
- простота архитектуры, упрощение компонентов, сокращение числа каналов и протоколов межсетевого взаимодействия;
- использование для построения системы стандартных, аутентичных

компонентов совместимых друг с другом;

- внедрение только протестированных программных решений, плюсы и минусы которых очевидны;
- минимальные доработки имеющихся лицензионных программных продуктов силами собственных или привлеченных исполнителей;
- эшелонированность защиты, предполагающая использование, как правило последовательно, ряда независимых методов защиты информации;
- обеспечение контроля за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты, регистрация как несанкционированных, так и санкционированных действий пользователей;
- централизованность управления, связана с необходимостью проведения единой корпоративной политики в области безопасности информационных ресурсов.

Аппаратные, аппаратно-программные и программные средства в составе технических систем защиты информации:

- должны быть отечественного производства в соответствии с постановлением Правительства Российской Федерации от 17.07.2015 № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации», что должно подтверждаться наличием действующих записей в Реестре российского ПО и / или в РРПП;
- должны быть серийного производства, применение заказных технических средств защиты информации единичного производства должно быть исключено;
- должны быть обеспечены гарантией и технической поддержкой производителя в процессе всего периода эксплуатации;
- должны соответствовать типовым решениям, принятым в Группе.

В соответствии с указом Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» должно быть полностью исключено использование средств защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

Процессы реализации технических мер по обеспечению безопасности информации должны включать следующие основные этапы:

1. Идентификация и классификация информации, обрабатываемой в ИС/АСУ/ИТКС.
2. Оценка угроз безопасности информации в ИС/АСУ/ИТКС.
3. Разработка требований к системе / подсистеме ИБ.
4. Разработка проектных решений по реализации установленных требований ИБ.
5. Реализация проектных решений (в т.ч. создание и испытания систем/подсистем ИБ).
6. Эксплуатация систем ИБ (в т.ч. регламентация мер ИБ; выявление и устранение угроз, уязвимостей и инцидентов ИБ в ИС/АСУ/ИТКС; оценка защищенности ИС/АСУ/ИТКС; модернизация систем ИБ).

Детальные требования и описание процессов обеспечения безопасности определяются Политикой информационной безопасности Группы.

4.1 План обеспечения непрерывности бизнеса и восстановления после аварии (нештатной ситуации и/или компьютерного инцидента)

Общество должно иметь план обеспечения непрерывности бизнеса и восстановления после нештатной ситуации и/или компьютерного инцидента, согласованный с Управлением кибербезопасности, созданный в соответствии с требованиями Политики информационной безопасности. Данный план должен включать в себя следующие пункты, которые необходимы для регламентации работ в области ИТ:

- Перечень внешних и внутренних угроз для бизнеса. К внешним угрозам необходимо отнести техногенные, природные, человеческие и прочие угрозы.
- План обеспечения бесперебойного функционирования организации в случае нештатной ситуации/компьютерного инцидента – детальный перечень мероприятий, которые должны быть выполнены до, во время и после события повлекшего нарушение штатного режима функционирования. Этот план должен в случае нештатной ситуации/компьютерного инцидента регламентировать действия по локализации, устранению причин, ликвидации последствий и восстановлению нормального функционирования из имеющихся в наличии резервных копий критически важных информационных ресурсов.
- План должен учитывать определенное целевое время восстановления данных (RTO), которое определяется с точки зрения требований к непрерывности бизнес-процессов.
- Резервному копированию подлежат все программы и данные (включая их настройки), обеспечивающие работоспособность системы и выполнение ею своих задач (системное и прикладное ПО, базы данных и

другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д. Резервному копированию подлежат также все настройки активного сетевого оборудования.

- 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 ответственных за создание, хранение и использование резервных копий данных.

- В целях обеспечения сохранности резервных копий должен быть реализован механизм резервного копирования, обеспечивающий создание отчуждаемой резервной копии (на физическом носителе типа «лента» или его аналоге).

- Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала.

- Каждый носитель, содержащий резервную копию, должен иметь метку, содержащую данные о классе, ценности, назначении хранимой информации, ответственном за создание, хранение и использование, дату последнего копирования, место хранения и прочее.

5 ТРЕБОВАНИЯ К УНИФИЦИРОВАННОЙ СИСТЕМЕ МОНИТОРИНГА ТЕХНИЧЕСКОГО СОСТОЯНИЯ ИТ- ИНФРАСТРУКТУРЫ

Данный раздел рассматривает общие требования к унифицированной системе мониторинга технического состояния ИТ-инфраструктуры.

5.1 Требования к функциональности

Унифицированная система мониторинга технического состояния ИТ-инфраструктуры (СМТС) должна удовлетворять следующим требованиям:

- построение по модульному принципу;
- агрегация и корреляция данных мониторинга от объектов ИТ-инфраструктуры разных типов, приведение их к единому формату;
- агрегация и корреляция данных мониторинга должны обеспечиваться для всех управляемых объектов ИТ-инфраструктуры (оборудование ИТ-инфраструктуры, включая инфраструктуру АСТУ, инфраструктуру ИБ и т.д.);
- наличие средств обнаружения и инвентаризации контролируемых объектов, сохранение и предоставление этой информации для нужд собственных модулей и подсистем, а также внешних систем;

- наличие следующих способов организации мониторинга и управления:

- агентский способ – подразумевает установку на управляемое оборудование агента управления СМТС;
- безагентский способ – подразумевает использование встроенных средств мониторинга оборудования или ПО без установки специального агента управления СМТС.

- масштабируемость в рамках контролируемой инфраструктуры;
- мониторинг контролируемых объектов различных типов и производителей в гетерогенной среде;

- возможность включения в контур мониторинга существующих и проектируемых объектов ИТ-инфраструктуры;

- режим работы СМТС должен совпадать с режимом функционирования объектов ИТ-инфраструктуры;

- управление правами пользователей СМТС для разграничения на области компетенции по решению возникающих проблем;

- наличие средств интеграции с инфраструктурными сервисами (корпоративный каталог, электронная почта, SMS-шлюзы и т.д.);

При построении СМТС необходимо использовать преимущественно отечественное ПО, а также возможно использование ПО с открытым исходным кодом и соответствующей лицензией на его использование.

5.2 Требования к структуре СМТС

Унифицированная система управления мониторинга технического состояния ИТ-инфраструктуры должна включать следующие подсистемы:

- подсистема корреляции данных мониторинга;
- подсистема мониторинга ИТ-оборудования;
- подсистема мониторинга оборудования производственных систем;
- подсистема контроля качества каналов связи;
- подсистема мониторинга приложений;
- подсистема управления ИТ-услугами и процессами поддержки;
- подсистема мониторинга и управления бизнес-услугами;
- подсистема интеграции.

6 ТРЕБОВАНИЯ К ВВОДУ ИНФОРМАЦИОННЫХ СИСТЕМ В ЭКСПЛУАТАЦИЮ

Порядок приемки ИС и ввода их в эксплуатацию определяется Положением о порядке приемки в эксплуатацию ИС, утвержденным приказом Общества от 02.09.2022 № 654.

Для каждой внедряемой информационной системы, обрабатывающей персональные данные, необходимо разработать модель угроз.

Конкретные требования к документации с точки зрения удовлетворения действующим нормативным документам изложены в Приложении 5 «Требования к документированию». Уточненный состав требований к документации приводится в Техническом задании. Требования к документированию определяются ЛНД(А) Общества в части закупочной деятельности.

6.1 Требования к вводу в действие

Требуется осуществлять все этапы испытаний системы перед ее вводом в действие, а именно:

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

Для крупных инфраструктурных систем рекомендуемый срок опытно-промышленной эксплуатации должен составлять не менее 2 месяцев.

Оборудование и ПО, вводимое в промышленную эксплуатацию в Группе, должно иметь соответствующие сертификаты соответствия, если это предусмотрено требованиями законодательства Российской Федерации и / или требованиями внутренних ЛНД(А) Общества, в т.ч. сертификаты соответствия:

- в системе «Связь», если оборудование подсоединяется к сети связи общего пользования;
- в системе сертификации ФСТЭК России (в части технических и программных средств защиты информации);
- в системе сертификации ФСБ России (в части технических и программных средств криптографической защиты информации).

Для ПО должна быть предусмотрена разработка, поставка и проверка актуальности на момент проведения опытной эксплуатации (контрольная компиляция и сборка).

Начало промышленной эксплуатации ИС (включая инфраструктуру) должно оформляться организационно-распорядительным документом о начале промышленной эксплуатации.

Организационно-распорядительный документ должен определять:

- должностное лицо, отвечающее за эксплуатацию и обеспечение работоспособности сегмента инфраструктуры, вводимого в промышленную эксплуатацию; требования к времени реакции эксплуатирующей организации (структурного подразделения или привлекаемого по договору внешнего

контрагента), отвечающей за выполнение параметров соглашения об уровне услуг;

- периодичность проведения анализа инфраструктуры с целью выявления единых точек отказа по общей причине и формирования предложений по модернизации инфраструктуры для повышения надежности (для КСПД – не реже 1 раза в год).

6.2 Базовые меры защиты при вводе в эксплуатацию

Для ИС, обрабатывающих информацию, доступ к которой ограничен (информация ограниченного доступа) законодательством РФ меры защиты реализуются в соответствии с требованиями, указанными в разделе 4 Технической политики, для иных ИС должны быть реализованы следующие базовые меры защиты:

- обязательная идентификация и аутентификация всех субъектов доступа при входе в ИС с запретом любых действий до успешной аутентификации;

- идентификация, аутентификация и управление идентификаторами пользователей;

- разработка ролевой модели, разграничивающей доступ пользователей к возможностям ИС на основе выполняемых функций, с выделением отдельной роли администратора ИС;

- регистрация в журнале событий ИС попыток доступа субъектов к ИС, её критичным функциям или компонентам, а также к обрабатываемой информации с указанием предъявленного идентификатора и результата, регистрация действий администраторов по изменению конфигурации ИС;

- реализация в журнале событий ИС возможности чтения, поиска и/или выгрузки записей с доступом только для администратора ИС;

- отправка событий ИС в системный журнал ОС и сторонние системы в формате syslog.

Обеспечение взаимодействия (интеграции и т.п.) ИС, обрабатывающих информацию ограниченного доступа с ИС, не обрабатывающих информацию ограниченного доступа, допускается только при условии проведения оценки угроз безопасности информации для такого взаимодействия и реализации соответствующих мер защиты информации для ИС обрабатывающих информацию ограниченного доступа.

Идентификация, аутентификация и управление идентификаторами пользователей должны быть реализованы с использованием механизмов

сквозной аутентификации и авторизации (SSO). При удалённом доступе — на основе доменной аутентификации и авторизации.

В случаях, когда достаточно применения механизма делегированной авторизации и аутентификации (без необходимости предоставления пароля пользователя для доступа к ресурсам ИС), а также при необходимости авторизации и аутентификации в веб-приложениях, должен использоваться провайдер идентификации (Identity Provider), совместимый с Keycloak (протоколы OpenID Connect (OIDC), OAuth 2.0 и/или SAML 2.0).

В случае необходимости аутентификации и авторизации в рамках одной организации (исключая подконтрольные организации) могут быть использованы протоколы Kerberos и LDAPS.

7 ТРЕБОВАНИЯ К ПОДКЛЮЧЕНИЮ ФИЛИАЛОВ ОБЩЕСТВА И ПОДКОНТРОЛЬНЫХ ОРГАНИЗАЦИЙ К ИНФОРМАЦИОННЫМ РЕСУРСАМ ПАО «РУСГИДРО»

7.1 Требования к подключению Филиалов

Обмен данными между сетями передачи данных компаний Группы должен осуществляться с помощью каналов связи, построенных на базе виртуальных частных сетей IP VPN (с применением технологии MPLS); допускается подключение по физическим линиям связи (ВОЛС). Подключения сетей передачи данных должны быть зарезервированы аналогичными каналами связи.

Все филиалы Общества должны быть подключены к корпоративным ИС и инфраструктурным сервисам в строгом соответствии с типовыми проектами по подключению к ИТ-инфраструктуре и требованиями к мультисервисной сети, указанными в Приложении 4.

7.2 Требования к подключению подконтрольных организаций

Подключения для подконтрольных организаций к информационным ресурсам делятся на 3 типа.

- Тип 1. Для подконтрольных организаций численностью от 100 пользователей и выше необходимо организовать подключение в строгом соответствии с типовыми проектами по подключению к корпоративным инфраструктурным сервисам корпоративной мультисервисной сети с учетом требования п. 7.1 Технической политики по ИТ.

- Тип 2. Для подконтрольных организаций численностью от 30 до 100 пользователей необходимо организовать подключение с использованием типовых проектов по подключению к корпоративным инфраструктурным сервисам и корпоративной мультисервисной сети с учетом требования п. 7.1 Технической политики по ИТ. Допускаются следующие отклонения от типовых:

- организация подключения к корпоративной сети по средствам только VPN-канала с использованием алгоритмов ГОСТ через сеть Internet.
- создание ИТ-инфраструктуры подконтрольных организаций с использованием минимально необходимого комплекта оборудования, такого как: мультисервисный маршрутизатор для подключения к корпоративной сети, криптокоммутатор для использования технологии VPN с поддержкой алгоритмов ГОСТ; серверы для обеспечения ИБ.

- Тип 3. Для подконтрольных организаций численностью до 30 пользователей допускается создание учетных записей и организация доступа к информационным ресурсам через сеть Internet с использованием технологии VPN и средств шифрования по алгоритмам ГОСТ, а также терминального доступа.

8 ТРЕБОВАНИЯ К ПОСТАВЩИКАМ, ПРОИЗВОДИТЕЛЯМ И ПРОВЕДЕНИЮ КОНКУРСОВ

Основные требования, касающиеся выбора поставщиков программно-аппаратных комплексов и услуг, производителей программно-аппаратных комплексов и системных интеграторов определяются в Едином положении о закупках продукции для нужд Группы.

Закупочная деятельность должна обеспечивать своевременное и качественное снабжение Группы закупаемой продукцией и исключать закупку продукции, противоречащей требованиям Технической политики по ИТ. В особых случаях, допускаются исключения из приведенных ниже требований по решению Центральной закупочной комиссии.

8.1 Общие требования

К поставщикам и производителям элементов ИТ-инфраструктуры и ИС, а также к внешним провайдерам ИТ-услуг предъявляются следующие требования:

- Поставщики и производители должны соответствовать требованиям к участникам закупки, предъявляемым в соответствии с законодательством Российской Федерации и Единым положением о закупках продукции для нужд Группы.
- Деятельность поставщиков и производителей должна быть лицензирована, если таковое предусматривает законодательство Российской Федерации в отношении предмета закупки.
- Предпочтение должно отдаваться поставщикам услуг, входящим в группу компаний, с целью формирования внутренних компетенций.
- В случае наличия заключенных корпоративных соглашений с вендорами, приобретение ПО необходимо осуществлять централизованно в рамках данных соглашений.

- Аппаратная платформа и ПО должны быть стандартизованы и сертифицированы на соответствие стандартам, считающимися общепринятыми в предметной области данного программно-аппаратного обеспечения, иметь гибкую и масштабируемую архитектуру.

- Предлагаемое поставщиком оборудование и ПО должно быть коммерчески доступно на протяжении не менее 3-х лет.

- Поставщики сложного программно-аппаратного обеспечения для Группы должны своевременно получать сертификаты соответствия на всю гамму поставляемого оборудования и ПО в соответствии с действующими техническими требованиями в полном объеме, а также обновлять сертификаты при появлении новых версий программного и аппаратного обеспечения поставляемой продукции.

- Все заказное ПО должно поставляться с задокументированным кодом в электронном виде.

- Поставщики должны осуществлять гарантийную поддержку поставленного оборудования и ПО согласно требованиям, к услугам эксплуатации и сопровождения.

- Поставщики программно-аппаратного обеспечения должны предоставлять услуги первичного обучения специалистов, эксплуатирующих данное программно-аппаратное обеспечение, а также их переподготовки при внедрении новых версий и типов оборудования и ПО. Уровень предоставляемого обучения должен быть достаточным для последующей эксплуатации и администрирования данного программно-аппаратного обеспечения.

- Поставщики программно-аппаратного обеспечения должны обеспечивать гарантию замены утерянного, поврежденного при транспортировке или выбракованного при первичном осмотре оборудования (указывать в договоре максимальный срок замены в днях).

8.2 Требования к поставщикам услуг по эксплуатации и сопровождению

Поставщики услуг по технической поддержке (сопровождению) и участники конкурсов, проводимых компаниями Группы для поставки программно-аппаратного обеспечения в части гарантийного обслуживания, должны удовлетворять следующим минимальным требованиям к организации поддержки и эксплуатации:

- Сервис-центр должен находиться в приемлемой удаленности от заказчика услуг, чтобы иметь возможность устранить неисправность с выездом к заказчику услуг в сроки, установленные соответствующими регламентами взаимодействия, которые, в свою очередь, должны опираться на

требования непрерывности, готовности и доступности элементов ИТ-комплекса.

- Эксплуатация сложного программно-аппаратного обеспечения, гарантийный срок на которое истек, должна осуществляться на основе контракта на послегарантийное обслуживание. Указанный контракт должен заключаться сервис-центром, расположенным на территории Российской Федерации и обеспечивающим послегарантийное обслуживание программно-аппаратного обеспечения данного типа.

- В отдельных случаях допускается осуществлять послегарантийное обслуживание силами внутреннего провайдера ИТ-услуг, при наличии специалистов, прошедших соответствующее обучение (что подтверждается сертификатами поставщика), необходимого оснащения, запасных частей и оформленных должным образом взаимоотношений с системой сервисной поддержки фирмы-поставщика или производителя.

- Поставщик услуг по эксплуатации и сопровождению оборудования должен иметь склад запасных частей.

- Поставщик услуг по эксплуатации и сопровождению должен иметь соответствующий персонал, сертифицированный на оказание данных услуг.

- Поставщики сложного программно-аппаратного обеспечения должны силами сервис-центров, расположенных на территории Российской Федерации, осуществлять модернизацию находящегося в эксплуатации программно-аппаратного обеспечения с целью поддержания его на современном техническом уровне и внедрения новых современных функций и услуг.

- Обслуживание и модернизация должны осуществляться для всех установленных типов оборудования и ПО данного поставщика и для всех версий указанного оборудования.

- Сервис-центры поставщика услуг по эксплуатации и сопровождению или службы поддержки производителя должны обеспечивать:

- поддержку пользователей, в соответствии с требованиями непрерывности, по телефону и с помощью электронной почты;

- решение проблем, возникающих при работе программно-аппаратного обеспечения в объеме, возложенном на данный сервис-центр;

- возможность внесения оперативных коррекций в ПО, находящееся в эксплуатации с использованием современных средств передачи информации (сетей передачи данных и др.);

- возможность выезда специалистов для устранения неисправностей в соответствии с установленным регламентом. Использовать следующие требования для экстренного выезда специалистов: выезд специалиста в течение не более 12

часов и с прибытием на место в течение не более 24 часов с момента обращения (без учета транспортных задержек, не зависящих от сервис-центра);

- не допускается несанкционированное руководителем ИТ вмешательство (в том числе дистанционное) сервис-центров в работу находящегося в эксплуатации программно-аппаратного обеспечения;

- срок ремонта или замены сервис-центром неисправных узлов оборудования определяется требованиями ИТ-услуг, но не должен превышать двух недель с момента передачи узла на сервис-центр. Для этого сервис-центр должен иметь необходимый комплект запасных узлов, а также, при необходимости – ремонтные оборудование и службы.

8.3 Особые требования к поставщикам инновационных ИС и услуг

В случае, если решения, предоставляемые поставщиками программно-аппаратных комплексов и услуг, производителями программно-аппаратных комплексов, а также системными интеграторами обладают обоснованными признаками инновационности или принципиальной новизны (в частности, проекты, внесенные в список инновационных) требования Технической политики по ИТ к ним являются рекомендательными. Особые технические требования к подобным проектам согласуются с ДИТ индивидуально.

9 ПРИЛОЖЕНИЯ

Приложение 1. Требования к типовому рабочему месту пользователя

1. Введение

Данный документ определяет состав и характеристики типового рабочего места пользователя Группы (далее – АРМ), необходимые для эффективного и безопасного взаимодействия пользователя с информационными ресурсами и информационной инфраструктурой при получении услуг ИТ.

1.1. К базовому пакету ИТ-услуг относятся:

- электронный документооборот;
- доступ к информационному portalу Группы;
- доступ к сетевым файловым ресурсам;
- услуга электронной почты;
- корпоративная телефонная связь;
- услуга ВКС;
- услуга хранения и обмена электронной информацией;
- функции печати и сканирования документов.

1.2. Доступ к базовым информационным ресурсам производится с помощью АРМ, выстроенного в соответствии с требованиями Технической политики по ИТ.

1.3. Контакты пользователей с информационной организацией в процессе потребления информационных услуг должны производиться через единую точку контакта – СПП.

1.4. Требования к типовому рабочему месту пользователя обязательны для соблюдения всеми пользователями ПАО «РусГидро» (включая его филиалы), а также пользователями подконтрольных организаций, использующих в своей деятельности информационные ресурсы Общества и Группы.

2. Типовое рабочее место пользователя Группы

Рабочее место является основным элементом информационной инфраструктуры, через который происходит доступ пользователей к остальным информационным услугам.

Рабочее место представляет собой сконфигурированную в соответствии с принятыми в Обществе правилами совокупность:

- Учетной записи пользователя⁷;
- Вычислительных технических средств;
- ОС и Системное ПО;

⁷ Учетная запись предоставляет пользователю доступ к корпоративным удаленным ресурсам, в том числе к корпоративной почте и корпоративному portalу.

- Прикладного ПО;
- Средств телефонии.

2.1. Учетная запись пользователя

2.1.1. Пользователь получает идентификационные данные УЗ:

- регистрационное имя (login name);
- пароль (password);
- запись в домене (domain).

2.1.2. Регистрационное имя пользователя формируется исходя из его фамилии и инициалов. Регистрационное имя уникально и позволяет однозначно идентифицировать пользователя.

2.1.3. Все компьютерное и офисное оборудование (технические средства) является собственностью Группы и передается работникам во временное использование в качестве составных частей рабочего места для выполнения должностных обязанностей.

2.1.4. Для обмена электронной почтой каждому пользователю создается адрес электронной почты размещаемый в облачном пространстве Общества, доступ к почте осуществляется через веб-браузер по адресу: e.mail.ru. По умолчанию почтовый адрес для пользователей Общества и работников внешних подрядных организаций, использующих почтовую систему Общества в рамках заключенных договоров, имеет вид **«сетевое_регистрационное_имя»@rushydro.ru**.

2.2. Вычислительные технические средства

2.2.1. Перечень, состав и вычислительная мощность технических средств для персональной или групповой работы определяется приложением к приказу Общества от 10.11.2023 № 819.

2.2.2. Пользователи не вправе самостоятельно изменять аппаратную конфигурацию предоставленных им в использование технических средств, кроме штатных случаев, предусмотренных конструкцией технических средств. Решение об изменении аппаратной конфигурации принимается исходя из аппаратных требований, предъявляемых приложениями, которые устанавливаются на данный ПК.

2.2.3. В целях обеспечения ИБ при работе на ПК пользователям обязательно выполнять следующие требования:

- запрещено оказывать воздействия на работу программ антивирусной защиты (останавливать работу программы, изменять настройки без согласования с работниками СПП);
- запрещено работать с внешними носителями информации (дискеты, CDROM, флеш-накопитель usb и т.д.), если этого не требуется для исполнения непосредственных функциональных обязанностей Пользователя;

- при необходимости работы с внешними носителями информации требуется написать обращение в СПП для согласования разблокировки USB-портов с ответственным за ИБ и проверять носитель сразу после того, как он был вставлен в соответствующее устройство для чтения на предмет наличия вирусов;
- запрещено скачивать из Интернет исполняемые файлы (файлы, имеющие расширения .exe, .com, .vbs и т.д. для среды Linux: .sh и другие помеченные как исполняемые файлы скрипты и т.д.);
- при обнаружении зараженных файлов, во избежание распространения вирусов по локальной сети, требуется прекратить работу на ПК и немедленно известить работников СПП.

2.3. Операционная система и Системное ПО.

2.3.1. Операционная система (ОС) — это комплекс системных управляющих и обрабатывающих программ компьютера, взаимодействующих как между собой, так и с пользователем. ОС AlterOS передается пользователю в настроенном виде и является неотъемлемой частью ПК и не поставляется отдельно от него.

2.3.2. ОС AlterOS является типовым техническим решением и включает в себя предустановленное ПО: файловый менеджер, веб-браузер, текстовый редактор, менеджер архивов, инструмент захвата экрана, просмотр изображений, средства печати и сканирования, калькулятор, клиент мгновенного обмена сообщениями, медиаплеер, средство удаленной поддержки и подключений.

2.3.3. Набор предустановленного ПО обеспечивает доступ к инфраструктурным сервисам и обеспечивает пользователю базовые возможности для работы с файлами: архивирование просмотр и печать текстовых, растровых файлов, просмотр и прослушивание аудио- и видеофайлов а также возможности передачи файлов и сообщений по корпоративной сети.

2.3.4. Использование ОС возможно только с помощью созданной УЗ пользователя без предоставления расширенных привилегий администратора системы. При использовании ОС могут вводятся программные аппаратные ограничения в виде ограничения объема хранимой информации на диске, длины пути до конечного файла в файловой системе работы с портативными и флэш запоминающими устройствами. Установка дополнительного ПО, предоставление доступа к другим ИС, внесение изменений в параметры работы ОС ПО и ПК решается обращением в СПП.

2.4. Прикладное программное обеспечение

2.4.1. Для подготовки электронных офисных документов используется

пакет AlterOffice в составе:

- ACell (программ для работы с электронными таблицами);
- AText (программ для работы с электронными документами);
- AGraph (векторный графический редактор, редактор диаграмм и блок-схем);
- AConcept (программа подготовки и просмотра презентаций).

2.4.2. Для использования ПО совместимого исключительно с ОС Windows используется Citrix Workspace как решение доставки Windows приложений.

2.4.3. Яндекс-браузер (используется для просмотра страниц, содержания веб-документов доступ в ИС).

2.4.4. Облачный сервис корпоративной ИС электронного документооборота КСД (Documino).

2.4.5. Пользователю запрещается самостоятельно изменять программную конфигурацию ПК, параметры ОС и установленных приложений, устанавливать дополнительные приложения⁸. В случае необходимости использования какого-либо ПО, не установленного на компьютер Пользователя, необходимо оформить запрос на обслуживание в СПП. Вопрос об установке того или иного дополнительного ПО будет решаться специалистами ДИТ на основании анализа должностных инструкций и функциональных обязанностей пользователя по согласованию с его руководством. В случае положительного решения по запросу на установку ПО оно будет приобретено и установлено силами работников СПП.

2.5. Средства телефонии

2.5.1. Корпоративная телефония предназначена для информационного обеспечения деятельности офиса, организационного управления и коммуникационного взаимодействия между ИА, филиалами и подконтрольными организациями.

2.5.2. Корпоративной телефонией связаны все филиалы и подконтрольные организации.

2.5.3. Номер абонента ИА, филиалов и подконтрольных организаций можно найти в корпоративном телефонном справочнике, расположенном на корпоративном портале <https://ab.rushydro.ru>.

2.5.4. По умолчанию на АРМ доступны звонки на местные телефонные номера, номера операторов мобильной связи и междугородные звонки.

2.5.5. В ИА принят 7-значный номерной план, где первые 3 цифры

⁸ В случае, если какие-либо приложения не работоспособны, допускается временная возможность использования отечественных систем класса VDI, а также ПО WINE@Etersoft в качестве программного продукта, позволяющего запускать приложения, использующие операционную систему Windows, в операционных системах семейства AlterOS.

(префикс или код) определяют структурное подразделение / Филиал / подконтрольная организация, последующие 4 цифры – номер абонента. Пример: 001 (код ИА) – 1911 (СПП).

2.5.6. При звонках в филиалы / участки / структурные подразделения подконтрольных организаций может понадобиться большее количество цифр при наборе номера, в таком случае после набора префикса может потребоваться дополнительный префикс. Пример: 074 (ИА ПАО «ДРСК») – 761 (ЮЭС) – 781 (ЦЭС, г. Уссурийск) – номер абонента.

2.5.7. При звонках за пределы корпоративной телефонии установлен следующий порядок набора номеров: 9 – 8 – 3-значный префикс оператора, либо географический код – номер абонента. Пример: 9 – 8 – 495 (код Москвы) – 122-05-55 (номер абонента) или: 9 – 8 – 925 (префикс Мегафон) – 400-04-44 (номер абонента).

3. Организация файлового сервиса

3.1. Общие правила организации файлового сервиса

3.1.1. Все ПК Общества объединены в общую локальную сеть, что позволяет использовать общие сетевые ресурсы (серверы, принтеры, сканеры, факсы и т.д.).

3.1.2. Данные, хранящиеся на локальных дисках ПК пользователей, не подвергаются резервному копированию. Поэтому все данные, утеря которых может нанести ущерб Обществу или привести к нарушениям бизнес процессов, должны храниться на файловом сервере. Если для автономной работы требуется наличие данных на мобильных компьютерах, то по обращению в СПП может быть организована репликация данных между сервером и мобильным компьютером. Первичный документ (исходный документ) должен быть размещен на файловом сервере. Это требование не касается файлов, не содержащих официальные документы. Архивы, устаревшие или утратившие актуальность файлы, рекомендуется хранить на сервере, однако Пользователь сам должен определить необходимость обеспечения сохранности данных файлов.

3.1.3. Для хранения файлов на серверах Общества создана структура папок, обеспечивающая упорядоченное хранение документов и архивов. В процессе регистрации Пользователя в сети происходит подключение сетевых дисков, каждый из которых имеет уникальное имя, состоящее из буквы латинского алфавита и двоеточия (например, H:, R:, W: и т.д.).

3.2. Структура файловой системы серверов Общества

3.2.1. Вся информация на файловых серверах Общества структурирована по следующим принципам:

- Домашние каталоги Пользователей (например, диск H:);

- Каталоги рабочих документов подразделений (диск W:);
- Каталоги готовых документов подразделений (диск R:);
- Каталоги для приложений, запуск которых возможен непосредственно с файлового сервера (предустановленные приложения) (диск T:);
- Каталог для обмена файлами (диск S:).

Имена дисков снабжены текстовыми заголовками, поясняющими их назначение.

3.2.2. Каждый Пользователь имеет на одном из файл-серверов свой собственный домашний каталог (далее – Домашний каталог). Доступ к Домашнему каталогу происходит при регистрации в сети подключением сетевого диска H:. В Домашнем каталоге Пользователь должен хранить наиболее важные документы и файлы, которые нужны ему для выполнения его должностных обязанностей, но только ему лично.

4. Видеоконференцсвязь

Сервис организации ВКС предоставляется в составе базового ВКС различного формата (конференции, совещания, лекции, вебинары), обеспечивает запись мероприятий. Доступ к системе предоставляется web-приложением, доступным по адресу <https://iva.rushydro.ru/>.

5. Функции печати и сканирования документов

5.1.1. Функции сканирования и печати документов с использованием АРМ пользователя входят в базовый пакет ИТ-услуг.

5.1.2. Печать документов производится с АРМ пользователя с использованием приложения контроля доступа к сетевой печати, устанавливаемого на АРМ пользователя. Система контроля доступа к сетевой печати создает виртуальную среду печати, с помощью которой пользователи могут безопасно печатать документы в любое время и в любом месте независимо от его местоположения. С помощью системы контроля доступа к сетевой печати пользователи могут ставить задания в общую очередь и печатать их на любом поддерживаемом устройстве вывода (например, МФУ). Это гарантирует защиту конфиденциальных документов и позволяет снизить отходы, которые возникают при печати документов в отсутствие пользователя. Функция сканирования документов в сетевые папки и на рабочее место пользователя доступна также с любого устройства ввода-вывода.

6. Форматы офисных электронных документов

Для использования в работе пользователей Группы установлены следующие форматы документов (расширение файлов) (приводятся по их соответствию программным продуктам Microsoft Office):

Тип документа	Приложения AlterOS\ Microsoft Office	Формат (расширение)
Текстовый документ	AText \ MS Word	odt
Текстовый документ, используемый как шаблон	AText \ MS Word	ott
Текстовый документ, используемый как шаблон для HTML-документов	AText \ MS Word	oth
Электронная таблица	ACell \ MS Excel	ods
Электронная таблица, используемая как шаблон	ACell \ MS Excel	ots
Документ презентации	AConcept \ MS Powerpoint	odp
Документ презентации, используемый как шаблон	AConcept \ MS Powerpoint	otp
Документ формулы	AMath \ MS Office Access	odf
Документ формулы, используемый как шаблон	AMath \ MS Office Access	Otf
Документ диаграмма или схема	ACMOграф \ MS Visio	vsd / vsdx
Документ диаграмма или схема, используемый как шаблон	ACMOграф \ MS Visio	vst

Приложение 2. Реестр типовых технических и программных средств, применяемых в ИТ инфраструктуре Группы РусГидро

Настоящий Реестр содержит используемые и / или рекомендуемые для использования в Группе технические решения в области информационно-технологической инфраструктуры и рабочих мест в части аппаратного и программного обеспечения информационных технологий (таблица 1), решения в части информационной безопасности (таблица 2).

Перечень подготовлен с целью унификации проектируемых технических решений в соответствии с требованиями законодательства Российской Федерации, в том числе, в части импортозамещения, а также в соответствии со Стратегией ЦТ.

В случае, если при проведении проектирования выявлены условия, при которых применение технического решения, зафиксированного в Перечне невозможно / нецелесообразно, допускается по дополнительному согласованию с ДИТ применение эквивалентов, которые могут дополнить настоящий Перечень.

Актуализация Реестра производится 1 раз в год, либо дополнительно по необходимости.

Типовая схема подключения подконтрольных организаций к КСПД представлена в Приложении 1.

Таблица 1. Технические решения в области информационно-технологической инфраструктуры и рабочих мест в части аппаратного и программного обеспечения информационных технологий

№ п/п	Информационно-технологические системы / типы ПО	Рекомендуемое для использования в КСПД оборудование и ПО / производитель	Рекомендуемое для использования в ТСПД (АСТУ, АСУТП и СДТУ) оборудование и ПО / производитель
1.	Серверное оборудование, системы хранения данных (оборудование)	1. Серверы DEPO / ООО «ДЕПО Электроникс» 2. Серверы ICL / ООО «АйСиЭл Техно» 3. Серверы OpenYard / ООО «Центр открытых разработок» 4. Серверы Yadro / ООО «Ядро Клиентские Системы» 5. Серверы Аквариус / ООО «ПК компания Аквариус» 6. Серверы Гравитон / ООО «Новый Ай Ти Проект»	
2.	Системы резервного копирования (ПО)	ПО Кибер Бэкап / ООО «Киберпротект»	
3.	Системы виртуализации (ПО)	ПО zVirt / ООО «Орион»	ПО SpaceVM / ООО «ДАКОМ М»
4.	Системы хранения данных (ПО)	ПО RAIDIX / ООО «Рэйдикс»	
5.	Сетевое оборудование (уровни ядра, агрегации и доступа)	1. Коммутаторы Eltex / ООО «Предприятие «Элтекс»	1. Коммутаторы Yarus / ГК «Эскара» 2. Коммутаторы Корунд / ГК «Ангстрем-телеком» 3. Коммутаторы Eltex / ООО «Предприятие «Элтекс» 4. Коммутаторы Инзер, Арлан / АО НПО «Полигон» 5. Коммутаторы Natex / АО «ГК Натекс»
6.	Сетевое оборудование (системы виртуализации)	Коммутаторы Eltex / ООО «Предприятие «Элтекс»	
7.	Сетевое оборудование (маршрутизаторы)	Маршрутизаторы Eltex / ООО «Предприятие «Элтекс»	
8.	Системы агрегации сетевого трафика	Брокер сетевых пакетов DS Integrity NG / ООО «Цифровые решения»	
9.	Системы управления базами данных	1. СУБД Tanor / ООО «Лаборатории Тантор» 2. СУБД Postgres Pro / ООО «Постгрес Профессиональный»	СУБД PostgreSQL / ООО «РусБИТех-Астра»
10.	Операционные системы серверные	ОС AlterOS / ООО «АЛМИ Партнер»	1. ОС специального назначения Astra Linux SE / ООО «РусБИТех-Астра» 2. ОС AlterOS / ООО «АЛМИ Партнер»
11.	Службы каталогов	ПО «ALD Pro» / ООО «РусБИТех-Астра»	
12.	Системы оркестрации контейнеризированных приложений	Платформа контейнеризации Боцман / ООО «РусБИТех-Астра»	

№ п/п	Информационно-технологические системы / типы ПО	Рекомендуемое для использования в КСПД оборудование и ПО / производитель	Рекомендуемое для использования в ТСПД (АСТУ, АСУТП и СДТУ) оборудование и ПО / производитель
13.	Системы удаленного доступа, управления и администрирования	ПО Ассистент / ООО «САФИБ»	
14.	Приложения симуляции/виртуализации аппаратных средств (ЖМД, ОД, электронных ключей, ЛВС) и центрального процессора	1. ПАК NIO-EUSB / ООО «НИО-ЭЛЕКТРОНИКС» 2. ПО EVE-NG Community Edition / EVE-NG Ltd (нет полноценных российских аналогов)	1. ПАК NIO-EUSB / ООО «НИО-ЭЛЕКТРОНИКС»
15.	Приложения для работы с машинными носителями информации (HDD, SSD и др.): тестирование, диагностика, восстановление данных, создание образов, резервное копирование и дублирование	1. R.saver / R.lab 2. Victoriya / свободное ПО 3. R-Studio / R-Tools Technology (нет полноценных российских аналогов) 4. Acronis True Image (Acronis Cyber Protect Home Office) / Acronis (нет полноценных российских аналогов)	Не используется
16.	Средства разработки и программирования, средства отладки объектных модулей ПО	1. VSCodium / свободное ПО 2. Python / свободное ПО 3. Perl / свободное ПО 4. Geany / свободное ПО	Не используется
17.	Автоматизированные рабочие места пользователей	1. 2. 3. 4. Системы»	ПК Аквариус / ООО «ПК компания Аквариус» ПК KVADRA / ООО «Ядро Клиентские ПК ICL / ООО «АйСиЭлТехно» ПК Гравитон / ООО «Новый Ай Ти Проект»
18.	Операторские панели с комплектным ПО (для малых локальных систем управления)	-	1. Серия NLCON / ООО «НИЛ «АП» 2. Серия СТАБУР / ООО «ПО «Промсвязь»
19.	Операторские панели / Промышленные ПК	-	1. Серия PANEL-PC / ООО «НИЛ «АП» 2. Серия FRONT / ООО ПК «КОМИНТЕХ»
20.	Операционные системы автоматизированных рабочих мест пользователей	ОС AlterOS / ООО «АЛМИ Партнер»	1. ОС специального назначения Astra Linux SE / ООО «РусБИТех-Астра» 2. ОС AlterOS / ООО «АЛМИ Партнер»
21.	Графическое окружение операционных систем	Cinnamon (в AlterOS) / свободное ПО	Встроенные средства ОС
22.	Приложения для изменения настроек и оптимизации операционных систем (твикеры), удаления данных	Встроенные средства ОС	

№ п/п	Информационно-технологические системы / типы ПО	Рекомендуемое для использования в КСПД оборудование и ПО / производитель	Рекомендуемое для использования в ТСПД (АСТУ, АСУТП и СДТУ) оборудование и ПО / производитель
23.	Установщики и менеджеры ПО/драйверов	Встроенные средства ОС	
24.	Утилиты рабочего стола	1. Gnome-screenshot / свободное ПО 2. Flameshot / свободное ПО 3. Kazam / свободное ПО 4. SimpleScreenRecorder / СПО 5. Xed / свободное ПО 6. Gnome-calculator / свободное ПО 7. Gucharmap / свободное ПО 8. Gnome-font-viewer / свободное ПО	-
25.	Межсетевые экраны уровня операционной системы	1. Встроенные средства ОС 2. Firewallld / свободное ПО	Встроенные средства ОС
26.	Системы автоматического управления конфигурацией операционной системы	1. Foreman / свободное ПО 2. Puppet / свободное ПО	Встроенные средства ОС
27.	Офисные пакеты автоматизированных рабочих мест пользователей	ПО AlterOffice / ООО «АЛМИ Партнер»	Встроенные средства ОС
28.	Системы электронной почты	1. VK WorkSpace / ООО «ВК Цифровые технологии» 2. RuPost / ООО «РуПост»	-
29.	Клиенты электронной почты	1. AMail (в AlterOS) / ООО «АЛМИ Партнер» 2. Evolution / свободное ПО 3. VK WorkSpace / ООО «ВК Цифровые технологии»	-
30.	Системы терминального доступа, виртуальных приложений и рабочих столов	Диспетчер подключений виртуальных рабочих мест Термидеск / ООО «Увеон»	-
31.	Клиенты для удаленного подключения к терминальным серверам, рабочим столам, консолям виртуальных машин	1. Remmina / свободное ПО 2. X11VNC (через SSL) / свободное ПО 3. Virt-viewer / свободное ПО 4. XRDP / свободное ПО 5. Putty / свободное ПО	-
32.	Эмуляторы терминала	1. Gnome-terminal / свободное ПО 2. Konsole / свободное ПО 3. Tmux / свободное ПО	-

№ п/п	Информационно-технологические системы / типы ПО	Рекомендуемое для использования в КСПД оборудование и ПО / производитель	Рекомендуемое для использования в ТСПД (АСТУ, АСУТП и СДТУ) оборудование и ПО / производитель
33.	Архиваторы	1. 7Zip / свободное ПО 2. FileRoller / свободное ПО 3. PeaZip / свободное ПО	Встроенные средства ОС
34.	Файловые менеджеры	1. Nemo / свободное ПО 2. Double Commander / свободное ПО 3. Midnight Commander / свободное ПО 4. Krusader / свободное ПО 5. Tunar / свободное ПО	Встроенные средства ОС
35.	Клиенты облачных файловых хранилищ	1. Яндекс. Диск / ООО «Яндекс» 2. VK WorkSpace / ООО «ВК Цифровые технологии» 3. Nextcloud / свободное ПО	-
36.	Браузеры	1. Яндекс Браузер для организаций / ООО «Яндекс» 2. Chromium Gost / свободное ПО	1. Яндекс Браузер для организаций / ООО «Яндекс»
37.	Средства просмотра документов	1. Evince / свободное ПО 2. Xreader / свободное ПО 3. Pix / свободное ПО 4. Xviewer / свободное ПО 5. MSG Viewer / свободное ПО 6. DWG Viewer (de.caff viewer) / свободное ПО	-
38.	Средства сканирования и распознавания изображений и документов	1. Simple-scan / свободное ПО 2. gscan2pdf / свободное ПО 3. xSane / свободное ПО 4. OCRFeeder / свободное ПО 5. ContentReader PDF / Content AI (ООО «Контент ИИ»)	-
39.	Специализированные редакторы PDF-документов	1. Master PDF Editor / ООО «Коде Индастри» 2. PDFSam / свободное ПО	-
40.	Приложения для ведения заметок	1. Joplin / свободное ПО 2. Cherrytree / свободное ПО	-
41.	Приложения для работы с CD и DVD	Brasero / свободное ПО	Встроенные средства ОС
42.	Медиаплееры	Videolan (VLC) / свободное ПО	Встроенные средства ОС
43.	Приложения для работы с мультимедиа и 3D-	1. Audacity / свободное ПО	-

№ п/п	Информационно-технологические системы / типы ПО	Рекомендуемое для использования в КСПД оборудование и ПО / производитель	Рекомендуемое для использования в ТСПД (АСТУ, АСУТП и СДТУ) оборудование и ПО / производитель
	графикой	2. KDeLive / свободное ПО 3. Blender / свободное ПО	
44.	Редакторы векторной (деловой) и растровой графики	1. АСМОграф / АО «Информатика» 2. GIMP / свободное ПО 3. InkScape / свободное ПО	-
45.	Системы автоматизированного проектирования	1. Платформа nanoCAD / АО «Нанософт» 2. ПК КРЕДО / ООО «Компания «Кредо-Диалог» 3. ПО КОМПАС-3D / ООО «Аскон - Системы Проектирования» 4. ПО СПДС Model Studio CS, GraphiCS, EnergyCS / АО «СиСофт Девелопмент»	-
46.	Системы мгновенного обмена сообщениями, организации видеоконференций и голосовых чатов	VK WorkSpace / ООО «ВК Цифровые технологии»	-
47.	Системы видеоконференцсвязи	1. Сервер видеоконференций IVA MCU / ООО «ИВКС» 2. Яндекс.Телемост / ООО «Яндекс» 3. VK Workspace / ООО «ВК Цифровые технологии»	-
48.	Справочные правовые системы	1. СПС КонсультантПлюс / ЗАО «Консультант Плюс» 2. ЭПС «Система ГАРАНТ» / ООО «НПП «Гарант-Сервис-Университет» 3. ИСС «Техэксперт» / АО «Информационная компания «Кодекс»	-
49.	Системы электронного документооборота	1. СЭДО DocuSign / ООО «АйДи – Технологии управления» 2. 1С ЭДОиЭА / ООО «РГИТС» 3. ИС КорПортал / ООО «ВК Цифровые технологии»	-
50.	Геоинформационные и навигационные средства (ГИС)	Яндекс Карты / ООО «Яндекс»	-
51.	Системы видеонаблюдения	1. TRASSIR профессиональная система видеонаблюдения / ООО «ДССЛ» 2. ПО Macroscop / ООО «Сателлит Инновация»	1. TRASSIR профессиональная система видеонаблюдения / ООО «ДССЛ» 2. ПО «Интеллект» / ООО «АйТиВи Групп» 3. ПО Macroscop / ООО «Сателлит Инновация» 4. ПО ISS(SecurOS) / ООО «ИСС-Софт»

№ п/п	Информационно-технологические системы / типы ПО	Рекомендуемое для использования в КСПД оборудование и ПО / производитель	Рекомендуемое для использования в ТСПД (АСТУ, АСУТП и СДТУ) оборудование и ПО / производитель
52.	Система контроля управления доступом	-	1. Контроллеры Sigur / ООО «ПромАвтоматика Софт» 2. Proximity-карты MIFARE Plus SE 7b 1K V2 и выше 3. Считыватели MIFARE с поддержкой OSDP предпочтительно SIGUR
53.	Системы проводной телефонной связи	Телефония Eltex / ООО «Предприятие «Элтекс»»	1. ECSS-10 - семейство IP-АТС / ООО «Предприятие «Элтекс» 2. Комбинированная АТС МиниКом MX-1000 / ГК «Информтехника»
54.	Системы радиосвязи	-	1. Комплекс цифровой радиосвязи «Волновая сеть» / ООО «Радиотехника» (для объектов с площадью радиопокрытия единицы квадратных километров) 2. Система микросотовой радиосвязи МиниКом-DECT (для объектов с площадью радиопокрытия единицы квадратных километров) / ГК «Информтехника» 3. Цифровая система радиосвязи стандарта DMR (для объектов с площадью радиопокрытия десятки квадратных километров) / ООО «КБ-Пульсар-телеком»
55.	Системы односторонней командно-поисковой связи и оповещения	-	1. Комплекс аппаратно-программных средств оповещения / ООО «Армтел» 2. Система связи DVS-21 / ООО «Промтрейд»
56.	Системы гарантированного электропитания АСУТП/СДТУ	-	1. Агрегаты бесперебойного питания (шкаф) / ООО «ЭКРА» 2. Агрегат бесперебойного питания двойного преобразования «Штиль PS220/2000К» (встраиваемый в шкаф) / ГК «Штиль» 3. Агрегаты бесперебойного питания/ ООО «НТЦ СГЭП» 4. Агрегаты бесперебойного питания/ ООО «Импульс»

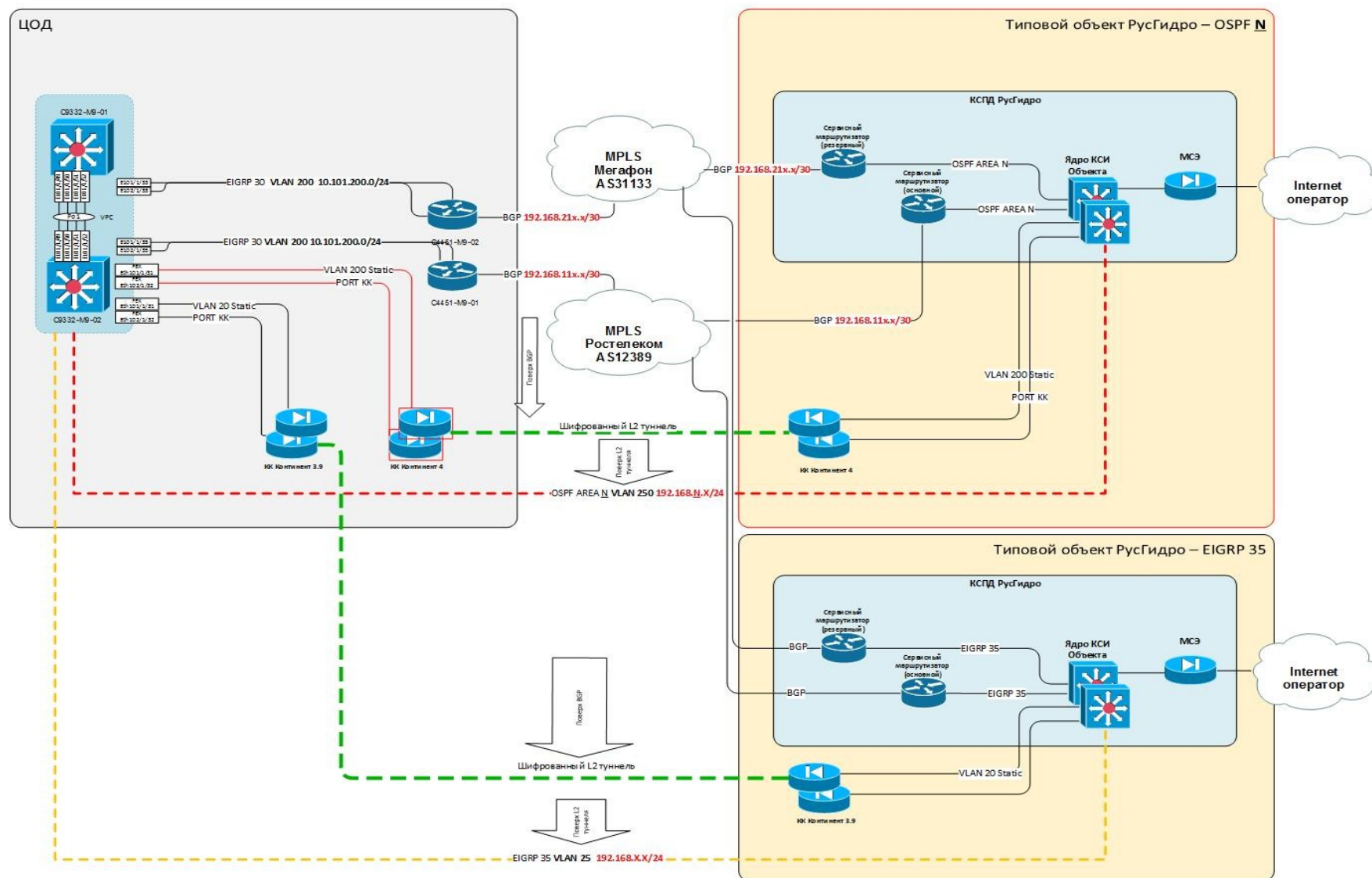
№ п/п	Информационно-технологические системы / типы ПО	Рекомендуемое для использования в КСПД оборудование и ПО / производитель	Рекомендуемое для использования в ТСПД (АСТУ, АСУТП и СДТУ) оборудование и ПО / производитель
57.	SCADA-системы для АСТУ ЦУС, РЭС	-	1. Платформа СК-11 / АО «Монитор Электрик» 2. Программный комплекс «С- Платформа» / ООО «Сигма-Софт Автоматизация»
58.	SCADA-система для АСТУ ЦУГ, генерирующих объектов	-	Программный комплекс «С- Платформа» / ООО «Сигма-Софт Автоматизация»
59.	SCADA-системы для центральной приемопередающей станции (ЦППС) и системы однонаправленной передачи информации	-	1. Программный комплекс КОТМИ-14 / ООО «Децима» 2. Платформа СК-11 / АО «Монитор Электрик»
60.	SCADA-система для автоматизации инженерных систем зданий	Программный комплекс «С- Платформа» / ООО «Сигма-Софт Автоматизация»	
61.	Автоматизированные информационно-измерительные системы коммерческого учета электроэнергии (АИИС КУЭ)	-	ПО «Пирамида 2.0» / ООО «АСТЭК»
62.	Автоматизированные информационно-измерительные системы коммерческого учета энергоресурсов (АИИС КУЭР)		ПО «Пирамида 2.0» / ООО «АСТЭК»
63.	Программное обеспечение системы мониторинга системных регуляторов / концентратор синхронизированных векторных данных	-	APDC / ООО «АПСофт»
64.	Многофункциональные измерительные преобразователи	-	1. ESM-HV / ООО «Инженерный центр «Энергосервис» 2. ЭНИП-2 УСВИ / ООО «ИЦ «Энергосервис» 3. ARIS-11XX / ООО «Прософт-Системы»
65.	Программируемые логические контроллеры и модули УСО	-	1. Линейка Regul R500 / ООО «РегЛаб» 2. Контроллеры Elicont-100 с модулями УСО серии Elicont-200 / АО «Элара» 3. Линейка Regul R050 / ООО «РегЛаб»

Таблица 2. Технические решения в области информационно-технологической инфраструктуры и рабочих мест в части аппаратного и программного обеспечения информационной безопасности.

№ п/п	Информационно-технологические системы / типы ПО	Рекомендуемое для использования в КСПД оборудование и ПО / производитель	Рекомендуемое для использования в ТСПД (АСТУ, АСУТП и СДТУ) оборудование и ПО / производитель
1.	Системы защиты каналов передачи данных, в том числе криптографическими методами	1. ПО СКЗИ Континент-АП и АПКШ Континент / ООО «Код Безопасности» 2. ПО семейства ViPNet и ПАК ViPNet Coordinator / АО «Инфотекс»	АПКШ Континент / ООО «Код Безопасности»
2.	Системы межсетевого экранирования (на стыке с Интернет)	UserGate NGFW / ООО «Юзергейт»	-
3.	Системы однонаправленной передачи данных	InfoDiode / ООО «АМТ-ГРУП»	1. InfoDiode / ООО «АМТ-ГРУП» 2. ОПТИ ИК,ДИОД / АО «Интерматик»
4.	Системы контроля конфигураций и анализа защищенности сетевого оборудования	ПО Efros Config Inspector и Efros Defence Operations / ООО «Газинформсервис»	-
5.	Приложения для анализа принимаемого/отправляемого трафика, перехвата и извлечения каких-либо данных из файлов	1. Tcpdump / свободное ПО 2. Wireshark / свободное ПО	-
6.	Системы обнаружения и/или предотвращения вторжений (атак) (анализ сетевого трафика, выявление и расследование инцидентов ИБ, защита от комплексных и целевых атак)	1. Positive Technologies Sandbox, также Network Attack Discovery, также Application Firewall и PT Industrial Security Incident Manager / АО «Позитив Текнолоджиз» 2. Kaspersky Anti Targeted Attack, также Endpoint Detection and Response и Industrial CyberSecurity for Networks / АО «Лаборатория Касперского»	1. PT Industrial Security Incident Manager / АО «Позитив Текнолоджиз» 2. Kaspersky Industrial CyberSecurity for Networks / АО «Лаборатория Касперского»
7.	Системы управления событиями информационной безопасности	1. MaxPatrol Security Information and Event Management /АО «Позитив Текнолоджиз» 2. Kaspersky Unifred Monitoring and Analysis Platform / АО «Лаборатория Касперского»	-
8.	Системы антивирусной защиты	Kaspersky Total Security и Industrial CyberSecurity for Nodes / АО «Лаборатория Касперского»	Kaspersky Industrial CyberSecurity for Nodes / АО «Лаборатория Касперского»
9.	Системы защиты от несанкционированного доступа к информации	Secret Net Studio/Secret Net LSP / ООО «Код Безопасности»	-
10.	Системы контроля действий привилегированных пользователей	СКДПУ НТ / ООО «АйТи Бастион»	-

№ п/п	Информационно-технологические системы / типы ПО	Рекомендуемое для использования в КСПД оборудование и ПО / производитель	Рекомендуемое для использования в ТСПД (АСТУ, АСУТП и СДТУ) оборудование и ПО / производитель
11.	Системы обнаружения уязвимостей, контроля и анализа защищенности	XSpider и MaxPatrol VM / АО «Позитив Текнолоджиз»	Сканер-ВС/НПО Эшелон
12.	Система обнаружения и предотвращения утечек информации (DLP)	ПО Solar Dozor / ООО «СОЛАР Секьюрити»	-
13.	Системы криптографической защиты информации и электронной подписи	Семейство КриптоПро / ООО «КриптоПро»	-
14.	Приложения для управления ключевыми носителями	1. ПК Единый клиент JaCarta / АО «Аладдин Р.Д.» 2. Семейство Рутокен / АО «Актив-софт»	-
15.	Системы автоматизации процессов информационной безопасности	1. ПО АльфаДок. Платформа / ООО «НПЦ «КСБ» 2. Security Vision: Центр интеллектуального мониторинга и управления информационной безопасностью / ООО «Триметр»	-
16.	Средства автоматизации управления инцидентами ИБ (взаимодействие с ГосСОПКА)	ПК Security Vision Security Orchestration Automation and Response / ООО «Интеллектуальная безопасность»	-
17.	Системы управления доступом к информационным ресурсам (средство двухфакторной аутентификации)	1. МУЛЬТИФАКТОР / ООО «Мультифактор» 2. Bitrix OTP (только для ИС на базе продуктов 1С-Битрикс) / ООО «БИТРИКС»	-
18.	Системы для безопасного хранения, управления и совместного использования паролей	Менеджер паролей Пассворк / ООО «Пассворк»	-
19.	Системы аккумулирования и контроля служебной переписки	Архива / ООО «Дата Оушен»	-
20.	Системы регистрации телефонных вызовов и речевых сообщений	Многоканальная система регистрации телефонных вызовов и речевых сообщений Незабудка II / ООО «Центр речевых технологий»	Многоканальный цифровой комплекс регистрации сообщений «Фантом» / ЗАО «МДИС»

Приложение 1
Типовая схема подключения подконтрольных обществ к КСПД



2.1. Минимальные требования к характеристикам ПК

Технические характеристики	Стационарное рабочее место	Мобильное рабочее место
Процессор	Intel Core i5 поколения X ⁹ -2 или аналог по производительности	Intel Core i5 поколения X-2 или аналог по производительности
Оперативная память	8 ГБ DDR4	8 ГБ DDR4
Накопитель	256 ГБ SSD pcie m.2	256 ГБ SSD pcie m.2
Внешние порты ввода/вывода	4xUSB 2.0/3.0 (не менее 2 шт. версии 3.0), HDMI или DisplayPort (любые 2 из указанных разъёма для видео)/ Type C, Аудио: комбинированный выход (наушники) / вход (микрофон) 3,5 мм, RJ-45	2xUSB 3.0, HDMI, Type C (с выводом видео), Аудио: комбинированный выход (наушники) / вход (микрофон) 3,5 мм, RJ-45
Экран	-	14-16" ips 1920x1080, 350 кд/м ²
Видео	Не менее 2 ГБ видеопамати, поддержка 2х мониторов разрешением 2560*1440p 60 Гц	Не менее 2 ГБ видеопамати, поддержка 2х мониторов разрешением 2560*1440p 60 Гц
Монитор	IPS 24-27" с HDMI/ DisplayPort/ 1920*1080p, 60 Гц, регулировка по высоте, встроенный блок питания, видеокабель HDMI или DP в комплекте, яркость 250 кд/м ² , контрастность 1000:1, углы обзора 178 град. по горизонтали и вертикали	IPS 27" с HDMI/ DisplayPort/ 2560*1440p, 60 Гц, регулировка по высоте, встроенный блок питания, видеокабель HDMI или DP в комплекте, яркость 250 кд/м ² , контрастность 1000:1, углы обзора 178 град. по горизонтали и вертикали
Коммуникационные порты	100/1000	100/1000, IEEE 802.11 a/b/g/n/ac/ax, bluetooth v5.0
Устройства ввода/вывода	Проводные оптическая мышь, клавиатура	Беспроводные оптическая мышь, клавиатура, док-станция с собственным блоком питания, power delivery 60 Вт и поддержкой 2х мониторов разрешением 2560*1440p 60 Гц, 2 порта HDMI/DP, 4 USB (не менее 2 шт. версии 3.0)
Гарантия	3 года, выездная на основное устройство и монитор	3 года, выездная на основное устройство и монитор
Производитель основного устройства ¹⁰	РФ	РФ

9 X – последнее официально объявленное и поступившее в продажу поколение процессоров Intel на дату использования данного приложения (планирования закупки, запроса предложения и т.д.). На 09.2023 это 13-2=11, т.е. процессор i5-11 или аналог. Предпочтение отдаётся максимальному индексу частоты процессора.

10 При отсутствии оборудования с необходимыми характеристиками в реестре Минпромторга допускается использовать оборудование, произведённое в другой стране при соблюдении требований законодательства.

Для «мобильного рабочего места руководителя» относительно «мобильного рабочего места» должно быть в 2 раза больший объём оперативной памяти и накопителя, процессор Intel Core i7 поколения X-1 или аналог, сенсорный экран и не менее 2560x1440 разрешение, вес не более 1.5 кг, монитор с разрешением 3840x2160 (возможен тип матрицы OLED), поддержка 2х мониторов с разрешением 3840x2160 видеокартой основного устройства и док-станцией, беспроводные эргономичные клавиатура и мышь с поддержкой Bluetooth, не применяются требования к стране производства при выполнении общих требований по импортозамещению.

Для «высокопроизводительного стационарного рабочего места» относительно «стационарного рабочего места» должно быть в 4 раза больше объём оперативной памяти и жесткого диска, процессор Intel Core i7 поколения X-1 или аналог, 2 монитора 27" с разрешением 3 3840x2160 или один широкоформатный монитор размером 36" с разрешением не менее 3 840 по длинной стороне, внешняя видеокарта уровня, соответствующего по характеристикам NVIDIA Y¹¹070ti с объёмом видеопамати не менее 8 Гб, не применяются требования к стране производства при выполнении общих требований по импортозамещению.

Минимальные требования к «специализированному рабочему месту отсутствуют», оборудование выбирается по заявкам подразделений с подробным обоснованием потребности, не применяются требования к стране производства при выполнении общих требований по импортозамещению.

2.2. Минимальные требования к системному ПО рабочих мест пользователей

Версии ПО:

AlterOS («АльтрОС») Бизнес 2025 , Версия 64 бит с поддержкой TLS, ядро не ниже 6.6

AlterOffice («АльтрОфис») Бизнес 2025 версия не ниже 3.0.1, в составе:

- AText – текстовый процессор;
- ACell – табличный процессор;
- AConcept – приложение для работы с презентациями;
- AGraph – векторный графический процессор для создания схем, диаграмм, технических иллюстраций и изображений;
- AMail – приложение для управления почтой, календарем и контактами.

Kaspersky Total Security 14.0.

¹¹ Y – последнее официально объявленное и поступившее в продажу поколение видеокарт NVIDIA на дату использования данного приложения (планирования закупки, запроса предложения и т.д.). На 09.2023 это 4-1=3, т.е. NVIDIA 3070ti или аналог.

Все используемое ПО должно быть лицензировано в установленном порядке.

2.3. Минимальные требования к периферийным устройствам печати

2.3.1 Требования к принтерам

№	Вид	Категория	Характеристика	Минимальное значение
1.	Принтер лазерный монохромный	Персональный	Скорость монохромной печати А4	15 стр./мин (формат А4)
			Разрешение при печати	600х600 точек на дюйм
			Время выхода первого отпечатка	не более 10 с
			Устройство подачи бумаги	кассета на 250 листов
			Формат бумаги	А4, А5, LTR
			Интерфейс с ПК	USB, Fast Ethernet
2.	Принтер цветной офисный лазерный	Персональный	Скорость печати	цветная печать: 10 стр./мин (формат А4)
			Разрешение при печати	600х600 точек на дюйм
			Время выхода первого отпечатка	не более 20 с в монохромном и цветном режиме
			Устройства подачи бумаги	кассета на 250 листов
			Формат бумаги	А4, А5, LTR
			Интерфейс с ПК	USB, Ethernet
3.	Принтер лазерный	Групповой	Тип	Монохромный или цветной
			Двусторонняя печать	Да, динамическая
			Скорость монохромной печати А4	30 стр./мин (формат А4)
			Разрешение при печати	1200х1200 точек на дюйм
			Время выхода первого отпечатка	не более 10 с
			Устройство подачи бумаги	кассета на 500 листов не менее 2х штук
			Формат бумаги	А3, А4, А5, LTR
			Интерфейс	Fast Ethernet
			Поддержка языков	PCL5e, PCL6

2.3.2. Требования к сканерам

№	Вид	Категория	Характеристика	Минимальное значение
1.	Сканер	Персональный офисный	Тип	Настольный планшетный
			Сканирование	Чёрно белое и цветное
			Оптическое разрешение	1200x1200 точек на дюйм
			Интерфейс	USB, Ethernet
			Разрядность сканирования	24 бита
			Максимальный формат документа	A4

2.3.3. Требования к многофункциональным устройствам

№	Вид	Категория	Характеристика	Минимальное значение
1.	МФУ с лазерной печатью	Персональный	Скорость монохромной печати A4	20 стр./мин (формат A4)
			Разрешение при печати	600x600 точек на дюйм
			Функции аппарата	печать, двухстороннее автоматическое сканирование в почту и копирование
			Тип сканера	Планшетный с автоподатчиком оригиналов
			Время выхода первого отпечатка	не более 10 с
			Устройство подачи бумаги	кассета на 250 листов
			Формат бумаги	A4, A5, LTR
			Разрешение при сканировании	1200x1200 точек на дюйм
			Глубина цветного сканирования	24 бита
			Разрешение при копировании	600x600 точек на дюйм
			Скорость копирования	20 копий/мин
			Интерфейс с ПК	USB, Fast Ethernet
2.	МФУ с	Групповой	Принцип	цифровой

№	Вид	Категория	Характеристика	Минимальное значение
	лазерной печатью		Запас бумаги	кассета на 500 листов
			Формат бумаги	A4, A5, LTR
			Функции аппарата	печать, двухстороннее автоматическое сканирование в почту и сетевые ресурсы, копирование
			Плотность бумаги	60 – 160 г/м ²
			Время выхода первой копии (1:1, A4)	10 с
			Скорость копирования (1:1, A4)	30 копий/мин
			Разрешение сканирования	600x600 dpi аппаратное
			Разрешение печати	1200x1200 dpi с интерполяцией
			Языки описания страниц	PCL5c, PCL6
			Двусторонняя печать	Да, автоматическая
			Автоподача при сканировании	Да автоматическая
			Интерфейс	Fast Ethernet
3.	МФУ с лазерной печатью	Корпоративный	Принцип	цифровой
			Функции аппарата	печать, двухстороннее сканирование, копирование, сканирование в электронный почтовый ящик и сетевые ресурсы.
			Запас бумаги	2 лотка на 500 листов
			Формат бумаги	A3, A4, A5, LTR
			Плотность бумаги	60 – 200 г/м ²
			Время выхода первой копии (1:1, A4)	10 с
			Скорость копирования и печати, цвет и ч/б	30 копий/мин
			Разрешение сканирования	600x600 dpi аппаратное
			Разрешение печати	1200x1200 dpi с интерполяцией

№	Вид	Категория	Характеристика	Минимальное значение
			Материалы для копирования	Обычная бумага, пленки (прозрачные, матовые и самоклеящиеся), конверты, трансферные материалы, фотобумага
			Максимальное количество копий за один цикл	500
			Языки описания страниц	PCL5c, PCL6
			Жесткий диск	20Гбайт
			Двусторонняя печать	Да, автоматическая
			Автоподача при сканировании	Да, автоматическая
			Установка	Напольная тумба
			Дополнительно	Считыватель для авторизации или штатное место под него
			Интерфейс	Fast Ethernet

2.4 Требования к телефонным аппаратам

Телефонные аппараты должны распределяться между работниками согласно занимаемой должности.

Всего должно быть выделено 3 класса устройств:

- Телефонный аппарат стандартный;
- Телефонный аппарат улучшенный;
- Телефонный аппарат руководителя.

2.4.1 Требования к стандартным телефонным аппаратам

Стандартный телефонный аппарат должен удовлетворять следующим минимальным требованиям:

- Поддержка протокола SIP;
- Наличие дисплея с подсветкой размером не менее 3 дюймов;
- Наличие встроенного интерфейса Ethernet 10/100 Base T с вторичным портом Ethernet 10/100 Base T для подключения ПК с возможностью разделения портов в VLAN;
- Поддержка технологии Power over Ethernet (PoE);
- Поддержка протокола LLDP или аналог;
- Наличие дуплексного спикерфона с кнопкой отключения микрофона;
- Возможность подключения гарнитуры;
- Поддержка кодеков G.711a/μ, G.722, G.729a;

- Поддержка русского языка;
- Наличие ПО на Linux позволяющее обеспечивать автоматическую настройку парка телефонных аппаратов.

Наличие аппаратных клавиш удержание, конференция, перевод вызова, увеличение / уменьшение громкости.

2.4.2 Требования к улучшенным телефонным аппаратам

Улучшенный телефонный аппарат должен удовлетворять следующим минимальным требованиям:

- Поддержка протокола SIP;
- Наличие дисплея с подсветкой размером не менее 5 дюймов;
- Наличие встроенного интерфейса Ethernet 10/100/1000 Base T с вторичным портом Ethernet 10/100/1000 Base T для подключения ПК с возможностью разделения портов в VLAN;
- Поддержка технологии Power over Ethernet (PoE);
- Возможность подключения клавишного модуля;
- Поддержка протокола LLDP или аналог;
- Наличие дуплексного спикерфона с кнопкой отключения микрофона;
- Возможность подключения гарнитуры;
- Поддержка кодеков G.711a/μ, G.722, G.729a;
- Поддержка русского языка;
- Наличие ПО на Linux позволяющее обеспечивать автоматическую настройку парка телефонных аппаратов;
- Наличие аппаратных клавиш удержание, конференция, перевод вызова, телефонная книга, увеличение/уменьшение громкости;
- Блок питания в комплекте.

2.4.3 Требования к телефонным аппаратам для руководителей

Телефонный аппарат для руководителей должен удовлетворять следующим минимальным требованиям:

- Поддержка протокола SIP;
- Наличие цветного дисплея размером не менее 5 дюймов;
- Наличие встроенной камеры;
- Поддержка разрешения 720p HD (кодирование и декодирование)
- Наличие встроенного интерфейса Ethernet 10/100/1000 Base T с вторичным портом Ethernet 10/100/1000 Base T для подключения ПК с возможностью разделения портов в VLAN;
- Поддержка технологии Power over Ethernet (PoE);
- Возможность подключения не менее двух клавишных модулей с цветным экраном и индикацией занятой линии, 1 модуль в комплекте;
- Поддержка протокола LLDP или аналог;

- Наличие дуплексного спикерфона с кнопкой отключения микрофона;
- Возможность подключения проводной и беспроводной гарнитуры;
- Поддержка кодеков G.711a/μ, G.722, G.729a;
- Поддержка видеокодека H.264;
- Поддержка русского языка;
- Наличие ПО на Linux позволяющее обеспечивать автоматическую настройку парка телефонных аппаратов;
- Наличие аппаратных клавиш удержание, конференция, перевод вызова, телефонная книга, увеличение/уменьшение громкости;
- Блок питания в комплекте для телефона и клавишного модуля при необходимости.

2.5 Требования к клиентскому программному обеспечению системы телефонии, аудио-конференцсвязи и ВКС.

Клиентское ПО системы телефонии, аудио-конференцсвязи и ВКС должно обеспечивать:

- возможность работы под ОС Windows, MacOS, Android, iOS, AlterOS;
- поддержку голосовых и видео вызовов в режиме точка-точка и точка-многоточка;
- возможность передачи текстовых сообщений, динамических статусов, файлов, пиктограмм, изображающие эмоции;
- возможность организации групповых чатов;
- доступ к сервисам телефонии, аудио-конференцсвязи и ВКС, а также сервисам унифицированных коммуникаций, как в пределах среды передачи данных Группы, так и из публичной сети.

Приложение 3. Реестр запрещенных к использованию типов программного обеспечения в Группе РусГидро

В Группе запрещено использование любого ПО, не входящего в Реестр типовых технических и программных средств, применяемых в ИТ инфраструктуре Группы, без согласования с Управлением кибербезопасности ДИТ (далее УКБ ДИТ).

Согласование установки дополнительного ПО осуществляется работниками УКБ ДИТ на основании должностных инструкций и функциональных обязанностей пользователя. Типы ПО, запрещенные к использованию в информационно-технологической инфраструктуре Группы, указаны в Таблице:

№ п/п	Тип программного обеспечения, запрещенного к использованию
1	Вредоносное (трояны, вирусы, сетевые черви, эксплойты, руткиты, кейлогеры, программы-шпионы, -вымогатели, -майнеры, рекламные/маркетинговые программы и т.п.)
2	Взлома другого программного обеспечения (различного рода «кряки», активаторы, средства генерации паролей и серийных ключей и т.п.)
3	Копирования и изменения данных в оперативной памяти, загрузки и/или модификации контекста объектных модулей в регистрах центрального процессора, оказания влияния на запущенные процессы и выполняемые программы
4	Удаленного доступа, управления и администрирования*
5	Изменения настроек и оптимизации операционных систем (твикеры), удаления данных*
6	Установщики и менеджеры программного обеспечения/драйверов*
7	Средства разработки и программирования, средства отладки объектных модулей программного обеспечения*
8	Анализа принимаемого/отправляемого трафика, перехвата и извлечения каких-либо данных из файлов*
9	Тестирования на проникновение (пентест-инструменты)*
10	Симуляции/виртуализации аппаратных средств (ЖМД, ОД, электронных ключей, ЛВС) и центрального процессора*
11	Симуляции/виртуализации операционных систем, подпрограмм операционных систем или средств вычислительной техники целиком*
12	Организации виртуальных частных сетей*
13	Анонимного сетевого соединения
14	Создания и использования I2P-сетей и mesh-сетей
15	Шифрования/дешифрования, криптографического анализа и защиты*
16	Системы мгновенного обмена сообщениями, организации видеоконференций и голосовых чатов*
17	Для работы с машинными носителями информации (HDD, SSD и др.): тестирование, диагностика, восстановление данных, создание образов, резервное копирование и дублирование*

18	Торрент-клиенты и другие менеджеры загрузок
19	Системы/сервисы обмена файлами, размещенные вне сетевого периметра Группы**

В случае обнаружения на рабочем месте пользователя программного обеспечения указанных типов оно подлежит немедленному удалению Службой поддержки пользователей с оповещением УКБ ДИТ.

* Здесь и далее: за исключением ПО, включенного в Перечень.

** За исключением:

- ПО, включенного в Реестр;

- внешних сервисов обмена файлами, с которыми заключен договор на оказание услуг и подписано соглашение о конфиденциальности, а также приняты меры по предотвращению утечки информации.

Приложение 4. Минимальные требования к мультисервисной сети

4.1. Минимальные требования к корпоративной распределенной мультисервисной сети

4.1.1. Общие требования

Схема резервирования оборудования мультисервисной сети для Объектов I уровня должна быть организована (для Объектов II уровня рекомендуется), в соответствии со следующими принципами:

- На уровне ядра сети должно быть не менее двух высокопроизводительных коммутаторов уровня L3 объединенных в стек между собой не менее чем двумя интерфейсами, пропускной способностью 10/40/100 GigabitEthernet, в соответствии с заранее определенными требованиями к необходимой пропускной способности.

- Каждый коммутатор уровня доступа должен иметь не менее одного соединения полосой пропускания не менее 10 Gigabit Ethernet с каждым коммутатором уровня распределения или коммутатором уровня ядра.

- Каждый коммутатор уровня распределения должен иметь не менее одного соединения полосой пропускания 10/40 Gigabit Ethernet с каждым коммутатором уровня ядра.

- В мультисервисной сети должно быть не менее двух пограничных маршрутизаторов, обеспечивающих передачу данных между КСПД и операторами связи, предоставляющими услуги доступа в Интернет и услуги выделенных VPN каналов между корпоративными и технологическими площадками Группы. Услуги доступа в Интернет и услуги VPN должны быть зарезервированы на уровне сети передачи данных одного оператора связи (иметь два географически разнесенных, взаиморезервируемых канала связи до площадки Группы) или путем организации резервных каналов через разных операторов связи. Каждый пограничный маршрутизатор должен быть связан с двумя устройствами, обеспечивающими функциональность МСЭ с поддержкой IDS/IPS.

- Пограничные маршрутизаторы должны поддерживать протоколы динамической маршрутизации, такие как OSPF, IS-IS, BGP.

- Производительность сети для Объектов I и II уровня должна быть обеспечена следующим образом:

- Этажные коммутаторы (коммутаторы доступа) должны соединяться с коммутаторами уровня распределения с использованием интерфейсов пропускной способностью не менее 10 Gigabit Ethernet, через оптические линии связи, допускается организация подключения через медные

линии связи, если при этом соблюдаются технические требования, определенные группой стандартов IEEE 802.3.

- Серверное оборудование должно подключаться к коммутаторам серверной фермы.

- Коммутаторы серверной фермы должны быть выбраны в соответствии с требуемой производительностью и типами интерфейсов.

- При выборе производителя и модели коммутаторов серверной фермы необходимо руководствоваться техническими требованиями к среде передачи данных серверного оборудования.

- 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.

- Для организации связи между соседними зданиями одного Объекта, требуется использовать оптические линии связи.

- Для организации связи между удаленными объектами, использовать выделенные каналы связи VPN, арендуемые у операторов.

- Пользовательские и периферийные устройства подключаются к коммутаторам доступа по Ethernet 10/100/1000 Base-T. В зависимости от типов интерфейсов и требуемой пропускной способности подключаемых устройств.

Требуется 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

Требования к коммутаторам

Требуется закупать коммутаторы, которые поддерживают следующие протоколы:

- 802.1s Multiple Spanning Tree;
- 802.1p Priorities;

- 802.1q VLAN Tagging;
- 802.3ad Link Aggregation;
- 802.3ae 10 GbE;
- 802.1w Rapid STP;
- GVRP;
- IGMP v3 (RFC 2236);
- IGMP Snooping;
- ECMP (8 Paths);
- Diff Serv;
- PoE для коммутаторов уровня доступа;
- MST,802.1x;
- LLDP;
- LAG;
- LACP.

Требуется закупать коммутаторы, которые обладают следующими минимальными требованиями к производительности:

	Коммутатор доступа	Коммутатор уровня распределения	Коммутатор ядра
Многоуровневая коммутация	Базовая функциональность, уровень 2	Полноценная функциональность, уровни 2 и 3	Базовая функциональность, уровни 2 и 3
Полоса пропускания	128 Гбит/с	800 Гбит/с	3000 Гбит/с
Производительность	80 Mpps	500 Mpps	1500 Mpps
SDRAM	128 Мб	2000 Мб	16000 Мб
FLASH	256 Мб	4000 Мб	32000 Мб
Число одновременных VLAN	1000	4000	4 000
Наработка "на отказ" (MTBF)	от 150,000 часов	от 150,000 часов	от 150,000 часов

Все коммутаторы должны:

- Иметь SFP порты / слоты для стекирования или поддерживать виртуальное стекирование
- Быть неблокируемыми.

Требуется маршрутизаторы, которые поддерживают следующие протоколы:

Маршрутизаторы	Пограничные маршрутизаторы
-----------------------	-----------------------------------

General Routing (RFC 1812)	General Routing (RFC 1812)
RIP v1/v2 (RFC 2453)	RIP v1/v2 (RFC 2453)
RIP ECMP	RIP ECMP
OSPF v2 (RFC 2328)	OSPF v2 (RFC 2328)
OSPF Graceful Restart	OSPF Graceful Restart
OSPF ECMP	OSPF ECMP
OSPF NSSA (RFC 1587)	OSPF NSSA (RFC 1587)
IS-IS (RFC 1195)	IS-IS (RFC 1195)
IS-IS Graceful Restart	IS-IS Graceful Restart
IS-IS ECMP	IS-IS ECMP
VRRP (RFC 2338)	BGP-4 (RFC 1771)
DVMRP	BGP-4 Graceful Restart
PIM-SM	VRRP (RFC 2338)
Route Redistribution	DVMRP
	DMVPN
	PIM-SM
	Route Redistribution

Требуется закупать маршрутизаторы, которые обладают следующими минимальными требованиями к производительности:

	Маршрутизатор
Производительность	300 kpps
DRAM	512 Мб
FLASH	256 Мб
Наработка "на отказ" (MTBF)	от 150,000 часов

Требования к точке радиодоступа стандарта Wi-Fi

Требования к оборудованию Wi-Fi:

- поддержка семейства стандартов IEEE 802.11a/b/g/n/ac Wave 1 и Wave 2;
- виртуальные локальные сети (VLAN) – до 16 сегментов;
- приоритезация 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;
- протокол EAP (Extensible Authentication Protocol);
- протокол TKIP (Temporal Key Integrity Protocol);
- локальное и удаленное питание по витой паре;
- иметь встроенную антенну.

Требования к кодеку ВКС:

- поддерживать работу в сетях как IP (H.323), 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: RJ45 Ethernet, 10/100/1000 Мбит/с full/half duplex;
- обеспечивать подключение ПК и других источников сигнала (документкамера, видеокамера и т.д.).

Приложение 5. Минимальные требования к инфраструктуре центров обработки данных

5.1 Минимальные требования к системам обработки и хранения данных

5.1.1 Требования к серверам

Серверы должны удовлетворять следующим требованиям:

- CPU – последнего поколения;
- RAM – последнего поколения;
- дисковая подсистема:
- используемые контроллеры и диски должны поддерживать технологию горячей замены (hot swap);
- двухканальный RAID контроллер, кэш память контроллера с батарейной поддержкой, аппаратная поддержка RAID 0, 1, 1+0, 5, 6;
- минимум 2 диска для организации RAID 1;
- допускается использование бездисковых серверов с загрузкой ОС по SAN сети;
- минимум 2*USB 2.0 порта;
- минимум два порта Ethernet со скоростью не менее 1 Гбит/с;
- возможность установки дополнительных адаптеров Ethernet;
- возможность установки Fiber Channel Host Bus Adapter;
- наличие удаленного управления и мониторинга по сети Ethernet через выделенный Ethernet-порт обеспечивающее как минимум:
 - просмотр параметров и состояния всех аппаратных компонентов;
 - мониторинг температуры аппаратных компонентов;
 - управление питанием (включение, выключение, перезагрузка) сервера;
 - подключение к текстовой и графической консоли сервера;
 - изменение настроек BIOS/UEFI;
 - подключение к серверу CD/DVD-приводов, USB-устройств и образов ISO с рабочей станции администратора;
 - установку ОС;
- минимум 2 блока питания с горячей заменой,
- дизайн для установки в шкаф 19”.

5.1.2 Требования к Blade-серверам

Blade-системы должны удовлетворять следующим требованиям:

- Выбранная линейка должна содержать развитый модельный ряд серверов.
- Шасси предназначено для установки в шкаф 19”.
- Высота занимаемого пространства в шкафу не более 10U.

- Blade-система должна поддерживать удаленное управление и мониторинг по сети Ethernet через выделенный Ethernet-порт обеспечивающее как минимум:

- просмотр параметров и состояния всех аппаратных компонентов;
- мониторинг температуры аппаратных компонентов;
- управление питанием (включение, выключение, перезагрузка) серверов;
- подключение к текстовой и графической консоли сервера;
- изменение настроек BIOS/UEFI;
- подключение к серверу CD/DVD-приводов, USB-устройств и образов ISO с рабочей станции администратора;
- установку ОС.

- Шасси должно поддерживать следующие возможности монтажа аппаратных компонентов системы:

- 16 блейд-серверов, удовлетворяющих требованиям, указанным ниже;
- До 8 коммутаторов локальной вычислительной сети (LAN);
- До 6 коммутаторов сети хранения данных (SAN);
- Шасси должно обеспечиваться блоками питания с уровнем доступности N+N (N блоков необходимо для питания шасси в полной конфигурации, N – в горячем резерве);
- Шасси должно охлаждаться вентиляторными модулями достаточной мощности в количестве, необходимом для отказоустойчивой работы комплекса.

Блейд-серверы должны монтироваться в серверное шасси, удовлетворяющее требованиям, указанным выше, и сами удовлетворять следующим требованиям:

- Серверы должны комплектоваться не менее чем двумя дисками с поддержкой горячей замены с возможностью объединения в RAID 1. Допускается использование бездисковых серверов с загрузкой ОС по SAN сети.

- Серверы должны комплектоваться не менее чем двумя процессорами последнего поколения.

- Серверы должны комплектоваться оперативной памятью последнего поколения.

- Серверы должны комплектоваться двумя портами Fiber Channel для подключения к внешним СХД.

- Серверы должны комплектоваться двумя портами Ethernet.

Коммутаторы локальной вычислительной сети (LAN) должны монтироваться в серверное шасси, удовлетворяющее требованиям, указанным выше, и сами удовлетворять следующим требованиям:

- коммутаторы должны иметь не менее 4-х внешних портов SFP для установки как медных интерфейсов с разъемом RJ-45, так и оптических SX;
- коммутаторы должны иметь не менее восьми внешних портов с интерфейсами 10/100/1000Base-T;
- коммутаторы должны поддерживать все необходимые для работы серверов сетевые протоколы.

Коммутаторы сети хранения данных (SAN) должны монтироваться в серверное шасси, удовлетворяющее требованиям, указанным выше, и сами удовлетворять следующим требованиям:

- коммутаторы должны иметь не менее восьми внешних портов SFP для установки различных оптических трансиверов Fibre Channel (FC);
- коммутаторы должны поддерживать все протоколы, необходимые для совместной работы blade-серверов и внешних СХД.

Требования следующих ГОСТ при проектировании ЦОД:

1. ГОСТ Р 30134-1-2018 Информационные технологии (ИТ). ЦОД. Ключевые показатели эффективности. Часть 1. Основные положения и общие требования.

2. ГОСТ Р 30134-2-2018 Информационные технологии (ИТ). ЦОД. Ключевые показатели эффективности. Часть 2. Коэффициент энергоэффективности (PUE).

3. ГОСТ Р 30134-3-2018 Информационные технологии (ИТ). ЦОД. Ключевые показатели эффективности. Часть 3. Коэффициент возобновляемой энергии (REF).

4. ГОСТ Р 57875-2017 Телекоммуникации. Схемы соединения и заземление в телекоммуникационных центрах.

5. ГОСТ Р 58811-2020 ЦОД. Инженерная инфраструктура. Стадии создания.

6. ГОСТ Р 58812-2020 ЦОД. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация.

7. ГОСТ Р 59486-2021 Слаботочные системы. Кабельные системы. Кабельные системы для высокопроизводительных сетей в ЦОД. Основные положения.

Приложение 6. Требования к документированию

Документация, создаваемая при проектировании и внедрении систем должна выпускаться с учетом требований следующих нормативных документов:

- ГОСТ 2.105-2019. Единая система конструкторской документации. Общие требования к текстовым документам.
- ГОСТ 2.119-2013. Единая система конструкторской документации. Эскизный проект.
- ГОСТ 2.304-81. Единая система конструкторской документации. Шрифты чертежные.
- ГОСТ 2.601-2019. Единая система конструкторской документации. Эксплуатационные документы.
- ГОСТ 2.701-2008. Единая система конструкторской документации. Схемы. Виды и типы. Общие требования к выполнению.
- ГОСТ 2.780-96. Единая система конструкторской документации. Обозначения условные графические. Кондиционеры рабочей среды, емкости гидравлические и пневматические.
- ГОСТ 34.201-2020. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.
- ГОСТ 34.602-2020. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
- ГОСТ Р 2.101-2023. Единая система конструкторской документации. Виды изделий.
- ГОСТ Р 57193-2025. Системная и программная инженерия. Процессы жизненного цикла систем.
- ГОСТ Р 59792-2021. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем.
- ГОСТ Р 59795-2021. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.

Окончательные требования к документированию в зависимости от объекта определяются в технических требованиях и технических заданиях на создание систем.