

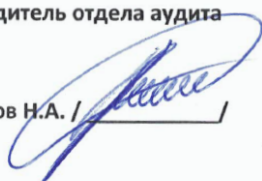
Отчет

об аудите средств информационных технологий

ФГБУ РАН

Подготовлено:

Руководитель отдела аудита

Кузнецов Н.А. / 

УТВЕРЖДАЮ:

Генеральный директор ООО
«Виртуализация ИТ»

Кузнецов Н.А. / 

М. П.



Оглавление

ЦЕЛЬ АУДИТА.....	3
МЕСТО ПРОВЕДЕНИЯ АУДИТА	3
ХАРАКТЕРИСТИКА ОБЪЕКТА ОБСЛЕДОВАНИЯ	4
СОДЕРЖАНИЕ РАБОТ	5
СУЩЕСТВУЮЩАЯ ДОКУМЕНТАЦИЯ ЗАКАЗЧИКА	6
ОБЩАЯ ИНФОРМАЦИЯ	9
ИНФОРМАЦИОННЫЕ СИСТЕМЫ	13
ВЫЧИСЛИТЕЛЬНОЕ ОБОРУДОВАНИЕ.....	15
СХД	18
ОБОРУДОВАНИЕ СЕТИ ХРАНЕНИЯ ДАННЫХ.....	20
ОБОРУДОВАНИЕ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ	22
ОБОРУДОВАНИЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ.....	24
СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	29
СРЕДСТВА ВКС	46
СРЕДСТВА ИНЖЕНЕРНОЙ ИНФРАСТРУКТУРЫ	47
ОРГАНИЗАЦИОННАЯ СТРУКТУРА	52
ПОЛЬЗОВАТЕЛЬСКИЕ АРМ	54
ОСНОВНЫЕ ВЫВОДЫ.....	55
РЕКОМЕНДАЦИИ	56
РЕКОМЕНДОВАННАЯ КОНЦЕПЦИЯ РАЗВИТИЯ ИТ ИНФРАСТРУКТУРЫ.....	58
ПРЕДЛАГАЕМАЯ СХЕМА РЕАЛИЗАЦИИ СЕРВЕРНОЙ ИНФРАСТРУКТУРЫ	66

Цель аудита

Проведение аудита ИТ-инфраструктуры обусловлено необходимостью получения Заказчиком наиболее полной, систематизированной и достоверной информации о её текущем состоянии с целью:

- Принятия дальнейших решений по управлению и эксплуатации ИТ-инфраструктурой;
- Снижения расходов, связанных с совокупной стоимостью владения ИТ-инфраструктурой;
- Выявления существующих проблем в ИТ-инфраструктуре и выработки рекомендаций по их устранению;
- Выявления и определения степени соответствия ИТ-инфраструктуры основным задачам, стоящим перед Заказчиком;
- Повышения эффективности работы ИТ-инфраструктуры, соответствия требованиям по информационной безопасности и надежности функционирования бизнес-процессов Заказчика;
- Последующей разработки проектного решения по развитию, модернизации и повышению качества ИТ-инфраструктуры Заказчика.

Место проведения аудита

- г. Москва, Ленинский проспект, дом 14;
- г. Москва, Ленинский проспект, дом 14 (стр. 1; стр. 2; стр. 2а);
- г. Москва, Ленинский проспект, дом 20, корп. 2;
- г. Москва, Ленинский проспект, дом 20, корп. 2 (стр. 1; стр. 2; стр. 3);
- г. Москва, Ленинский проспект, дом 32а.

Характеристика объекта исследования

Федеральное государственное бюджетное учреждение "Российская академия наук" - высшее научное учреждение Российской Федерации, ведущий центр координации фундаментальных научных исследований и поисковых научных исследований, проводимых по важнейшим направлениям естественных, технических, медицинских, сельскохозяйственных, общественных и гуманитарных наук.

Органами управления РАН являются Общее собрание Российской академии наук, Президиум Российской академии наук, президент Российской академии наук.

В структуру Академии входят региональные отделения Академии, региональные научные центры Академии и представительства Академии.

ИТ-инфраструктура Заказчика является разрозненной и территориально разнесенной. Ввиду данной архитектурной особенности она является сложной в управлении, требующей высоких затрат на ее обслуживание. Для правильного проектирования централизованной ИТ-инфраструктуры и снижения затрат, связанных с ее обслуживанием, необходимо актуализировать ее текущее состояние и получить рекомендации по устранению проблемных моментов.

Содержание работ

В рамках проведенного аудита были обследованы следующие компоненты:

- организационная структура ИТ-служб;
- существующая документация Заказчика
- информационные системы (в рамках требований обследуемых информационных систем к ИТ-инфраструктуре);
- вычислительное оборудование;
- системы хранения данных;
- оборудование сети хранения данных;
- оборудование резервного копирования и восстановления;
- оборудование сети передачи данных;
- средства информационной безопасности;
- оборудование и ПО видеоконференцсвязи (ВКС);
- инженерная инфраструктура (системы электропитания и кондиционирования серверных комнат);
- системное программное обеспечение (в рамках оценки текущей нагрузки), в составе:
 - программное обеспечение операционных систем;
 - программное обеспечение виртуализации;
 - программное обеспечение платформы корпоративных коммуникаций;
 - программное обеспечение систем управления базами данных (СУБД);
 - программное обеспечение системы резервного копирования и архивации;
 - программное обеспечение системы управления и мониторинга;
 - программное обеспечение системы поддержки пользователей.
- автоматизированные рабочие места (АРМ) пользовательского сегмента

Существующая документация Заказчика

Замечания:

У Заказчика отсутствует организационно-распорядительная документация, в частности отсутствуют регламенты по:

- Проведению плановых работ по обслуживанию оборудования и серверных комнат
- Обеспыливанию оборудования
- Планы аварийного восстановления
- Инструкции по работе с аппаратным и программным обеспечением
- Орг. структура отдела
- Планы тестирования серверного и сетевого оборудования
- Каталог ИТ услуг
- Пользовательские инструкции по работе с техникой

Отсутствует следующая документация по **информационным системам**:

- функциональная схема ИС
- технические требования ИС к ИТ-инфраструктуре
- политики хранения резервных и архивных копий ИС
- окна резервного копирования, требования RTO (recovery time objective) и RPO (recovery point objective) для ИС
- процедуры восстановления ИС и их компонентов при сбоях

Отсутствует следующая документация по **вычислительному оборудованию**:

- схемы расположения оборудования в монтажных шкафах серверных комнат
- имя устройства (уникальный идентификатор)
- таблицы IP адресации
- типы устройства
- производитель устройства
- серийные номера
- наличие и тип внутренней дисковой подсистемы
- конфигурация жестких дисков
- функциональное назначение устройства
- уровень производственной критичности устройства
- тип и версия операционной системы
- тип и количество адаптеров ввода-вывода

Отсутствует следующая документация по **системам хранения данных**:

- схема разбиения и презентации разделов СХД серверам;
- схемы расположения оборудования в монтажных шкафах серверных комнат;
- имя устройства (уникальный идентификатор);
- таблица IP адресации;
- тип устройства;
- производитель оборудования;
- общее дисковое пространство;

- используемый объем дискового пространства;
- неиспользуемый объем дискового пространства;
- конфигурация жестких дисков;
- тип и количество внешних портов;

Отсутствует следующая документация по **оборудованию сети хранения данных**:

- схема подключения к сети хранения данных компонентов ИТ-инфраструктуры;
- схемы расположения оборудования в монтажных шкафах серверных комнат;
- имя устройства (уникальный идентификатор);
- таблица IP адресации;
- тип устройства;
- производитель оборудования;
- тип и количество внешних портов;

Отсутствует следующая документация по **оборудованию резервного копирования и восстановления**:

- схемы расположения оборудования в монтажных шкафах серверных комнат;
- имя устройства (уникальный идентификатор);
- таблица IP адресации;
- тип устройства;
- производитель оборудования;
- число и тип лентопротяжных устройств (для ленточных библиотек);
- число и тип оптических накопителей (для оптических библиотек);
- число слотов для размещения носителей (для ленточных и оптических библиотек);
- число и тип используемых носителей (для ленточных и оптических библиотек);
- тип и версия ПО резервного копирования (для устройств резервного копирования);

Отсутствует следующая документация по **оборудованию сети передачи данных**:

- схемы расположения оборудования в монтажных шкафах серверных комнат;
- таблица IP адресации;
- назначение оборудования;

Отсутствует следующая документация по **средствам информационной безопасности**

- схемы расположения оборудования в монтажных шкафах серверных комнат;
- схемы взаимодействия средств информационной безопасности;
- обозначение устройства /ПО (идентификатор в инфраструктуре Заказчика);
- таблица IP адресации;
- производитель оборудования / ПО;
- модель оборудования / ПО;
- назначение оборудования /ПО;
- политики и контуры безопасности;
- ролевая модель и права доступа;
- модели угроз;
- результат анализа достаточности используемых средств информационной безопасности и их соответствие бизнес-задачам Заказчика, описывающий:
- правила и работу персонала с информацией;
- внутреннюю нормативную базу, определяющую тайну и конфиденциальную информацию;
- управление доступом к данным;

- организацию защиты от вредоносного ПО;
- организацию мониторинга событий в сфере информационной безопасности и реагирования на данные события;
- используемые политики (шифрование, управление паролями, обработки данных и пр.);
- использование различных носителей информации;
- порядок и требования предоставления доступа пользователям к каналам обмена информацией;
- порядок предоставления доступа к информации третьим лицам, не являющихся сотрудниками Заказчика;
- порядок мониторинга и контроля доступа к сети компании;

Отсутствует следующая документация по **средствам видеоконференцсвязи (ВКС)**:

- схема взаимодействия компонентов ВКС;
- схемы расположения оборудования в монтажных шкафах серверных комнат;
- обозначение устройства /ПО (идентификатор в инфраструктуре Заказчика);
- таблица IP адресации;

Результаты анализа достаточности предоставленной документации для решения текущих задач Заказчика:

Были предоставлены:

- Список аппаратных средств
- Схема сетевой инфраструктуры
- Схема каналов передачи данных

Предоставленная документация составляет около 5% всей необходимой документации для решения текущих и планируемых задач Заказчика

Рекомендации:

Необходимо разработать всю вышеуказанную документацию.

Общая информация

Результаты аудита:

Состав технических средств:

В рамках проведенного аудита путем анкетирования и письменных запросов Заказчику был определен следующий список технических средств:

№	Наименование	Количество	Параметры
1	Сервер Fujitsu PRIMERGY RX2540 M4 4x 3.5'	4 шт.	Процессор 2 шт. Xeon silver 4114, ОЗУ 128 Gb, HDD 2 шт. по 4 Тб и SSD 2 шт. по 400 Gb.
2	СХД Fujitsu ETERNIUS DX200 S4	2 шт.	Жесткие диски 9 шт. по 6Тб.
3	HP Proliant DL380 GEN10	1 шт.	Процессор 2 шт. Xeon gold 5115, ОЗУ 128 Gb, HDD 8 шт. по 4 Тб и SSD 2 шт. по 400 Gb.
4	HP Proliant DL380 GEN10	1 шт.	Процессор 2 шт. Xeon silver 4114, ОЗУ 128 Gb, HDD 2 шт. по 4 Тб и SSD 2 шт. по 400 Gb.
5	Reshield RX240 GEN2	2 шт.	Процессор 2 шт. Xeon silver 4114, ОЗУ 128 Gb, HDD 2 шт. по 4 Тб и SSD 2 шт. по 400 Gb.
6	СХД Reshield Terra infinity 3012	1 шт.	Жесткие диски 10шт. по 8Тб.
7	Dell Poweredge R430	3 шт.	Процессор 2 шт. Xeon E5-2620v4, ОЗУ 48 Gb.
8	СХД DELL EMC SCv3020	1 шт.	Жесткие диски 7 шт. по 1,2Тб.
9	SuperMicro	3 шт.	Процессор 2 шт. Xeon E5620 2.4 Ghz, ОЗУ 12 Gb, HDD 2 шт. по 500GB
10	Сервер DEPO	1 шт.	Процессор 2 шт. Xeon E5-2650 2.3 Ghz, ОЗУ 128 Gb, HDD 2 шт. по 2 Tb
11	Сервер DEPO	1 шт.	Процессор 2 шт. Xeon E3-1241 3.5 Ghz, ОЗУ 8 Gb, HDD 3 шт. по 2 Tb

Общая архитектурная схема:

Схема каналов передачи данных

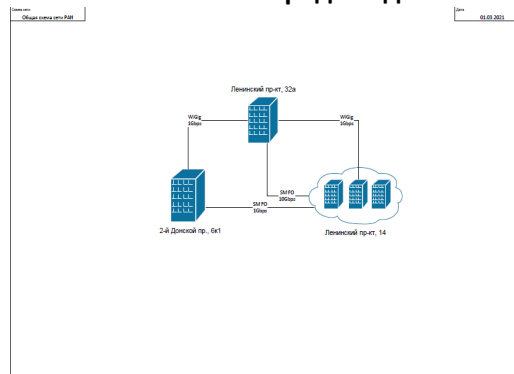
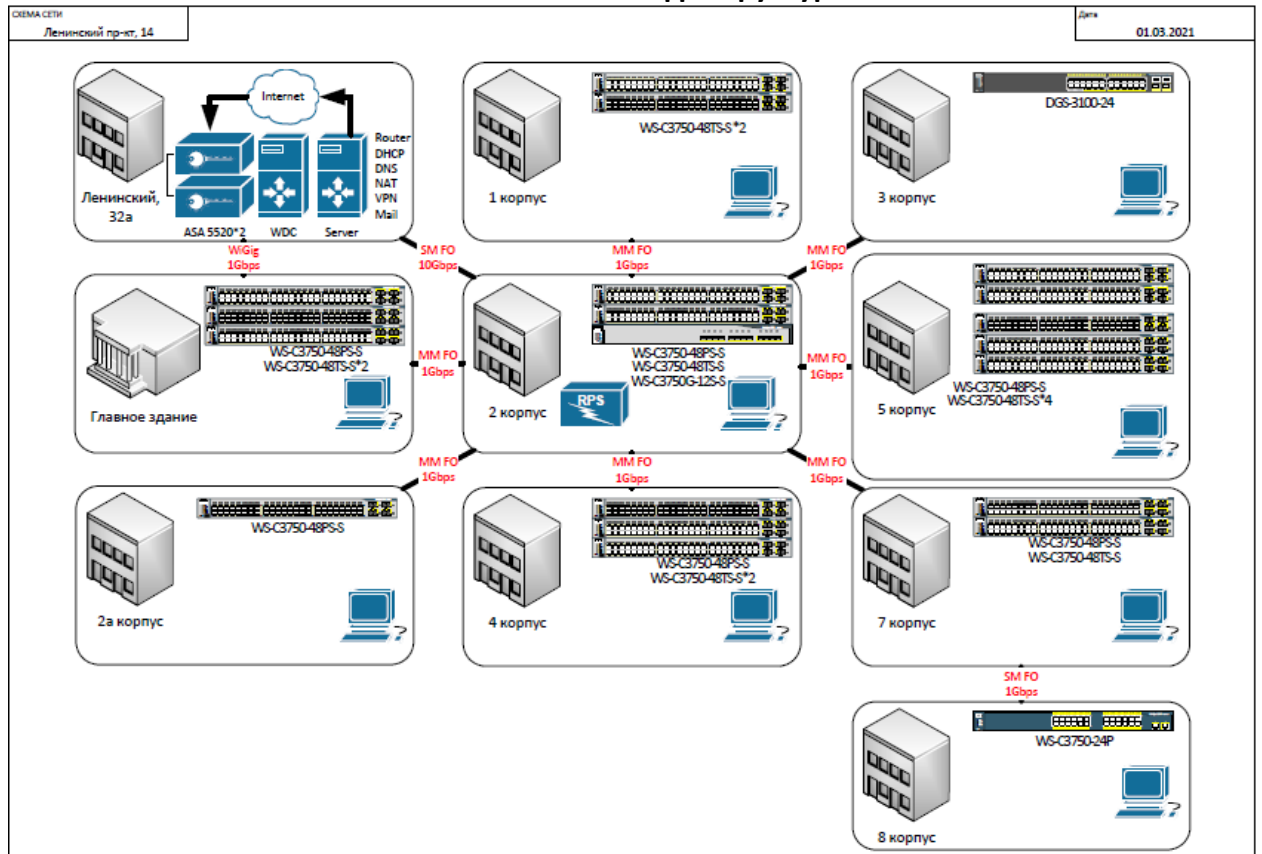


Схема сетевой инфраструктуры



Результаты анализа достаточности общей информации и ее соответствие бизнес-задачам Заказчика:

На момент проведения аудита предоставленная информация является недостаточной в связи с отсутствием у Заказчика подавляющего перечня документов, регламентов и процедур, в частности отсутствуют:

- схемы организационной структуры;
- регламенты и журналы обслуживания технических и программных средств
- инструкции по работе с техническими и аппаратными средствами
- функциональная схема ИС
- технические требования ИС к ИТ-инфраструктуре
- политики хранения резервных и архивных копий ИС
- окна резервного копирования, требования RTO (recovery time objective) и RPO (recovery point objective) для ИС
- процедуры восстановления ИС и их компонентов при сбоях
- схемы расположения оборудования в монтажных шкафах серверных комнат
- имена устройств вычислительного оборудования
- таблицы IP адресации
- типы устройства
- производитель устройства
- серийные номера
- конфигурация жестких дисков
- функциональное назначение устройства
- уровень производственной критичности устройства
- тип и версия операционной системы
- тип и количество адаптеров ввода-вывода
- схема разбиения и презентации разделов СХД серверам;
- схемы расположения оборудования в монтажных шкафах серверных комнат
- общее дисковое пространство СХД
- используемый объем дискового пространства СХД
- неиспользуемый объем дискового пространства СХД
- конфигурация жестких дисков СХД
- тип и количество внешних портов СХД
- схема подключения к сети хранения данных компонентов ИТ-инфраструктуры
- тип и количество внешних портов
- число и тип лентопротяжных устройств (для ленточных библиотек)
- число и тип оптических накопителей (для оптических библиотек)
- число слотов для размещения носителей (для ленточных и оптических библиотек)
- число и тип используемых носителей (для ленточных и оптических библиотек)
- тип и версия ПО резервного копирования (для устройств резервного копирования)
- схемы взаимодействия средств информационной безопасности;
- обозначение устройства /ПО (идентификатор в инфраструктуре Заказчика);
- политики и контуры информационной безопасности
- ролевая модель и права доступа
- модели угроз
- правила и работу персонала с информацией
- внутренняя нормативная база, определяющая тайну и конфиденциальную информацию
- политика управления доступом к данным
- политика организации защиты от вредоносного ПО

- мониторинг событий в сфере информационной безопасности и реагирования на данные события
- используемые политики (шифрование, управление паролями, обработки данных и пр.)
- использование различных носителей информации
- порядок и требования предоставления доступа пользователям к каналам обмена информацией
- порядок предоставления доступа к информации третьим лицам, не являющихся сотрудниками Заказчика
- порядок мониторинга и контроля доступа к сети компании
- схема взаимодействия компонентов ВКС

Определенный в ходе анкетирования состав технических средств, является неполным. В ходе аудита были выявлены сетевые устройства (коммутаторы), отвечающие за доставку пакетов к СПД и между устройствами. Документация по данным устройствам не была предоставлена Заказчиком. На момент проведения аудита мощности технических средств задействованы на 90%, что не позволяет Заказчику производить улучшения ИТ инфраструктуры и ее модернизацию.

Рекомендации:

В связи с тем, что вся серверная, сетевая и инженерная инфраструктура находится на территории стороннего подрядчика, Заказчик не располагает указанной в ТЗ документацией. Заказчику необходимо разработать и внедрить документацию, указанную в пункте **«Результаты анализа достаточности общей информации и ее соответствие бизнес-задачам Заказчика»** настоящего раздела, определить оборудование и ПО, отвечающее за ИБ, задокументировать планы резервного копирования, аварийного восстановления, а также планы аварийного тестирования.

Необходимо составить полный список коммутационного и сетевого оборудования, задокументировать его и составить планы резервного копирования, DRP (планы аварийного восстановления).

Необходимо определить список имеющегося серверного оборудования у Заказчика, разработать документацию по назначению оборудования с указанием инвентарных и серийных номеров.

Рекомендуется модернизировать ИТ инфраструктуру, а именно, унифицировать аппаратное обеспечение, унифицировать программное обеспечение, разработать регламенты и инструкции для каждого серверного узла и сетевого узла, а также разработать подробную общую схему с указанием назначения устройства, IP адреса, имени узла и зависимостями между ними.

Информационные системы

Состав, наименование и назначение ИС и ПО:

- Пользовательские операционные системы – Windows 7,8,10
- Серверная ОС – Windows server 2008, 2012 R2
- Видеоконференцсвязь – Zoom
- ERP (Бухгалтерский учет и управленческий учет) – 1С
- Система ЭДО – Тезис
- Система виртуализации – Proxmox
- Базы данных – MS SQL (1С), Postgres (Тезис), КДС (Нет информации)
- Управление пользователями – Active Directory на Linux по протоколу Samba
- Система мониторинга – Zabbix
- Резервное копирование – копирование виртуальных машин на СХД
- Почта – Postfix
- HelpDesk – нет.
 - Диспетчерская, ToDo в Майкрософт календаре
 - Всего около 500 пользователей
 - Приходит около 100 заявок в месяц
- Инф. Безопасность – Firewall у провайдера (МСТН)
- Web сайт – Обслуживается Управлением РАН

Результаты анализа достаточности используемых архитектурных решений, политик и соответствия требований ИС к ИТ-инфраструктуре:

На момент проведения аудита используемые архитектурные решения являются частично достаточными для функционирования организации. ИТ-инфраструктура соответствует требованиям используемых информационных систем.

У Заказчика отсутствуют политики по ИС полностью.

Получение и обработка заявок ведется в календаре, что является крайне неэффективным решением при работе с пользовательскими заявками.

Используются разрозненные производители баз данных, устаревшие пользовательские и серверные операционные системы, например, Windows server 2008 и Windows 7. Данные ОС более не поддерживаются Microsoft и для них не выпускаются обновления.

Заказчик доверил управление большинством ИС стороннему подрядчику, что может негативно сказаться на информационной безопасности, актуальности информации и конфигураций ИС и аппаратного обеспечения, а также реальном понимании ситуации. Заказчик рискует потерять свои данные или потерять управление ими в любой момент, например по причине компрометации учетных данных.

Замечания:

Отсутствуют:

- функциональная схема

- технические требования ИС к ИТ-инфраструктуре;
- политики хранения резервных и архивных копий ИС;
- окна резервного копирования, требования RTO (recovery time objective) и RPO (recovery point objective) для ИС;
- процедуры восстановления ИС и их компонентов при сбоях;

Рекомендации:

Рекомендуется использовать базу данных одного разработчика, например Ms SQL. Это позволит унифицированно настроить резервное копирование баз данных всех систем

По возможности необходимо использовать SaaS решения, для таких сервисов как видеоконференцсвязь (Уже используется Zoom), электронная почта, например MS Office 365.

Использование SaaS решений позволяет спрогнозировать затраты на ПО и гибко управлять лицензиями, в нужный момент сокращая расходы на ПО. А также SaaS решения позволяют всегда иметь последнюю версию ПО.

Закупить необходимое оборудование для размещения информационных систем на собственных мощностях с избыточностью 50% для возможности оперативного размещения новых ИТ сервисов и информационных систем.

Необходимо внедрить систему Helpdesk для управления заявками пользователей. Это позволит выгружать отчетность по заявкам и оптимизировать работу сотрудников, ответственных за решение пользовательских заявок.

Необходимо определить и разработать:

- Функциональную схему ИС
- технические требования ИС к ИТ-инфраструктуре
- политики хранения резервных и архивных копий ИС
- окна резервного копирования, требования RTO (recovery time objective) и RPO (recovery point objective) для ИС
- процедуры восстановления ИС и их компонентов при сбоях

Вычислительное оборудование

Серверная инфраструктура Заказчика размещена на арендованных мощностях у подрядчика. Ежегодно Заказчик проводит электронный аукцион по закупке услуги размещения своих сервисов на инфраструктуре подрядчика.

Вся аппаратная часть инфраструктуры физически находится не на территории Заказчика, что делает физическое обследование аппаратных средств невозможным. Данные по вычислительным мощностям были получены путем запроса стороннему подрядчику.

Список аппаратных средств

№	Наименование	Количество	Параметры
1	Сервер Fujitsu PRIMERGY RX2540 M4 4x 3.5'	4 шт.	Процессор 2 шт. Xeon silver 4114, ОЗУ 128 Gb, HDD 2 шт. по 4 Тб и SSD 2 шт. по 400 Gb.
2	СХД Fujitsu ETERNIUS DX200 S4	2 шт.	Жесткие диски 9 шт. по 6Тб.
3	HP Proliant DL380 GEN10	1 шт.	Процессор 2 шт. Xeon gold 5115, ОЗУ 128 Gb, HDD 8 шт. по 4 Тб и SSD 2 шт. по 400 Gb.
4	HP Proliant DL380 GEN10	1 шт.	Процессор 2 шт. Xeon silver 4114, ОЗУ 128 Gb, HDD 2 шт. по 4 Тб и SSD 2 шт. по 400 Gb.
5	Reshield RX240 GEN2	2 шт.	Процессор 2 шт. Xeon silver 4114, ОЗУ 128 Gb, HDD 2 шт. по 4 Тб и SSD 2 шт. по 400 Gb.
6	СХД Reshield Terra infinity 3012	1 шт.	Жесткие диски 10шт. по 8Тб.
7	Dell Poweredge R430	3 шт.	Процессор 2 шт. Xeon E5-2620v4, ОЗУ 48 Gb.
8	СХД DELL EMC SCv3020	1 шт.	Жесткие диски 7 шт. по 1,2Тб.
9	SuperMicro	3 шт.	Процессор 2 шт. Xeon E5620 2.4 Ghz, ОЗУ 12 Gb, HDD 2 шт. по 500GB
10	Сервер DEPO	1 шт.	Процессор 2 шт. Xeon E5-2650 2.3 Ghz, ОЗУ 128 Gb, HDD 2 шт. по 2 Tb
11	Сервер DEPO	1 шт.	Процессор 2 шт. Xeon E3-1241 3.5 Ghz, ОЗУ 8 Gb, HDD 3 шт. по 2 Tb

Из серверов и СХД собраны два кластера виртуализации по технологии KVM (окружение Proxmox) на которых развернуты:

- Сервер электронной почты с web-интерфейсом (m.pran.ru)
- Сервер PDC (Primary Domain Controller, Domain Name Server, DHCP, файловый сервер)
- Сервер SDC (Secondary Domain Controller)
- Сервер справочно-правовой системы Консультант Плюс и информационно-правовой системы "Гарант".

Результат анализа достаточности используемого вычислительного оборудования и его соответствие бизнес-задачам Заказчика:

На момент проведения аудита вычислительные мощности, используемые Заказчиком, являются частично достаточными.

ИТ-инфраструктура располагается на территории стороннего подрядчика, следовательно, невозможно однозначно определить момент внесения изменений в инфраструктуру, в связи с чем Заказчик может обладать неактуальными сведениями об архитектуре. Также доступные на момент аудита мощности не позволят внедрить новые информационные системы, организовать дополнительные механизмы по резервному копированию и размещению дополнительной информации, занимающей значительное место на жестких дисках.

Для размещения инфраструктуры на собственной территории, Заказчик не обладает достаточным набором собственных технических средств, а именно, серверных мощностей, сетевого и коммутационного оборудования, инженерного обеспечения серверных комнат.

Замечания:

Отсутствуют:

- схемы расположения оборудования в монтажных шкафах серверных комнат
- имя устройства (уникальный идентификатор)
- таблица IP адресации
- серийный номер
- наличие и тип внутренней дисковой подсистемы
- конфигурация жестких дисков
- функциональное назначение устройства
- уровень производственной критичности устройства
- тип и версия операционной системы
- тип и количество адаптеров ввода-вывода

Рекомендации:

Рекомендуется перенести все вычислительные мощности на территорию Заказчика, разработать схемы расположения оборудования в монтажных шкафах серверных комнат с указанием имен устройств, серийных номеров, конфигурацией жестких дисков, таблицей IP адресации, типом и версией операционной системы, типом и количеством адаптеров ввода-вывода. Также рекомендуется разработать документ, регламентирующий уровень производственной критичности устройств, а также определить SLA для каждого устройства.

Рекомендуется организовать архитектуру виртуализации на базе VmWare с отказоустойчивым кластером из двух аппаратных серверов и одного аппаратного сервера для реализации репликации виртуальных машин.

Отказоустойчивый кластер позволит избежать простоев при аппаратном сбое одного из хостов.

Сервер репликации позволит избежать сильных простоев при программных сбоях ВМ.

Схема реализации приведена ниже.

Рекомендуемая схема реализации серверной инфраструктуры

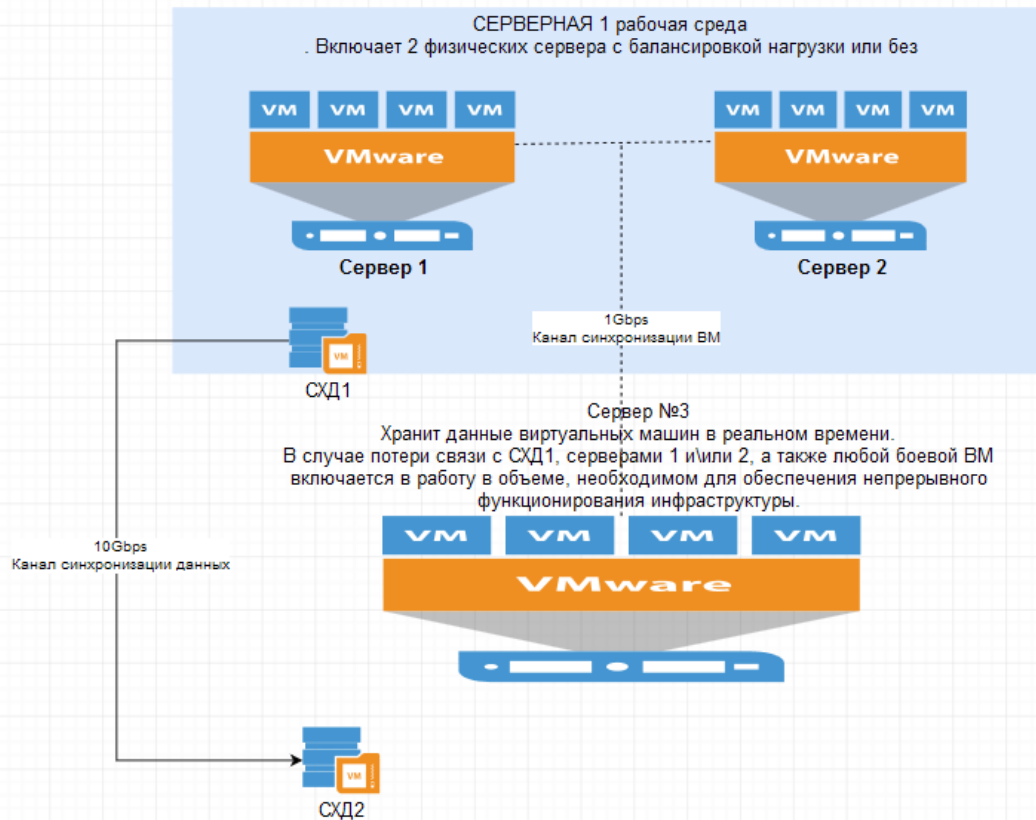
VMWARE "FAULT TOLERANCE" SHEMA

Паузы в предоставлении сервисов от 0 сек.

Предполагает полную синхронизацию виртуальных машин и их данных в реальном времени.

Работает даже в случае кратковременных проблем

Использование собственных ресурсов при использовании схемы Fault Tolerance позволяет обеспечить непрерывную работу всех сервисов даже в случае отказа всего оборудования в одной из серверных.



СХД

Состав технических средств СХД

№	Наименование	Количество	Параметры
1	СХД Fujitsu ETERNIUS DX200 S4	2 шт.	Жесткие диски 9 шт. по 6Тб.
2	СХД Reshield Terra infinity 3012	1 шт.	Жесткие диски 10шт. по 8Тб.
3	СХД DELL EMC SCv3020	1 шт.	Жесткие диски 7 шт. по 1,2Тб.

Отсутствуют сведения об:

- схеме разбиения и презентации разделов СХД серверам
- схемах расположения оборудования в монтажных шкафах серверных комнат
- именах устройств (уникальный идентификатор)
- таблице IP адресации
- используемом объеме дискового пространства
- неиспользуемом объеме дискового пространства
- конфигурации жестких дисков
- типе и количестве внешних портов
- схеме подключения к сети хранения данных компонентов ИТ-инфраструктуры
- схемах расположения оборудования в монтажных шкафах серверных комнат

Результат анализа достаточности используемых систем хранения данных и их соответствие бизнес-задачам Заказчика:

На момент проведения аудита, используемые Заказчиком СХД, являются частично достаточными. Количество и объем жестких дисков достаточен для используемых Заказчиком сервисов и информационных систем, однако архитектура использования СХД нуждается в модернизации.

Замечания:

Используются СХД разных производителей. Данная конфигурация в некоторых случаях может привести к несовместимости оборудования и программного обеспечения, что в свою очередь приведет к невозможности реализации ряда изменений и улучшений.

Рекомендации:

Рекомендуется использовать два физических СХД. Один для кластера серверов и сервера репликации и один для бэкапов. Данная схема позволит реализовать отказоустойчивое информационное пространство с минимальным временем простоя в случае сбоев.

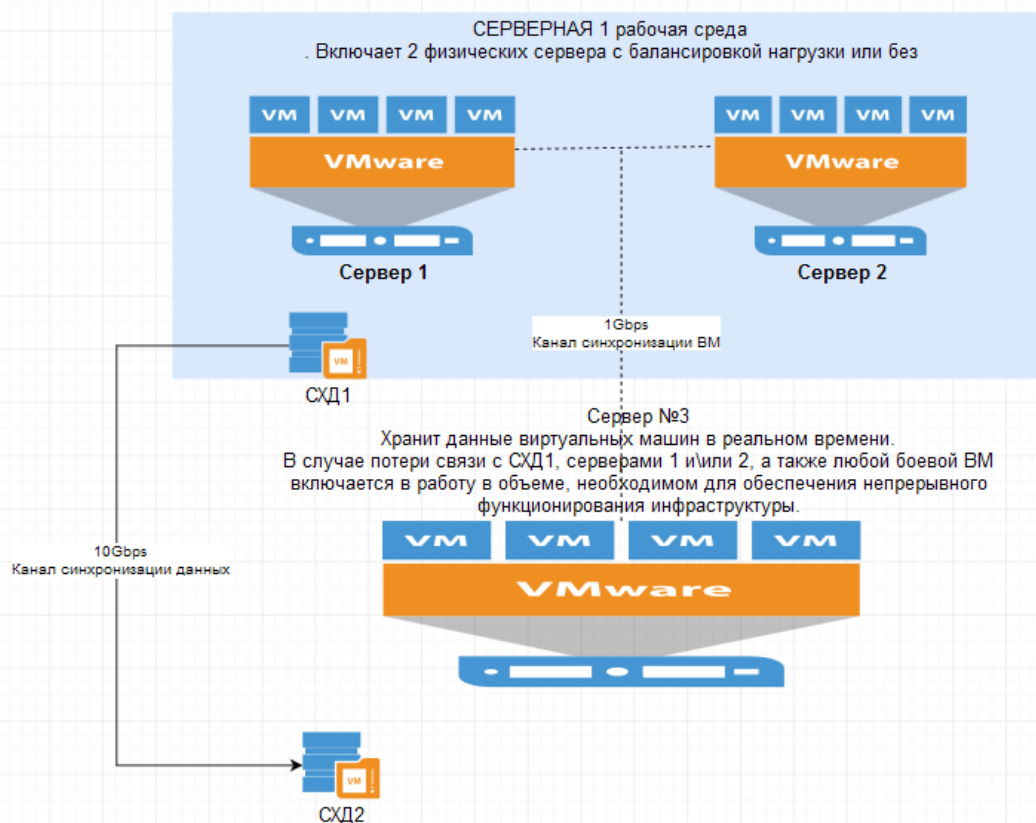
Рекомендуемая схема подключения СХД

VMWARE "FAULT TOLERANCE" SHEMA

Паузы в предоставлении сервисов от 0 сек.

Предполагает полную синхронизацию виртуальных машин и их данных в реальном времени.

Работает даже в случае кратковременных проблем



Использование собственных ресурсов при использовании схемы Fault Tolerance позволяет обеспечить непрерывную работу всех сервисов даже в случае отказа всего оборудования в одной из серверных.

Рекомендуется разработать перечень документации:

- схема разбиения и презентации разделов СХД серверам
- схемы расположения оборудования в монтажных шкафах серверных комнат
- имя устройства (уникальный идентификатор)
- таблица IP адресации
- тип устройства
- используемый объем дискового пространства
- неиспользуемый объем дискового пространства
- конфигурация жестких дисков
- тип и количество внешних портов
- схема подключения к сети хранения данных компонентов ИТ-инфраструктуры

Оборудование сети хранения данных

Состав СХД

№	Наименование	Количество	Параметры
1	СХД Fujitsu ETERNIUS DX200 S4	2 шт.	Жесткие диски 9 шт. по 6Тб.
2	СХД Reshield Terra infinity 3012	1 шт.	Жесткие диски 10шт. по 8Тб.
3	СХД DELL EMC SCv3020	1 шт.	Жесткие диски 7 шт. по 1,2Тб.

В ходе опроса и анкетирования было выявлено отсутствие следующей документации:

- схема подключения к сети хранения данных компонентов ИТ-инфраструктуры
- схемы расположения оборудования в монтажных шкафах серверных комнат
- имя устройства (уникальный идентификатор)
- таблица IP адресации
- тип устройства
- производитель оборудования
- тип и количество внешних портов

Результат анализа достаточности используемого оборудования сети хранения данных и его соответствие бизнес-задачам Заказчика:

В СХД используются вперемешку диски HDD и SSD. Используется большой объем жестких дисков.

Основным недостатком является то, что аппаратное обеспечение не обновлялось больше 3 лет, что подвергает сервисы Заказчика большим простоям в связи с выходом из строя оборудования.

На момент проведения аудита нет информации на какие СХД осуществляется резервное копирование, на каких СХД хранятся диски виртуальных машин.

Нет информации о типах RAID. Нет информации какие диски для каких задач используются. Так, например для 1С необходимо использовать либо зеркало из SSD дисков, либо RAID 10.

Существующая сеть хранения данных не соответствует бизнес-задачам Заказчика.

Рекомендации:

Рекомендуется использовать два физических СХД. Один для кластера и сервера репликации и один для бэкапов.

В данном случае подойдет СХД среднего уровня. Системы хранения данных такого класса отличает оптимальное соотношение функциональность/цена, обладают обширным функционалом, высокой производительностью, хорошо масштабируются, совместимы с большинством популярных операционных систем. Такие системы позволяют эффективно решать большинство задач хранения данных средних и крупных заказчиков: средние и крупные СУБД, электронная почта, важнейшие файловые сервисы, CAD/CAM, кластеры высокой доступности для важнейших задач, таких как ERP, CRM и т.п.

К таким можно отнести Dell EMC Powerstore.

PowerStoreOS может быть запущена непосредственно на «железе», либо в виртуальной машине встроенного гипервизора VMware. Благодаря модульной структуре PowerStoreOS можно

развернуть не только на самой СХД, но и на отдельных серверах, либо в облаке, что дает гибкость в построении систем хранения для конкретных задач.

Аппаратная начинка нового массива стандартная для среднего уровня: платформа 2U с двумя контроллерами, 25 отсеков для 2,5 дюймовых накопителей (поддерживаются NVMe SSD объемом до 15,36 Тбайт и Intel Optane объемом до 750 Гбайт), поддержка Fibre Channel 32 Гбит/с и Ethernet 25 Гбит/с

Необходимо разработать следующую документацию:

- схема подключения к сети хранения данных компонентов ИТ-инфраструктуры
- схемы расположения оборудования в монтажных шкафах серверных комнат
- имя устройства (уникальный идентификатор)
- таблица IP адресации
- тип устройства
- производитель оборудования
- тип и количество внешних портов

Оборудование резервного копирования и восстановления

Состав оборудования для резервного копирования и восстановления

№	Наименование	Количество	Параметры
1	СХД Fujitsu ETERNIUS DX200 S4	2 шт.	Жесткие диски 9 шт. по 6Тб.
2	СХД Reshield Terra infinity 3012	1 шт.	Жесткие диски 10шт. по 8Тб.
3	СХД DELL EMC SCv3020	1 шт.	Жесткие диски 7 шт. по 1,2Тб.

Результат анализа достаточности используемого оборудования резервного копирования и их соответствие бизнес-задачам Заказчика:

Резервное копирование организовано штатными средствами Proxmox (создание образа виртуальной машины на отдельном СХД), дополнительно на почтовом сервере используется инкрементальный бэкап файловой системы. Резервное копирование производится каждую ночь. Отказоустойчивость обеспечивается кластером Proxmox поддерживающим он-лайн миграцию и СХД с резервируемым подключением к серверам.

Замечания:

На данный момент механизмы резервного копирования недостаточны. Необходимо не только обеспечить резервное копирование виртуальной машины на отдельный СХД, но и обеспечить зеркалирование всех виртуальных машин в отказоустойчивом кластере.

Отсутствует следующая документация:

- схемы расположения оборудования в монтажных шкафах серверных комнат;
- имя устройства (уникальный идентификатор);
- таблица IP адресации;
- тип устройства;
- число и тип лентопротяжных устройств (для ленточных библиотек);
- число и тип оптических накопителей (для оптических библиотек)
- число слотов для размещения носителей (для ленточных и оптических библиотек);
- число и тип используемых носителей (для ленточных и оптических библиотек)

Рекомендации:

Для организации серверной инфраструктуры предлагается использовать VmWare с технологией Fault Tolerance и VmWare High Availability, например VmWare Essentials Kit Plus

Рекомендуется организовать следующую схему резервного копирования и восстановления:

- Организовать кластер серверов из 2 физических хостов одинаковой конфигурации (в дальнейшем, в рамках улучшений количество серверов в кластере можно будет увеличить до необходимого количества)

- Основную серверную инфраструктуру, на которой располагаются боевые виртуальные машины разместить в кластере серверов
- Один физический сервер использовать для репликации виртуальных машин с боевого кластера
- Один СХД необходимо использовать для хранения жестких дисков виртуальных машин
- Второй СХД необходимо использовать для бэкапов виртуальных машин и бэкапов отдельных файлов.
- Все СХД должны быть соединены 10 GB/sec fiber channel с серверами
- Кластеризация позволит обеспечить автоматическое переключение на резервный сервер в случае выхода из строя основного по аппаратной ошибке
- Сервер репликации позволит переключиться на резервные виртуальные машины в случае программной ошибки в кластере или выхода из строя основного кластера полностью
- СХД и резервное копирование на него виртуальных машин и файлов позволит восстановить данные в течение 15-20 минут в случае выхода из строя кластера и сервера репликации.

Оборудование сети передачи данных

Результат анализа достаточности используемого оборудования сети передачи данных и их соответствие бизнес-задачам Заказчика:

ЛВС построена по технологии Ethernet с использованием стека протоколов TCP-IP, имеет доменную архитектуру на основе службы каталогов Active Directory с использованием динамического распределения IP-адресов для пользователей, не осуществляющих обработку информации в ГИС и статического - для системных администраторов и операторов ГИС.

Вертикальная подсистема (межэтажная разводка) ЛВС выполнена с использованием оптоволоконных линий связи, горизонтальная (поэтажная разводка) - с использованием витой пары. Скорость передачи данных для всех линий связи составляет 1 Гбит/с

Внешнее подключение к сети Интернет серверов ГИС защищено несертифицированным межсетевым экраном.

Между зданиями используется оптическая линия связи.

Доступ системных администраторов и операторов к ресурсам системы осуществляется по локальной вычислительной сети с использованием персональных идентификаторов и паролей, права предоставляются на основании функциональных обязанностей пользователей.

Схема каналов передачи данных

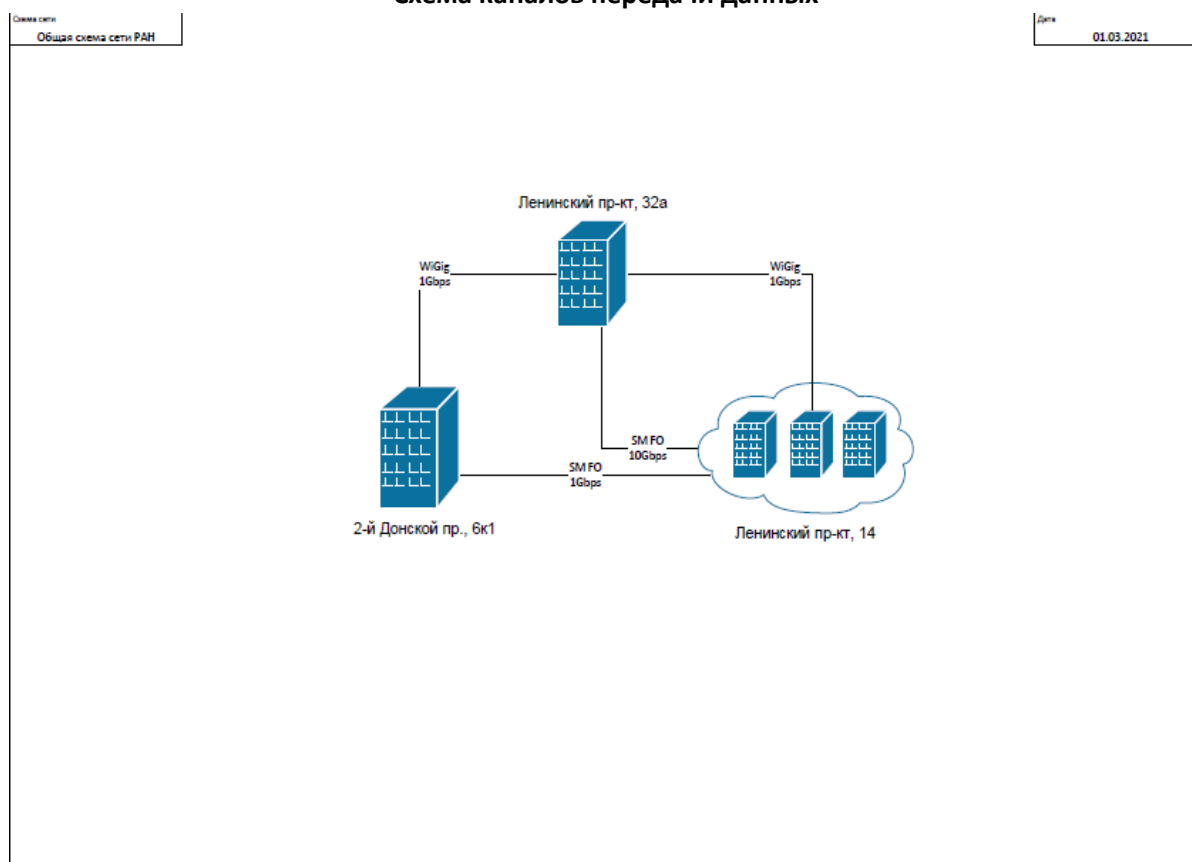
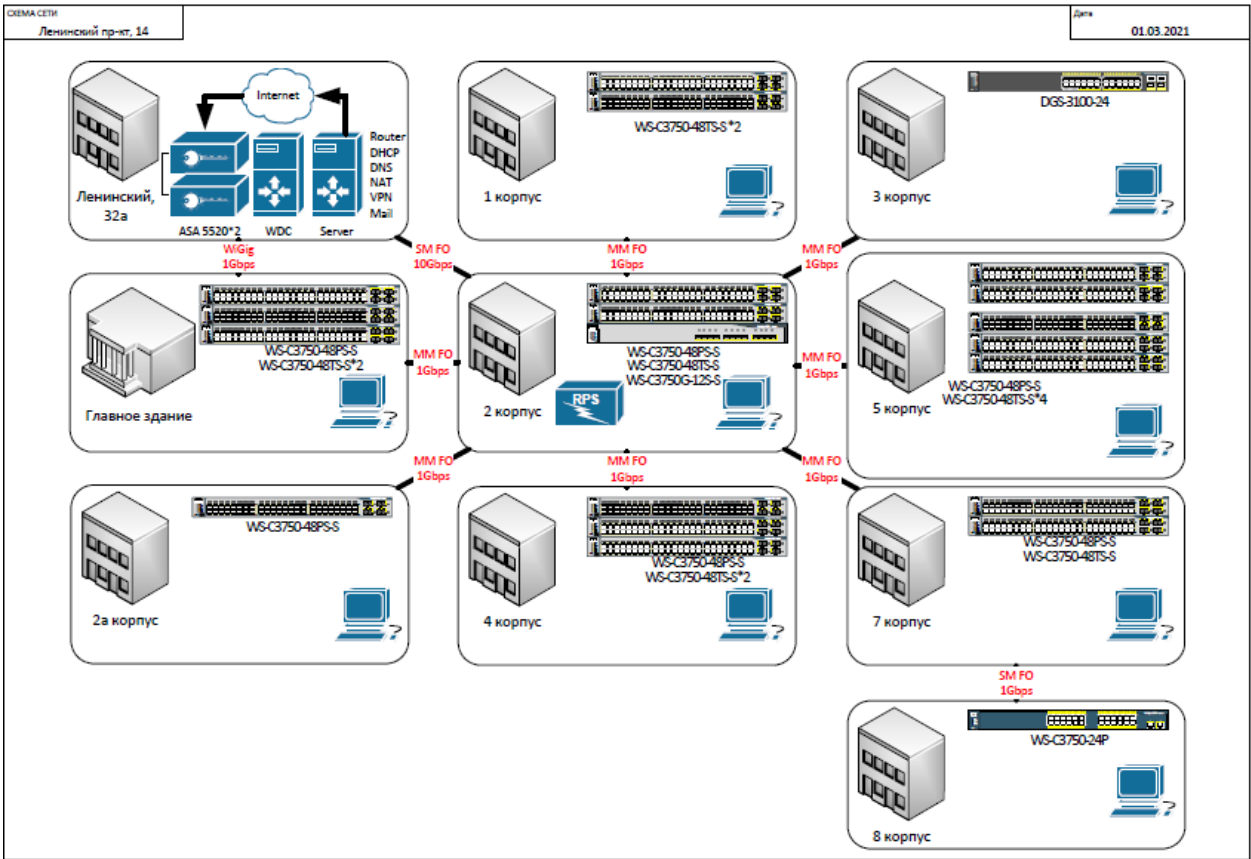


Схема сетевой инфраструктуры



Отсутствует:

- таблица IP адресации

Рекомендации:

Рекомендуется использовать сетевые устройства со стекированием из списка ТОРП.

Главное здание необходимо оборудовать коммутатором ядра.

Второстепенные здания необходимо оборудовать коммутаторами агрегации в главных серверных комнатах. На каждом этаже необходимо использовать коммутаторы доступа.

Рекомендуется документально зафиксировать таблицу IP адресации, а также сделать резервные копии конфигураций всех сетевых устройств. Это позволит в кратчайшие сроки восстановить сетевую конфигурацию в случае сбоев.

Рекомендованная спецификация сетевого оборудования

1. Коммутатор уровня ядра сети

QTECH QSW-6410-52F

Порты 10GbE SFP+ - 48 портов

Порты 40GbE QSFP+ - 4 порта

Порты консоли - 1 порт RS-232 (RJ45)

Порты управления MGMT - есть (на передней панели)

USB интерфейс - 1 порт USB 2.0

Расположение разъемов питания - на задней панели

ACL - Стандартный/Расширенный/Экспертный ACL, Расширенный ACL по MAC, IPv6 ACL, ACL-логирование, ACL counter, ACL remark, Глобальный ACL, ACL redirect, ACL с диапазоном времени ACL80(Userdefined ACL)

Jumbo Frame - 9K

Коммутационная матрица - 2,56 Tbps

Пропускная способность - 960 Mpps

Размер таблицы MAC адресов - 128K MAC адресов

Размер таблицы маршрутизации - До 16K (IPv4/IPv6)

Память - 2 Гб RAM + 512 Мб

DHCP - DHCP-сервер, DHCP-клиент, DHCP snooping, DHCP relay, IPv6 DHCP relay

Spanning Tree Protocols - IEEE 802.1d STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP, Port fast, BPDU filter, BPDU guard, TC guard, TC protection, ROOT guard

VLAN - 4K 802.1q VLANs, Port-based VLAN, MAC-based VLAN, Super VLAN, Protocol-based VLAN, Private VLAN, QinQ, IP subnet-based VLAN, GVRP

VLAN функционал - 4K VLAN

Агрегирование портов - Поддержка LACP

Зеркалирование трафика - Many-to-one mirroring, One-to-many mirroring, Flow-based mirroring, Over devices mirroring, VLAN-based mirroring, VLAN-filtering mirroring, AP-port mirroring, RSPAN, ERSPAN

Поддержка функции маршрутизации Статическая маршрутизация, RIP, OSPF, OSPFv3, IS-IS, IS-IS v6, RIPng, BGP, BGP4+, ECMP, PBR

Протоколы маршрутизации IPv4 - Статическая маршрутизация, RIP, OSPF, IS-IS, RIP, BGP, ECMP, Policy based routing(PBR)

Протоколы маршрутизации IPv6 - Статическая маршрутизация, Equal-cost routing, Policy based routing(PBR), RIPng, OSPFv3, BGP4+, IS-IS v6

Протоколы резервирования - GR для OSPF / IS-IS / BGP, Обнаружение BFD, ERPS (G.8032), Технология быстрого переключения REUP, RLDP (Rapid Link Detection Protocol), Резервирование питания 1 + 1, Модули питания с возможностью горячей замены, Резервирование вентилятора 2 + 1

Протоколы управления - SNMP v1/v2c/v3, CLI (Telnet/консоль), RMON (1, 2, 4, 9), SSH, Syslog, NTP/ SNTP, SNMP через IPv6, поддержка IPv6 MIB для SNMP, SSHv6, Telnetv6, FTP/ TFTPv6, DNS v6, NTP для v6, Traceroute v6, Поддержка sFlow; выборку трафика на коммутаторе можно производить с помощью технологии произвольной выборки данных из потока.

Стекирование До 8 коммутаторов в стеке, рекомендованное количество до 4

Тип коммутации - Storage and Forwarding

Уровень коммутатора - L3

2. Коммутатор агрегации

QTECH QSW-4000-12F

Порты 10/100/1000BASE-T - 8 портов

Порты 10GbE SFP+ - 12 портов

Порты консоли - 1 порт RS-232 (RJ45)

Расположение разъемов питания на задней панели

ACL - IPv4 standard ACL, IPv4 extended ACL, IPv6 extended ACL, MAC extended ACL, Time based ACL

Jumbo Frame 9K

Коммутационная матрица - 256 Гбит/с
Пропускная способность - 192.5 Мпак/с (Mpps)
Размер таблицы MAC адресов - 32K MAC адресов
Размер таблицы маршрутизации - До 32K
Память - 512 Мб RAM + 16 Мб
DHCP - IPv4/IPv6 DHCP Client, IPv4/IPv6 DHCP Server, IPv4/IPv6 DHCP Snooping, DHCP Relay Option 82
Green Ethernet - IEEE 802.3az (Energy Efficient Ethernet)
Spanning Tree Protocols - 802.1D (STP), 802.1W (RSTP), 802.1S (MSTP), BPDU protection, root protection и ring protection
VLAN - IEEE802.1Q, Voice VLAN, Port-based VLAN, Protocol-based VLAN, MAC-based VLAN, Private VLAN, QinQ, VLAN Mapping 1 to 1, N to 1, GVRP
VLAN функционал - 4K VLAN
Агрегирование портов - 8 групп / 8 портов
Зеркалирование трафика - Port Mirror
Протоколы маршрутизации IPv4 - Static, PBR, RIPv2, OSPFv2, ISIS, BGP4
Протоколы маршрутизации IPv6 - Static, PBR, RIPv6, OSPFv3, ISISv6, BGP4+
Протоколы резервирования - 802.1D STP, 802.1W RSTP, 802.1S MSTP, PVST, Stack, LACP, EAPS, MEAPS, ERPS, Flex Link, VRRP, BFD, ECMP
Протоколы управления - TFTP/FTP, SNMPv1/v2c/v3, SNMP Trap, CLI (Console / Telnet / SSH), Web/SSL, Public & Private MIB interface RMON (1,2,3,9), Ping, Trace Route, Syslog, NTP, Multiple Configuration Files, VCT, DDM, ULDP, LLDP/LLDP MED
Стекирование - Да
Тип коммутации - Storage and Forwarding
Управление - Console, Telnet, SSH 2.0, WEB доступ, SNMP v1/v2/v3, RMON
Уровень коммутатора - L3

3. Коммутатор доступа

QTECH QSW-4600-52TX-AC

Порты 10/100/1000BASE-T - 48 портов
Порты 10GbE SFP+ - 4 порта
Порты консоли - 1 порт RS-232 (RJ45) (на передней панели)
Расположение разъемов питания - на задней панели
ACL - 1500 / 500
Jumbo Frame - 9K
Коммутационная матрица - 176 Гбит/с
Пропускная способность - 132.3 Мпак/с
Размер таблицы MAC адресов - 16K MAC адресов
Размер таблицы маршрутизации - 500
Память - 512 Мб RAM + 256 Мб
DHCP - IPv4/IPv6 DHCP Client, IPv4 DHCP Server, IPv4/IPv6 DHCP Snooping, DHCP Relay Option 82, DHCPv6 Relay Option 37
Green Ethernet - IEEE 802.3az (Energy Efficient Ethernet)
VLAN - IEEE802.1Q, Voice VLAN, Port-based VLAN, Protocol-based VLAN, MAC-based VLAN, Private VLAN, QinQ, VLAN Mapping 1 to 1, N to 1
VLAN функционал - 4K VLAN
Агрегирование портов - 128 групп / 8 каналов
Зеркалирование трафика - Port Mirror, RSPAN, ERSPAN
Протоколы резервирования - 802.1D STP, 802.1W RSTP, 802.1S MSTP, LACP, ERPS, Flex Link, DLDP, IP event dampening
Стекирование - Да
Тип коммутации - Storage and Forwarding

**4. Коммутатор доступа с поддержкой стандарта IEEE 802.3af/at
QTECH QSW-4600-52TX-POE**

Порты 10/100/1000BASE-T PoE - 46 портов

Порты 10GbE SFP+ - 2 порта

Порты консоли - 1 порт RS-232 (RJ45) (на передней панели)

Расположение разъемов питания - на задней панели

ACL - 1500 / 500

Jumbo Frame - 9K

Коммутационная матрица - 176 Гбит/с

Пропускная способность - 132.3 Мпак/с

Размер таблицы MAC адресов - 16K MAC адресов

Размер таблицы маршрутизации - 500

Память - 512 Мб RAM + 256 Мб

DHCP - IPv4/IPv6 DHCP Client, IPv4 DHCP Server, IPv4/IPv6 DHCP Snooping, DHCP Relay Option 82, DHCPv6 Relay Option 37

Green Ethernet - IEEE 802.3az (Energy Efficient Ethernet)

VLAN - IEEE802.1Q, Voice VLAN, Port-based VLAN, Protocol-based VLAN, MAC-based VLAN, Private VLAN, QinQ, VLAN Mapping 1 to 1, N to 1

VLAN функционал - 4K VLAN

Агрегирование портов - 128 групп / 8 каналов

Зеркалирование трафика - Port Mirror, RSPAN, ERSPAN

Протоколы резервирования - 802.1D STP, 802.1W RSTP, 802.1S MSTP, LACP, ERPS, Flex Link, DLDP, IP event dampening

Стекирование - Да

Тип коммутации - Storage and Forwarding

Средства информационной безопасности

Замечания:

Отсутствуют следующие нормативные документы:

- схемы расположения оборудования в монтажных шкафах серверных комнат;
- схемы взаимодействия средств информационной безопасности;
- обозначение устройства /ПО (идентификатор в инфраструктуре Заказчика);
- таблица IP адресации;
- производитель оборудования / ПО;
- модель оборудования / ПО;
- назначение оборудования /ПО;
- политики и контуры безопасности;
- ролевая модель и права доступа;
- модели угроз;
- правила и работу персонала с информацией;
- внутреннюю нормативную базу, определяющую тайну и конфиденциальную информацию;
- управление доступом к данным;
- организацию защиты от вредоносного ПО;
- организацию мониторинга событий в сфере информационной безопасности и реагирования на данные события;
- политики (шифрование, управление паролями, обработки данных и пр.);
- порядок и требования предоставления доступа пользователям к каналам обмена информацией;
- порядок предоставления доступа к информации третьим лицам, не являющихся сотрудниками Заказчика;
- порядок мониторинга и контроля доступа к сети компании

Результат анализа достаточности используемых средств информационной безопасности и их соответствие бизнес-задачам Заказчика:

- правила работы персонала с информацией – **правила и регламенты отсутствуют**
- внутренняя нормативная база, определяющая тайну и конфиденциальную информацию - **отсутствует**
- управление доступом к данным – **доступ к данным управляется посредством Active Directory и Group Policy**
- организация защиты от вредоносного ПО – **защита организована с помощью антивируса**
- организация мониторинга событий в сфере информационной безопасности и реагирования на данные события – **мониторинг инфраструктуры осуществляется Zabbix, установленным у стороннего подрядчика. Правила и триггеры мониторинга не предоставлены**
- используемые политики (шифрование, управление паролями, обработки данных и пр.) – **политики, регламенты и инструкции отсутствуют**
- использование различных носителей информации – **пользователи могут использовать внешние флеш накопители, жесткие диски на своих АРМ. Групповыми политиками это не запрещено**
- порядок и требования предоставления доступа пользователям к каналам обмена информацией – **регламент предоставления доступа отсутствует**
- порядок предоставления доступа к информации третьим лицам, не являющихся сотрудниками Заказчика – **регламент отсутствует**

- порядок мониторинга и контроля доступа к сети компании - **мониторинг инфраструктуры осуществляется Zabbix, установленным у стороннего подрядчика. Правила и триггеры мониторинга не предоставлены**

Модель угроз информационной безопасности

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИС и частота (вероятность) реализации рассматриваемой угрозы.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности информации для данной ИС в складывающихся условиях обстановки. Используем четыре вербальных градации этого показателя:

- **маловероятно** – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
- **низкая вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
- **средняя вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны;
- **высокая вероятность** – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты.

Для составления перечня актуальных угроз безопасности каждой градации вероятности возникновения угрозы ставим в соответствие числовой коэффициент Y_2 :

- **0** – для маловероятной угрозы;
- **2** – для низкой вероятности угрозы;
- **5** – для средней вероятности угрозы;
- **10** – для высокой вероятности угрозы.

$$Y = (Y_1 + Y_2) / 20.$$

По значению коэффициента реализуемости угрозы Y формируем вербальную интерпретацию реализуемости угрозы следующим образом:

- если $0 \leq Y \leq 0.3$, то возможность реализации угрозы признается низкой;
- если $0.3 < Y \leq 0.6$, то возможность реализации угрозы признается средней;
- если $0.6 < Y \leq 0.8$, то возможность реализации угрозы признается высокой;
- если $Y > 0.8$, то возможность реализации угрозы признается очень высокой.

Оценка опасности (ущерба) каждой угрозы выполняется экспертным путем, при котором определяется вербальный показатель, имеющий три значения:

- **низкая опасность** – если реализация угрозы может привести к незначительным негативным последствиям;
- **средняя опасность** – если реализация угрозы может привести к негативным последствиям;
- **высокая опасность** – если реализация угрозы может привести к значительным негативным последствиям.

Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность. Решение об актуальности угрозы безопасности информации принимается в соответствии с таблицей ниже.

Уровень актуальности угрозы

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

В качестве исходных данных об угрозах безопасности информации и их характеристиках, используется банк данных угроз безопасности информации, сформированный и поддерживаемый ФСТЭК России, а также иные источники, в том числе опубликованные в общедоступных источниках информации.

Модели угроз

Наименование угрозы	Y ₂	Y	Возможность реализации угрозы	Опасность (ущерб)	Актуальность
Угрозы утечки информации по техническим каналам					
Угрозы утечки видовой информации:					
Просмотр информации на дисплее АРМ в составе ИС не допущенными работниками	2	0,6	Средняя	Средний	Актуальная
Просмотр информации на дисплее АРМ в составе ИС посторонними лицами, находящимися в помещении, в котором ведется обработка информации	2	0,6	Средняя	Средний	Актуальная
Просмотр информации на дисплее пользователей ИС посторонними лицами, ведущими наблюдение (регистрацию) из-за границ контролируемой зоны	0	0,5	Средняя	Низкая	Неактуальная
Просмотр информации на дисплеях пользователей ИС с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка информации.	0	0,5	Средняя	Низкая	Неактуальная
Угроза анализа криптографических алгоритмов и их реализации: Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у	2	0,5	средняя	средняя	Актуальная

нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки					
--	--	--	--	--	--

Угроза аппаратного сброса пароля BIOS: Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера	0	0,5	Средняя	Низкая	Неактуальная
Угроза внедрения вредоносного кода в BIOS: Угроза заключается в возможности заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения BIOS/UEFI на версию, уже содержащую вредоносный код. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI и заменой чипсета BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера	0	0,5	средняя	низкая	Неактуальная
Угроза внедрения кода или данных: Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему или IoT-устройство вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями, автоматически при выполнении определённого условия (наступления определённой даты, входа пользователя в систему и т.п.) или с использованием аутентификационных данных, заданных «по умолчанию», а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов, и блокирования работы устройства при выполнении определенных команд. Данная угроза обусловлена: наличием уязвимостей программного обеспечения; слабостями мер антивирусной защиты и разграничения доступа; наличием открытого Telnet-порта на IoT-устройстве (только для IoT-устройств). Реализация данной угрозы возможна: в случае работы дискредитируемого пользователя с файлами, поступающими из	0	0,5	средняя	Низкая	Неактуальная

недоверенных источников; при наличии у него привилегий установки программного обеспечения; в случае неизмененных владельцем учетных данных IoT-устройства (заводских пароля и логина)					
Угроза восстановления аутентификационной информации: Угроза заключается в возможности подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе. Данная угроза обусловлена значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой, что определяет два следствия: время подбора в основном определяется не объёмом аутентификационной информации, а объёмом данных её хеш-кода; восстановленная аутентификационная информация может не совпадать с исходной (при применении некоторых алгоритмов для нескольких наборов исходных данных могут быть получены одинаковые результаты – хеш-коды). Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную»	2	0,6	средняя	Низкая	Неактуальная
Угроза выхода процесса за пределы виртуальной машины: Угроза заключается в возможности запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора. Данная угроза обусловлена уязвимостями программного обеспечения гипервизора, реализующего функцию изолированной программной среды для функционирующих в ней программ, а также слабостями инструкций аппаратной поддержки виртуализации на уровне процессора. Реализация данной угрозы приводит не только к компрометации гипервизора, но и запущенных в созданной им виртуальной среде средств защиты, а, следовательно, к их неспособности выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора	2	0,6	средняя	высокая	актуальная
Угроза длительного удержания вычислительных ресурсов пользователями: Угроза заключается в возможности ограничения нарушителем доступа конечных пользователей к вычислительному ресурсу за счёт принудительного удержания его в загруженном состоянии путём осуществления им многократного выполнения определённых деструктивных действий или эксплуатации уязвимостей программ, распределяющих вычислительные ресурсы между задачами. Данная угроза обусловлена слабостями механизмов балансировки нагрузки и распределения	2	0,6	средняя	низкая	Неактуальная

вычислительных ресурсов. Реализация угрозы возможна в случае, если у нарушителя имеется возможность делать запросы, которые в совокупности требуют больше времени на выполнение, чем запросы пользователя					
Угроза доступа к защищаемым файлам с использованием обходного пути: Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы. Реализация данной угрозы возможна при условиях: наличие у нарушителя прав доступа к некоторым объектам файловой системы; отсутствие проверки вводимых пользователем данных; наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с её помощью	2	0,6	средняя	Низкая	Неактуальная
Угроза доступа к локальным файлам сервера при помощи URL: Угроза заключается в возможности передачи нарушителем дискредитируемому браузеру запроса на доступ к файловой системе пользователя вместо URL-запроса. При этом браузер выполнит этот запрос с правами, которыми он был наделён при запуске, и передаст данные, полученные в результате выполнения этой операции, нарушителю. Данная угроза обусловлена слабостями механизма проверки вводимых пользователем запросов, который не делает различий между запросами на доступ к файловой системе и URL-запросами. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	2	0,6	средняя	средняя	Актуальная
Угроза доступа/перехвата/изменения HTTP cookies: Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации (учётным записям пользователей, сертификатам и т.п.), содержащейся в cookies-файлах, во время их хранения или передачи, в режиме чтения (раскрытие конфиденциальности) или записи (внесение изменений для реализации угрозы подмены доверенного пользователя). Данная угроза обусловлена слабостями мер защиты cookies-файлов: отсутствием проверки вводимых данных со стороны сетевой службы, использующей cookies-файлы, а также отсутствием шифрования при передаче cookies-файлов. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к cookies-файлам и	0	0,5	средняя	низкая	Неактуальная

отсутствии проверки целостности их значений со стороны дискредитируемого приложения					
Угроза загрузки нештатной операционной системы: Угроза заключается в возможности подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии доступности нарушителю следующего параметра настройки BIOS/UEFI – указания источника загрузки операционной системы	0	0,5	средняя	низкая	Неактуальная
Угроза заражения DNS-кеша: Угроза заключается в возможности перенаправления нарушителем сетевого трафика через собственный сетевой узел путём опосредованного изменения таблиц соответствия IP- и доменных имён, хранимых в DNS-сервере, за счёт генерации лавины возможных ответов на запрос DNS-сервера легальному пользователю или за счёт эксплуатации уязвимостей DNS-сервера. Данная угроза обусловлена слабостями механизмов проверки подлинности субъектов сетевого взаимодействия, а также уязвимостями DNS-сервера, позволяющими напрямую заменить DNS-кеш DNS-сервера. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий, достаточных для отправки сетевых запросов к DNS-серверу	0	0,5	средняя	низкая	Неактуальная
Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг: Угроза заключается в возможности осуществления потребителем облачных услуг (нарушителем) рассылки спама, несанкционированного доступа к виртуальным машинам других потребителей облачных услуг или осуществления других деструктивных программных воздействий на различные системы с помощью арендованных ресурсов облачного сервера. Данная угроза обусловлена тем, что потребитель облачных услуг может устанавливать собственное программное обеспечение на облачный сервер. Реализация данной угрозы возможна путём установки и запуска потребителем облачных услуг вредоносного программного обеспечения на облачный сервер. Успешная реализация данной угрозы потребителем облачных услуг оказывает негативное влияние на репутацию поставщика облачных услуг	0	0,5	средняя	низкая	Неактуальная
Угроза злоупотребления доверием потребителей облачных услуг: Угроза заключается в возможности нарушения (случайно или намеренно) защищённости информации потребителей облачных услуг внутренними нарушителями поставщика облачных услуг. Данная угроза обусловлена тем, что значительная часть функций безопасности переведена в сферу ответственности	0	0,5	средняя	низкая	Неактуальная

поставщика облачных услуг, а также невозможностью принятия потребителем облачных услуг мер защиты от действий сотрудников поставщика облачных услуг. Реализация данной угрозы возможна при условии того, что потребители облачных услуг не входят в состав организации, осуществляющей оказание данных облачных услуг (т.е. потребитель действительно передал поставщику собственную информацию для осуществления её обработки)					
Угроза использования альтернативных путей доступа к ресурсам: Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса). Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации, слабостями фильтрации входных данных. Реализация данной угрозы возможна при условии наличия у нарушителя: возможности ввода произвольных данных в адресную строку; сведений о пути к защищаемому ресурсу; возможности изменения интерфейса ввода входных данных	2	0,6	средняя	низкая	Неактуальная
Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами: Угроза заключается в возможности существенного снижения производительности вычислительного поля суперкомпьютера и эффективности выполнения на нём текущих параллельных вычислений из-за потребления вычислительных ресурсов суперкомпьютера «паразитными» процессами («процессами-потомками» предыдущих заданий или процессами, запущенными вредоносным программным обеспечением). Данная угроза обусловлена слабостями мер очистки памяти от «процессов-потомков» завершённых заданий, а также процессов, запущенных вредоносным программным обеспечением. Реализация данной угрозы возможна при условии некорректного завершения выполненных задач или наличия вредоносных процессов в памяти суперкомпьютера в активном состоянии	0	0,5	средняя	низкая	Неактуальная
Угроза использования информации идентификации/аутентификации, заданной по умолчанию: Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты. Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по умолчанию», предназначенные для первичного входа в	2	0,6	средняя	Высокая	Актуальная

систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset). Реализация данной угрозы возможна при одном из следующих условий: наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты; успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты					
Угроза использования механизмов авторизации для повышения привилегий: Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки. Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе	0	0,5	средняя	низкая	актуальная
Угроза нарушения доступности облачного сервера: Угроза заключается в возможности прекращения оказания облачных услуг всем потребителям (или группе потребителей) из-за нарушения доступности для них облачной инфраструктуры. Данная угроза обусловлена тем, что обеспечение доступности не является специфичным требованием безопасности информации для облачных технологий, и, кроме того, облачные системы реализованы в соответствии с сервис-ориентированным подходом. Реализация данной угрозы возможна при переходе одного или нескольких облачных серверов в состояние «отказ в обслуживании». Более того, способность динамически изменять объём предоставляемых потребителям облачных услуг может быть использована нарушителем для реализации угрозы. При этом успешно реализованная угроза в отношении всего лишь одного облачного сервиса позволит нарушить доступность всей облачной системы	0	0,5	средняя	низкая	Неактуальная
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины: Угроза заключается в возможности нарушения безопасности пользовательских данных программ, функционирующих внутри виртуальной машины, вредоносным программным обеспечением, функционирующим вне виртуальной машины. Данная	5	0,5	высокая	высокая	Актуальная

угроза обусловлена наличием уязвимостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри виртуальной машины, от несанкционированного доступа со стороны вредоносного программного обеспечения, функционирующего вне виртуальной машины. Реализация данной угрозы возможна при условии успешного преодоления вредоносным программным кодом границ виртуальной машины не только за счёт эксплуатации уязвимостей гипервизора, но и путём осуществления такого воздействия с более низких (по отношению к гипервизору) уровней функционирования системы					
Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин: Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через неё на другие системы путём осуществления несанкционированного доступа к образам виртуальных машин. Данная угроза обусловлена слабостями мер разграничения доступа к образам виртуальных машин, реализованных в программном обеспечении виртуализации. Реализация данной угрозы может привести: к нарушению конфиденциальности защищаемой информации, обрабатываемой с помощью виртуальных машин, созданных на основе несанкционированно изменённых образов; к нарушению целостности программ, установленных на виртуальных машинах; к нарушению доступности ресурсов виртуальных машин; к созданию ботнета путём внедрения вредоносного программного обеспечения в образы виртуальных машин, используемые в качестве шаблонов (эталонные образы)	5	0,6	высокая	высокая	Актуальная
Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения: Угроза заключается в возможности возникновения у потребителя облачных услуг непреодолимых сложностей для смены поставщика облачных услуг из-за технических сложностей в реализации процедуры миграции образов виртуальных машин из облачной системы одного поставщика облачных услуг в систему другого. Данная угроза обусловлена тем, что каждый поставщик облачных услуг использует для реализации своей деятельности аппаратное и программное обеспечение различных производителей, часть которого может использовать специфические (для данного производителя) инструкции, протоколы, методы, схемы коммутации и другие особенности реализации своего	0	0,5	средняя	Низкая	Неактуальная

функционала. Реализация данной угрозы возможна в случае несовместимости стандартных программных интерфейсов обмена данными (API) для реализации процедуры миграции образов виртуальных машин между различными поставщиками облачных услуг в одном или обоих направлениях. Также данная угроза обуславливает ограничение возможности смены производителей аппаратного и программного обеспечения поставщиком облачных услуг, что может привести к нарушению целостности и доступности информации по вине поставщика облачных услуг					
Угроза недобросовестного исполнения обязательств поставщиками облачных услуг: Угроза заключается в возможности раскрытия или повреждения целостности поставщиком облачных услуг защищаемой информации потребителей облачных услуг, невыполнения требований к уровню качества (уровню доступности) предоставляемых потребителям облачных услуг доступа к их программам или иммигрированным в облако информационным системам. Данная угроза обусловлена невозможностью непосредственного контроля над действиями сотрудников поставщика облачных услуг со стороны их потребителей. Реализация данной угрозы возможна в случаях халатности со стороны сотрудников поставщика облачных услуг, недостаточности должностных и иных инструкций данных сотрудников, недостаточности мер по менеджменту и обеспечению безопасности облачных услуг и т.д.	5	0,7	высокая	высокая	высокая
Угроза незащищённого администрирования облачных услуг: Угроза заключается в возможности осуществления опосредованного деструктивного программного воздействия на часть или все информационные системы, функционирующие в облачной среде, путём перехвата управления над облачной инфраструктурой через механизмы удалённого администрирования. Данная угроза обусловлена недостаточностью внимания, уделяемого контролю вводимых пользователями облачных услуг данных (в том числе аутентификационных данных), а также уязвимостями небезопасных интерфейсов обмена данными (API), используемых средствами удалённого администрирования. Реализация данной угрозы возможна в случае получения нарушителем аутентификационной информации (при их вводе в общественных местах) легальных пользователей, или эксплуатации уязвимостей в средствах удалённого администрирования	0	0,5	средняя	низкая	Неактуальная
Угроза некачественного переноса инфраструктуры в облако: Угроза заключается в возможности снижения реального уровня защищённости иммигрирующей в облако информационной системы из-за ошибок, допущенных	2	0,5	средняя	высокая	Актуальная

при миграции в ходе преобразования её реальной инфраструктуры в облачную. Данная угроза обусловлена тем, что преобразование даже части инфраструктуры информационной системы в облачную зачастую требует проведения серьёзных изменений в такой инфраструктуре (например, в политиках безопасности и организации сетевого обмена данными). Реализация данной угрозы возможна в случае несовместимости программных и сетевых интерфейсов или несоответствий политик безопасности при осуществлении переноса информационной системы в облако					
Угроза некорректной реализации политики лицензирования в облаке: Угроза заключается в возможности отказа потребителям облачных услуг в удалённом доступе к арендуемому программному обеспечению (т.е. происходит потеря доступности облачной услуги SaaS) по вине поставщика облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками лицензирования использования программного обеспечения различных производителей в облаке. Реализация данной угрозы возможна при условии, что политика лицензирования использования программного обеспечения основана на ограничении количества его установок или числа его пользователей, а созданные виртуальные машины с лицензируемым программным обеспечением использованы много раз	0	0,5	средняя	Низкая	Неактуальная
Угроза неопределённости в распределении ответственности между ролями в облаке: Угроза заключается в возможности возникновения существенных разногласий между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей в части обеспечения информационной безопасности. Данная угроза обусловлена отсутствием достаточного набора мер контроля за распределением ответственности между различными ролями в части владения данными, контроля доступа, поддержки облачной инфраструктуры и т.п. Возможность реализации данной угрозы повышается в случае использования облачных услуг, предоставляемых другими поставщиками (т.е. в случае использования схемы оказания облачных услуг с участием посредников)	0	0,5	средняя	низкая	Неактуальная
Угроза неопределённости ответственности за обеспечение безопасности облака: Угроза заключается в возможности невыполнения ряда мер по защите информации как поставщиком облачных услуг, так и их потребителем. Данная угроза обусловлена отсутствием чёткого разделения ответственности в части обеспечения безопасности информации между потребителем и поставщиком облачных услуг. Реализация данной угрозы возможна при условии недостаточности документального разделения сфер	0	0,5	средняя	Низкая	Неактуальная

ответственности между сторонами участвующими в оказании облачных услуг, а также отсутствия документального определения ответственности за несоблюдение требований безопасности					
Угроза неправомерного ознакомления с защищаемой информацией: Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.	2	0,6	средняя	средняя	Актуальная
Угроза неправомерных действий в каналах связи: Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных. Реализация данной угрозы возможна при условии осуществления нарушителем несанкционированного доступа к сетевому трафику	2	0,5	средняя	средняя	актуальная
Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети: Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путём эксплуатации уязвимостей программного и (или) микропрограммного обеспечения указанного оборудования. Данная угроза обусловлена ограниченностью функциональных возможностей (наличием слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры, наличием у данного оборудования фиксированного сетевого адреса. Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении	2	0,6	средняя	Средняя	Актуальная

сетевого оборудования					
Угроза несанкционированного доступа к аутентификационной информации: Угроза заключается в возможности извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации. Данная угроза обусловлена наличием слабостей мер разграничения доступа к защищаемой информации. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа к участкам оперативного или постоянного запоминающих устройств, в которых хранится информация аутентификации	0	0,5	средняя	низкая	Неактуальная
Угроза несанкционированного доступа к виртуальным каналам передачи: Угроза заключается в возможности осуществления нарушителем несанкционированного перехвата трафика сетевых узлов, недоступных с помощью сетевых технологий, отличных от сетевых технологий виртуализации, путём некорректного использования таких технологий. Данная угроза обусловлена слабостями мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных). Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации	0	0,5	средняя	низкая	Неактуальная
Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети: Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор через его подключение к физической вычислительной сети. Данная угроза обусловлена наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной и (или) физической сетью, уязвимостями гипервизора, а также уязвимостями программных средств и ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности. Реализация данной угрозы возможна в одном из следующих случаев: наличие у нарушителя привилегий, достаточных для осуществления деструктивного программного воздействия из виртуальных машин; наличие у гипервизора активного интерфейса	0	0,5	средняя	низкая	Неактуальная

взаимодействия с физической вычислительной сетью					
<p>Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение:</p> <p>Угроза заключается в возможности нарушения вредоносной программой, функционирующей внутри виртуальной машины, целостности программного кода своей и (или) других виртуальных машин, функционирующих под управлением того же гипервизора, а также изменения параметров её (их) настройки. Данная угроза обусловлена наличием слабостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения не только защищаемой информации и программного кода обрабатывающих её программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной виртуальной машины</p>	2	0,5	средняя	высокая	актуальная
<p>Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети:</p> <p>Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации. Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия</p>	2	0,5	средняя	высокая	актуальная
<p>Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин:</p> <p>Угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин с помощью различных механизмов</p>	0	0,5	средняя	низкая	Неактуальная

обмена данными между виртуальными машинами, реализуемых гипервизором и активированных в системе. Данная угроза обусловлена слабостями механизма обмена данными между виртуальными машинами и уязвимостями его реализации в конкретном гипервизоре. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий, достаточных для использования различных механизмов обмена данными между виртуальными машинами, реализованных в гипервизоре и активированных в системе					
Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети: Угроза заключается в возможности удалённого осуществления нарушителем несанкционированного доступа к виртуальным устройствам из виртуальной и (или) физической сети с помощью различных сетевых технологий, используемых для осуществления обмена данными в системе, построенной с использованием технологий виртуализации. Данная угроза обусловлена наличием слабостей в сетевых программных интерфейсах гипервизоров, предназначенных для удалённого управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий достаточных для осуществления обмена данными в системе, построенной с использованием технологий виртуализации	2	0,6	средняя	высокая	актуальная

Рекомендации:

Из приведенной выше модели угроз видно, что основную опасность представляет факт размещения серверной и сетевой инфраструктуры на территории стороннего подрядчика, что может привести к частичной или полной потере данных, большому времени простоя в случае остановки сервисов подрядчика и невозможности восстановления данных в связи с умышленными или случайными действиями подрядчика.

Заказчику рекомендуется разместить инфраструктуру на собственных мощностях, размещенных на собственной территории. Это позволит защитить данные от компрометации, умышленной или случайной утери и позволит значительно сократить время простоя в случае восстановления данных из собственных репозиториях.

Также рекомендуется организовать сеть с помощью оборудования ТОРП (см. стр. 17)

Рекомендуется ввести штатную единицу «Специалист по информационной безопасности», разработать стратегию внедрения и развития информационной безопасности, а также регламенты, инструкции, указанные ниже:

- схемы расположения оборудования в монтажных шкафах серверных комнат;
- схемы взаимодействия средств информационной безопасности;
- обозначение устройства /ПО (идентификатор в инфраструктуре Заказчика);
- таблица IP адресации;
- производитель оборудования / ПО;
- модель оборудования / ПО;
- назначение оборудования /ПО;
- политики и контуры безопасности;
- ролевая модель и права доступа;
- модели угроз;
- правила и работу персонала с информацией;
- внутреннюю нормативную базу, определяющую тайну и конфиденциальную информацию;
- управление доступом к данным;
- организацию защиты от вредоносного ПО;
- организацию мониторинга событий в сфере информационной безопасности и реагирования на данные события;
- политики (шифрование, управление паролями, обработки данных и пр.);
- порядок и требования предоставления доступа пользователям к каналам обмена информацией;
- порядок предоставления доступа к информации третьим лицам, не являющихся сотрудниками Заказчика;
- порядок мониторинга и контроля доступа к сети компании;

Средства ВКС

Результат анализа достаточности используемых средств ВКС и их соответствие бизнес-задачам Заказчика:

В качестве ПО для организации ВКС используется ПО Zoom. Данное ПО является SaaS решением, что позволяет гибко управлять пользовательскими лицензиями, а также организовывать видеоконференции из любой точки.

Zoom для государственных учреждений — это сервисы Zoom Meeting и Zoom Phone, предлагаемые компанией Zoom в облачной среде, соответствующей требованиям FedRAMP. Zoom для государственных учреждений позволяет клиентам использовать ограниченную версию сервисов Zoom в отдельной облачной среде, соответствующей требованиям FedRAMP, которая размещена в облаке Amazon Web Services Government Cloud и связанных центрах обработки данных Zoom (например, в Сан-Хосе, штат Калифорния, и Нью-Йорке), независимо от стандартной коммерческой облачной среды компании Zoom. Описание остальных функций и решений см. на сайте <https://www.zoomgov.com/>. Сервисы Zoom Meeting и Zoom для государственных учреждений — это независимые среды, и поэтому обмен данными между ними, в том числе данными мгновенных сообщений и данными чатов, невозможен.

Функции безопасности FedRAMP. Zoom для государственных учреждений прошел сертификацию FedRAMP Moderate ATO (средний уровень). Требуется протокол TLS 1.2 или выше

Отсутствует информация:

- схема взаимодействия компонентов ВКС;
- схемы расположения оборудования в монтажных шкафах серверных комнат;
- обозначение устройства /ПО (идентификатор в инфраструктуре Заказчика);
- таблица IP адресации;

Замечания:

Отсутствуют

Рекомендации:

Разработать схему взаимодействия аппаратного обеспечения Заказчика с системой ZOOM

Разработать инструкции по использованию ZOOM

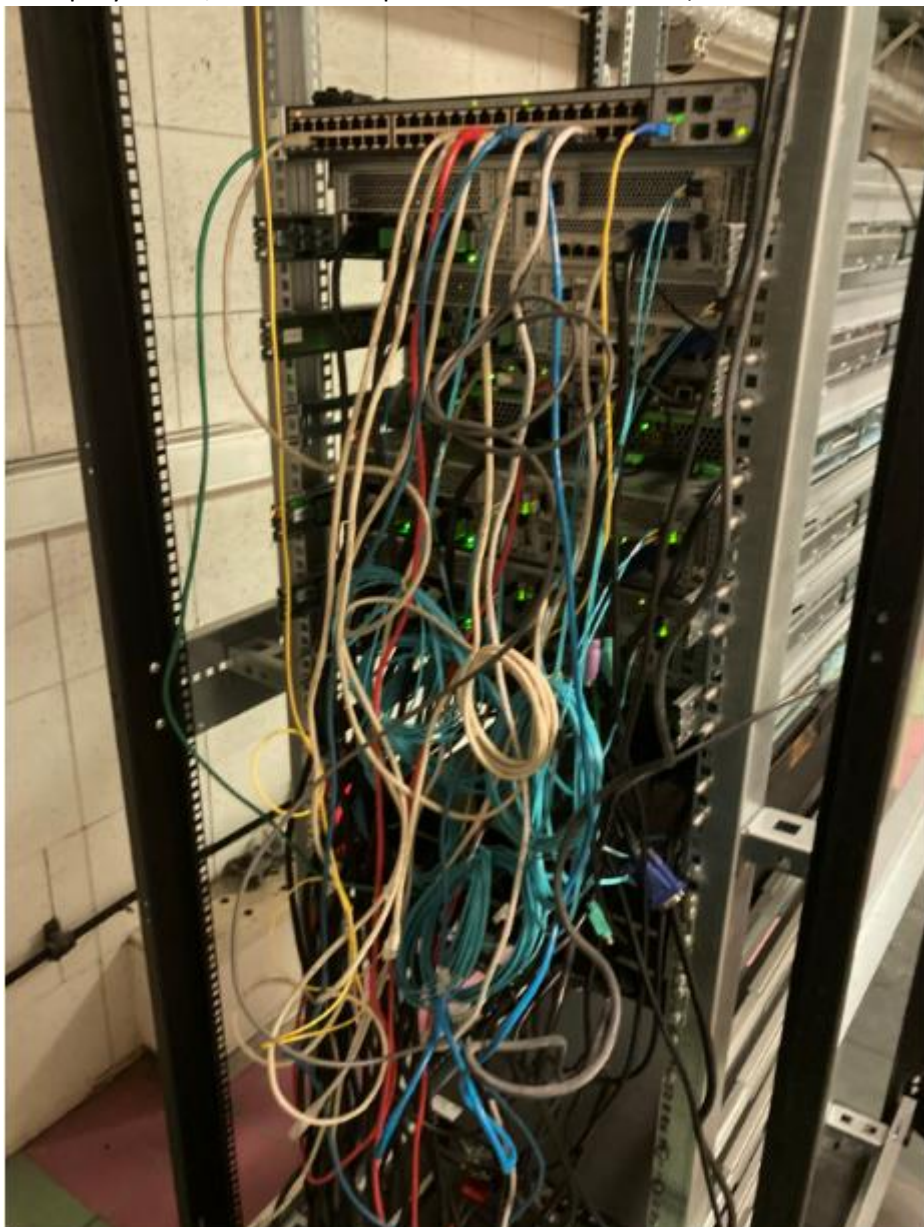
Разработать политики разграничения прав использования и организации видеоконференций в ZOOM.

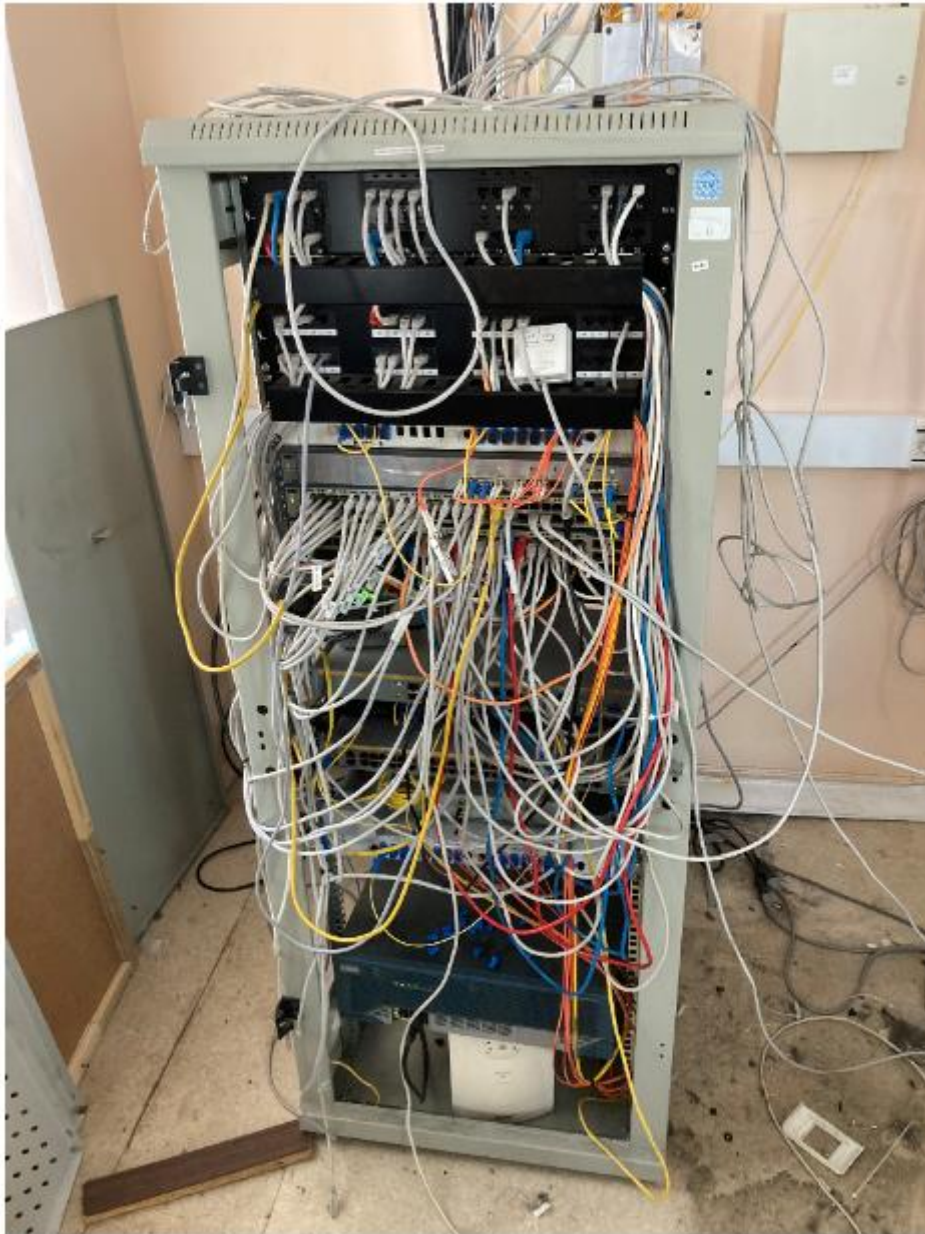
Средства инженерной инфраструктуры

Результат анализа достаточности используемых средств и их соответствие бизнес-задачам Заказчика:

Ниже приведены некоторые снимки серверных комнат Заказчика.

На картинках видно, что кабель нуждается в упорядочивании. Комнаты не оборудованы системами пожаротушения, пожарной сигнализацией и кондиционированием.







Замечания:

Серверные комнаты Заказчика не оборудованы системами пожаротушения, пожарной сигнализации, стабильным питанием, фальшполами, системами охлаждения и пылеотведения.

Рекомендации:

Помещения для размещения средств вычислительной техники и информатики (СВТИ согласно ГОСТ Р 50839-95) проектируются в соответствии с требованиями норм СНиП 11- 2-80 для зданий категории "В", "Инструкции по проектированию зданий и помещений для электронно-вычислительных машин СН 512-78" (утв. ГК СССР по делам строительства, пост. № 244 от 22.12.78). 1.4 Используемые СВТИ должны соответствовать требованиям ГОСТ Р 50839-95, ГОСТ Р 50377-92, ГОСТ 27201-87, ГОСТ 26329-84, ГОСТ 29216-91, ГОСТ Р 50628-93 и иметь сертификаты соответствия от Госстандарта и гигиенические сертификаты от Минздрава России, а также могут иметь знак соответствия ISO 9000, признанный в России.

Помещение вычислительного центра ИВС (далее - серверная) рекомендуется располагать без соприкосновения с внешними стенами здания и сообщения с посторонними помещениями. Трассы

обычного и пожарного водоснабжения, отопления и канализации должны быть вынесены за пределы серверной и не находиться непосредственно над ней на верхних этажах. Через серверную не должны проходить любые транзитные коммуникации. Местом расположения серверной или процессингового центра не может быть этаж обычного административного здания, который оборудован под требования для офисов. Меры безопасности и инфраструктура этажа, где расположена серверная, по своему назначению и высокой стоимости СВТИ проектируются с учетом более высоких требований по строительной части и инженерному оснащению здания. При расположении резервной серверной в подвальном помещении значение этих требований еще более возрастает. Для сокращения суммарной длины прокладываемых кабелей серверную (коммутационные шкафы) следует размещать ближе к середине здания. Это сократит расходы на материалы и позволит соблюдать требуемую международным стандартом ISO/IEC 11801 длину кабеля для структурированной сети 5 категории. Конструкция стен или перегородок серверной должна быть герметичной. Вход в серверную оборудуется герметичной дверью (тамбур-шлюзом). Серверная может оборудоваться фальшполом для размещения коммуникаций (подачи кондиционированного воздуха к устройствам). Высота подпольного пространства должна быть не менее 200 мм (рекомендованная - 300 мм).

Температура воздуха в помещениях - $20^{\circ}\pm 2^{\circ}\text{C}$ (не более 25°C). Для ресурса СВТИ лучше нижняя граница. Относительная влажность воздуха - 20-70 % (не более 75 % в холодный период, в теплый для 25°C - не более 65 %, для 24°C и ниже - не более 70 %). Оптимальная скорость потока воздуха - 0,2 м/с (не более 0,3 м/с для холодного, 0,5 м/с для теплого периодов). Запыленность воздуха помещений не должна превышать: в серверной - 0,75 мг/м³, с размерами частиц не более 3 мкм (атм. пыль, сажа, дым, споры, асбест); в помещениях обработки данных - 2 мг/м³. Допустимый уровень шума не более 65 дБ. Допустимый уровень вибрации не должен превышать по амплитуде 0,1 мм и по частоте 25 Гц. Поверхности стен и материалы напольного покрытия в помещениях для СВТИ (особенно в серверной) не должны выделять и накапливать пыль. Напольные покрытия должны иметь антистатические качества. При оборудовании помещения для хранения носителей данных или установке специального сейфа класса ДИС (магнитные носители) следует учитывать более жесткие требования, обусловленные тем, что температура хранения для магнитных носителей не может превышать 500 С, а максимально допустимая влажность воздуха при хранении не более 85%. Только в этом случае после воздействия высоких температур информация с магнитных носителей будет считываться. Целесообразно ограничиться установкой сейфа для хранения магнитных носителей, но при этом он должен иметь сертификат испытаний по стандартам страны-производителя и сертификат соответствия ГОСТ 50862-96. Это не предотвратит опасных воздействий для всех СВТИ, но позволит гарантированно сохранить данные при любом неблагоприятном исходе, даже при пожаре.

Основой для пожарной безопасности служат нормативные документы, утвержденные в установленном порядке по согласованию с ГУ Государственной противопожарной службы МВД России. Нормы пожарной безопасности НПБ 110-99 определяют перечень зданий сооружений, помещений и оборудования, которые должны быть защищены автоматическими установками пожаротушения (АУПТ) и пожарной сигнализации (АУПС), которые проектируются в соответствии со СНиП 2.04.09-84. Категория зданий и помещений по взрывопожарной и пожарной опасности определяется в соответствии с НПБ 105-95. Противопожарная защита устанавливается обязательно и независимо от ведомственной принадлежности, организационно-правовой формы и площади помещений. Согласно "Перечню" НПБ 110-99 помещения связи (таблица 3, п. 4.16-4.20) и помещения общественного назначения для размещения ЭВМ (таблица 3, п. 4.38), которые, с учетом современных технологий, имеют в своем составе СВТИ, также подлежат защите. Исключение составляют СВТИ, размещенные на рабочих местах пользователей и не требующих выделения зон обслуживания.

Противодымную защиту следует проектировать в соответствии с требованиями СНиП 2.04.05-91 "Отопление, вентиляция и кондиционирование"

Серверная (основная и резервная) и телекоммуникационная оборудуются автоматическими установками газового пожаротушения (АУГП), согласно требованиям по проектированию зданий и помещений для ЭВМ (раздел 3, СН-512-78). АУГП предусматривается для помещений, где располагается оборудование управления ИВС (серверная, центр управления, процессинговый центр). Огнегасящим веществом должен быть газ, который имеет российский сертификат. Таким средством тушения может быть газ "игмер" (октафторциклобутан, хладон 318Ц, ТУ 2412-001-13181581-96, код К-ОКП 241249, сертификат соответствия № РОСС RU.ББ02. Н00073 от 10.04.96, одобренный НИИ медицины труда РАМН) или двуокись углерода, заправленная в модули высокого давления типа МГП. Использование фреона 114В2 (тетрафтордибромэтан) и порошковых огнегасителей в этих помещениях категорически запрещено.

Рекомендуемы размеры серверного помещения

КОЛИЧЕСТВО РАБОЧИХ ЗОН	РАЗМЕРЫ СЕРВЕРНОГО ПОМЕЩЕНИЯ, м2
до 100	14
101-400	37
401-800	74
801-1200	111

Необходимо установить:

- Систему пожаротушения
- Пожарной сигнализации
- Видеонаблюдения
- СКУД
- Кондиционирование с резервированием

Необходимо доработать:

- Убрать провода в кабель каналы
- Сделать биркование и маркировку
- Закрыть серверные шкафы дверьми и убрать ключи на охрану под роспись
- Для каждого сетевого или серверного сервиса использовать провода разных цветов

Организационная структура

Общая информация:

На момент проведения аудита документация об орг. Структуре отсутствовала.

Все данные, указанные ниже были получены путем очного интервью с Заказчиком.

Структура отдела:

- Советник вице-президента по информатизации
- Начальник отдела ИТ
- Заместители ОИТ (ведение локальных проектов, например ВКС, СКУД, IP телефония)
- Главные специалисты
- Аутсорсинговая компания – Серверы, AD, почта, файл-сервер, интернет, локальная сеть

Всего у Заказчика работает порядка 500 сотрудников пользователей АРМ. В состав ИТ отдела входит 8 человек, из которых 6 человек входят в управляющий состав.

На данный момент количество сотрудников оптимальное. Но если Заказчик примет решение разворачивать собственную инфраструктуру, необходимо увеличить штат сотрудников.

Рекомендации:

Необходимо четко определить роли каждого сотрудника, для каждого сотрудника составить должностную инструкцию. Это позволит оптимально использовать временной ресурс каждого сотрудника. Рекомендуемая орг. структура отдела с собственной инфраструктурой:

- Руководитель отдела
- Заместитель руководителя отдела
- Старший системный администратор
- Сетевой инженер
- Системный администратор – 2 человека
- Руководитель технической поддержки
- Специалист тех. Поддержки – 3 человека
- Специалист по информационной безопасности

Зоны ответственности персонала отдела ИТ:

- Руководитель отдела – Общее руководство отделом, постановка и контроль исполнения задач линейному персоналу, разработка глобальных ИТ решений.
- Заместитель руководителя отдела – Замещение руководителя отдела, ведение договорной документации, подготовка технических заданий для тендерных процедур, руководство отделом, внедрение ИТ решений, подготовка проектной документации для внедрения ИТ решений, подготовка дорожных карт, разработка ИТ документации и поддержание ее в актуальном состоянии.
- Старший системный администратор – Постановка задач системным администраторам и контроль их исполнения, администрирование серверной и сетевой инфраструктуры Заказчика, разработка планов восстановления систем, разработка системы защиты сети.
- Сетевой инженер – Администрирование сети, администрирование сетевого оборудования, проведение аудита сети, разработка дизайн схем ЛВС, подбор оборудования для внедрения, разработка документации и планов защиты информации совместно со специалистом по ИБ.

- Системный администратор – 2 человека – администрирование сетевого и серверного оборудования, администрирование AD, GPO, DNS, DHCP, Firewall, NAT, администрирование пользовательских АРМ, пользовательского ПО и железа, администрирование СКУД, системы видеонаблюдения, IP телефонии.
- Руководитель технической поддержки – Постановка задач специалистам тех. Поддержки и контроль их исполнения, внедрение тикет-системы, настройка тикет-системы, составление отчетов по заявкам пользователей, разрешение споров между пользователями и специалистами тех. Поддержки, исправление ошибок с пользовательскими АРМ, ПО и оборудованием, ведение учета пользовательского и серверного оборудования, ведение учета ПО
- Специалист тех. Поддержки – 3 человека – Обработка пользовательских заявок, исправление ошибок с пользовательскими АРМ, периферийным оборудованием, ПО и железом, мелкий ремонт АРМ и периферийного оборудования, чистка печатающей техники, замена картриджей, ведение учета расходных материалов, организация ВКС.
- Специалист по информационной безопасности – разработка стратегии по защите информации, разработка моделей угроз, тестирование на проникновение, разработка документации и отчетов, отслеживание попыток внешних и внутренних атак, разработка и внедрение системы защиты информации.

Пользовательские АРМ

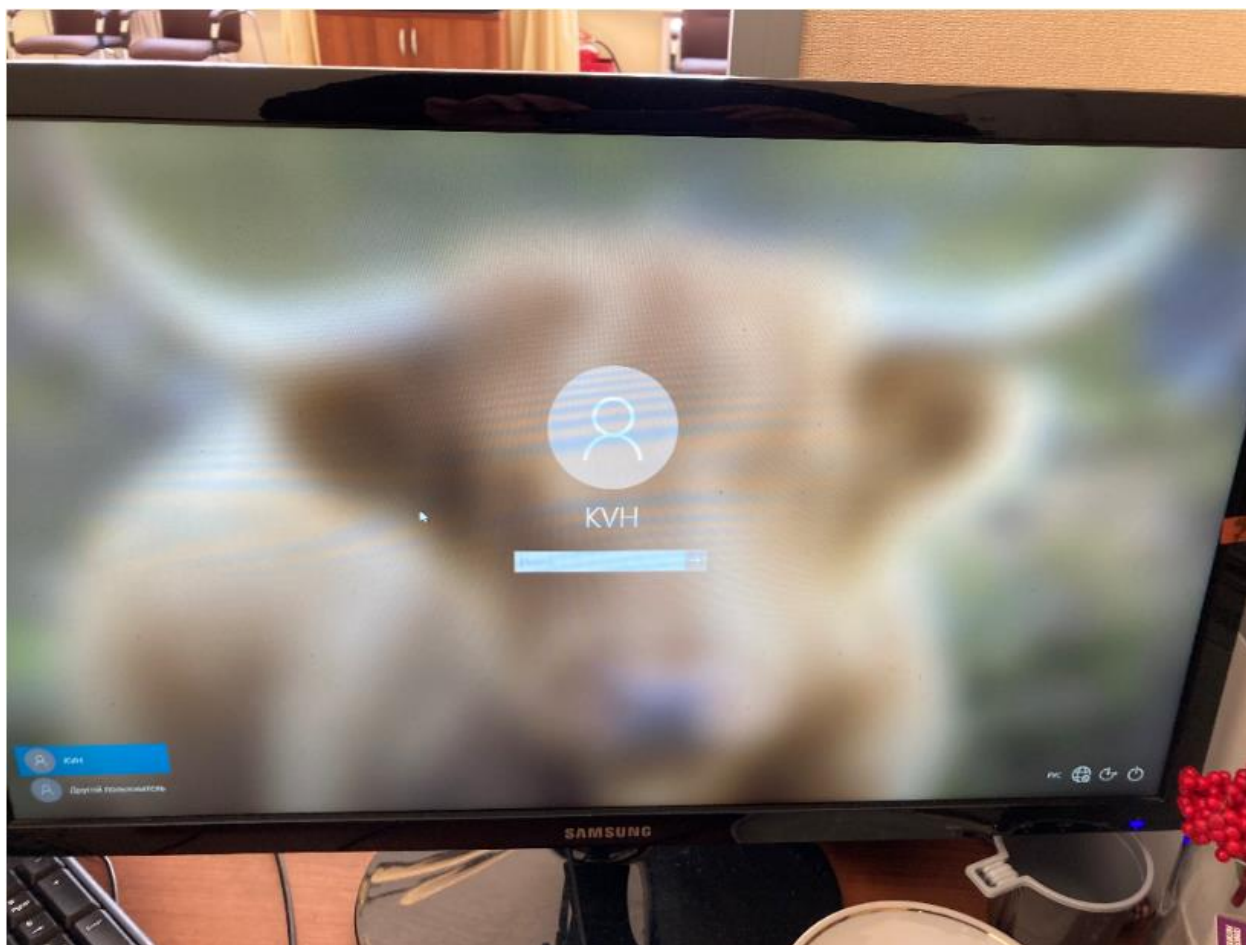
Общая информация:

Практически все АРМ введены в корпоративный домен в Active Directory. На выбранных АРМ установлена лицензионная ОС.

Пользователи входят в доменную учетную запись, что дает системному администратору возможность гибкого управления ПК, учетными записями и правами доступа к сетевым ресурсам.

Некоторые пользователи используют локальные учетные записи на АРМ.

Также на некоторых АРМ установлена Windows 7.



Рекомендации:

Необходимо обновить все операционные системы до последней версии, к примеру Windows 10 Pro. Все АРМ необходимо ввести в домен.

В Active Directory необходимо развернуть SCCM.

Рекомендуется привести все аппаратное и программное обеспечение к единообразию: обновить все ПО до последних версий, закупить идентичные АРМ и серверы, а также периферийное оборудование. Это позволит унифицировать программное и аппаратное обеспечение, выбрать 1-2 подрядчиков, которые специализируются на выбранном оборудовании, в случае поломки, быстро отремонтировать вышедшее из строя оборудование.

Основные выводы

- Арендуемая серверная инфраструктура достаточна для обеспечения потребностей Заказчика.
- Практически полностью отсутствует документация, описывающая оборудование, ПО, сервисы.
- Отсутствуют регламенты, описывающие резервное копирование, восстановление данных.
- Отсутствуют пользовательские инструкции.
- Отсутствуют регламенты и документация по обеспечению информационной безопасности.
- Отсутствует документация по орг. Структуре.
- В основном используются HDD диски, что может негативно сказываться на скорости работы приложений и информационных систем.
- Основные сервисы, такие как Active Directory зарезервированы. Используется отказоустойчивый кластер с СХД.
- Архитектура системы резервного копирования и СХД нуждается в доработке
- На аппаратной инфраструктуре сторонние организации не размещаются (по словам стороннего подрядчика)
- Заказчик несет высокий риск потери над управлением собственными данными по причине компрометации учетных данных, либо по причине саботажа.
- На данный момент заказчик не обладает необходимыми мощностями для размещения ИТ инфраструктуры на собственной территории.
- У Заказчика полностью отсутствует отдел по информационной безопасности. Данной области не уделяется необходимое внимание. Присутствует множество нарушений по ИБ, в том числе отсутствие полного контроля над сетевым и серверным оборудованием.
- Заказчик частично использует устаревшее ПО и оборудование.
- Не организована должным образом служба технической поддержки пользователей. Нет специализированного ПО.
- Данные о сетевой и серверной инфраструктуре, которыми располагает Заказчик могут оказаться неактуальными, т.к. существует риск того, что сторонний подрядчик, который сдает Заказчику оборудование в аренду, может вовремя не уведомлять Заказчика об изменениях.

Рекомендации

- Рекомендуется развертывание собственной инфраструктуры.
- Для развертывания серверной и сетевой инфраструктуры на территории Заказчика, рекомендуется оборудовать 2 серверные комнаты в одном или в двух зданиях. Архитектура должна подразумевать отказоустойчивый кластер виртуализации с установленными виртуальными машинами. Отказоустойчивый кластер должен иметь жесткие диски на СХД.
- Серверные необходимо оборудовать системами кондиционирования, пожарной сигнализации и СКУД с разграничением прав доступа и фиксацией проходов в режиме 24/7.
- Все провода в серверных комнатах необходимо уложить в кабель-органайзеры. Рекомендуется использовать патч-корды разных цветов для идентификации различных сервисов.
- Все АРМ необходимо ввести в домен, чтобы у пользователей были централизованные права на компьютеры.
- На некоторых АРМ установлена ОС Windows 7. Данная ОС больше не поддерживается Microsoft. Рекомендуется обновить все ОС до Windows 10. Серверные ОС рекомендуется обновить до Windows sever 2019.
- Пользовательские заявки оформляются в задачнике Microsoft. Рекомендуется закупка и развертывание тикет системы HelpDesk, в которой будет указываться статус заявки, заказчик, исполнитель. В системе должна присутствовать база знаний и повторяющихся ошибок.
- Инвестиционные затраты на собственную инфраструктуру выше, чем на арендованную, однако арендованная инфраструктура обладает рядом существенных минусов, по сравнению с собственной:
 - Исходя из того, что Заказчик выбирает подрядчика путем проведения закупки по 44-ФЗ ежегодно, существует большая вероятность того, что инфраструктура следующего заказчика окажется ненадежной, менее производительной.
 - Также при перемещении сервисов с одной инфраструктуры на другую в процессе смены контракта, существует большая вероятность остановки сервисов на время проведения миграции, что в пересчете на стоимость каждого дня работы Заказчика может стать гораздо дороже, чем развертывание и содержание собственной инфраструктуры.
- Операционные расходы на арендованную инфраструктуру за 5 лет превысят инвестиционные на собственную в пять раз!
- Необходимо определить оборудование и ПО, отвечающее за ИБ, задокументировать планы резервного копирования, аварийного восстановления, а также планы аварийного тестирования.
- Необходимо составить полный список коммутационного и сетевого оборудования, задокументировать его и составить планы резервного копирования, DRP (планы аварийного восстановления).
- Необходимо определить список имеющегося серверного оборудования у Заказчика, разработать документацию по назначению оборудования с указанием инвентарных и серийных номеров.
- Рекомендуется модернизировать ИТ инфраструктуру, а именно, унифицировать аппаратное обеспечение, унифицировать программное обеспечение, разработать регламенты и инструкции для каждого серверного узла и сетевого узла, а также разработать подробную общую схему с указанием назначения устройства, IP адреса, имени узла и зависимостями между ними
- Рекомендуется перенести все вычислительные мощности на территорию Заказчика, разработать схемы расположения оборудования в монтажных шкафах серверных комнат с указанием имен устройств, серийных номеров, конфигурацией жестких дисков, таблицей IP адресации, типом и версией операционной системы, типом и количеством адаптеров ввода-

вывода. Также рекомендуется разработать документ, регламентирующий уровень производственной критичности устройств, а также определить SLA для каждого устройства.

- Рекомендуется организовать архитектуру виртуализации на базе VmWare с отказоустойчивым кластером из двух аппаратных серверов и одного аппаратного сервера для реализации репликации виртуальных машин. Отказоустойчивый кластер позволит избежать простоев при аппаратном сбое одного из хостов. Сервер репликации позволит избежать сильных простоев при программных сбоях ВМ.
- Рекомендуется использовать базу данных одного разработчика, например Ms SQL. Это позволит унифицированно настроить резервное копирование баз данных всех систем
- По возможности необходимо использовать SaaS решения, для таких сервисов как видеоконференцсвязь (Уже используется Zoom), электронная почта, например MS Office 365. Использование SaaS решений позволяет спрогнозировать затраты на ПО и гибко управлять лицензиями, в нужный момент сокращая расходы на ПО. А также SaaS решения позволяют всегда иметь последнюю версию ПО.
- Закупить необходимое оборудование для размещения информационных систем на собственных мощностях с избыточностью 50% для возможности оперативного размещения новых ИТ сервисов и информационных систем.
- Рекомендуется использовать сетевые устройства со стекированием из списка ТОРП.
- Рекомендуется документально зафиксировать таблицу IP адресации, а также сделать резервные копии конфигураций всех сетевых устройств. Это позволит в кратчайшие сроки восстановить сетевую конфигурацию в случае сбоев.
- Рекомендуется оптимизировать и модернизировать орг. Структуру отдела ИТ с учетом будущих изменений.
- Рекомендуется составить план развития ИТ на 1 год и на 3 года вперед.

Рекомендованная концепция развития IT инфраструктуры ФГБУ РАН

Основными задачами развития IT являются:

- Переход на единую промышленную платформу, которая позволит обеспечить максимальную поддержку деятельности компании
- Создание системы управления единой нормативно – справочной информацией
- Создание основного и резервного центров обработки данных
- Обеспечение бесперебойной работы удаленных пользователей с максимальным уровнем безопасности
- Переход к процессной модели управления IT
- Развитие системы обучения пользователей
- Создание системы мониторинга ИТ инфраструктуры

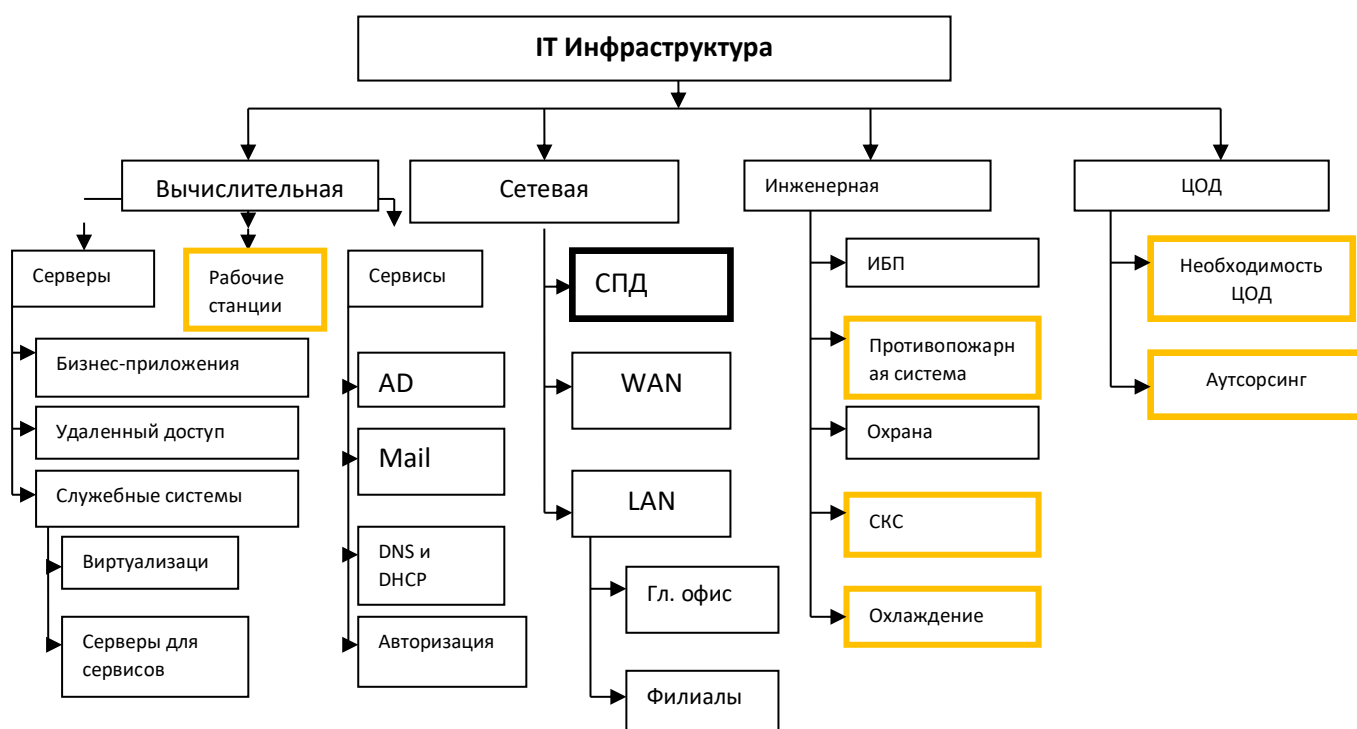
1. IT инфраструктура

Всю IT инфраструктуру можно разбить на несколько областей:

- Сетевая
 - Локальная вычислительная сеть
 - Система передачи данных
 - Телефония
 - Подключение к интернету
- Вычислительная
 - Аппаратное и программное обеспечение
 - Виртуализация серверов
 - Пользовательские сервисы
 - Резервное копирование
 - СХД
- Инженерная
 - СКС
 - Противопожарная система
 - Электропитание
 - Система управления климатом

Благодаря данной разбивке можно сделать структуру, которая наглядно позволит быстро определить те сегменты, которые требуют улучшений и особого внимания к себе.

Блок схема ИТ инфраструктуры



В ходе аудита были выявлены несколько сегментов, нуждающихся в доработке. На схеме они отмечены оранжевым цветом.

Были определены все используемые серверные платформы, программное обеспечение и сетевое оборудование во всех филиалах (см. стр. 2 и 4). Это позволит унифицировать и подобрать используемое оборудование при развертывании инфраструктуры в будущем.

Необходимо дать оценку всем областям ИТ инфраструктуры по следующим критериям:

Критерии оценки ИТ инфраструктуры

- Общие вопросы
 - **Соответствие ИТ инфраструктуры требованиям непрерывности предоставляемых сервисов** – соответствует
 - **Управление ИТ инфраструктурой** – управление всей инфраструктурой передано сторонней организации. Это может повлечь Заказчик выбирает подрядчика путем проведения закупки по 44-ФЗ ежегодно, существует большая вероятность того, что инфраструктура следующего заказчика окажется ненадежной, менее производительной.
 - Также при перемещении сервисов с одной инфраструктуры на другую в процессе смены контракта, существует большая вероятность остановки сервисов на время проведения миграции, что в пересчете на стоимость каждого дня работы Заказчика может стать гораздо дороже, чем развертывание и содержание собственной инфраструктуры
 - **Документирование** – Не соответствует. Документация отсутствует.
- Вычислительная инфраструктура
 - **Рабочие места** – На рабочих местах установлены лицензионные ОС. За редким исключением компьютеры введены в домен. На некоторых местах установлены устаревшие ОС, например Windows 7, которые не поддерживаются производителем
 - **ПО** – В ходе аудита не было выявлено нелегального ПО

- **СХД, резервное копирование и архивирование** – на данный момент у подрядчика, у которого размещается инфраструктура Заказчика имеет систему резервного копирования (см. стр. 2-4). Отсутствует документация проведения тестирования отказов оборудования. Необходимо провести тестовое отключение боевых серверов с переключением на резервные. Также необходимо провести тестирование восстановления виртуальных машин из системы бэкапов.
- **Серверы** – Серверная инфраструктура на данный момент расположена у стороннего подрядчика. Рекомендуется размещение собственных серверов на своей территории. Характеристики серверов достаточны для обеспечения потребностей заказчика. Однако такое решение не обеспечивает достаточную информационную безопасность:
 - Возможен доступ сторонних лиц к данным Заказчика. Заказчик не может это контролировать.
 - В случае утери данных возможен большой период восстановления.
 - Существует вероятность сознательного отключения Заказчика от инфраструктуры
- **Сетевая инфраструктура**
 - **Время простоя после сбоя** – Не определено. Необходимо провести тестовое отключение основных сетевых устройств с переключением на резервные. Необходимо задокументировать время простоя, доступность всех сервисов после подключения к резервному оборудованию.
 - **Защита передаваемых данных** – На данный момент используется аппаратный сетевой экран Cisco ASA 5520 с резервированием. Данное оборудование отвечает современным стандартам и способно обеспечить шифрование данных, достаточное для их защиты. Данное решение можно оставить при развертывании собственной инфраструктуры и отказа от аренды у стороннего подрядчика.
 - **Резервирование оборудования** – Зарезервированы основные узлы:
 - Сетевые экраны
 - Хосты виртуализации
 - Каналы СПД
- **Соответствие архитектуры сети требованиям** – Соответствует частично. Резервирование сетевого оборудования имеет место только в главном здании по адресу Ленинский проспект 32. Рекомендуется зарезервировать коммутаторы агрегации по всем адресам Заказчика с автоматическим переключением в случае отключения основного устройства
- **Системы инженерного обеспечения**
 - **Состояние серверных помещений** – Серверные помещения, в которых сейчас размещена серверная инфраструктура обследовать не представляется возможным, т.к. они находятся на территории подрядчика. Были обследованы серверные помещения Заказчика. На данный момент они не отвечают требованиям по:
 - Кабелированию: необходимо уложить кабель в лотки, кабель-органайзеры. Кабель не подписан: рекомендуется использовать биркование.
 - Питанию и его резервированию
 - Охлаждению: оборудованы частично
 - СКУД: не оборудованы
 - Системы пожарного оповещения и пожаротушения
- **Система мониторинга** – Используется Zabbix. Данное решение отвечает всем требованиям наблюдения и обнаружения неисправностей аппаратного и программного обеспечения.
- **СКС** – Необходимо весь кабель оснастить бирками по всей длине трасс. Необходимо уложить его в кабельные лотки, в серверных уложить кабель в кабель-органайзеры

- Кондиционирование серверных помещений – Необходимо дооснастить серверные кондиционерами с возможностью охлаждения до 30 куб. м с резервированием.

Большую роль в правильном формировании планов развития ИТ инфраструктуры играет адекватная оценка текущего состояния проектов, для которой можно дать следующие критерии:

Критерии оценки ИТ проектов

- Оценка бюджета
- Степень завершенности проекта
- Использование стандартов
- Возможности развития платформы
- Типовое решение
- Степень критичности
- Эффективность развития и поддержки
- Эффективность реализации проекта

Эти критерии помогут дать объективную оценку проекту и принять решение о его продолжении или закрытии.

Исходя из полученных во время аудита данных, можно предложить несколько вариантов ИТ инфраструктуры:

- С резервным ЦОД
 - Размещение резервного ЦОД на территории Заказчика
 - Размещение резервного ЦОД у провайдера
- Организация резервного копирования, Storage.

1. С резервным ЦОД

Данный способ необходимо применять, когда есть существенная потребность в высокой отказоустойчивости системы и минимальных временных простоях.

Задача РЦОД: Обеспечить бесперебойную работу **основных** информационных систем.

Требования к РЦОД:

- Наличие дублирующей инфраструктуры
- Качественный канал связи с основным ЦОД
- Территориальная удаленность от основного ЦОД

Сравнительная таблица для вариантов размещения инфраструктуры в коммерческом РЦОД и в собственном РЦОД

Способы организации РЦОД				
	Начальные затраты	Надежность	Стоимость услуг	Мобильность
Собственный РЦОД	Высокие	Высокая	Низкая	Средняя
Аренда вычислительных мощностей в коммерческом ЦОД	Низкие	Средняя	Средняя	Низкая
Аренда услуги в коммерческом ЦОД	Низкие	Высокая	Высокая	Высокая

Из данной таблицы можно сделать вывод, что несмотря на высокую стоимость инвестиций в собственную инфраструктуру, данный вариант наиболее подходящий, ввиду высокой надежности, информационной безопасности и низких операционных расходов.

Далее представлены варианты размещения РЦОД у провайдера.

- Аренда площадей. Размещение собственного оборудования в ЦОД провайдера
- Аренда оборудования. Размещение своего ПО на аппаратном обеспечении провайдера. Администрирование серверов производится силами пользователя услуг.
- Аренда администрирования. ПО пользователя размещается на мощностях провайдера. Администрирование производится силами провайдера.
- Аренда сервисов. ИС используются как услуги. Гарантия работы ИС достигается заключением договора SLA, где оговаривается качество предоставляемых услуг

Зависимость качества и стоимости услуг от уровня SLA.

	Аренда площадей	Аренда оборудования	Аренда администрирования	Аренда сервисов
Количество	Минимум	Среднее	Максимум	Максимум
Качество	Низкое	Среднее	Выше среднего	Высокое
Цена	Низкая	Средняя	Высокая	Выше средней

Из таблицы видно, что лучшим решением является аренда сервисов, либо аренда аппаратного обеспечения и администрирования.

Данное решение обладает существенными недостатками:

- Низкая информационная безопасность
- Зависимость Заказчика от подрядчика. В случае чего, Заказчик не сможет получить оперативно свои данные.

2. Организация резервного копирования и Storage

Цель: Обеспечение сохранности данных в случае потери всей информации.

Требования:

- Наличие системы хранения данных
- Распределенная серверная структура

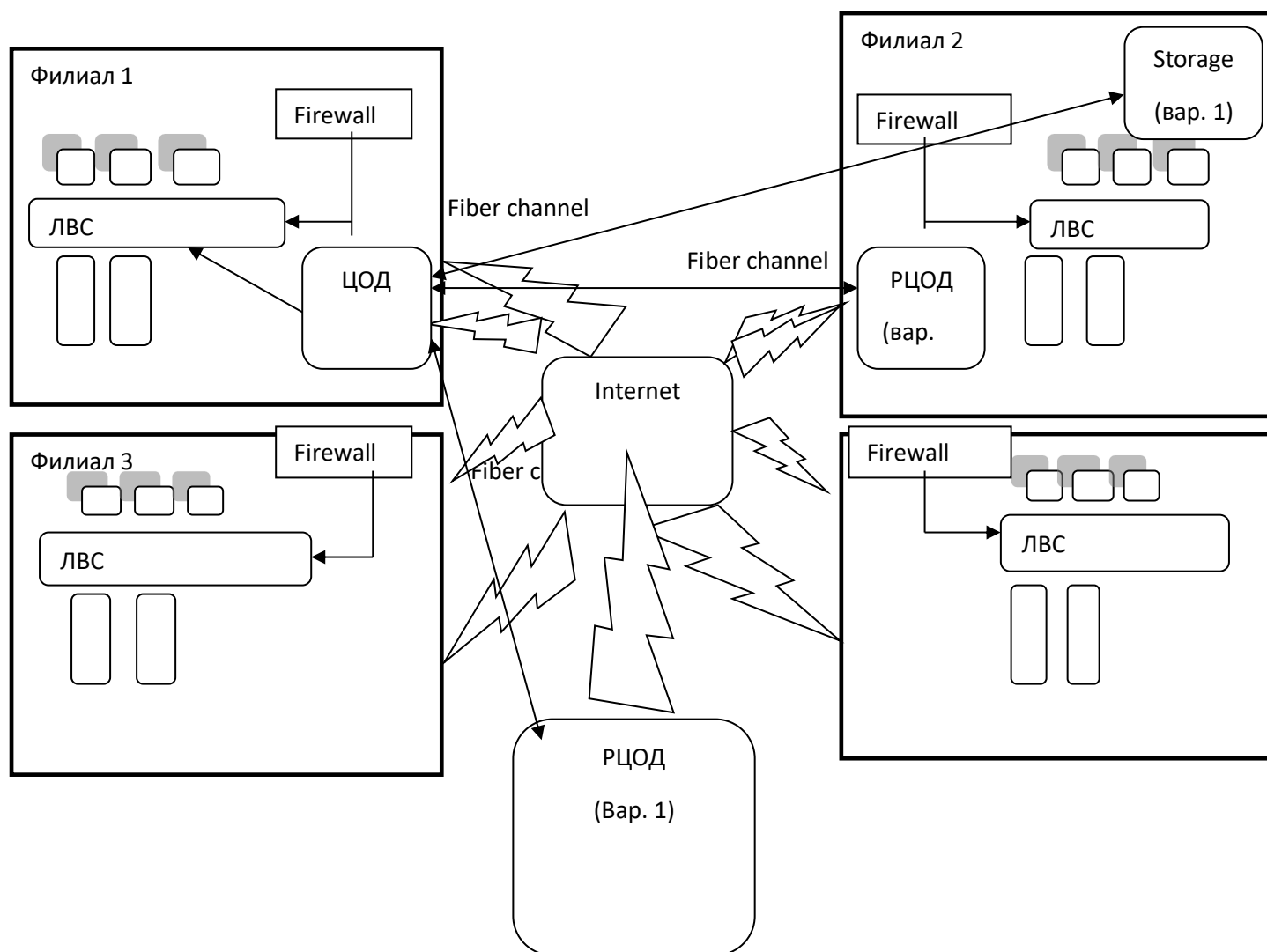
В отличие от варианта в РЦОД данный способ не позволяет оставить процесс использования основных систем прозрачным для пользователей. Так же существенно увеличивается время простоя систем в случае аварии. Но основным плюсом данного метода является низкая стоимость реализации, так как он не требует дополнительного оборудования для «сплитирования» системы, необходимое оборудование стоит существенно меньше, есть возможность использования встроенных механизмов резервного копирования в серверных ОС Windows.

Данный метод допустим в случае отсутствия необходимости работы системы в режиме 24/7.

Администрирование в таком случае берет на себя команда внутренней IT службы.

Для обоих вариантов необходимо сделать резервный канал передачи данных. Это позволит удаленным пользователям подключаться к системам в случае падения основного канала.

Схема логической организация сети обоих вариантов



2. Управление ИТ

Можно выделить следующие основные области анализа и развития ИТ управления:

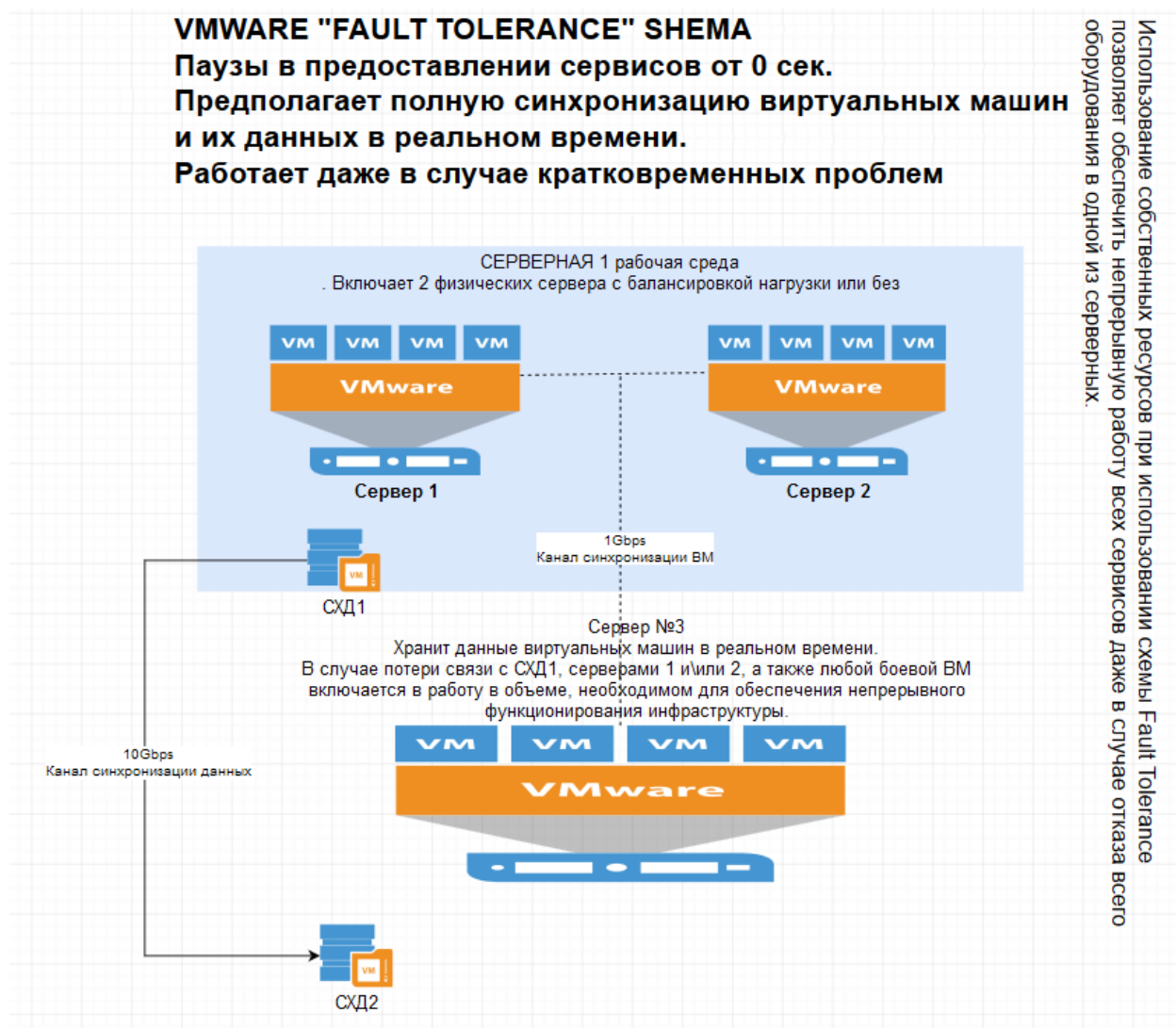
- Организационная структура ИТ отдела
 - Определить и сформировать оптимальную структуру ИТ
 - Определить зоны ответственности каждого из сотрудников, закрепив их должностными инструкциями
 - Внедрить метод segregation of duties для распределения прав доступа к системам и сервисам
 - Перейти к оценке эффективности на основе ключевых показателей KPI
- Уровень развития процессов поддержки
 - Разработка процессов управления на основе ITSM
 - Проблемами
 - Изменениями
 - Инцидентами
 - Конфигурациями
 - Уровнем обслуживания
 - Непрерывностью
 - Доступностью
 - План восстановления систем
 - Обучение персонала
 - Бюджетирование
 - Согласование планов развития бизнеса и планов развития ИТ
- Уровень документации
 - Разработка и поддержание в актуальном состоянии необходимой ИТ документации
 - Должностные инструкции
 - ИТ политика
 - Рабочие инструкции
 - Техническая документация и руководства пользователей
- Уровень автоматизации деятельности ИТ
 - Внедрение ПО поддержки
 - Help Desk
 - Специализированное ПО для учета технических средств
 - Системы удаленной диагностики, установки ПО (SCCM), управления рабочими местами пользователей
 - Системы мониторинга сетевой инфраструктуры (LAN, WAN)

Цели, которые будут достигнуты в результате анализа и развития ИТ управления:

- Повышение эффективности управления ИТ и оптимизация затрат
- Рационализация орг. Структуры ИТ
- Преобразование деятельности руководства ИТ в предоставление сервисов ИТ
- Систематизация ИТ процессов в ITIL
- Соответствие управления ИТ потребностям Заказчика и его развитию

Предлагаемая схема реализации серверной инфраструктуры

Для организации серверной инфраструктуры предлагается использовать VmWare с технологией Fault Tolerance и VmWare High Availability. В спецификации на серверную инфраструктуру заложены три мощных сервера, которые позволят создать отказоустойчивый кластер (из двух серверов) и сделать Backup (третий сервер) всех виртуальных машин с периодом 15 минут. Кластеризация обеспечит максимальный уровень отказоустойчивости даже в случае аппаратного сбоя, а Backup позволит быстро восстановить систему без потери данных в случае программного сбоя. Для хранения данных используется СХД Dell. Инфраструктура предполагает базирование всех информационных систем, сайта, 1С, Active Directory, файл сервера, сервера баз данных, сервера приложений, сервера антивирусной защиты. В качестве системы виртуализации предлагается использовать VmWare. Все серверы и СХД оснащены SSD дисками, что позволит работать всем приложениям без задержек (это очень критично при размещении ИС). На СХД делается Backup всех виртуальных машин на случай аппаратного сбоя.



Спецификация серверного оборудования

Для реализации серверной инфраструктуры рекомендуется использовать следующее оборудование:

Товары (работы, услуги)
Сервер Dell PowerEdge R730 (up to 8 x 3.5" HDD/SSD) rack 2U / 1 x Intel Xeon E5-2630v4 (2.2GHz, 10C, 25MB, 8.0GT/s QPI, 85W) / 4 x 32Gb PC4-19200(2400MHz) DDR4 ECC Registered DIMM / 6 x 3.84TB SSD SAS Read Intensive 12Gbps HS 2.5" in 3.5" Carrier / PERC H730p RAID(0,1,5,6,10,50,60) Controller 2Gb NV Cache 12Gb/s with battery / DVD-RW / iDRAC 8 Enterprise 16GB SD card / Intel X710 2x10Gb DA/SFP+, + I350 2x1Gb, Network Adapter, Daughter Card / 2 x Power Supply, 1100W, Hot-plug / MS Windows Server 2019, Standard Edition(MUI), 40 cores (Only for Dell Poweredge) / 3Y Prosupport NBD
Система хранения данных Dell EMC PowerVault ME4024 (up to 24 x 2.5" SAS HDD/SSD) FC/SFP+ iSCSI / 2 x Storage Raid Controller(RAID 0, 1, 10, 5, 6) 8GB Cache, 2 x 16Gb/s SFP ports + 2 x SFP+ 10Gb iSCSI port / 2 x SFP Transceiver SW, FC 16Gb/s / 2 x SFP+ Transceiver, SR, 10GbE / 24 x 960GB SSD SAS Read Intensive 12Gbps HS 2.5" / 2 x QLogic QLE2692, Dual Port, 16Gbps Fibre Channel PCIe HBA Card / 2 x QLogic QLE2662, Dual Port, 16Gbps Fibre Channel PCIe HBA Card Low Profile / 4 x 5M LC-LC Optical Fibre Cable Multimode / 2 x Power Supply, AC 220V 580W/ Rails / 3Y Prosupport NBD
MS SQL Server 2019
VmWare на 3 сервера
MS Windows Server 2019