

**В ногу со временем.
ИТ инфраструктура медицинского
учреждения**

22 года

безупречной работы на рынке информационных технологий

15 000 серверов в год –
мощности производства

42 города РФ - гарантийное
сервисное обслуживание

20 крупных проектов по
системной интеграции в год

30 000 зарегистрированных
посетителей на форуме Тринити

120 сертифицированных
ИТ-экспертов с богатым опытом
реализации сложных проектов

36 ключевых производителей

3 подразделения: Москва, Санкт-
Петербург, Екатеринбург

Ключевые особенности ИТ инфраструктуры Лечебно-Профилактического Учреждения (ЛПУ)

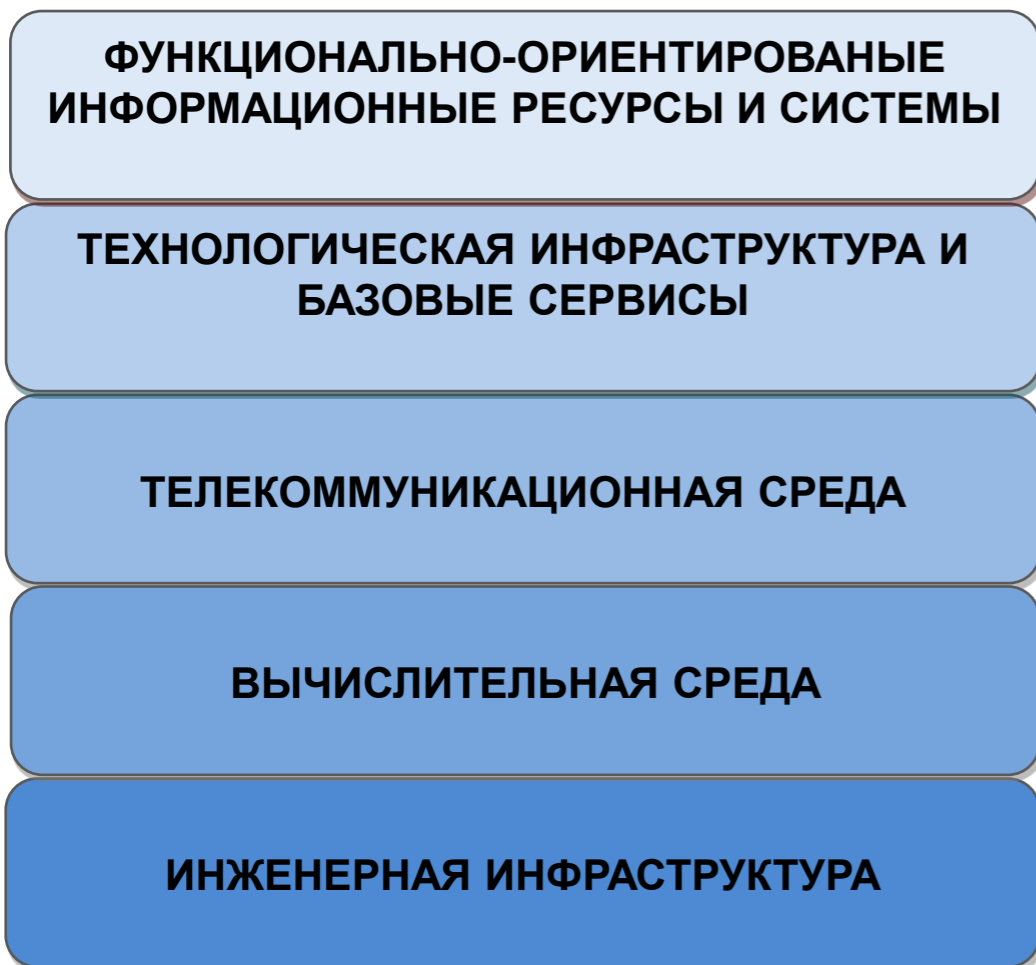


- Крайне высокий уровень социальной ответственности накладываемый спецификой деятельности ЛПУ;
- Безопасность пациентов;
- Качество медицинской помощи;
- Доступность медицинской помощи;
- Непрерывность медицинской помощи;
- Вовлеченность пациентов (обратная связь) ;
- Координация действий и обмен информацией между различными медицинскими организациями;
- Взаимодействие с государственными органами;
- Обработка критически значимых персональных данных пациентов;
- Интеграция с ЕГИСЗ;
- Соответствие отечественным и международным стандартам



Федеральный закон от 21.11.2011 г. №323-ФЗ (ред. от 23.07.2013 с изменениями, вступившими в силу с 03.08.2013) «Об основах охраны здоровья граждан в Российской Федерации»

Архитектура информационной инфраструктуры ЛПУ



Медицинская информационная система (МИС) — комплексная автоматизированная информационная система для автоматизации деятельности ЛПУ, в которой объединены система поддержки принятия медицинских решений, электронные медицинские записи о пациентах, данные медицинских исследований в цифровой форме, данные мониторинга состояния пациента с медицинских приборов, средства общения между сотрудниками, финансовая и административная информация.

Архитектура информационной системы - концепция, определяющая модель, структуру, выполняемые функции и взаимосвязь компонентов информационной системы.



Сервисная поддержка и аутсорсинг

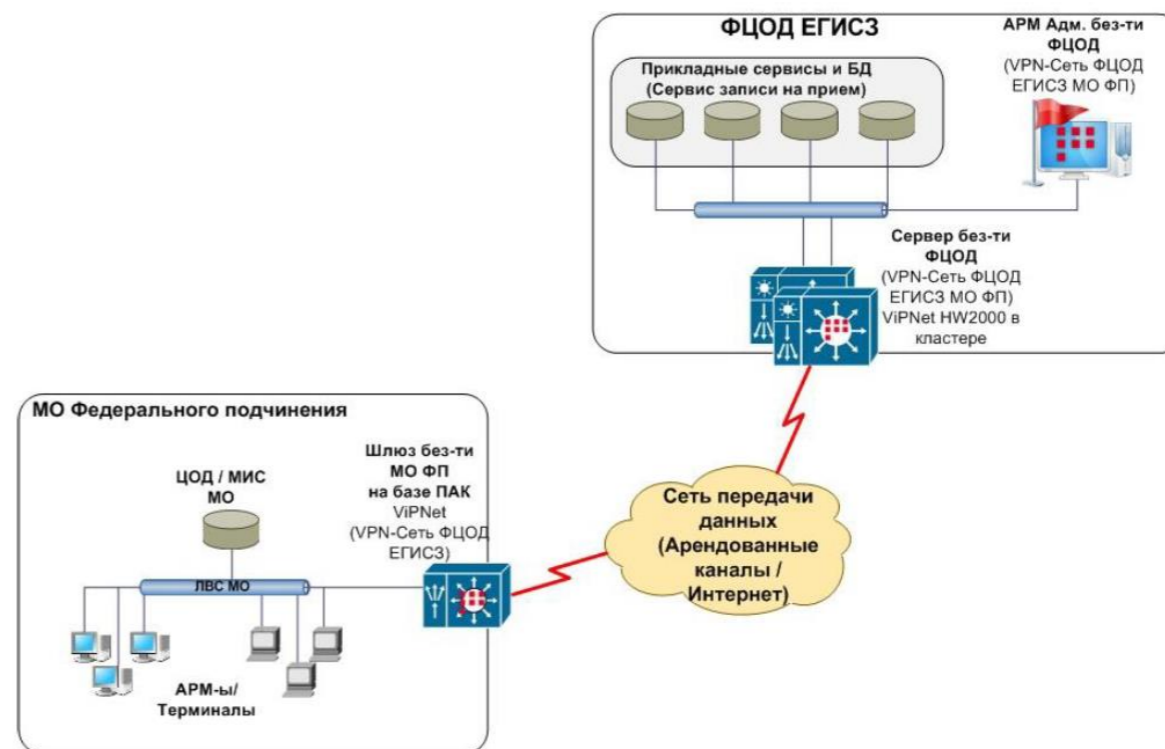
- **ГОСТ Р 52636-2006** «Электронная история болезни. Общие положения».
- **ГОСТ Р ИСО/ТС 18308-2008** «Информатизация здоровья. Требования к архитектуре электронного учета здоровья».
- **ГОСТ Р 52979-2008** «Информатизация здоровья. Состав данных сводного регистра застрахованных граждан для электронного обмена этими данными. Общие требования».
- **ГОСТ Р 52977-2008** «Информатизация здоровья. Состав данных о взаиморасчетах за пролеченных пациентов для электронного обмена этими данными. Общие требования».
- **ГОСТ Р 52978-2008** «Информатизация здоровья. Состав данных о лечебно-профилактическом учреждении для электронного обмена этими данными. Общие требования».
- **ГОСТ Р 52976-2008** «Информатизация здоровья. Состав первичных данных медицинской статистики лечебно-профилактического учреждения для электронного обмена этими данными. Общие требования».
- **ГОСТ Р 53395-2009** «Информатизация здоровья. Основные положения».

Методические рекомендации

Методические рекомендации по составу и техническим требованиям к сетевому телекоммуникационному оборудованию учреждений системы здравоохранения для регионального уровня единой государственной информационной системы в сфере здравоохранения, а также функциональные требования к ним.

Тип	Региональный мед. Центр	Количество АРМ/Комментарии
№ 1	Центр обработки данных	3 типа
№ 2	ЛПУ – крупный стационар	более 150
№ 3	ЛПУ – стационар	От 51 до 150
№ 4	ЛПУ, ФОМС и другие учреждения уровня субъекта Федерации	От 6 до 50
№ 5	Малое ЛПУ, аптека	От 2 до 5
№ 6	Единичное рабочее место, подключаемое через Интернет	1 ПК

Документ подготовлен во исполнение решения заседания президиума Совета при Президенте Российской Федерации по развитию информационного общества в Российской Федерации 22 декабря 2010 г. (утверждено 30 декабря 2010 г. № А4-18040) по вопросу о порядке реализации региональных программ модернизации здравоохранения в части внедрения информационных технологий.



Методические рекомендации медицинским организациям по обеспечению криптографической защиты каналов при взаимодействии в рамках единой государственной информационной системы в сфере здравоохранения

Документ подготовлен в соответствии с «Концепцией создания единой государственной информационной системы в сфере здравоохранения», утвержденной Приказом Минздравсоцразвития России от 28 апреля 2011г. № 364, «Методическими рекомендациями для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости» Минздравсоцразвития России от 24.12.2009г. и письмом Минздравсоцразвития России от 21 февраля 2011г., регламентирующим порядок организации и функционирования защищенного межведомственного взаимодействия по телекоммуникационным каналам передачи данных общего пользования при обмене электронными документами между участниками корпоративной информационной системы на основе технологии ViPNet.

Международные стандарты обмена, управления и интеграции электронной медицинской информации



HL7, Health Level 7 — синтаксический стандарт для обмена, управления и интеграции электронной медицинской информации.

Эталонная информационная модель ([англ.](#) *The Reference Information Model, RIM*) — ключевой элемент HL7 - средство построения карты медицинской системы, описания жизненного цикла событий, осуществляемых с помощью сообщений, представления семантических и контекстуальных связей между полями передаваемых сообщений.



CEN/TC 251 (COMITÉ EUROPÉEN DE NORMALISATION Technical Committee 251) – европейский комитет по стандартам, разрабатывающий средства и структуры медицинских данных для целей совместимости и взаимного использования независимыми медицинскими системами. Организован в 1990 году, секретариат расположен в Стокгольме, Швеция. Текущая версия стандартов - ENV находится на стадии доработки.



ANSI/TIA-1179: «Стандарт телекоммуникационной инфраструктуры для учреждений здравоохранения»



DICOM ([англ.](#) *Digital Imaging and Communications in Medicine*) — отраслевой стандарт создания, хранения, передачи и визуализации медицинских изображений и документов обследованных пациентов.

Обработка персональных данных



Операторы персональных данных должны выполнить ряд **требований по защите персональных данных физических лиц**, обрабатываемых в информационных системах ЛПУ, и предпринять ряд действий:

- Уведомление Роскомнадзора об обработке персональных данных (Закон № 152-ФЗ Ст. 22 п. 3)
- Проведение классификации информационной системы
- Разработка модели угроз безопасности персональным данным
- Выбор средств защиты инструмента обработки персональных данных (средства защиты должны быть сертифицированными, либо пройти сертификацию)
- Выбор испытательной лаборатории
- Проведение испытаний
- Подготовка организационно-распорядительных документов
- Оформление и утверждение документов
- Аттестация инструмента обработки персональных данных
- Проверка Роскомнадзора, ФСТЭК и ФСБ
- Получение письменного согласия субъекта персональных данных на обработку своих персональных данных (Закон № 152-ФЗ ст. 9 п. 4)
- Уведомление субъекта персональных данных о прекращении обработки и об уничтожении персональных данных (Закон № 152-ФЗ ст. 21 п. 4)
- Прохождение внеплановых проверок



Федеральный закон от 21.07.2014 N 242-ФЗ (ред. от 31.12.2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»

Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями и дополнениями)

Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (Зарегистрировано в Минюсте России 14.05.2013 N 28375)

Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Решаем ИТ задачи любого масштаба



Тринити – это качественная реализация проекта любой сложности в срок и в рамках бюджета.

Совместимость и работоспособность проектных решений гарантируется **высоким уровнем компетенций** инженеров Тринити, собственным **демо-центром** и **прямым взаимодействием** с техническими подразделениями ИТ-вендоров.



Развитие бизнеса: создание ИТ-инфраструктуры нового бизнеса, подразделения «под ключ».



Информационная безопасность: защищённость информации от внешних и внутренних угроз, соблюдение требований закона и отраслевых стандартов, коммерческой тайны, управление жизненным циклом информации.



Новые требования бизнеса: новый бизнес-процесс или оптимизация существующих бизнес-процессов, модернизация и повышение конкурентоспособности бизнеса.



Оптимизация расходов: снижение операционных расходов бизнеса и совокупной стоимости владения ИТ-инфраструктурой, увеличение ROI.



Непрерывность бизнес-процессов: бесперебойная работа ИТ-сервисов, высокая доступность и сохранность данных, гарантии восстановления после аварий.





Действующие:

- Сертификат соответствия
- Лицензия на осуществление распространения шифровальных (криптографических) средств
- Сертификат соответствия Системы менеджмента качества предприятия стандартам ГОСТ Р ИСО 9001-2001, ГОСТ РВ 0015-2003, ГОСТ Р ЕН 9100-2011
- Лицензия ФСБ на проведение работ, связанных с использованием сведений, составляющих государственную тайну
- Сертификат соответствия Системы менеджмента качества предприятия стандартам ГОСТ ISO 9001 – 2011
- Сертификат соответствия требованиям правил применения средств связи
- Декларация Минсвязи
- Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации

Отказоустойчивое и масштабируемое решение в Международной клинике MEDEM



Задача

В связи с ростом бизнеса необходимо было обеспечивающие непрерывную работу всех бизнес-процессов и доступность всех сервисов и приложений как для медицинского персонала, так и для пациентов клиники.

Решение

- Серверные решения плотной компоновки, системы хранения данных, ленточная библиотека.
- Для связи компонентов системы используется высокоскоростной и масштабируемый интерфейс Fibre Channel (FC) на основе оптоволоконного соединения. Все связи задублированы. Средства управления СХД зарезервированы.

Результат

- Повышение отказоустойчивости
- Обеспечение свободной масштабируемости решения
- Обеспечение работы сред виртуализации
- Снижение уровня энергопотребления
- Обеспечение эффективной системы управления серверным парком
- Обеспечение технических требований по эффективному функционированию программных продуктов



Международная клиника MEDEM — многопрофильное лечебное учреждение, предоставляющее широкий спектр высокоспециализированных медицинских услуг и уникальную возможность решить большинство проблем со здоровьем в одном учреждении. MEDEM является крупным специализированным медицинским центром федерального значения.



Оптимизация хранения для многопрофильной клиники «Скандинавия»



Задача

Оперативное обеспечение доступности медицинских данных пациентов, обращающихся в разные отделения клиники.

Решение

Проект консолидации информационных ресурсов.

- Оборудование: Системы хранения данных, ленточная библиотека, коммутаторы сети хранения данных.
- ПО: Программное обеспечение управления хранением данных

Результат

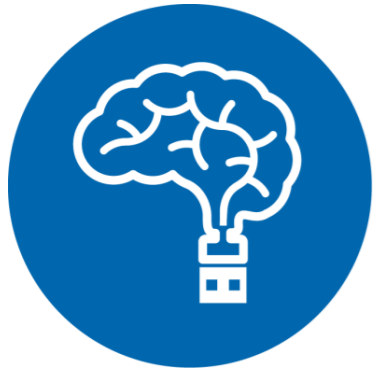
- На новую инфраструктуру переведен практически весь бизнес клиники «Скандинавия».
- Новая Информационная инфраструктура решила все проблемы предприятия, связанные с нехваткой дискового пространства и обеспечением отказоустойчивости.



Клиника «Скандинавия» – передовой многопрофильный высокотехнологичный медицинский центр в Санкт-Петербурге с широкой сетью районных амбулаторных отделений. Входит в состав международной сети клиник ABA.



План действий:



- 1) Детальная презентация специалистам на местах
- 2) Утверждение концептуальных решений
- 3) Полевое обследование ЛПУ
- 4) Разработка детального системного проекта
- 5) Разработка инженерной составляющей проекта
- 6) Разработка вычислительной составляющей проекта
- 7) Разработка телекоммуникационной составляющей проекта
- 8) Системная интеграция на основе разработки технологической инфраструктуры и базовых сервисов
- 9) Адаптация функционально ориентированных информационных ресурсов и систем.
- 10) Подготовка предложений на двух-трехлетнюю перспективу

Контакты



Владимир Быков Директор по продажам

+7 (812) 327-59-60 доб. 2840

v.bykov@trinitygroup.ru

Электронная почта
info@trinitygroup.ru

Телефон
8 800 200 5960

Сайт
www.trinitygroup.ru

Москва
+ 7 (495) 232-92-30

Технический форум
www.3nity.ru

Санкт-Петербург
+7 (812) 327-59-60

Технический блог
www.blog.trinitygroup.ru

Екатеринбург
+7 (343) 378-41-50