kraftway
ДЛЯ ЗДРАВООХРАНЕНИЯ

АВТОМАТИЗАЦИЯ ДЕЯТЕЛЬНОСТИ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ

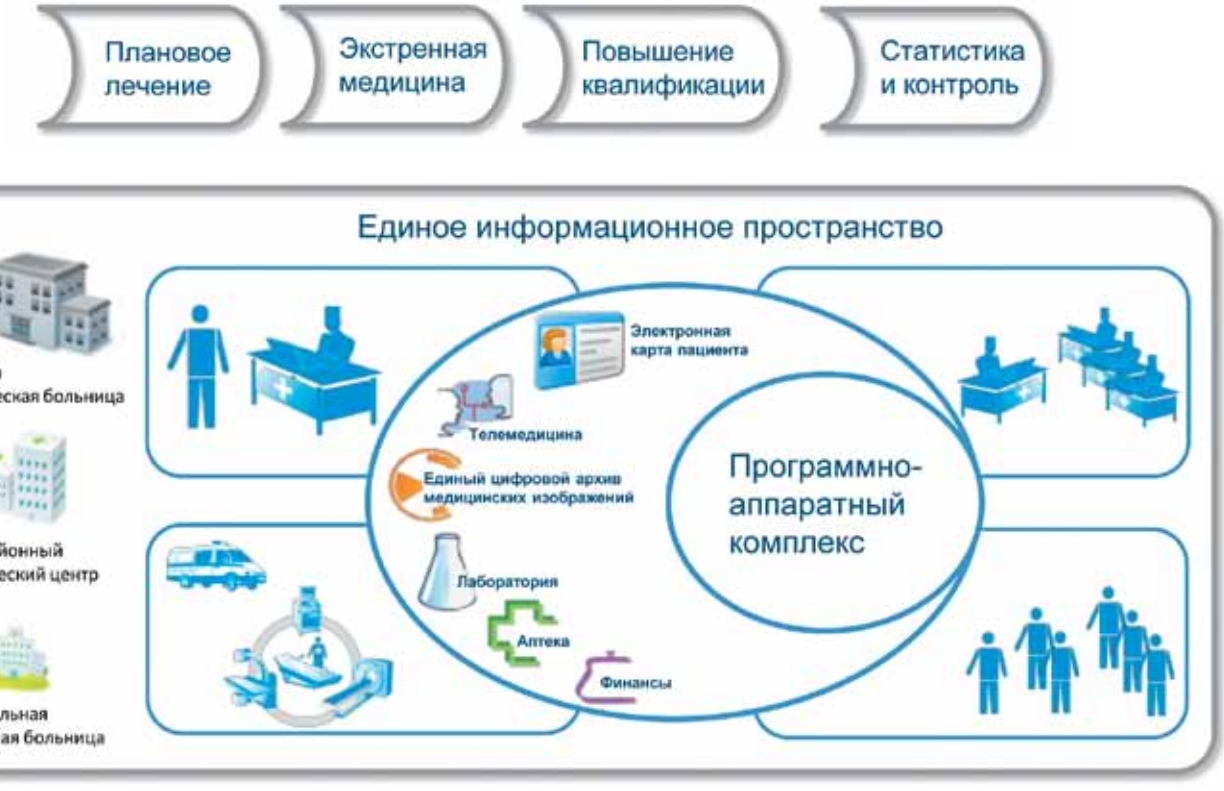
kraftway®
ТЕХНОЛОГИИ ДЛЯ ЛЮДЕЙ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – МЕДИЦИНЕ

В рамках приоритетного национального проекта «Здоровье» для повышения управляемости, эффективности и качества услуг системы здравоохранения на всех уровнях большое внимание уделяется вопросам комплексного подхода к модернизации медицинской отрасли. В задачи программы преобразования медицины в России входят, в том числе, внедрение современных информационных систем и укрепление материально-технической базы лечебно-профилактических учреждений (ЛПУ).

На данный момент в нашей стране оказание медицинских услуг автоматизировано слабо, а используемые в отдельных учреждениях медицинские информационные системы (МИС) разнородны. Комплексная автоматизация здравоохранения, создание единого информационного пространства в этой области способны поднять качество оказания медицинских услуг на новый уровень. При этом под комплексностью подразумевается автоматизация не только административных, финансовых функций, но и технологических процессов предметной области работы медицинского учреждения вне зависимости от его профиля и размеров (регистратура, запись на приём, ведение электронных историй болезни и т.д.).

КОНЦЕПЦИЯ РЕШЕНИЯ



ПОДХОДЫ

Общая концепция единого информационного пространства предполагает создание распределённой многоуровневой структуры с объединением центров обработки данных согласно принципам сервисно-ориентированной модели информационных систем (SOA), с учётом централизации ключевых сервисов (SaaS), при условии поддержки территориально распределённой иерархической модели информационного взаимодействия.

Существует два подхода к организации информационного взаимодействия инфраструктуры лечебно-профилактических учреждений с «облаком». Первый предполагает высокую степень независимости ЛПУ от региональных центров обработки данных (ЦОД). В таком случае в инфраструктуре ЛПУ размещается промежуточная копия полнофункциональной медицинской информационной системы (МИС) с локальным хранилищем данных, а обмен информацией с «облаком» происходит посредством сервисов через шину электронного взаимодействия или напрямую через механизмы синхронизации информационных систем верхнего и нижнего уровней.

В такой архитектуре существует 3 типа сервисов:

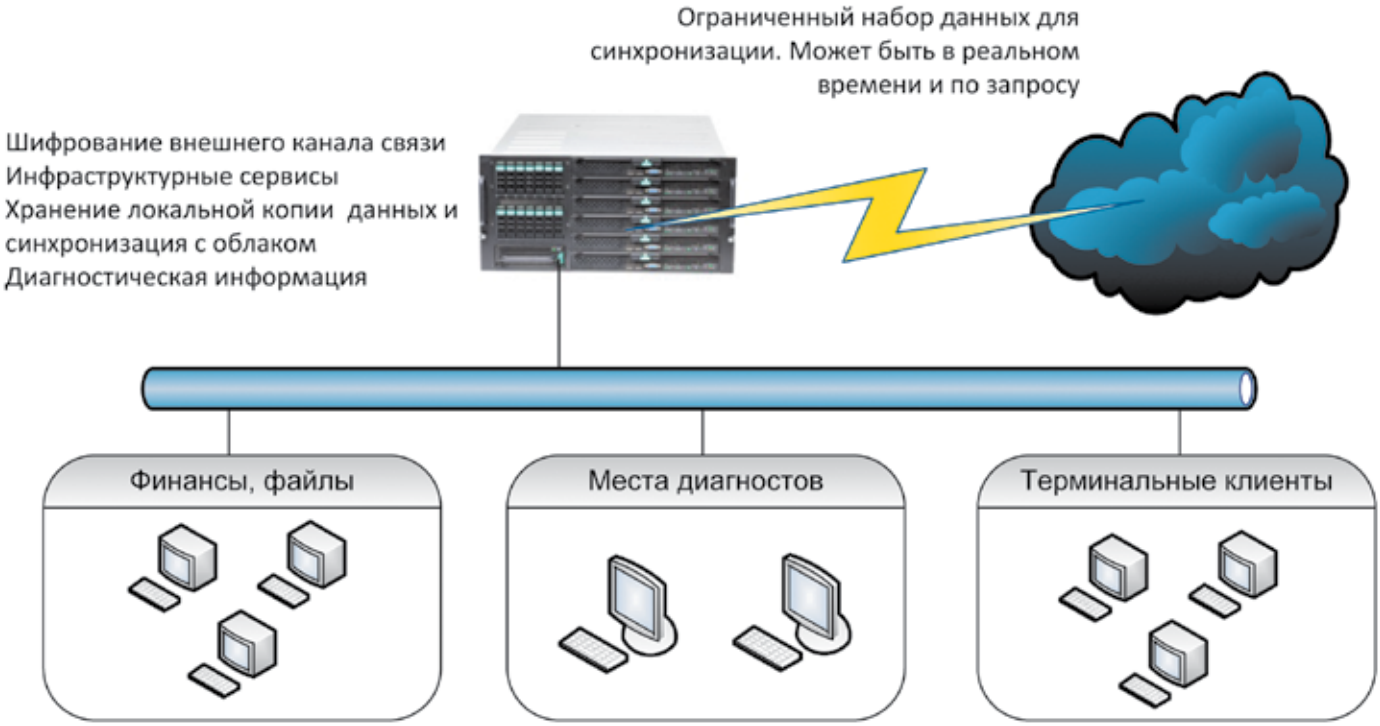
- Централизованные, или SaaS сервисы (исполняются только в ЦОД и служат источником для остальных сервисов). Типичные примеры – нормативно-справочная информация, сервисы аналитики, некоторые сервисы по информационной безопасности.
- Централизованно-децентрализованные (могут исполняться как локально, так и централизованно, с использованием механизмов синхронизации). Типичный пример – сервисы записи на приём в распределённой инфраструктуре лечебно-профилактических учреждений субъекта Федерации, при использовании различных механизмов записи (регистратура, call-центр, портал госуслуг, портал лечебного учреждения и пр.).
- Локальные сервисы каждого ЛПУ (исполняются локально и могут служить источником данных для всех типов сервисов). Типичный пример – PACS или сервисы инструментальных исследований на специализированном уникальном оборудовании консультационно-диагностических центров.

Такой подход позволяет получить следующие преимущества:

- объединить МИС, финансовые системы и PACS в единый информационный комплекс;
- достичь высокой защищённости решения;
- создать возможность использования локальных сервисов, например файловое хранилище, IP-телефония, локальная онлайн-аналитика;
- обеспечить простоту администрирования;
- избежать зависимости от качества каналов связи, что очень важно, учитывая неоднородность коммуникационной инфраструктуры.

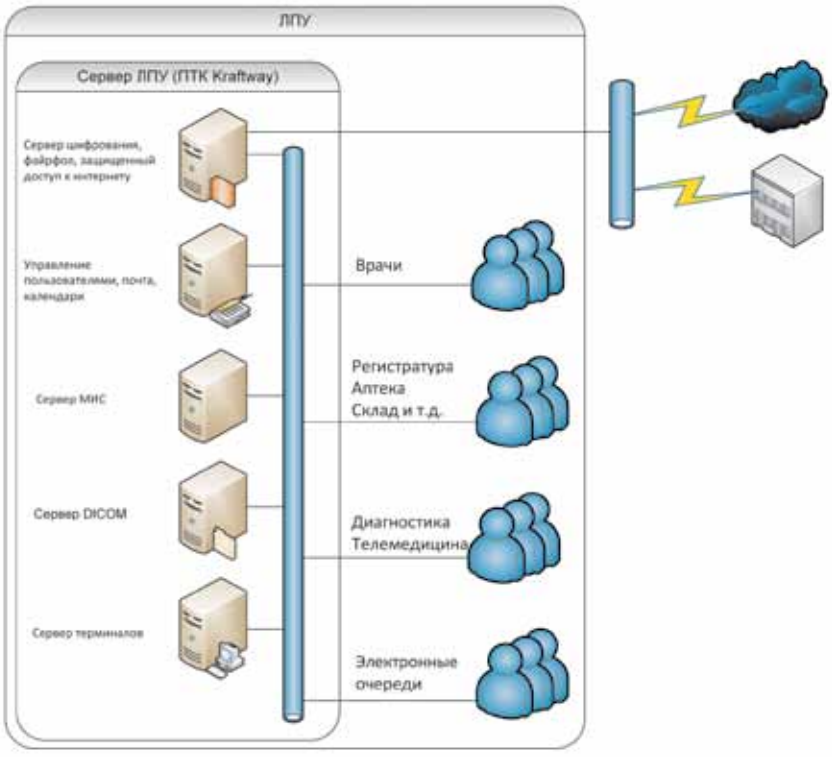
Для воплощения перечисленных преимуществ комбинированной модели необходимо достаточно мощное типовое комплексное решение для каждого лечебно-профилактического учреждения.

Второй подход, напротив, предъявляет меньшие требования к оборудованию в инфраструктуре ЛПУ, так как подразумевает наличие лишь базовых локальных сервисов для обеспечения административной, финансовой поддержки, хранения диагностической информации. Специализированного и высокопроизводительного промежуточного хранилища не требуется, но при этом теряется возможность тесной интеграции МИС и PACS-систем, возникает критическая зависимость от каналов связи и усложняется администрирование всей инфраструктуры в целом.



ЛЕЧЕБНО-ПРОФИЛАКТИЧЕСКОЕ УЧРЕЖДЕНИЕ

Важной задачей является разработка максимально унифицированного инфраструктурного решения на местах, в различных лечебно-профилактических учреждениях. При этом унификация не должна сказаться на гибкости и функциональности решения, а также возможности адаптации для нужд разнопрофильных учреждений здравоохранения. Инфраструктура должна обеспечивать работу типовых наборов функциональных сервисов ЛПУ (регистратура, call-центр, история болезни, назначения на диагностику и госпитализацию, лабораторные исследования, лекарственное обеспечение, DICOM-сервисы инструментальных медицинских исследований, базовые пользовательские сервисы,



почты, календарей и документооборота, сервисы информационной безопасности) и автоматизировать базовые технологические процессы, но при этом оставлять возможности для масштабирования и расширения.

Таким образом, инфраструктурное решение должно соответствовать следующим требованиям:

- быть простым в обслуживании и не предъявлять высоких требований к квалификации обслуживающего персонала;
- не ставить высоких эксплуатационных требований, обеспечивать дистанционную диагностику и исправление проблем, а также дистанционное обновление программного обеспечения;
- не предъявлять специальных требований к размещению и пуско-наладке оборудования;
- соответствовать современным требованиям по энергоэффективности в пересчёте на каждого пользователя;
- быть инвариантным к медицинским информационным системам и поддерживать работу всех распространённых МИС;
- иметь достаточную вычислительную мощность для обслуживания локальных сервисов, поддержку терминальных режимов работы пользователей, поддержку DICOM сервисов, обеспечивать прозрачную маршрутизацию к централизованным сервисам;
- обеспечивать контур защиты информации в соответствии с законом № 152-ФЗ «О персональных данных»;
- оставлять возможности для масштабирования и выполнения новых функциональных задач.

Структура типового решения для ЛПУ призвана стать основой для создания медицинских систем более высокого уровня, а его качество и надёжность во многом будут определять своевременность и качество оказываемых медицинских услуг.

ЧТО ПРЕДЛАГАЕТ КОМПАНИЯ KRAFTWAY?

Компания Kraftway на протяжении многих лет поставляет технику и создаёт интеграционные решения для государственных служб. Огромный опыт позволяет компании всегда быть впереди, в технологическом авангарде, предоставлять действительно качественные и современные продукты. Компания участвует в разработке типовых интеграционных решений национального проекта «Здоровье» с момента его запуска. Результаты работы были по достоинству оценены Президентом РФ Д. А. Медведевым во время визита на завод Kraftway и при ознакомлении с опытной платформой автоматизации ЛПУ на Тверском инновационном форуме в июле 2010 года.

Предлагаемый комплекс позволит автоматизировать все этапы оказания медицинской помощи и оптимизировать работу всех подразделений ЛПУ независимо от профиля медучреждения. Это решение повышает эффективность работы врачей, работников регистратуры, сотрудников отдела статистики, бухгалтеров и управленческого персонала, обеспечивая тем самым повышение качества и доступности медицинской помощи. Комплекс разработан в тесном сотрудничестве с ведущими разработчиками медицинских информационных систем.

Внедрение решения Kraftway позволяет обеспечить инфраструктурную составляющую комплексной автоматизации всех ключевых технологических и административных процессов в медицинском учреждении:

- автоматизация рабочих мест врачей-специалистов, среднего медперсонала, научных сотрудников, приемного отделения, аптеки, лабораторий и диагностических кабинетов;
- создание единой информационной сети, в которую включены автоматизированные рабочие места каждого сотрудника с подключением диагностического и другого медицинского оборудования;
- информатизация процесса оказания медицинских услуг;
- внедрение технологии электронных медицинских карт;
- автоматизация процессов ОМС;

- автоматизация учета лекарственных препаратов;
- организация информационного взаимодействия внутри ЛПУ;
- создание объединенной информационной сети ЛПУ;
- создание инфраструктуры доступа в информационную систему ЛПУ для посетителей.

Решение, предлагаемое компанией Kraftway, может стать надёжной основой для информатизации отрасли здравоохранения. Универсальный PACS-комплекс собственной разработки, комплектация рабочих мест современными средствами визуализации (медицинские мониторы, выводящие 14-битное изображение, способные отобразить рентгеновские снимки самых современных рентгено-диагностических комплексов с высокой точностью) дополняют и без того широкий список преимуществ. Наличие широкой сети сервисного обслуживания (более 270 центров) по всей территории страны обеспечивает высокое качество гарантийного обслуживания, а круглосуточная линия техподдержки позволит получить помощь в решении возникающих проблем.

Обкатка и оптимизация разработанного комплекса проходит на опытных площадках в реальных учреждениях здравоохранения совместно с ведущими разработчиками МИС: в Российском кардиологическом научно-производственном комплексе и Российском онкологическом центре им. Блохина. В настоящее время решение Kraftway проходит процедуру регистрации в Министерстве здравоохранения и социального развития России как изделие медицинского назначения.

По условиям приоритетного национального проекта «Здоровье», финансирование выполнения задач, поставленных первыми лицами государства, в регионах будет осуществляться лишь при наличии согласованной региональной программы модернизации. Компания Kraftway не только предлагает комплексное решение для автоматизации лечебно-профилактических учреждений, но в качестве эксперта оказывает содействие регионам в разработке программ модернизации, проводит полный комплекс предпроектных и интеграционных мероприятий.

Современные, хорошо оснащенные лечебно-профилактические учреждения призваны оказывать населению высококачественную медицинскую помощь.

МОДУЛЬНЫЙ СЕРВЕР

В качестве программно-аппаратной платформы для средних и больших ЛПУ компания Kraftway предлагает Программно-технический комплекс (ПТК) №1, созданный на основе модульной системы, которая базируется на вычислительной архитектуре Intel®. Комплекс демонстрирует отличный уровень гибкости, масштабируемости и производительности. Это высокотехнологичное решение совмещает в себе передовые разработки в области вычислительной техники, благодаря чему достигаются высокие показатели производительности, надёжности, эффективности, простота и удобство управления и обслуживания.

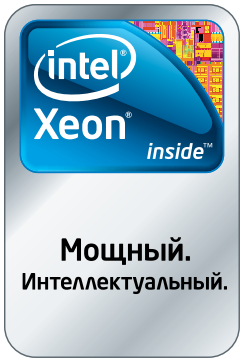
В ПТК может быть установлено до шести высокопроизводительных двухпроцессорных вычислительных модулей на базе многоядерных серверных процессоров Intel® Xeon® 5600. Объём оперативной памяти может достигать 96 Гбайт на каждый модуль, подсистема хранения включает до 14 дисков, объединённых в разделяемый массив с возможностью «горячей» замены. Конструкция предполагает наличие избыточных элементов (источников питания, системы охлаждения, сетевых коммутаторов), которые делают систему высоконадежной и изначально готовой для работы в режиме 24 x 7 x 365.

Серверная подсистема комплекса включает в себя следующие типы blade-серверов, которые функционально обеспечивают логически законченную инфраструктуру ЛПУ:

- вычислительный модуль для обеспечения типовых инфраструктурных сервисов (служба каталога, почта, файловое хранилище, сервер печати, мониторинг и управление, внутренний портал и пр.);
- вычислительный модуль для организации терминального доступа;
- вычислительный модуль для DICOM-хранилища данных;
- вычислительный модуль с приложением МИС;
- вычислительный модуль базы данных МИС;
- вычислительный модуль криптомаршрутизатора.

Вычислительный модуль для обеспечения инфраструктурных сервисов предназначен для предоставления возможности работы со службой каталогов, электронной почтой, доступа к корпоративным файловым ресурсам.

Вычислительный модуль терминального доступа предназначен для технической организации и ведения сеанса связи терминальной станции пользователя с информационными ресурсами комплекса.



Вычислительный модуль терминального доступа обеспечивает:

- Формирование системного окружения в соответствии с правилами политики безопасности на терминальной станции;
- Организацию и ведение сеанса связи терминальной станции с информационными ресурсами на уровне пользовательских сессий.

Вычислительный модуль для DICOM-хранилища данных выполняет функцию DICOM-сервера и сервера БД. Сервер обеспечивает сохранение информации о пациенте, его исследованиях, DICOM сериях и изображениях, находящихся в этих сериях. Работа сервера начинается с разбора DICOM-команд и DICOM-файлов на компоненты, значимые описания которых сохраняются в БД. Сервер БД обрабатывает SQL-запросы от DICOM-клиентов, и отправляет результаты обработки, а также при необходимости исход-

Функциональная схема модульного сервера

Технические характеристики:

Подсистема	Характеристики
Вычислительный модуль	2 процессора Intel® Xeon® 56XX (QPI 4,8 Гт/с - 6,4 Гт/с) Системная логика Intel® 5520 + ICH10R до 96 Гбайт регистровой памяти DDR3 с эффективной частотой 1333 МГц в режиме шестиканального доступа контроллер SAS HBA LSI 106e сетевой контроллер Intel® 82575EB Gigabit Ethernet видеочип Server Engines LLC Pilot II
Дисковый контроллер	дублирование для повышения надёжности, поддержка горячей замены носителей, автономный источник питания RAID 0, 1, 1E, 5, 6, 10, 50, 60 вывод для подключения внешнего массива SAS RAID через порт min-SAS x4 6 x полнодуплексных внутренних SAS-порта
Сетевой модуль-коммутатор	дублирование для повышения надёжности 10 x внешних полнодуплексных портов с поддержкой Gigabit Ethernet 12 x внутренних полнодуплексных портов (по два на модуль)
Модуль удалённого управления	встроенный KVM мониторинг показателей работы и оповещение о событиях в системе в режиме реального времени
Питание	Четыре независимых источника питания мощностью 1 кВт каждый, конфигурация с избыточностью N+1
Охлаждение	Дублированная, трёхзонная (модули ввода/вывода, система хранения и питания, вычислительные модули) система охлаждения с возможностью горячей замены

ные файлы, запросившему их клиенту по тому же протоколу.

Вычислительный модуль с установленным ПО для МИС предназначен для обеспечения функционирования приложения МИС.

Вычислительный модуль БД МИС предназначен для организации управления доступом приложений к данным информационных ресурсов и предоставления их через соответствующие приложения пользователям.

Криптомаршрутизатор обеспечивает криптографическую защиту информации, передаваемой по открытым каналам связи между составными частями VPN, которыми могут являться локальные вычислительные сети, их сегменты и отдельные компьютеры.

Назначение и функции криптомаршрутизатора:

- объединение в одном модуле функций межсетевого экрана, маршрутизатора и средства построения VPN-сетей (защита данных по ГОСТ 28147-89).
- организация криптографической защиты информации, передаваемой по открытым каналам связи;
- Защита виртуальных частных сетей (VPN);
- Защита локальных вычислительных сетей (ЛВС), входящих в состав домена Windows.

Ключевые возможности крипотомаршрутизатора:

- «Прозрачность» для любых приложений и сетевых сервисов, работающих согласно протоколу TCP/IP, включая IP-телефонию и видеоконференции;
- Защита высокоприоритетного трафика (VoIP и видеоконференции) без потери качества;
- Резервирование гарантированной полосы пропускания для отдельных сервисов;
- Поддержка технологии NAT/PAT позволяет скрывать структуру защищаемых сегментов сети;

Криптографическая защита передаваемых данных осуществляется в соответствии с ГОСТ 28147-89.

Гибкость конфигурирования и хороший потенциал для дальнейшего масштабирования делают разработанное Kraftway решение оптимальным для использования в целевой инфраструктуре. Добавление новых компонентов и узлов не вызовет дополнительных трудностей даже у специалиста начального уровня, поскольку физически эта операция будет представлять собой добавление модуля в специализированную «корзину» без необходимости внешней коммутации. Дальнейшую настройку системы опытный системный администратор может проводить дистанционно.

Использование модульного сервера делает реализуемые решения менее затратными, позволяет тратить меньше времени на инсталляцию, масштабировать систему в соответствии с возникающими потребностями в информационных ресурсах. Таким образом, применение данного решения позволяет получить следующие преимущества:

- низкая стоимость решения в сравнении с методом комплексирования разнородного оборудования в рамках локальной инфраструктуры;
- высокий базовый уровень надёжности;
- низкие требования к электропитанию, охлаждению и подготовке помещения;
- возможность физически изолированного исполнения служб и сервисов на разных вычислительных модулях;
- возможность установки, инициализации и предварительной настройки приложений в цикле производства
- низкая стоимость монтажа и пуско-наладочных работ;
- низкая стоимость эксплуатации, малые требования к обслуживающему персоналу;
- отказоустойчивость и ремонтопригодность, длительный жизненный цикл серийного производства модульных систем гарантирует доступность систем до 2018 года, доступность комплектующих до 2020 года;
- хорошая масштабируемость без изменения архитектуры решения.

Для соответствия специальным требованиям к разрабатываемой системе, связанным с особенностями, масштабом и темпом реализации программы модернизации здравоохранения, комплекс был доработан специалистами компании Kraftway. В вычислительные модули был установлен аппаратно-программный модуль доверенной загрузки (АПМДЗ) со средствами строгой двухфакторной аутентификации с помощью USB-ключей, защищающий сервер от несанкционированного доступа. Данная особенность делает серверное решение Kraftway в форм-факторе серверов-лезвий уникальным на рынке. Интеграция АПМДЗ в аппаратную часть блэйд-сервера позволила реализовать все необходимые функции безопасности в рамках единого модульного дизайна системы.

В целях соответствия санитарным требованиям к шумовому загрязнению, принятым в учреждениях здравоохранения, для размещения модульного сервера в ЛПУ компанией Kraftway был разработан вандалозащищённый шумопоглощающий шкаф. Его использование не только позволяет защитить модульный сервер от внешнего воздействия при установке в общественном месте, но и снизить уровень производимого шума до уровня типового персонального компьютера даже при максимальной нагрузке на вычислительные модули.

Высокие показатели шумоизоляции были достигнуты благодаря:

- организации воздушных потоков внутри шкафа;
- пассивного шумоподавления за счёт применения звукопоглощающих материалов;
- активного шумоподавления на выходе воздушных потоков.

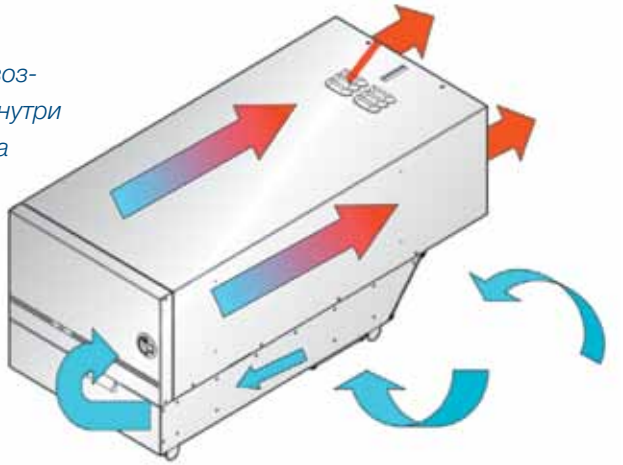
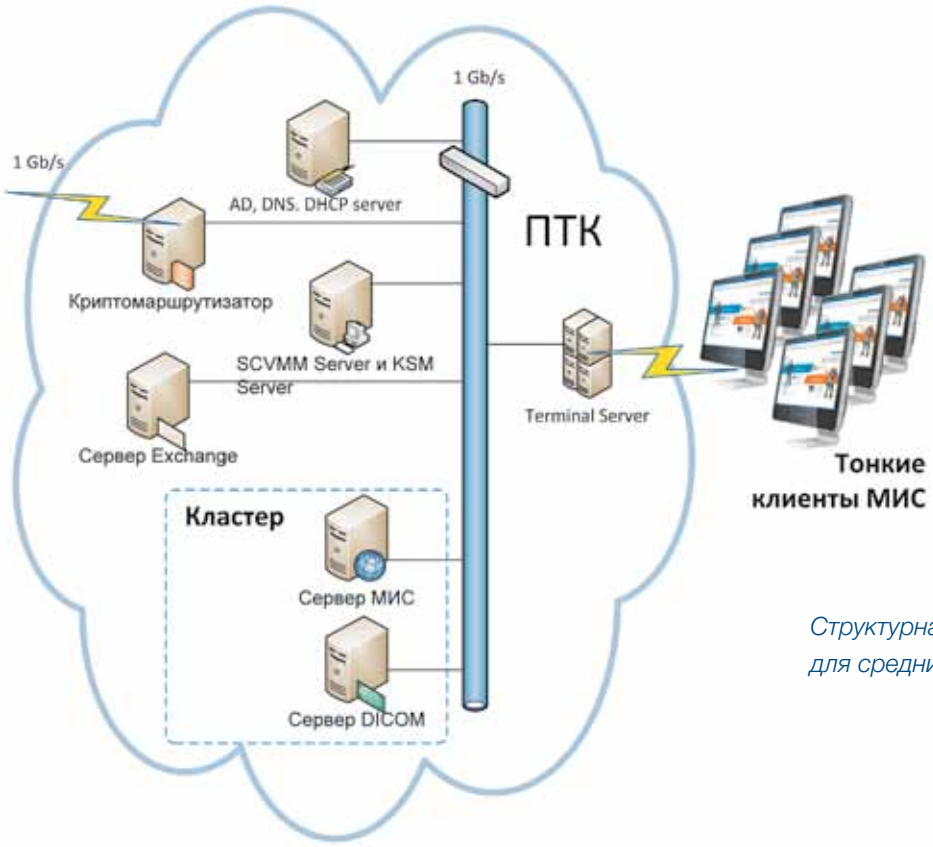


Схема движения воздушных потоков внутри серверного шкафа

ПТК №1 ДЛЯ СРЕДНИХ И БОЛЬШИХ ЛПУ



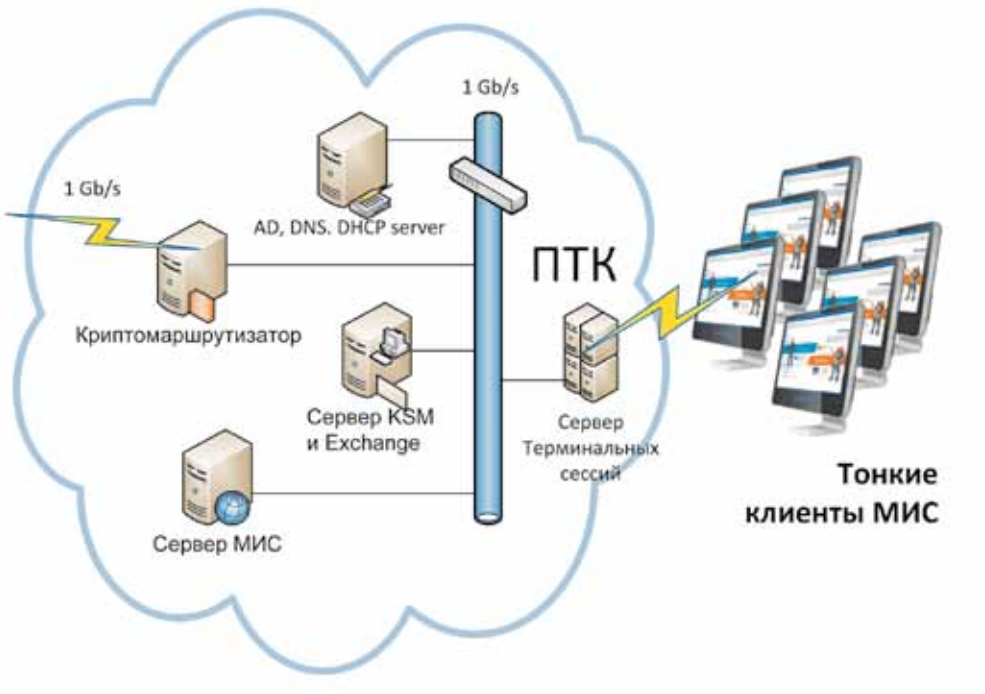
Структурная схема ПТК №1 для средних и больших ЛПУ

Спецификация типового ПТК №1 для средних и больших ЛПУ

	Шасси	1
Шасси	Шасси модульной серверной системы	1
Жесткие диски	Жесткий диск 7200rpm SAS 6Gb/s 1Tb	14
Система хранения	RAID-контроллер SAS с дублированием	1
LAN	Встроенный коммутатор ЛВС с дублированием	1
Корпус	Шкаф Kraftway с активным шумоподавлением	1
	Процессорное лезвие 1	2
Процессор	Intel® Xeon® E5606 (2,13 GHz 8MB cache)	1
ОЗУ	4 GB DIMM DDR3-1333 ECC Registered	2
	Процессорное лезвие 2	3
Процессор	Intel® Xeon® E5620 (2,4 GHz 12MB cache)	2
Контроль загрузки	Модуль доверенной загрузки «Соболь»	1
ОЗУ	8 GB DIMM DDR3-1333 ECC Registered	8
	Криптомаршрутизатор 1Gbs	1
Процессор	Intel® Xeon® E5620 (2,4 GHz 12MB cache)	2
ОЗУ	DIMM 2GB DDR3-1333 ECC Registered	2
ПО криптомаршрутизатора	VipNET	1

ПТК №2 ДЛЯ НЕБОЛЬШИХ ЛПУ

Для организации вычислительной инфраструктуры небольших ЛПУ предлагается использовать ПТК №2, который по набору сервисов полностью соответствует всем функциональным характеристикам ПТК №1, но при этом поддерживает меньшее число пользователей (до 50) и обладает меньшими возможностями по масштабируемости и резервированию ресурсов. ПТК №2 смонтирован в вандалозащищённом, шумопоглощающем шкафу и может быть быстро развёрнут в неподготовленном помещении, в том числе в комнате, где располагаются клиентские рабочие места, не нарушая санитарно-эпидемиологических норм.



Структурная схема ПТК №2 для небольших ЛПУ

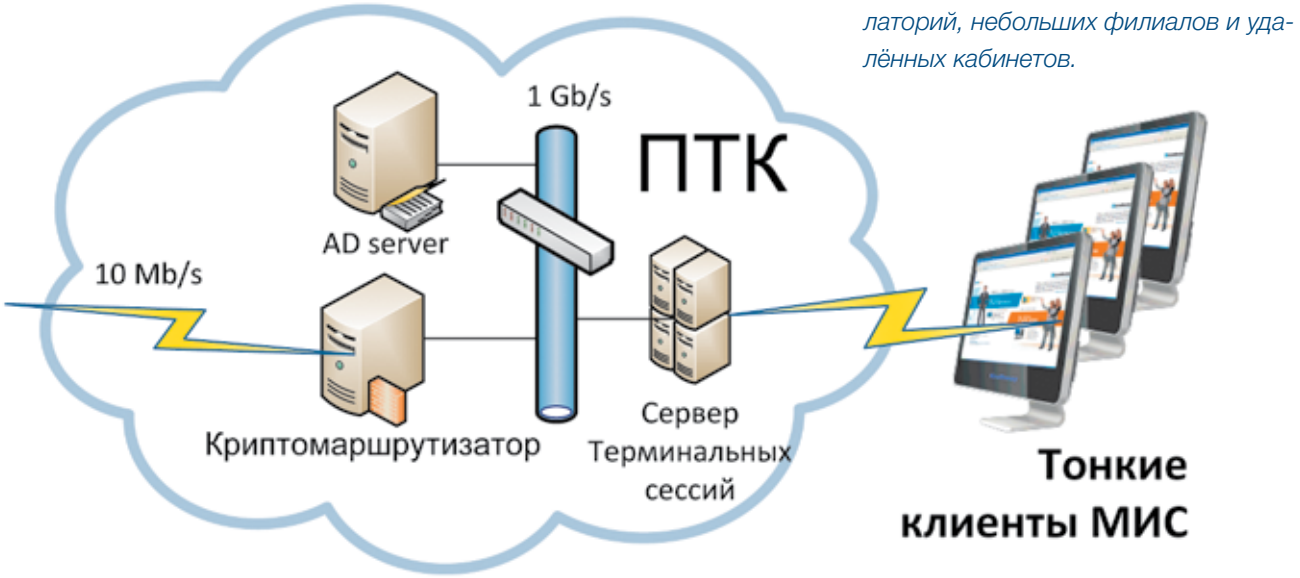
Спецификация типового ПТК №2 для небольших ЛПУ

	Инфраструктура	**1**
Корпус	Шкаф Kraftway с активным шумоподавлением	1
Сетевое оборудование	Коммутатор управляемый 16 портов 10/100/1000	1
	Сервер 1	**4**
Платформа	Шасси сервера «4 в 1»	1
Функции контроля и управления сервером	Модуль удаленного управления	1
Процессор	Intel® Xeon® X3470 (2,93 GHz, cache 8 MB)	1
Память	DIMM 2GB DDR3-1333 ECC Registered	2
Жесткие диски	HDD 500GB, SATA, 7200rpm	1
	Сервер 2	**1**
Платформа	Шасси сервера с интегрированной системой хранения	1
Функции контроля и управления сервером	Модуль удаленного управления	1
Процессор	Intel® Xeon® E5620 (2,40 GHz, cache 12 MB)	2
Память	DIMM 2GB DDR3-1333 ECC Registered	9
Жесткие диски	HDD 3 TB, SATA, 7200rpm	4
	Программное обеспечение	**1**
ПО криптомаршрутизатора	VipNET	1

ПТК №3 ДЛЯ АМБУЛАТОРИЙ, НЕБОЛЬШИХ ФИЛИАЛОВ И УДАЛЁННЫХ КАБИНЕТОВ

Учитывая современные тенденции по миграции приложений, сервисов и даже инфраструктуры в облачную информационную среду, специалисты Kraftway разработали ПТК №3, который позволяет подключить к единому информационному пространству даже самые небольшие по количеству рабочих мест медицинские учреждения. Но при этом информационная безопасность сохраняется на уровне больших учреждений в соответствии с требованиями закона «О персональных данных». Пользователь ПТК №3 не будет ощущать никаких ограничений по функциональности медицинских и общесистемных сервисов. Ограничением может являться доступность информационных сервисов, которая в ПТК №3 (в отличие от других решений) целиком и полностью определяется качеством канала связи. Но, учитывая небольшое число пользователей (не более 10), ПТК №3 обеспечивает комфортную работу пользователей в режиме «тонкого клиента» на канале связи со средней пропускной способностью.

Структурная схема ПТК №3 для амбулаторий, небольших филиалов и удалённых кабинетов.



Спецификация типового ПТК №3

	Сервер	
Шасси	Kraftway Express Lite модель EL13	1
UPS	1000VA Smart	1
ОЗУ	RAM 8 GB DDR3-1333 ECC (4*2 GB)	1
Процессор	Intel® Xeon® X3430 (2,40 GHz, cache 8 MB)	1
Жесткие диски	HDD SATA 1000GB 7200 rpm	4
Корпус	Шкаф Kraftway с активным шумоподавлением	1
Криптомаршрутизатор	Криптотерминал KWN10	1
	Программное обеспечение	
ПО криптомаршрутизатора	VipNET	1

ТОНКИЕ КЛИЕНТЫ KRAFTWAY

Для противодействия современным угрозам и соответствия уровню развития технологий, а также для максимального удобства использования и управления средствами защиты, компанией Kraftway разработано решение, позволяющее создать АРМ оператора МИС на базе защищённого «тонкого» клиента.

Рассмотрим более подробно одну из наиболее сложных современных угроз – утечку персональных данных и готовность продукции Kraftway к противодействию этой угрозе.

В настоящее время широко внедряются технологии виртуализации, которые позволяют на одной физической машине эмулировать любое аппаратное обеспечение, а также представлять одну физическую машину как несколько виртуальных. Непосредственно эмуляцией аппаратного обеспечения и управлением физическими ресурсами компьютера занимается специализированная программа – гипервизор.

Виртуализация при помощи гипервизоров уровня ОС и с использованием специализированных ОС условно является контролируемой. Но виртуализация уровня BIOS не подлежит контролю никакими средствами.

Базовая система ввода-вывода – это своеобразный посредник между любым программным обеспечением (в том числе ОС) и аппаратными компонентами компьютера. Любые операции с «железом» выполняются при участии BIOS, кроме прямых обращений между устройствами, команды на исполнение которых тоже передаются через BIOS.

Использование защищенных тонких клиентов позволяет существенно повысить уровень информационной безопасности при обработке конфиденциальной информации.

В случае наличия на уровне BIOS гипервизора, в микросхеме BIOS может присутствовать неконтролируемый код, который имеет возможность эмулировать любое аппаратное обеспечение с целью обхода различных проверок и контроля всех действий, выполняемых на компьютере. Обнаружить данный гипервизор средствами самого компьютера невозможно в силу того, что операции контроля выполняются также средствами BIOS, то есть при необходимости гипервизор отдает контролирующей программе нужные значения. Неэффективна и процедура обновления BIOS, так как гипервизор будет обновлять только ту часть кода, которая относится к выполнению операций ввода-вывода для конкретного эмулируемого аппаратного обеспечения, а остальной код останется неизменным. Анализ временных характеристик быстродействия компьютера также не позволяет выявить наличие

гипервизора, поскольку выполнение низкоуровневых операций анализа потока данных дает снижение производительности в рамках значений погрешности измерений.

Обработка конфиденциальной информации, в том числе имеющей гриф секретности, в автоматизированных системах всегда связана с вопросами разделения доступа к обрабатываемым данным, контролем используемых для обработки средств, идентификацией и аутентификацией пользователей автоматизированных систем.

При обработке конфиденциальной информации доступ к средствам обработки должен быть всегда строго регламентирован. Несанкционированное использование компьютера как средства обработки может привести к нарушению режима конфиденциальности.

Поэтому необходимо предусмотреть средства защиты от несанкционированного доступа, которые позволяли бы провести идентификацию и аутентификацию пользователя до загрузки операционной системы и блокировать дальнейшую загрузку в случае неудачной аутентификации.

Электронные замки и АПМДЗ не позволяют контролировать требуемые параметры компьютера (контроль целостности программной среды, загрузка с определенного носителя и др.), так как гипервизор уровня BIOS имеет возможность подменить реальные значения физических параметров.

Единственный метод удалить гипервизор уровня BIOS – снять чип BIOS и «перепрошить» его на внешнем программирующем устройстве.

Код BIOS устанавливается для конкретных материнских плат или конфигураций компьютеров на этапе производства. Это означает, что сегодня не существует средств построить защищенный компьютер на основе комплектующих, производство которых не контролируется.

Для противодействия угрозам, включая использование гипервизора на уровне BIOS, компания Kraftway разработала и производит ряд материнских плат с интегрированным модулем доверенной загрузки.

В отличие от традиционного АПМДЗ, решение, предлагаемое Kraftway, является неразъемным, оно

Терминальное решение Kraftway имеет целый ряд дополнительных преимуществ по сравнению со стандартными терминальными решениями:

- малые габариты 205x135x30 мм;
- возможность крепления на задней стенке монитора на стандартный разъём VESA;
- отсутствие шума;
- низкое энергопотребление 20Вт;
- интеграция АПМДЗ (TSM) в BIOS материнской платы

интегрированно с BIOS материнской платы, является его штатным модулем и не может быть извлечено из ПК.

Благодаря заложенным архитектурным и техническим решениям защищенный тонкий клиент обладает существенными преимуществами по сравнению с традиционными аппаратно-программными модулями доверенной загрузки (АПМДЗ), установленными в слоты расширения вычислительных систем.

Отличительной особенностью интегрированного АПМДЗ является невозможность его извлечения, защита от перезаписи BIOS, а также невозможность сброса настроек BIOS, что предотвращает несанкционированное использование тонкого клиента даже при наличии полного доступа к его аппаратной составляющей. Тесная интеграция АПМДЗ с BIOS материнской платы защищает тонкий клиент Kraftway от новых угроз в виде низкоуровневых виртуальных гипервизоров, нарушающих информационную безопасность системы, которые не всегда обнаруживаются традиционными АПМДЗ.

Использование защищенных тонких клиентов позволяет существенно повысить уровень информационной безопасности при обработке конфиденциальной информации путем предотвращения несанкционированного доступа и изменения средств обработки, ведения журнала событий доступа, в независимости от используемых программных средств, операционных систем и комплектующих.

В основе защищённого тонкого клиента лежит материнская плата KWN10 собственной разработки Kraftway, которая в полной мере реализует потенциал энергоэффективной платформы Intel® Pine Trail. Микропроцессор Intel® Atom N450 представляет собой высокоинтегрированное решение, включающее универсальное вычислительное ядро, контроллер памяти и графику в однокристальной компановке. Работая на тактовой частоте 1,66 ГГц, он обеспечивает комфортный уровень производительности при низком уровне потребления энергии. На плате может быть установлено до 2 Гбайт памяти DDR2 с эффективной частотой работы 667 МГц.

В состав решения для защищенного тонкого клиента входит модифицированный BIOS разработки компании Kraftway, а также модуль строгой двухфакторной аутентификации пользователей от компании «Аладдин Р.Д.» (Trusted Security Module). Тесная интеграция BIOS с модулем доверенной загрузки TSM позволяет проводить во время операции POST (Power-On Self Test) аутентификацию пользователей ещё до загрузки операционной системы тонкого клиента.

Доверенный BIOS обладает следующими уникальными возможностями:

- разграничение доступа (защита от перезаписи, ограничение прав чтения) к настройкам BIOS, TSM, журналам регистрации событий;
- защита от несанкционированной модификации BIOS (в том числе и запрет функции recovery), области хранения настроек BIOS (подмена микросхемы CMOS);
- ограничение доступа к BIOS SETUP по роли пользователя;
- регистрация событий, вызванных действиями пользователей, логирование ошибок с возможностью дальнейшей выгрузки журнала в форматах Microsoft Excel или CSV (Comma-Separated Values).
- многоуровневый контроль целостности программной среды (BIOS, файловых систем NTFS\FAT16\FAT32, критичных секторов носителей информации);
- интеграция с решениями компании «Аладдин Р.Д.» для защиты от НСД;
- полная руссификация интерфейса.

Trusted Security Module проходит сертификацию по следующим направлениям:

- на соответствие требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 4 уровню контроля.
- на соответствие требованиям ФСТЭК России для применения в АС до класса 1В включительно и ИСПДн до 1 класса включительно.

Применение модуля двухфактороной аутентификации от компании «Аладдин Р.Д.» позволяет использовать электронные ключи eToken-5 (в форм-факторе USB-токенов и смарт-карт), обладающие сертификатом соответствия ФСТЭК России № 1883 от 11.08.2009 года на применение в АС до класса 1Г включительно и ИСПДн до 1 класса включительно.

С помощью стандартных средств материнской платы можно производить гибкие настройки системы в соответствии с принятой политикой информационной безопасности без необходимости использования дополнительных средств. Наличие в комплекте поставки сертифицированных средств защиты позволяет проводить аттестацию рабочих мест и систем на соответствие требованиям к уровню информационной безопасности по различным классификациям, в том числе к ИСПДн до 1 класса включительно.

Новый тонкий клиент Kraftway поставляется в специально разработанном металлическом компактном корпусе черного цвета, который может быть закреплен на задней панели любого монитора. Таким образом, устройство не занимает места на рабочем столе пользователя. При установке на штатное место клеммы заземления и при использовании укороченного кабеля для подключения к монитору практически полностью устраняется возможность дистанционного считывания конфиденциальной информации с помощью специальных средств электронного шпионажа.

Устройство может быть рекомендовано для решения задач, связанных с информационной безопасностью данных, когда необходимо обеспечить надежную защиту информации, разделение доступа к обрабатываемым данным, контроль программной среды, аутентификацию пользователей автоматизированных систем с использованием сертифицированных средств. Активация АПМДЗ может быть произведена как в процессе производства, так и в процессе эксплуатации системы через специальное меню в BIOS при приобретении лицензии на средство защиты.

Тонкий клиент Kraftway работает под управлением операционных систем семейства Linux и Microsoft Windows Embedded и может поставляться с бесплатной версией Kraftway Terminal Linux, оптимизированной под определённые задачи в соответствии с требованиями заказчика.

KRAFTWAY TERMINAL LINUX

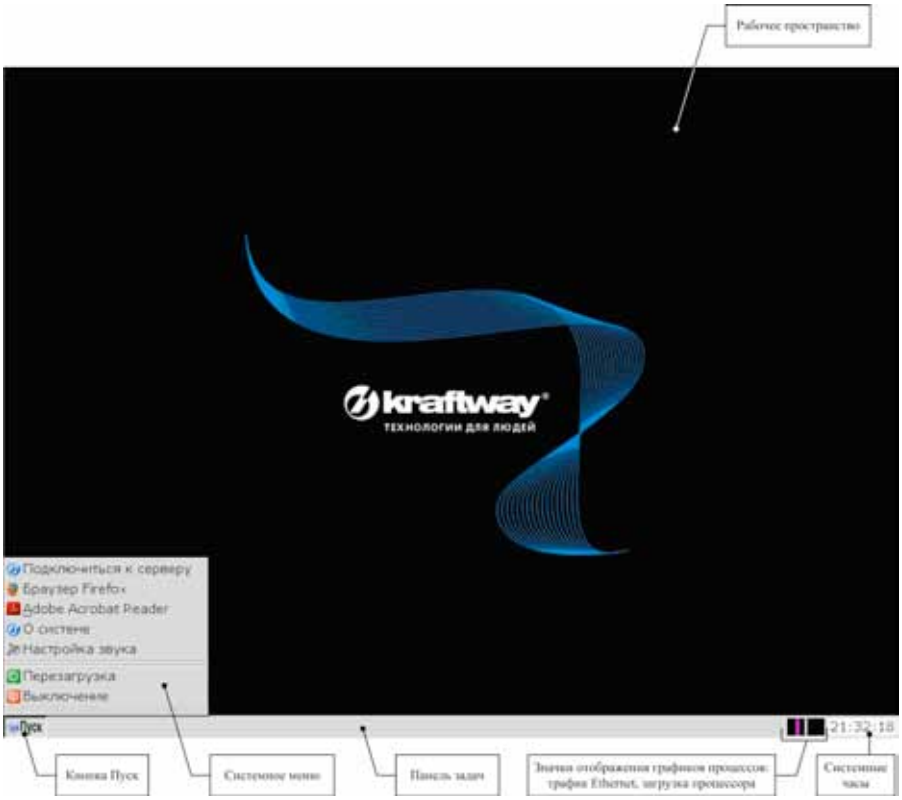
Тонкие клиенты Kraftway работают под управлением операционной системы Kraftway Terminal Linux (KTL), разрабатываемой компанией в течение нескольких лет. Эта ОС в полной мере раскрывает возможности свободного программного обеспечения и неотступно следует принципам открытости стандартов. На «тонкие» клиенты Kraftway KTL устанавливается абсолютно бесплатно. К ключевым особенностям этой операционной системы можно отнести:

- широкий набор протоколов терминального доступа (RDP, Citrix, NX, X, VNC, OpenSSH) с использованием полного набора возможностей (перенаправление периферии, носителей в сессию, поддержка видеорежимов, смарт-карт и USB-ключей для двухфакторной аутентификации);
- поддержка наиболее распространённых моделей принтеров, возможность работы в качестве принт-сервера, скан-сервера;
- возможность автономной работы с использованием браузера (Mozilla Firefox) и VoIP клиента (Skype);
- удобные и функциональные средства управления и настройки: web-интерфейс с исчерпывающим набором возможностей, а также опционально консоль удалённого централизованного администрирования, позволяющая значительно упростить обслуживание тонких клиентов.

Таким образом, использование в ЛПУ инфраструктуры с терминальным доступом и тонких клиентов Kraftway обеспечивает:

- простоту администрирования и развертывания рабочих мест;
- высокую степень защищенности от несанкционированного доступа с помощью встроенных средств контроля доступа;

Kraftway Terminal Linux.
Рабочий стол и меню терминальной станции



- информационную безопасность благодаря хранению всех данных на сервере;
- защиту от вредоносного программного обеспечения за счет отсутствия устройств долговременного хранения;
- надежность и длительный срок эксплуатации устройств благодаря отсутствию в тонком клиенте механических движущихся элементов;
- благоприятные эргономические характеристики рабочего места;
- экономию на техническом обслуживании, модернизации аппаратного и программного обеспечения, электроэнергии, что делает совокупную стоимость владения очень низкой.

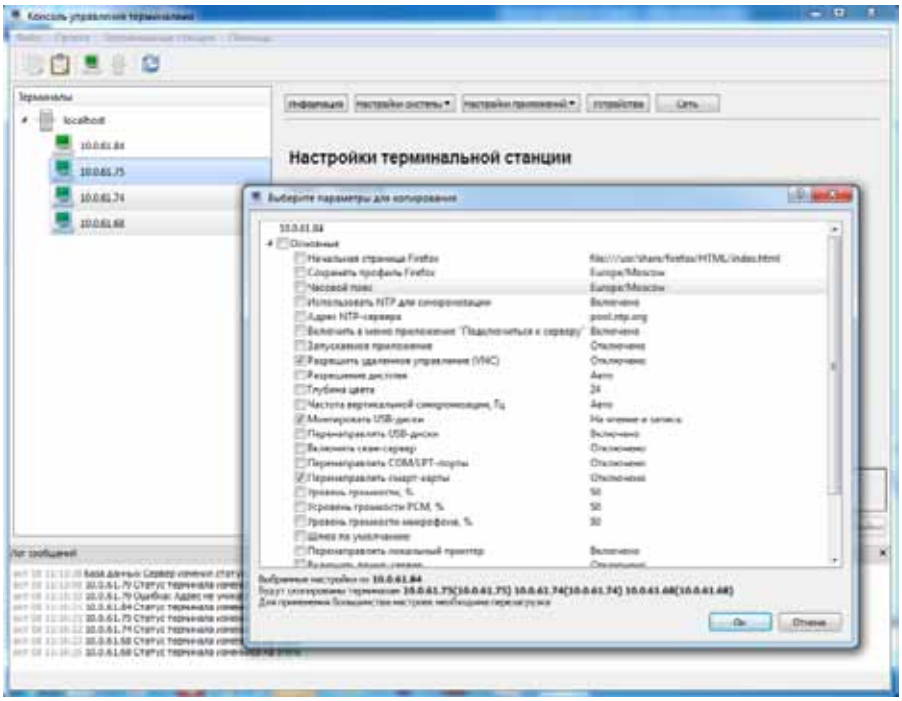
КОНСОЛЬ УПРАВЛЕНИЯ ТЕРМИНАЛЬНЫМИ СТАНЦИЯМИ

Для целей удалённого централизованного администрирования терминальных станции компания Kraftway разработала специализированную консоль. Она предоставляет полный набор функций управления и настройки тонких клиентов с возможностью выполнения групповых операций через удобный пользовательский интерфейс. К ключевым особенностям решения относятся:

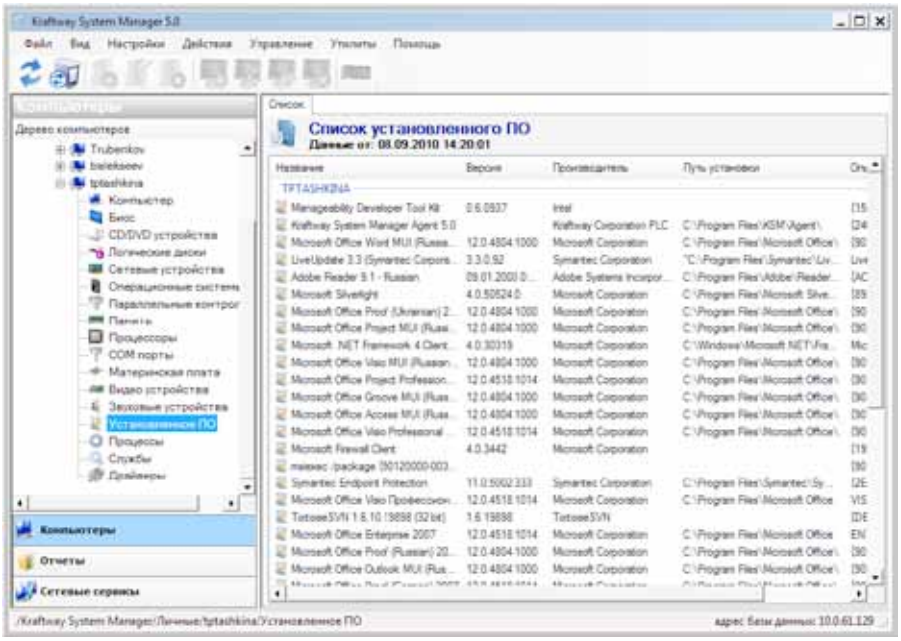
- возможность настройки терминальных подключений, создание и менеджмент сценариев;
- настройка периферийного (мониторы, принтеры, скан-сервер, принт-сервер) и встроенного оборудования (параметры звука, сетевые настройки);
- управление тонким клиентом (перезагрузка, выключение);
- обновление программного обеспечения (KTL);

Консоль управления доступна как для операционных систем семества Windows, так и для дистрибутивов Linux.

Консоль управления терминалами. Перенос настроек на группу терминальных станций



KRAFTWAY SYSTEM MANAGER (KSM)



Kraftway System Manager. Информация об установленном ПО

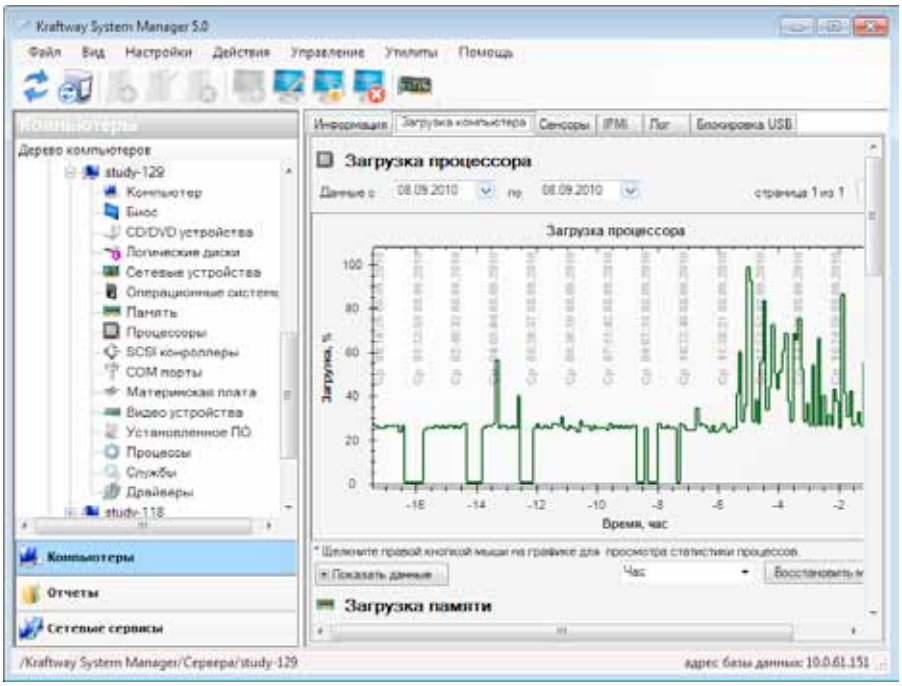
Компания Kraftway разрабатывает собственное инструментальное средство для обслуживания и мониторинга инфраструктуры – Kraftway System Manager. KSM представляет собой мощный комплекс, позволяющий значительно упростить администрирование парка вычислительной техники. Функциональные возможности включают:

- централизованный сбор, хранение и анализ информации об установленном ПО, конфигурации и состоянии аппаратных компонентов ПК, распределённых серверных систем;
- мониторинг и анализ информации о загрузке наблюдаемых систем, о работе сетевых сервисов;
- дистанционное управление ПК и серверами на аппаратном уровне в сетях, построенных на основе стека протоколов TCP/IP;
- предсказание аппаратных сбоев;
- конфигурируемую систему опове-

щений о происходящих в инфраструктуре событиях с помощью почты и SMS-рассылки.
- графическую консоль управления, предоставляющая удобный и интуитивно понятный интерфейс для централизованного управления.

Kraftway System Manager (KSM) использует архитектуру «клиент-сервер». В качестве протокола для взаимодействия агента и сервера выбран международный стандарт WS-Management. Применение стандарта WS-Management позволяет обеспечить шифрование данных (протокол S-HTTP: HTTP + SSL), взаимную аутентификацию агента и сервера. WS-Management является индустриальным стандартом для систем мониторинга, что обеспечивает базу для интеграции KSM с другими системами мониторинга, поддерживающими этот стандарт.

Возможность управления серверными платформами в KSM реализована в соответствии со стандартами IPMI 1.5 и 2.0 в режиме Out-Of-Band (OOB). Независимо от типа и работоспособности операционной системы системный администратор может дистанционно перезапустить, выключить или включить сервер, считать события аппаратного журнала для последующего анализа.



Kraftway System Manager. График загрузки процессора

С использованием KSM процесс администрирования становится значительно проще и эффективнее.

ИНФОРМАЦИОННЫЕ КИОСКИ

В инфраструктуру решения для ЛПУ могут быть включены специализированные информационные киоски, в функцию которых будет входить предоставление информации об оказываемых медицинских услугах, а также запись на приём к врачу. С их помощью возможно создание так называемой электронной очереди: пациент выбирает удобные день и время приёма в графике нужного врача и записывается. Тем самым решается постоянная проблема очередей в ЛПУ. Регистрация на приём может быть интегрирована с порталом государственных услуг.

kraftway
ДЛЯ ЗДРАВООХРАНЕНИЯ

О КОМПАНИИ KRAFTWAY

Kraftway – одна из крупнейших российских компаний, занимающихся промышленным производством широкого спектра ИТ-оборудования и программных средств, а также созданием и внедрением инфраструктурных решений.

Стратегическими заказчиками корпорации являются крупнейшие государственные и коммерческие структуры.
В 2009 году компании Kraftway было присуждено звание «лучшего поставщика для государственных и муниципальных нужд в сфере информационных технологий».

В 2010 году Президент РФ Д.А.Медведев посетил производственно-логистический комплекс компании в г. Обнинске и провел в цехе завода совещание Комиссии по модернизации и технологическому развитию экономики России.

Для наиболее полного удовлетворения запросов и нужд клиентов Kraftway сосредоточил усилия на нескольких важнейших направлениях работы:

- Исследовательская деятельность и экспертиза, создание инновационных продуктов и решений для вертикальных рынков, в т.ч. для здравоохранения;
- Промышленное производство как серийной компьютерной техники, так и уникальных продуктов;
- Реализация крупных интеграционных проектов;
- Проведение спецпроверок и специсследований, защита персональных данных;
- Сервис и поддержка клиентов во всех субъектах РФ

Компания накопила уникальный опыт подготовки архитектурных, общесистемных и технических решений по информатизации здравоохранения от уровня ЛПУ до уровня субъекта Федерации (в т. ч. для задач персонифицированного учета медицинских услуг, ведения электронной медицинской карты, записи к врачу в электронном виде, телемедицины и документооборота).

Узнайте больше

о продуктах и решениях Kraftway для автоматизации медицинских учреждений по телефону консультационной линии

8 495 969 24 00

или на сайте

www.kraftway.ru

kraftway®
ТЕХНОЛОГИИ ДЛЯ ЛЮДЕЙ