СОГЛАСОВАНО

Директор РНПЦ МТ

_____ М.М.Сачек

«__10__» ____декабря____ 2018 г.

М.П.

УТВЕРЖДАЮ

Заместитель
Министра здравоохранения
Республики Беларусь

_____ В.Д.Шило

«__15__» ____декабря____ 2018 г.

М.П.

Методические рекомендации по проведению работ в организациях здравоохранения в рамках создания централизованной информационной системы здравоохранения

РАЗРАБОТАНО

Заместитель директора по ИТ
РНПЦ МТ

_____ С.В.Новиков

«__10__» ____12____ 2018 г.

Системный архитектор
ОФЭЗ РНПЦ МТ

_____ А.Л.Забабуха

«__10__» ____12____ 2018 г.

Специалист по информационному обеспечению ОФЭЗ РНПЦ МТ

_____ С.И.Карпилов

«__10__» ____12____ 2018 г.

В рамках Программы социально-экономического развития Республики Беларусь на 2016 – 2020 годы, утвержденной Указом Президента Республики Беларусь от 15 декабря 2016 года № 466 и в соответствии с рекомендациями по созданию национальной стратегии электронного здравоохранения, предоставленными Всемирной организацией здравоохранения и Международного союза электросвязи начат процесс создания централизованной информационной системы здравоохранения (далее – ЦИСЗ) для формирования единого информационного архива пациентов и обмена медицинскими данными.

Создание ЦИСЗ соответствует стратегической цели развития системы здравоохранения, предусмотренной Национальной стратегией устойчивого социально-экономического развития Республики Беларусь на период до 2030 года, одобренной Президиумом Совета Министров Республики Беларусь (протокол Президиума Совета Министров Республики Беларусь от 2 мая 2017 года №10).

Практические работы проводятся на основании Соглашения о займе между Республикой Беларусь и Международным банком реконструкции и развития от 25 ноября 2016 года и в соответствии с Приказом Министерства здравоохранения от 14.04.2017 г. № 407 «О некоторых вопросах реализации Соглашения о займе (проект «Модернизация системы здравоохранения Республики Беларусь»).

В данном документе приведены сведения об общей архитектуре электронного здравоохранения и предложения по организации работ по созданию системы электронного здравоохранения в рамках проекта «Модернизация системы здравоохранения Республики Беларусь» (далее – Проект) для организаций здравоохранения.

Основным элементом электронного здравоохранения Республики Беларусь станет ЦИСЗ. Создание ЦИСЗ осуществляется в качестве комплексного проекта с точки зрения объединения вычислительной, информационной и телекоммуникационной инфраструктуры.

При создании ЦИСЗ будут решены следующие ключевые задачи:

1) разработка и принятие единых стандартов, справочников и форматов заполнения и обмена медицинской информацией;

2) завершение комплексной информатизации лечебно-диагностического процесса в организациях здравоохранения для перехода к ведению медицинских документов в электронном виде;

3) формирование и ведение интегрированной электронной медицинской карты (ИЭМК), электронное взаимодействие субъектов системы здравоохранения, а также предоставление широкого спектра медицинских электронных сервисов;

4) создание государственного информационного ресурса электронного здравоохранения как основы для полноценного оказания электронных услуг, выполнение государственных и административных процедур;

5) создание системы поддержки принятия клинических решений для повышения качества оказания медицинской помощи и системы поддержки принятия управленческих решений;

6) создание комплексной системы защиты информации ЦИСЗ;

7) интеграция услуг электронного здравоохранения с общегосударственной автоматизированной информационной системой (далее – ОАИС) и Белорусской интегрированной сервисно-расчетной системой (БИСРС);

8) проведение обучающих мероприятий по вопросам использования централизованной информационной системы здравоохранения.

При создании ЦИСЗ будут использованы современные технологии облачных вычислений и технологии web-клиента, программное обеспечение с открытым кодом, сервис-ориентированная архитектура. Верхний уровень ЦИСЗ – Центральная программная платформа (ЦП) и информационные ресурсы малых и средних организаций здравоохранения будут размещены на республиканской платформе, действующей на основе технологий облачных вычислений.

На уровне ЦП будет осуществляться функционирование подсистем ЦИСЗ, хранение и обработка и обеспечение оперативного доступа к информации посредством интеграционной шины, создан единый информационный архив пациентов на основе интегрированной электронной медицинской карты с обеспечением круглосуточного скоростного доступа к нему организаций здравоохранения и иных медицинских служб в режиме реального времени. Общая архитектура ЦИСЗ представлена на рисунке 1. На рисунке 2 представлена примерная техническая архитектура и маршрутизация информационных потоков уровня организаций здравоохранения.

Общая архитектура «Электронного здравоохранения»

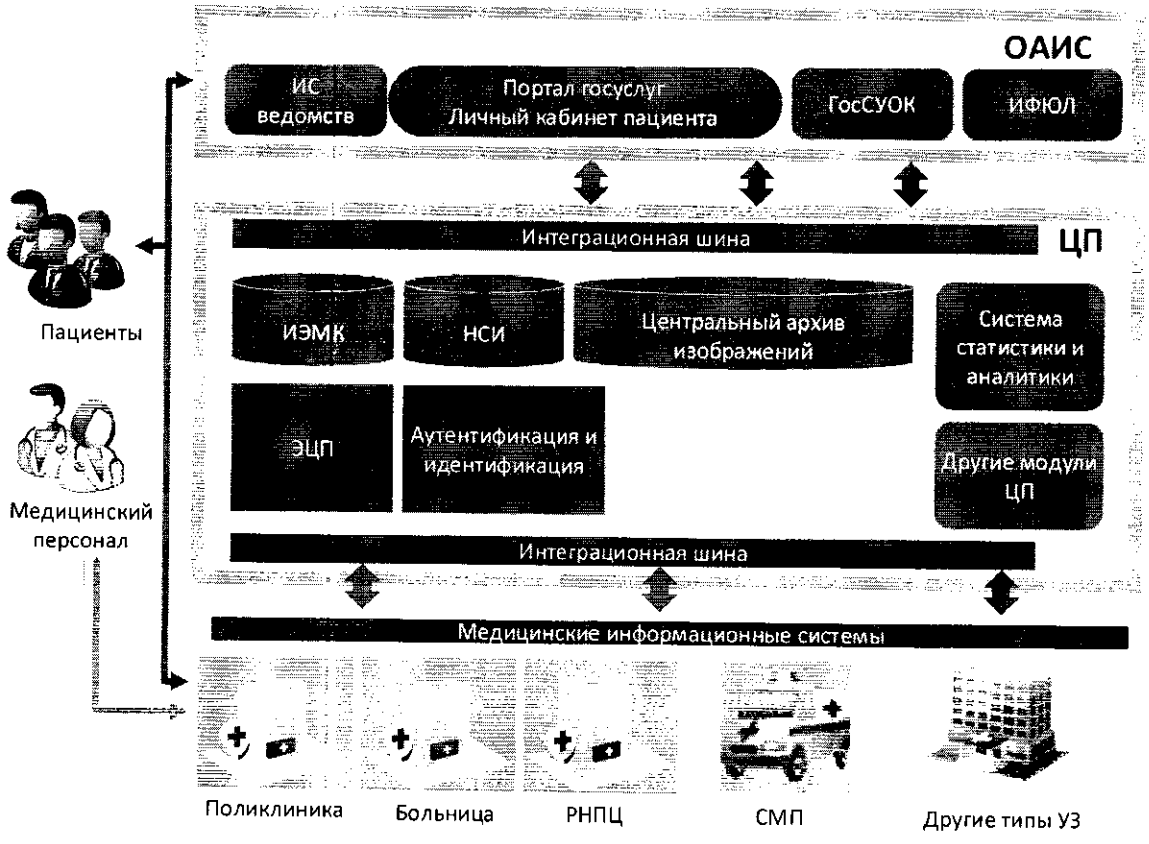

Рис. 1

Архитектура на уровне организации здравоохранения

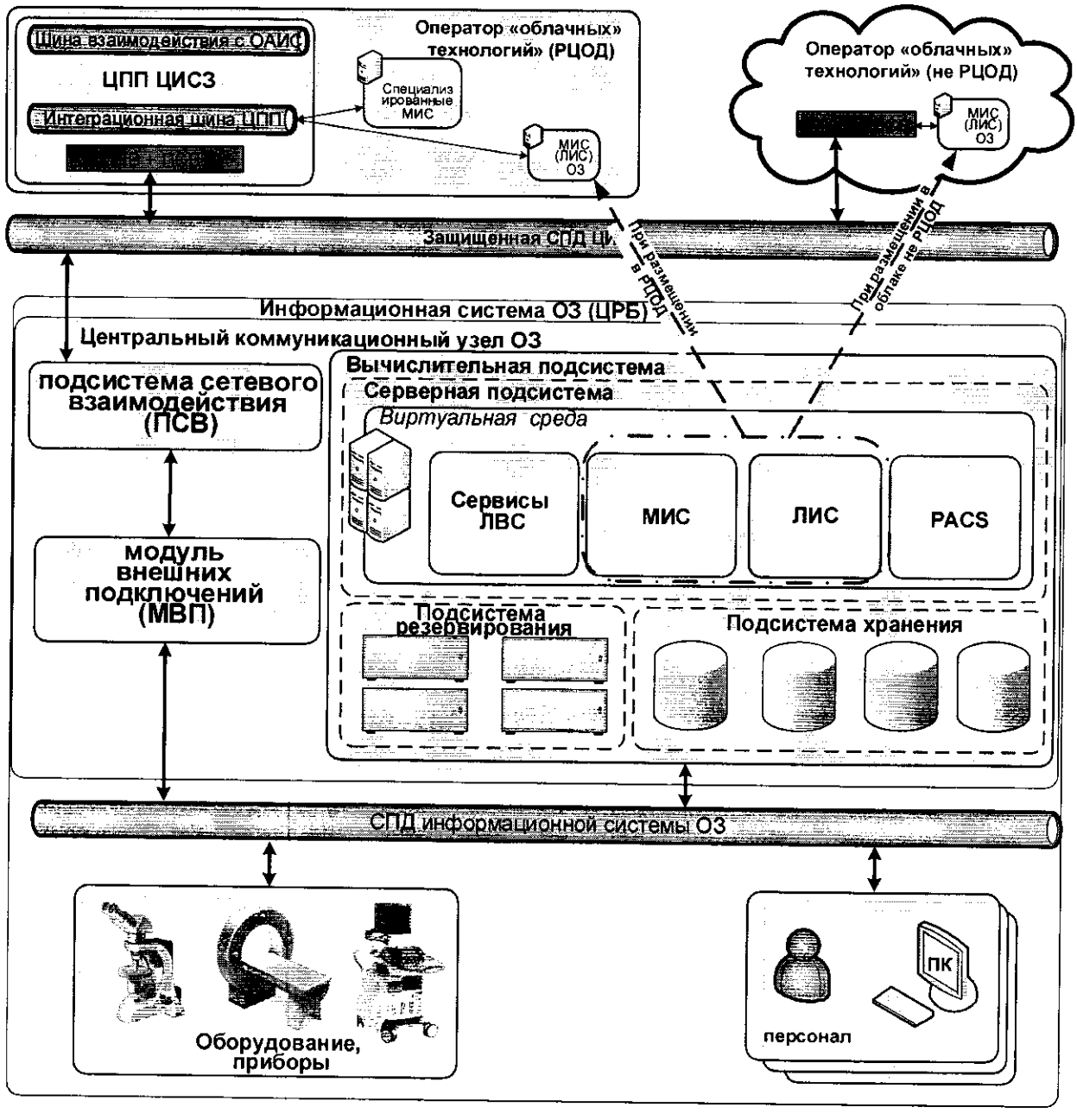

Рис. 2

1. Наличие и состав модуля внешних подключений (МВП) определяется на этапе проектирования системы защиты информации ИС ОЗ.
2. Оборудование подсистемы сетевого взаимодействия (ПСВ) предоставляется оператором защищенных каналов связи при организации подключения к защищенной СПД ЦИСЗ.
3. Конкретный состав вычислительной подсистемы центрального коммуникационного узла определяется на стадии разработки проектно-сметной документации на строительство (модернизацию) ЛВС.

Организации здравоохранения в рамках работ по созданию системы электронного здравоохранения могут проводить работы по модернизации структурированных кабельных сетей (СКС), дооснащению средствами вычислительной техники (СВТ) и прочей цифровой техникой, внедрению (дооснащению дополнительными рабочими местами) медицинских информационных систем (МИС).

При проведении данных работ предлагаем учитывать следующие рекомендации:

1. Подключение к ВОЛС (волоконно-оптическим линиям связи) производить в соответствии с планами подключения медицинских организаций РУП «Белтелекомом» или иным провайдером.

2. Осуществить подключение к корпоративной сети Министерства здравоохранения Республики Беларусь (VPN).

3. Разработать проект модернизации (строительства) локальной вычислительной сети (ЛВС) ОЗ. Проектно-сметную документацию, разработать с учетом требований:

- ТКП 45-1.02-298-2014 «Строительство. Предпроектная документация. Состав и порядок разработки»;
- ТКП 45-1.02-104-2008 (02250) «Проектная документация на ремонт, модернизацию и реконструкцию жилых и общественных зданий и сооружений. Порядок разработки и согласования;
- СТБ 2255-2012 Система проектной документации для строительства. Основные требования к документации строительного проекта.

Для осуществления проектных работ подготовить (актуализировать) следующую техническую документацию (исходно-разрешительную документацию, исходные данные):

- архитектурно-планировочные и конструктивные решения, чертежи фасадов и разрезы (АР/АС, КЖ, КМ) зданий (корпусов) учреждения в объеме, необходимом для выполнения работ ;
- копию инженерно-топографического плана с расположением существующих инженерных сетей в масштабе 1:500 (при проектировании наружных сетей (коммуникаций);
- чертежи (схемы) систем электроснабжения, электрооборудования (ЭМ/ЭО/ЭС) в объеме, необходимом для выполнения работ;
- проектную документацию на существующую ЛВС, включая информацию о связи между коммутационными узлами (КУ), с указанием типа и пропускной способности;
- проектную документацию на существующую сеть электроснабжения;
- схему существующих электрощитов, которые в соответствии с ТУ на электроснабжение будут являться точками подключения;

- при наличии выделенной сети электроснабжения компьютерной техники – схему подключения оборудования начиная от ВРУ (с указанием мощности оборудования), планировки с расположением оборудования и силовых щитов (проект). Технические условия на электроснабжение;
- при наличии – протоколы измерения сопротивления заземляющих устройств (наличие контура заземления 4 Ом);
- при наличии – документацию на оборудование существующей системы кондиционирования телекоммуникационных узлов (модели и комплектация кондиционеров), указать на планах места размещения внутренних и наружных блоков, а также трасс прокладки дренажа;
- техническую документацию на медицинское оборудование.

При проектировании предусмотреть наличие сетевой точки доступа для каждого рабочего места медицинского персонала, требующего ведения (использования) информации МИС и для каждой единицы медицинской техники, имеющей техническую возможность сетевой интеграции. При наличии нескольких рабочих мест в одном помещении (ординаторские, лаборатории и т.д.) запланировать дополнительную точку сетевого доступа для МФУ (1 МФУ на несколько рабочих мест).

4. Осуществить (при необходимости) прокладку межкорпусных соединений с преимущественным использованием оптоволоконных кабелей. При этом в комплект исходно-разрешительной документации добавляется архитектурно-планировочное задание.

5. Осуществить (при необходимости) модернизацию электрических сетей с учетом увеличения потребляемой мощности за счет дополнительных рабочих мест и контура заземления 4 Ом.

6. Оборудовать отдельное помещение для размещения центрального телекоммуникационного узла, придерживаясь требований, изложенных в Приложении 1.

7. Осуществить строительство (модернизацию) ЛВС с оснащением каждого рабочего места точкой сетевого доступа.

8. При закупке серверного, телекоммуникационного, компьютерного и прочего цифрового оборудования ориентироваться на следующие технические характеристики, учитывая архитектурные решения (см. рис. 2):

Требования к вычислительной подсистеме (ВП)

ВП является неотъемлемой частью информационной системы ОЗ и предназначена для организации функционирования сервисов в ЛВС, размещения автоматизированных информационных систем (подсистем) ОЗ и должна состоять из:

- серверной подсистемы (СП);
- системы хранения данных (СХД);
- платформы виртуализации (ПВ);
- подсистемы резервного копирования и архивирования (ПРК).

Аппаратное и программное обеспечение вычислительной подсистемы должно обеспечить непрерывное функционирование системных процессов и сервисов ЛВС ОЗ, с необходимым качеством обслуживания и требуемым уровнем производительности.

Оборудование, применяемое в составе комплекса, должно обеспечивать требуемый уровень надежности.

8.1. Серверная подсистема

СП должна иметь:

- форм-фактор одного вычислительного узла не более 2U;
- не менее 2-х блоков питания на каждый вычислительный узел при номинальном напряжении 230В;
- все вычислительные узлы СП должны быть одного производителя.

Для каждого из вычислительных узлов предусмотреть по 2 твердотельных диска (SSD) для установки на них host системы. Емкость определить при проектировании.

Вычислительный узел должен удовлетворять требованиям:

- 1 или 2 процессора, не менее 18 ядер каждый, тактовая частота не менее 2600 GHz;
- наличие в составе 2-х адаптеров по 2 порта 10 Gb Ethernet с поддержкой протокола iSCSI.

Вычислительные узлы СП должны обеспечивать работу систем виртуализации и быть сертифицированы для следующих операционных систем:

- Microsoft Windows Server;
- Red Hat Enterprise Linux (RHEL);
- SUSE Linux Enterprise Server (SLES);
- VMware ESX.

Тип/модель, количество и конфигурация вычислительных узлов определяется на этапе проектирования и зависят от количества сервисов в ЛВС и автоматизированных процессов ОЗ.

Вычислительные узлы соответствующим образом должны быть объединены и подключены к коммутационному ядру ЛВС.

При проектировании предусмотреть наличие необходимого количества лицензий на использование операционных систем, с соответствующим количеством клиентских лицензий, а также лицензирование систем виртуализации и удаленных рабочих мест пользователей.

8.2. Система хранения данных

СХД может входить в состав вычислительных узлов (программно-определяемое) и должна:

- обеспечить необходимую емкость для хранения информации системных, технологических и производственных процессов и сервисов, эксплуатируемых в ЛВС ОЗ. Объем, тип и количество накопителей для ОЗ определить в процессе подготовки проекта (в рамках сбора недостающих данных);
- иметь возможность наращивания ресурсов хранения, как путем добавления дисковых модулей, так и кластеризации дополнительных контроллерных модулей (вычислительных узлов);
- обеспечить подключение дополнительных дисковых модулей расширения, по отказоустойчивой схеме;
- иметь дублированные подсистемы питания и охлаждения, и модули ввода-вывода на дополнительных дисковых полках;
- поддерживать уровни RAID - 0, 1, 5, 6, 10
- иметь возможность установки в одном дисковом модуле дисков SAS, NL-SAS и SSD одного форм-фактора;
- иметь возможность расширения кэш-памяти контроллеров путем выделения отдельных SSD дисков;
- иметь встроенные средства многоуровневого хранения данных как минимум по 3-м уровням:
  - SSD;
  - HDD SAS;
  - HDD NL-SAS.
- обеспечить поддержку операционных систем:
  - Microsoft Windows Server;
  - Red Hat Enterprise Linux (RHEL);
  - SUSE Linux Enterprise Server (SLES);
  - VMware ESX.

Количество, типы и объемы дисков, а так же протоколы коммутации, количество и типы портов внешних подключений СХД, а так же состав и конфигурация функций определяются на стадии проектирования.

8.3. Платформа виртуализации

ПВ должна:

- обеспечить всестороннюю виртуализацию вычислительных ресурсов, ресурсов хранения, их объединение и тонкое выделение приложениям по требованию и в соответствии с производственными процессами;
- поддерживать автоматическое перемещение виртуальных машин между физическими узлами серверной подсистемы при сбое последних, а также перемещение в ручном режиме при необходимости плановых работ по обслуживанию вычислительной подсистемы;

• поддерживать наращивание ресурсов процессорных и памяти без прерываний в работе виртуальных машин;

• обеспечивать подключение виртуальных хранилищ данных и сетевых ресурсов, а также их удаление без прерываний в работе платформы;

• поддерживать расширение виртуальных дисков машин и/или добавление дополнительного виртуального хранилища к виртуальной машине без прерываний в работе последней.

ПВ, и ее конфигурация, определяются на этапе проектирования.

При проектировании предусмотреть наличие необходимого количества лицензий для обеспечения функционирования ПВ.

8.4. Подсистема резервного копирования и архивирования

При подготовке данных для проектирования ЛВС должно быть предусмотрено комплексное программно-аппаратное решение резервного копирования/восстановления и архивирования данных, которое:

• должно обеспечить надежное резервное сохранение и архивирование пользовательских данных в требуемых объемах;

• иметь возможность гибкого масштабирования;

• поддерживать высокопроизводительную архитектуру резервного копирования, обеспечивающую минимизацию окон резервного копирования;

• обеспечивать копирование/архивирование как физических серверов, так и виртуального окружения;

• должно иметь алгоритмы компрессии и дедупликации резервируемых данных.

Архитектура решения, вид/тип аппаратных средств, количество носителей согласно объемам резервируемых/архивируемых данных определяются на стадии проектирования. Предусмотреть наличие необходимого количества лицензий для обеспечения функционирования ПРК.

8.5. Коммуникационное оборудование

Кабельная система ЛВС должна соответствовать требованиям ТКП 45-4.04-27-2006 и международного стандарта ISO/IEC 11801 2nd Ed. Amendment2.

Использовать оборудование, имеющее все необходимые разрешения и сертификаты Республики Беларусь.

Для организации уровней ядра сети и распределения использовать отказоустойчивый стек из пары коммутаторов уровня L3 с поддержкой 10 Гбит/с интерфейсов для связи с серверным оборудованием/СХД и технологией полноскоростной коммутации третьего уровня модели OSI.

Предусмотреть организацию в ЛВС модуля внешних подключений для организации доступа во внешние сети и создания VPN-соединений с удаленными рабочими местами (сетями). Использовать для этих целей:

• межсетевой экран категории NGFW (Next Generation Firewall) и наличием не менее двух гигабитных интерфейсов для связи с коммутаторами ядра. Минимальное количество маршрутизируемых интерфейсов Gigabit LAN – 4 (необходимость использования и конфигурацию определить на стадии разработки решений по системе защиты информации).

• шлюз с установленной IPS (IDS) (необходимость использования и конфигурацию определить на стадии разработки решений по системе защиты информации).

При проектировании ЛВС должны использоваться полностью управляемые коммутаторы доступа для подключения конечного оборудования (ПК, принтеры, МФУ, медицинское оборудование и пр.) с возможностью централизованного управления и мониторинга. Количество точек ЛВС определить с учетом количества подключаемого конечного оборудования и 20% запаса для дальнейшего развития.

Более подробное описание требований к коммуникационному оборудованию приведено в Приложении 2.

8.6. Компьютерное оборудование:

Тип 1 – компьютерное оборудование для автоматизированных рабочих мест (АРМ), обеспечивающих информационную поддержку выполнения функциональных обязанностей главного врача, заведующих отделениями и т.д. в составе:

Процессор: базовая частота не менее 2 ГГц, количество физических ядер не менее 2-х, кэш L3 не менее 3 Мб;
ОЗУ: DDR4 не менее 4 Гб;
Винчестер: НЖМД – не менее 500 Гб SATA III 7200 rpm или SSD не менее 240 Гб;
Видеокарта: интегрированная, с видеовыходами, соответствующим монитору на рабочем месте (DVI/HDMI/Display Port);
Звуковая карта: интегрированная;
Сетевая карта: интегрированная, 1 Гбит/с;
USB: 2 порта USB 3.0 на передней панели;
Клавиатура: USB;
Мышь: USB;
Монитор: от 24", FullHD;
ИБП: Line-interactive от 650VA;
В зависимости от необходимости могут иметь дополнительно DVD-RW.

Тип 2 – компьютерное оборудование для АРМ, обеспечивающих информационную поддержку функционирования обязанностей медицинского персонала ординаторских и консультационных кабинетов, а также научных работников в составе:

Процессор: базовая частота не менее 2 ГГц, количество физических ядер не менее 2-х, кэш L3 не менее 3 Мб;

ОЗУ: DDR4 не менее 8 Гб;
Винчестер: НЖМД – не менее 1 Тб SATA III 7200 rpm или SSD – не менее 240 Гб + НЖМД – не менее 500 Гб SATA III 7200 rpm;
Видеокарта: интегрированная, с видеовыходами, соответствующим монитору на рабочем месте (DVI/HDMI/Display Port);
Звуковая карта: интегрированная;
Сетевая карта: интегрированная, 1 Гбит/с;
USB: 2 порта USB 3.0 на передней панели;
Клавиатура: USB;
Мышь: USB;
Монитор: от 22", FullHD;
ИБП: Line-interactive от 650VA;
В зависимости от необходимости могут иметь дополнительно DVD-RW.

Тип 3 – компьютерное оборудование для АРМ с подключением к диагностическому оборудованию в составе:

Процессор: базовая частота не менее 2 ГГц, количество физических ядер не менее 2-х, кэш L3 не менее 3 Мб;
ОЗУ: DDR4 не менее 8 ГБ;
Винчестер: НЖМД – не менее 1 Тб SATA III 7200 rpm или SSD – не менее 240 Гб + НЖМД – не менее 500 Гб SATA III 7200 rpm;
Видеокарта: со скоростью шины видеопамяти не менее 128 бит и объемом памяти не менее 512 МБ с видеовыходами, соответствующим монитору на рабочем месте (DVI/HDMI/Display Port);
Звуковая карта: интегрированная;
Сетевая карта: интегрированная, 1 Гбит/с;
USB: 2 порта USB 3.0 на передней панели;
Клавиатура: USB;
Мышь: USB;
Монитор: От 22", FullHD;
ИБП: Line-interactive от 650VA;
В зависимости от типа подключаемого медицинского оборудования могут иметь дополнительно во внутреннем, либо внешнем исполнении: сетевую карту, ТВ-тюнер, COM-порты, DVD-RW.

8.7. Принтеры и МФУ:

8.7.1. При закупке МФУ (принтеров) следует выбирать сетевые модели бизнес-класса с двусторонней печатью с учетом использования рабочими группами из нескольких рабочих мест.

8.7.2. Закупку сканеров штрих-кода производить из расчета: 2 – 4 единицы на амбулаторно-поликлиническое учреждение, 4 – 5 единиц на ЦРБ и клиническое учреждение из расчета:

- для поддержки функции электронного рецепта и т.п. – несколько единиц в регистратуре амбулаторного подразделения, 1 – в приемном отделении стационара, возможно 1 – в кабинете с централизованным

доступом пациентов (кабинет регистрация ВН или аналогичный);

- для лабораторных подразделений – количество определяет УЗ по потребности внутрилабораторного использования.

8.7.3. Закупку принтеров штрих-кода осуществлять только в случае наличия в учреждении соответствующего медицинского оборудования из расчета:

- для лабораторных подразделений – количество определяет УЗ по потребности внутрилабораторного использования;
- для прочих подразделений - по 1 единице на каждое клиническое отделение (для маркировки заборов биоматериала в отделениях).

8.8. Системное и общесистемное программное обеспечение

При закупке серверного и компьютерного оборудования предусматривать закупку необходимого коммерческого программного обеспечения с соответствующими лицензиями (разрешениями) правообладателей или использовать свободно-распространяемое программное обеспечение. Перечень и состав ПО, размещаемого на серверном оборудовании, определять в каждом конкретном случае, исходя из потребностей и требований, предъявляемых информационными системами, эксплуатируемыми в ОЗ.

Для оснащения компьютерного оборудования АРМ рекомендуется использовать следующее программное обеспечение:

Операционная система (ОС): MS Windows 10 Pro OEM или свободно-распространяемая;

Антивирусное ПО: антивирусное ПО, сертифицированное в установленном законодательством порядке, свободно-распространяемое или встроенное в приобретаемую ОС;

Офисное ПО: свободно-распространяемое (LibreOffice или аналог).

9. При закупке медицинского диагностического и лабораторного оборудования следует придерживаться следующих рекомендаций:

9.1. В заданиях на закупку медицинского диагностического и лабораторного оборудования обязательно предусматривать наличие в закупаемом медицинском оборудовании открытых цифровых интерфейсов взаимодействия (обмена) с внешними рабочими станциями для обеспечения передачи результатов диагностических и лабораторных исследований в МИС организации здравоохранения. При этом для диагностического оборудования должен использоваться цифровой интерфейс на основе международного стандарта обмена DICOM 3.0, а для лабораторного оборудования – интерфейс, предусмотренный производителем, но с обязательным предоставление его описания.

9.2. В заданиях на закупку медицинского диагностического и лабораторного оборудования и контрактах на его поставку обязательно предусматривать следующие требования:

• предприятие-поставщик медицинского оборудования должно обеспечить интеграцию получаемых результатов диагностических и лабораторных исследований в МИС организации здравоохранения;

• предприятие-поставщик медицинского оборудования должно обеспечить подключение сегментов ЛВС, создаваемых при поставке и монтаже медицинского оборудования, к общей ЛВС организации здравоохранения;

• по запросу руководства организации здравоохранения, в которую осуществляется поставка медицинского оборудования, предприятие-поставщик медицинского оборудования обязано предоставить услуги своих специалистов для соответствующей настройки интерфейсов поставляемого оборудования с целью передачи медицинских изображений и результатов лабораторных исследований в базу данных МИС (или на внешнюю рабочую станцию), а также оказывать содействие организациям, выполняющим работы по внедрению (обслуживанию) МИС в организации здравоохранения.

10. Система защиты информации

10.1. Требуемый уровень защищенности, информации обеспечивается использованием комплекса программных и технических средств защиты информации и организационных мер, который должен обеспечивать:

• управление доступом к информационным ресурсам в ЛВС на основе ролевой модели доступа;

• контроль потоков информации;

• регистрацию и учет событий, относящихся к безопасности, перечень которых будет определен на этапе разработки Задания по безопасности;

• периодическое тестирование и восстановление средств защиты информации.

10.2. Кроме этого, СЗИ должна обеспечить:

• требуемый уровень защиты информации от всех категорий нарушителей при всех режимах функционирования ЛВС в соответствии с требованиями нормативных правовых актов Республики Беларусь, регулирующих вопросы информационной безопасности и защиты информации;

• проведение учета и расследования случаев нарушения установленных норм и правил обеспечения безопасности информации;

• безопасное взаимодействие с внешними ИС.

10.3. Проектирование СЗИ должно проводиться в соответствии с требованиями нормативных правовых актов Республики Беларусь, регламентирующих вопросы обеспечения безопасности информации.

Проектирование СЗИ должно проводиться в соответствии с требованиями нормативных правовых актов Республики Беларусь, регламентирующих вопросы обеспечения безопасности информации.

Состав работ по проектированию СЗИ определен пунктом 7 Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 №62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 11.10.2017 №64).

Требования безопасности для проектируемой ЛВС должны быть определены в задании по безопасности на ЛВС и включать в себя требования безопасности, определенные в приложении 1 к указанному Положению для класса типовой информационной системы, к которому будет отнесена ЛВС согласно СТБ 34.101.30-2017 при проведении классификации ЛВС как информационной системы.

В ходе проектирования СЗИ должна быть разработана проектная документация на СЗИ, состав и содержание которой должны быть достаточными для представления доказательств соответствия СЗИ УГО, определенному заказчиком в соответствии с СТБ 34.101.3-2014.

Все средства защиты информации, в том числе средства криптографической защиты информации, предполагаемые к использованию в СЗИ, должны иметь сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь.

11. При подготовке заданий на закупку, разработку и дооснащение (увеличение количества рабочих мест) МИС обеспечить выполнение следующих требований:

11.1. ВС должна соответствовать требованиям, предъявляемым Министерством здравоохранения Республики Беларусь к информационным системам, которые эксплуатируются в медицинских учреждениях РБ.

11.2. МИС должна быть зарегистрирована в соответствии с требованиями законодательства РБ, в том числе Постановления Совета Министров Республики Беларусь от 26 мая 2009 г. № 673.

11.3. Система защиты информации (СЗИ) МИС должна быть аттестована в соответствии с Положением о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 «О некоторых вопросах технической и криптографической защиты информации».

11.4. МИС должна осуществлять формирование медицинских документов в соответствии с требованиями Приказа Министерства здравоохранения РБ от 25.05.2018 № 536.

11.5. МИС должна обеспечивать возможность использования ЭЦП РУЦ ГосСУОК для аутентификации и подпис и электронных документов, файлов и частей документов.

11.6. МИС должна в качестве основно го функционального стандарта использовать действующую интегральную версию стандарта «Fast Health Interoperability Resources» (HL7 FHIR) Release 3 (STU v3.0.1-11917) или более позднюю (Приказ Министерства здравоохранения РБ от 08.10.2018 № 1001).

11.7. При разработке (поставке) программного обеспечения должно быть проведено его тестирование и валидация на соответствие основному функциональному стандарту HL7 FHIR с представлением соответствующего протокола.

В случае невозможности выполнения требований, изложенных в п. 11.6 – 11.7, в договоре на создание (поставку) МИС должно содержаться обязательство исполнителя (поставщика) в течении 12 месяцев с момента заключения договора доработать МИС на соответствие профилю стандарта HL7 FHIR и предоставить соответствующий протокол валидации.

12. Финансирование вышеперечисленных работ осуществляется следующим образом:

12.1. Для организаций здравоохранения, включаемых в проект «Модернизация системы здравоохранения Республики Беларусь»:

- по п.п. 1, 2, 5 – за счет бюджетных и иных не запрещенных законодательством источников.
- по п.п. 3 – 4, 6 – 8 – за счет средств Проекта.

12.2. Для прочих организаций здравоохранения – все работы производятся за счет бюджетных и иных не запрещенных законодательством источников.

Приложение 1

Требования
к оборудованию помещения для размещения
центрального телекоммуникационного узла ОЗ

ТКП 45-4.04-27-2006* (02250)
(Устройства связи и диспетчеризации инженерного оборудования жилых и общественных зданий. Правила проектирования)

1. Минимальная площадь — 6 $м^2$.
2. Минимальная высота от пола до выступающих частей конструкций перекрытия — не менее 2,5 м.
3. Нормативная нагрузка на перекрытия от оборудования не должна превышать несущей способности плит перекрытия.
4. Тип покрытия пола — линолеум либо аналогичный материал, не образующий пыль.
5. Внутренняя отделка стен – антистатический материал, не образующий пыль.
6. Не допускается расположение телекоммуникационного узла под санузлами и другими сырыми помещениями. При возможности выбора предпочтение следует отдавать помещениям без окон.
7. Электроосвещение необходимо выполнять в соответствии с требованиями ТКП 45-2.04-153 (для телекоммуникационных помещений).
8. По возможности исключить отопление телекоммуникационного узла. При невозможности отключить радиаторы отопления.
9. Температуру в помещении телекоммуникационного узла следует принимать в диапазоне 18°-24°С.
10. Помещение телекоммуникационного узла должно быть оборудовано системой кондиционирования. Допустимая относительная влажность при температуре 20°С должна быть не более 65%.
11. Электропитание телекоммуникационных шкафов и стоек должно осуществляться от самостоятельной сети электропитания устройств ЛВС (при наличии двух вводов в здание — после АВР).
12. Электропитание серверов и активного сетевого оборудования должно осуществляться от источников бесперебойного электропитания, подключенных к самостоятельной сети электропитания устройств ЛВС.
13. Рекомендуется установка сетевой камеры видеонаблюдения в телекоммуникационный узел с хранением видеоархива 30 дней.

Приложение 2

Минимальные требования к активному сетевому оборудованию и кабельной системе при разработке проектной документации для построения(модернизации) ЛВС в объекте информатизации

Наименование активного сетевого оборудования	**Сертифицированные программно-аппаратные средства криптографической защиты сетевого трафика в IP сетях**
Описание требований	**1. Общие требования к программно-аппаратным средствам криптографической защиты информации** (далее - ПАС КЗИ)**:** 1.1. Поставляемые средства должны иметь действующий сертификат соответствия требованиям технического регламента ТР 2013/027/BY. 1.2. Все поставляемые вместе со средствами лицензии должны быть бессрочными. **2. Технические требования к ПАС КЗИ**: Требования указываются при организации мероприятий по созданию системы защиты информации.
Наименование активного сетевого оборудования	**Сетевое оборудование для межсетевого экранирования и разграничения сетевого трафика**
Описание требований	**1. Общие требования к сетевому оборудованию для межсетевого экранирования и разграничения сетевого трафика:** - возможность организации в рамках одного устройства совместно прозрачных (L2/Transparent) и маршрутизируемых (L3/Routed) виртуальных контекстов; - протоколы маршрутизации – статическая маршрутизация, OSPF, BGP; - поддержка протоколов (BFD, VRRP) повышения готовности; - поддержка Telnet, SSH, SNMP, web- интерфейса для управления; - питание AC 220В; - наличие декларации о соответствии требованиям оборудования технического регламента Таможенного союза «О безопасности низковольтного оборудования» (ТР ТС 004/2011), технического регламента Таможенного союза «Электромагнитная совместимость технических средств» (ТР ТС 020/2011); - наличие сертификата соответствия СТБ 2156-2014 (п.п. 5.1.4.2, 5.4.1, 5.4.2, р.7);

	- наличие сертификата соответствия требованиям Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) и взаимосвязанным стандартам на дату выдачи ОАЦ сертификата соответствия. **2. Технические требования к оборудованию предоставления сетевых сервисов (межсетевой экран)***: - сетевые интерфейсы (не менее) – 5xGE RJ45 ports (1xWAN port, 4xSwitch ports); - поддержка функций: • межсетевой экран (FW); • система предотвращения вторжений (IPS); • контроль работы приложений (AC); • сервис веб-фильтрации (Web-Filtering); • сервис антивирус (AV). - производительность функций: • FW – не хуже 900 Mbps (для пакетов 1518/512/64 byte UDP); • IPS – не хуже 0,5/0,25 Gbps (Http/Enterprise Mix); • NGFW (FW/IPS/AC) – не хуже 0,20 Gbps (Enterprise Mix); • Threat Protection (FW/IPS/AC/AV) – не хуже 0.15 Gbps (Enterprise Mix). - поддержка не менее 5 независимых виртуальных контекстов, каждый из которых способен поддерживать функции FW, IPS, AC, AV; - монтажный комплект для установки в шкаф 19”. * представлены ориентировочные требования. Конкретные технические требования указываются при выполнении мероприятий создания системы защиты информации.
Наименование активного сетевого оборудования	**Сетевой маршрутизатор**
Описание требований	**1. Общие требования к сетевому маршрутизатору**: - возможность организации в рамках одного устройства совместно прозрачных (L2/Transparent) и маршрутизируемых (L3/Routed) виртуальных контекстов; - поддержка Telnet, SSH, SNMP, web-интерфейса для управления; - питание AC 220В; - сертификат соответствия требованиям технического регламента Таможенного союза «О безопасности низковольтного оборудования» (ТР ТС 004/2011), технического регламента Таможенного союза

	«Электромагнитная совместимость технических средств» (ТР ТС 020/2011); - сертификат соответствия СТБ 2156-2014. **2. Технические требования к сетевому маршрутизатору**: - сетевые интерфейсы (не менее) – 24 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+, 1 RPS port; - возможность объединения в стек до 8 устройств; - протоколы и стандарты: IEEE 802.1w, PVST+, IEEE 802.1Q, IEEE 802.3ad, Redundant Ports, M-LAG, RFC 3619 Ethernet Automatic Protection Switching (EAPS), sFlow, HTTPS, Syslog, SSH-2, SNMPv3, TACACS+, RADIUS, IEEE 802.1x, MAC Security, IP Security, Layer 2/3/4 Access Control Lists (ACLs), IP Broadcast Forwarding Control, SYN attack protection, CPU DoS Protection, Static Unicast Routes, Static Multicast Routes, RIP v1, RIP v2, поддержка Jumbo Frame; - неблокирующая матрица коммутации для полнодуплексного режима всех портов: • пропускная способность не менее 128 Gbps; • производительность не менее 95 Mpps; • емкость таблицы MAC адресов не менее 16K; • latency (64-byte) менее 4 микросекунд.
Наименование	**Кабельная система ЛВС**
Описание требований	Кабельные трассы в помещениях и корридорах, прокладываются в настенном пластиковом кабельном канале. При наличии подвесных конструкций потолка использовать крепежные кронштейны и/или металлические лотки, монтируемые выше уровня фальшпотолка с надежным креплением к капитальным перекрытиям. Взаимную прокладку с иными кабельными системами исключить. Обеспечить разнос в пространстве с иными кабельными системами не менее 15 см. Пересечение с кабельными трассами иных систем осуществлять под прямым углом. Выполнить инсталляцию кабельной системы с помощью материалов, на основе экранированного кабеля витая пара категории 5е, либо оптоволокна. ЛВС должна обеспечивать пропускную способность передачи данных 1000Мбит/с (Gigabit Ethernet) от коммутационных узлов до рабочих мест и 10000Мбит/с (10 Gigabit Ethernet) – от коммутационных узлов до центрального телекоммуникационного узла. Каждое рабочее место ЛВС со стороны пользователя оконечивается одинарной или двойной розеткой с экранированными разъемами RJ-45 категории 5, со стороны коммутационного узла патч-панелью. Количество

	информационных розеток, кабельных соединений различного вида определяется на этапе проектирования. Узлы коммутации (там, где это будет необходимо) расположить в специализированных запирающихся телекоммуникационных шкафах. Шкаф должен быть оборудован боковыми панелями, профилями, креплениями, вентиляторами, разводкой питания и органайзерами для разводки проводов от патч-панелей к коммутатору. Кабели от рабочих мест терминируются на патч-панели. Панели необходимо комплектовать органайзерами.

При проектировании необходимо учитывать, что количество активного сетевого оборудования должно определятся индивидуально проектировщиком на основании представленной Заказчиком (представителями Заказчика) информации о действующей инфраструктуре для каждого объекта информатизации. Допускаются проектные решения, в которых возможно объединение функций описанного выше сетевого оборудования, при условии соответствия требованиям сертификации в Республике Беларусь данного типа устройств.