

информационных систем в медицинских учреждениях для обеспечения интеграции с федеральными компонентами.

• Финансовое обеспечение создания иных региональных информационных систем в сфере здравоохранения, в том числе в части обеспечения их информационной безопасности, осуществляется за счет бюджетов субъектов РФ и территориальных фондов обязательного медицинского страхования.

Список литературы

1. Горюнова В.В. [и др.] Особенности проектирования интегрированных медицинских систем на основе концептуальных спецификаций // *Фундаментальные исследования*. – 2013 – №11-9 – С. 67-73.
2. Кухтевич И.И., Горюнова В.В., Горюнова Т.И. Практика проектирования и использования телеконсультационных центров неврологического профиля // *Фундаментальные исследования*. – 2014 – №11-11 – С. 1767-1773.
3. Горюнова В.В., Горюнова Т.И., Жилиев П.С. Многоуровневые структуры интегрированных медицинских систем // *Современные наукоемкие технологии*. – 2014 – №5-1 – С. 122-122.
4. Жилиев П.С., Горюнова Т.И., [и др.] Автоматизированные системы для организации профилактических осмотров населения // *Современные наукоемкие технологии*. – 2014 – №5-1 – С. 126-126.
5. Горюнова В.В. [и др.] Использование информационных технологий и концептуальных спецификаций при оценке качества жизни населения // *Современные наукоемкие технологии*. – 2014 – №5-1 – С. 130-131.
6. Горюнова В.В. Использование модульных онтологий при создании центров обработки данных медицинского назначения // *Инновации на основе информационных и коммуникационных технологий*. – 2011. – № 1. – С. 300-303.

МОДЕЛИ УГРОЗ И НАРУШИТЕЛЯ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Горюнова В.В., Володин К.И., Горюнова Т.И.

ФГОУ ВПО «Пензенский государственный технологический университет», Пенза, e-mail: gvv17@ya.ru

Разработка модели угроз и нарушителя должна проводиться на основе методических документов ФСТЭК и ФСБ по защите персональных данных, а также с учетом типизации государственных учреждений здравоохранения.

Методы и задачи исследований. При выполнении вышеперечисленных работ должны быть определены защищаемые объекты, основные угрозы безопасности, величины информационных рисков и сформированы предположения о возможностях проведения атак на информационные и телекоммуникационные ресурсы, определены совокупности условий и факторов, создающих опасность нарушения характеристик безопасности объектов, технических средств обработки и передачи информации, а также предположения об ограничении этих возможностей [1-4].

Модель угроз информационной безопасности должна определять:

- защищаемые объекты;
- основные угрозы безопасности информации, включая угрозы техногенного характера, стихийные бедствия и угрозы, реализуемые нарушителями;
- критерии уязвимости и устойчивости информационных систем к деструктивным воздействиям.

Модель нарушителя информационной безопасности должна определять:

- классификацию типов возможных нарушителей информационной безопасности;
- предположения об имеющейся у нарушителя информации;
- основные каналы, цели и объекты атак;
- предположения об имеющихся у нарушителя средствах;
- перечень атак.

Между подсистемами централизованного сбора и корреляции событий безопасности и централизованного управления средствами защиты информации

должна быть обеспечена возможность интеграции в целях реализации возможности автоматизированного управления настройками средств защиты информации на основе собираемых данных о событиях безопасности.

Список литературы

1. Горюнова В.В. [и др.] Особенности проектирования интегрированных медицинских систем на основе концептуальных спецификаций // *Фундаментальные исследования*. – 2013 – №11-9 – С. 67-73.
2. Горюнова В.В., Горюнова Т.И., Жилиев П.С. Многоуровневые структуры интегрированных медицинских систем // *Современные наукоемкие технологии*. – 2014 – №5-1 – С. 122-122.
3. Жилиев П.С., Горюнова Т.И., [и др.] Автоматизированные системы для организации профилактических осмотров населения // *Современные наукоемкие технологии*. – 2014 – №5-1 – С. 126-126.
4. Горюнова В.В. Использование модульных онтологий при создании центров обработки данных медицинского назначения // *Инновации на основе информационных и коммуникационных технологий*. – 2011. – № 1. – С. 300-303.

СПЕЦИФИКАЦИИ И ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ТИПОВОМУ АВТОМАТИЗИРОВАННОМУ РАБОЧЕМУ МЕСТУ МЕДИЦИНСКОГО РАБОТНИКА

Горюнова Т.И., Вырыпаева А.В., Савина Т.А.

ФГОУ ВПО «Пензенский государственный технологический университет», Пенза, e-mail: gvv17@ya.ru

Типовое автоматизированное рабочее место медицинского работника (далее АРМ МР) – это специализированный защищенный персональный настольный компьютер с комплектом предустановленного и настроенного системного и прикладного программного обеспечения, располагающийся непосредственно на рабочем месте медицинского работника, снабженный необходимым периферийным оборудованием и обеспечивающий возможность эффективного взаимодействия медицинского работника с локальным и удаленным программным обеспечением и информационными ресурсами, необходимыми для выполнения им своих обязанностей.

Спецификации и требования к оборудованию.

1. Детальные технические, качественные и количественные требования к АРМ МР должны быть приведены в разделе «Спецификация».
2. Все оборудование должно иметь необходимые сертификаты, выданные в соответствии с законодательством Российской Федерации.
3. Оборудование, все его компоненты, а также используемые материалы должны быть новыми, не бывшими в эксплуатации.
4. Предлагаемое к поставке оборудование должно иметь количественные и качественные показатели не хуже, чем это указано в Спецификации [1-2].
5. Качество предлагаемой к поставке продукции и гарантийного обслуживания должно обеспечиваться системой управления качеством при производстве, монтаже и обслуживании персональных компьютеров, сертифицированной на соответствие требованиям ГОСТ РФ.
6. В случае, если в технических требованиях указаны конкретные производители, торговые марки, фирменные наименования, модели или источники происхождения, предложение к поставке аналогов допускается только с учетом возможности взаимодействия всего включенного в заявку оборудования между собой. При этом, качественные и количественные характеристики эквивалента должны быть равны или превосходить значения, указанные в технических требованиях.
7. Предлагаемые к поставке программно-технические комплексы должны быть полностью совместимы между собой на программном и аппаратном уровнях, иметь идентичный программный интерфейс. Все предлагаемые к поставке комплексы должны позволять обеспечивать санкционированный удаленный

доступ для осуществления администрирования и обслуживания комплексов в целом и каждого рабочего места в отдельности.

8. Предлагаемое к поставке оборудование должно соответствовать действующим стандартам и нормам по пожарной, санитарной и электрической безопасности, а также электромагнитной совместимости, в соответствии с номенклатурой продукции, в отношении которой законодательными актами Российской Федерации предусмотрена обязательная сертификация, с документальным подтверждением при исполнении Государственного контракта.

9. Участник размещения заказа должен указать в аукционной заявке конкретную торговую марку (включая производителя) и модель предлагаемой к поставке продукции, включая коды производителя, ее комплектацию и точные технические характеристики, а также полные наименования и версии предлагаемого к поставке программного обеспечения, в том числе и предустановленного на какое-либо оборудование. Каждая единица оборудования или программного обеспечения, входящая в состав предлагаемых к поставке товаров (комплектов или иной совокупности товаров), являющаяся отдельно производимым товаром, также должна быть представлена участником размещения заказа описанием с указанием кода производителя, торговой марки (включая производителя) и модели. В описании технических характеристик Участник указывает фактические сведения (точные значения технических характеристик и описание функциональных свойств, к которым установлены требования в документации об аукционе), соответствующие конкретным товарам, предлагаемым к поставке. Указание приблизительных значений (не более или не менее) не допускается.

Заключение. Условия эксплуатации предлагаемого к поставке оборудования являются обычными для рабочих помещений. Оборудование и программное обеспечение, надлежащим образом не представленное, считается не включенным в заявку участника размещения заказа (не предложенным к поставке). Вычислительная техника, кроме того, должна содержать полные наименования (торговые марки, коды производителей и модели) материнских плат, процессоров, оперативной памяти, НЖМД (накопитель на жестком магнитном диске), приводов чтения/записи/перезаписи оптических дисков, видеоадаптеров, клавиатур, манипуляторов типа «мышь», устройств чтения («ридеров») смарт-карт, а также любых других дополнительных контроллеров и устройств.

Список литературы

1. Горюнова В.В. [и др.] Особенности проектирования интегрированных медицинских систем на основе концептуальных спецификаций // *Фундаментальные исследования*. – 2013 – №11-9 – С. 67-73.
2. Горюнова В.В. Использование модульных онтологий при создании центров обработки данных медицинского назначения // *Инновации на основе информационных и коммуникационных технологий*. – 2011. – № 1. – С. 300-303.

НАЗНАЧЕНИЕ И ФУНКЦИИ СИСТЕМ ИНТЕГРИРОВАННОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИИ

Горюнова В.В., Порошин Д.П., Снопкова Е.В., Баулина О.В.

ФГОУ ВПО «Пензенский государственный технологический университет», Пенза, e-mail: gvv17@ya.ru

Система интегрированной медицинской информации (СИМИ) представляет собой централизованную информационную систему, размещаемую на обособленных централизованных вычислительных мощностях в составе областного центра обработки данных. Доступ к сервису конечных пользователей

амбулаторно-поликлинического звена системы здравоохранения города должен осуществляться через подсистему формирования пользовательского интерфейса с использованием технологии «тонкого клиента» [1-5].

Методы и задачи. Общегородской информационной сервис СИМИ, обеспечит консолидацию медицинской информации о пациентах в составе их интегрированных электронных медицинских карт. Под интегрированной электронной медицинской картой (далее – ИЭМК) понимается единое хранилище медицинской информации гражданина по всем обследованиям и случаям обращения гражданина в медицинские учреждения города. В составе ИЭМК будут содержаться следующие информационные разделы:

- Регистрационный идентификатор пациента;
 - Витальные медицинские данные (группа крови, наличие аллергий и лекарственной непереносимости, хронические заболевания, инвалидность пр.);
 - Эпизоды (амбулаторные обращения, госпитализации). В отношении госпитализаций, в составе ИЭМК предполагается хранение только значимой информации, представленной в выписном эпикризе. Доступ к более детальной информации карты стационарного больного будет реализован посредством автоматизированного запроса данных из МИС стационара;
 - Персональные электронные медицинские записи (врачебные осмотры, диагнозы, записи медсестер, протоколы исследований);
 - Медицинские мультимедийные данные (результаты функциональных исследований – рентген, томография, УЗИ, сканы бумажных документов);
 - Назначения (диагностические и лечебные манипуляции, медикаменты);
 - Данные лабораторных анализов.
- Заключение. Сервис СИМИ реализует следующие основные операции над данными ИЭМК:
- создание ИЭМК гражданина;
 - поиск ИЭМК в базе по задаваемым критериям;
 - доступ к информационным блокам медицинской информации (например, к блокам врачебного осмотра пациента, госпитализации и пр.);

Список литературы

1. Горюнова В.В. [и др.] Особенности проектирования интегрированных медицинских систем на основе концептуальных спецификаций // *Фундаментальные исследования*. – 2013 – №11-9 – С. 67-73.
2. Горюнова В.В., Горюнова Т.И., Жилиев П.С. Многоуровневые структуры интегрированных медицинских систем // *Современные наукоемкие технологии*. – 2014 – №5-1 – С. 122-122.
3. Горюнова В.В. Использование модульных онтологий при создании центров обработки данных медицинского назначения // *Инновации на основе информационных и коммуникационных технологий*. – 2011. – № 1. – С. 300-303.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ И СЕРВИСОВ В СФЕРЕ ЗДРАВООХРАНЕНИЯ

Жилиев П.С., Горюнова Т.И., Володин К.И.

ФГОУ ВПО «Пензенский государственный технологический университет», Пенза, e-mail: gvv17@ya.ru

Региональный фрагмент Единой государственной информационной системы в здравоохранении города представляет собой распределенную информационную систему, надлежащим образом интегрированную с соблюдением требований по защите информации как с Федеральным фрагментом Единой государственной информационно-аналитической системы (ЕМИАС) в здравоохранении, так и с общегородской информационной инфраструктурой города [1-4].

Надлежащее функционирование прикладных компонент обеспечивается за счет единого инфраструктурного уровня, который сформирован преимущественно на принципах централизации инфра-