Для реализации всех необходимых базовых функций по защите информации, предоставляемых защищенным окружением в состав систем должны входить следующие подсистемы:

– Подсистема защиты от DDoS, обеспечивающая функции защиты информационных сервисов от атак типа «отказ в обслуживании», направленных на блокирование работы сервисов.

– Подсистема защиты межсетевого взаимодействия, обеспечивающая функции сетевого разграничения различных информационных ресурсов и сервисов, а также их защиту от сетевых атак при взаимодействии между собой, сетями общего доступа и смежными ИС.

– Подсистема антивирусной защиты и защиты от спама, обеспечивающая функции защиты инфраструктуры и информационных систем от различного рода вредоносного программного обеспечения.

– Подсистема защиты прикладных систем, обеспечивающая функции защиты различных web приложений и баз данных от атак направленных на данные компоненты информационных систем с целью получения несанкционированного доступа к защищаемой информации и др.

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., Жиляев П.С. Многогоуровневые структуры интегрированных медицинских систем // Современные наукоемкие технологии. – 2014 –№5-1 – С. 122-122.

4. Жиляев П.С., Горюнова Т.И., [и др.] Автоматизированные системы для организации профилактических осмотров населения // Современные наукоемкие технологии. – 2014 –№5-1 – С. 126-126.

ТИПОВЫЕ ТЕХНОЛОГИЧЕСКИЕ И РЕСУРСНЫЕ ИНФОРМАЦИОННЫЕ МЕДИЦИНСКИЕ СИСТЕМЫ

[1]Горюнова В.В., [1]Горюнова Т.И., [2]Гапиенко Т.О., [1]Жиляев П.С.

[1]ФГОУ ВПО «Пензенский государственный технологический университет», Пенза, e-mail:gvv17@ya.ru;
[2]ГОУ ДПО «Пензенский институт усовершенствования врачей Минздравсоцразвития России, Пенза, e-mail:gvv17@mail.ru

Основная характеристика технологических информационных медицинских систем. Для данных медицинских информационных систем объектом описания является человек (пациент), пользователем – медицинский работник (врачи, лаборанты, медицинские сестры медицинских учреждений), информация интегрируется на уровне 1 пациента, решаемой социальной задачей – обеспечение автоматизации процесса сбора и обработки биомедицинской информации для диагностики состояния человеках[1-2].

Классификация технологических информационных медицинских систем может быть представлена следующим образом:

I. АСКЛИ – автоматизированные системы клинико-лабораторных исследований, включая программно-аппаратные комплексы, предназначенные для функциональной, лучевой и лабораторной диагностики;

II. АСКВД – автоматизированные системы консультативно-вычислительной диагностики, включая системы, основанные на методах математической статистики, экспертные системы и телемедицинские консультативные системы;

III. АСВЛТ – автоматизированные системы выбора лечебной тактики, расчета доз медикаментов или режима лучевого воздействия, физиотерапевтического лечения и др.;

IV. АСПИН – автоматизированные системы постоянного интенсивного наблюдения для послеоперационных палат, реанимационных отделений, ожоговых центров и т.д.;

V. АСПОН – автоматизированные системы профилактических осмотров населения.

Основная характеристика ресурсных информационных медицинских систем:

Сущность пользования данными системами сводится к информационному обеспечению отношений экономистов и бухгалтеров учреждений здравоохранения и руководителей этих учреждений, а также аналогичных сотрудников вышестоящего органа управления здравоохранением. Для данных информационных систем объектом описания являются финансовые документы, лекарства, материально-технические средства медицинского назначения, пользователями – менеджеры, финансовые работники лечебно-профилактических учреждений и органов управления здравоохранением, информация агрегируется по иерархическим уровням объектов и субъектов здравоохранения; решаемой социальной задачей – автоматизация планирования учета и отчетности объектов и субъектов здравоохранения [3-6].

Ресурсные информационные медицинские системы (РИМС) могут быть классифицированы следующим образом:

I. АСФОБ – автоматизированные системы финансового обеспечения,включая планирование бюджета, формирование программ госгарантий субъектов РФ и муниципальных ОУЗ, обеспечение текущего накопительногоучета расходов и формирование итоговой отчетности учреждениями здравоохранения, СМО и фондами ОМС;

II. АСКОБ – автоматизированные системы краткосрочного и среднесрочного планирования воспроизводства медицинских работников по профилям их деятельности;

III. АСМОБ – автоматизированные информационные системы медикаментозного обеспечения населения, включая льготников, а также планирования производства, закупки и распределения по территориальным аптечным складам, ЛПУ, аптечной сети;

IV. АСМТО – автоматизированные системы планирования производства, закупок и распределения изделий медицинской промышленности.

При разработке МИС также должна быть обеспечена поддержка конкуренции среди производителей медицинских информационных систем; информационных систем, автоматизирующих административно-хозяйственную деятельность медицинских организаций, а также иных специализированных прикладных информационных систем, создание и развитие которых может финансироваться за счет частных инвестиций в условиях конкурентного рынка.

Ресурсное обеспечение создания и сопровождения единой медицинской информационной системы предполагает:

• Финансовое обеспечение создания Федерального центра обработки данных (ЦОДа), а также временной площадки Федерального ЦОДа, в т.ч. в части обеспечения информационной безопасности, разработки и размещения на ней основных централизованных общесистемных компонентов.

• Финансовое обеспечение создания и внедрения региональных прикладных компонентов, обеспечения подключения медицинских учреждений к сети Интернет, их оснащения компьютерным, телекоммуникационным оборудованием и средствами информационной безопасности, а также внедрение федеральных транзакционных систем и доработка существующих

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. 1**767-1773.

3. Горюнова В.В., Горюнова Т.И., Жиляев П.С. Многогоуровневые структуры интегрированных медицинских систем // Современные наукоемкие технологии. – 2014 –№5-1 – **С.** 122-122.

4. Жиляев 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 ограничениях 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., Жиляев П.С. Многогоуровневые структуры интегрированных медицинских систем // Современные наукоемкие технологии. – 2014 –№5-1 – С. 122-122.

3. Жиляев 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