

# Защита информационной инфраструктуры медицинского учреждения

## ключевые слова

информатизация здравоохранения, АРМ, медицинская информационная система, ЦОД

С.Д. Рябко,  
канд. физ.-мат. наук,  
президент группы  
компаний "С-Терра"



Написать автору  
[www.zdrav.ru](http://www.zdrav.ru)

ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ В ПРАКТИКУ МЕДИЦИНСКИХ ОРГАНИЗАЦИЙ НАПРАВЛЕНО НА БОЛЕЕ ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ ЛПУ, УЛУЧШЕНИЕ ВЗАИМОДЕЙСТВИЯ МЕЖДУ РАЗЛИЧНЫМИ ПОДРАЗДЕЛЕНИЯМИ, МАКСИМАЛЬНУЮ АВТОМАТИЗАЦИЮ РАБОЧИХ ПРОЦЕССОВ.

ПРИ ЭТОМ С ЭТИЧЕСКОЙ И ЮРИДИЧЕСКОЙ ТОЧЕК ЗРЕНИЯ КРАЙНЕ ВАЖНО ОБЕСПЕЧИТЬ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ДАННЫХ. В СООТВЕТСТВИИ С ДЕЙСТВУЮЩЕЙ НОРМАТИВНО-ПРАВОВОЙ БАЗОЙ ИМЕННО ОРГАНИЗАЦИЯ – ОПЕРАТОР ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСЕТ ОТВЕТСТВЕННОСТЬ ЗА ЗАЩИТУ ДАННЫХ ПАЦИЕНТА.

В МАСШТАБАХ СТРАНЫ ОРГАНИЗОВАН КОНТРОЛЬ ЗА АТТЕСТАЦИЕЙ СИСТЕМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ЧТО ДЕЛАЕТ ВЕСЬМА АКТУАЛЬНОЙ ЗАДАЧУ ПРОЕКТИРОВАНИЯ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ СРАЗУ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ И НА ОСНОВЕ СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.

К рабочим местам специалистов в медицинских учреждениях предъявляются специфические требования.

**1. Простота эксплуатации** как для пользователя, так и для оператора. Врач и средний медицинский персонал, использующие средства информатизации, не должны испытывать затруднений при работе с ними. Для оператора, обеспечивающего эксплуатацию системы, простота позволяет гарантировать работоспособность систем массового обслуживания.

**2. Специализация.** Унифицированные рабочие места должны "подстраиваться" под разные условия использования: клинико-диагностические лаборатории, кабинеты функциональной диагностики, регистратуры, рабочие места врачей-специалистов и т.д.

**3. Централизация** – обеспечение доступа к ресурсам из любой точки системы. Возможность внесения данных осмотра, результатов обследований и консультативных приемов должна существовать у врача-специалиста как на рабочем месте, так и при вызове на дом, у бригады скорой медицинской помощи при

**БОЛЬНИЦЫ, ПОЛИКЛИНИКИ, ГОСПИТАЛИ, АМБУЛАТОРИИ И ПРОЧИЕ ЛЕЧЕБНЫЕ УЧРЕЖДЕНИЯ КАК ОПЕРАТОРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛУЧИЛИ ДОПОЛНИТЕЛЬНЫЕ ОГРАНИЧЕНИЯ И ТРЕБОВАНИЯ, КОТОРЫХ НЕТ У БОЛЬШИНСТВА ИНЫХ ОПЕРАТОРОВ. СВЕДЕНИЯ О СОСТОЯНИИ ЗДОРОВЬЯ И ИНТИМНОЙ ЖИЗНИ БЫЛИ ОТНЕСЕНЫ ЗАКОНОМ К СПЕЦИАЛЬНЫМ КАТЕГОРИЯМ ПЕРСОНАЛЬНЫХ ДАННЫХ.**

М. Емельянников, директор по развитию бизнеса ЗАО НИП "Информзащита"

выезде к пациенту, у врачей клинико-диагностической лаборатории, кабинета функциональной диагностики, у врачей-консультантов. Выполнение указанного требования обеспечивает полноту и актуальность данных пациента, что будет особенно важно при повсеместном запуске "электронных историй болезни".

**4. Надежность.** В медицинской практике, особенно когда требуется срочное принятие решений и быстрый доступ к данным пациента (уточнение наличия сопутствующих заболеваний, аллергологического анамнеза и пр.), недопустим отказ средств информатизации.

**5. Мультимедийность** – одновременное воспроизведение визуальной, звуковой и прочей информации, взаимно дополняющей друг друга. Это позволяет проводить удаленные консультации с созданием максимально "объемной" передачи данных (телемедицина).

**6. Персонализация** – свойства рабочей среды должны соответствовать функционалу специалиста, использующего ее.

**7. Сервисопригодность решения** – комплекс требований, выполнение которых обеспечивает возможность технического обслуживания средств информатизации в режиме услуги, предоставляемой преимущественно дистанционно внешним по отношению к ЛПУ подразделением или эксплуатационной организацией.

**8. Соблюдение требований информационной безопасности** в соответствии с действующим законодательством Российской Федерации.

С соблюдениями всех перечисленных требований была разработана защищенная инфраструктура, в которой могут работать медицинские информационные системы (далее – МИС).

Информационным ядром архитектуры является центр обработки данных (далее – ЦОД), в котором располагаются серверы медицинских приложений, а также элементы инфраструктуры доступа и безопасности. Централизация медицинских программ и данных обеспечивает их повсеместную доступность с различных ра-

## Оценка рисков



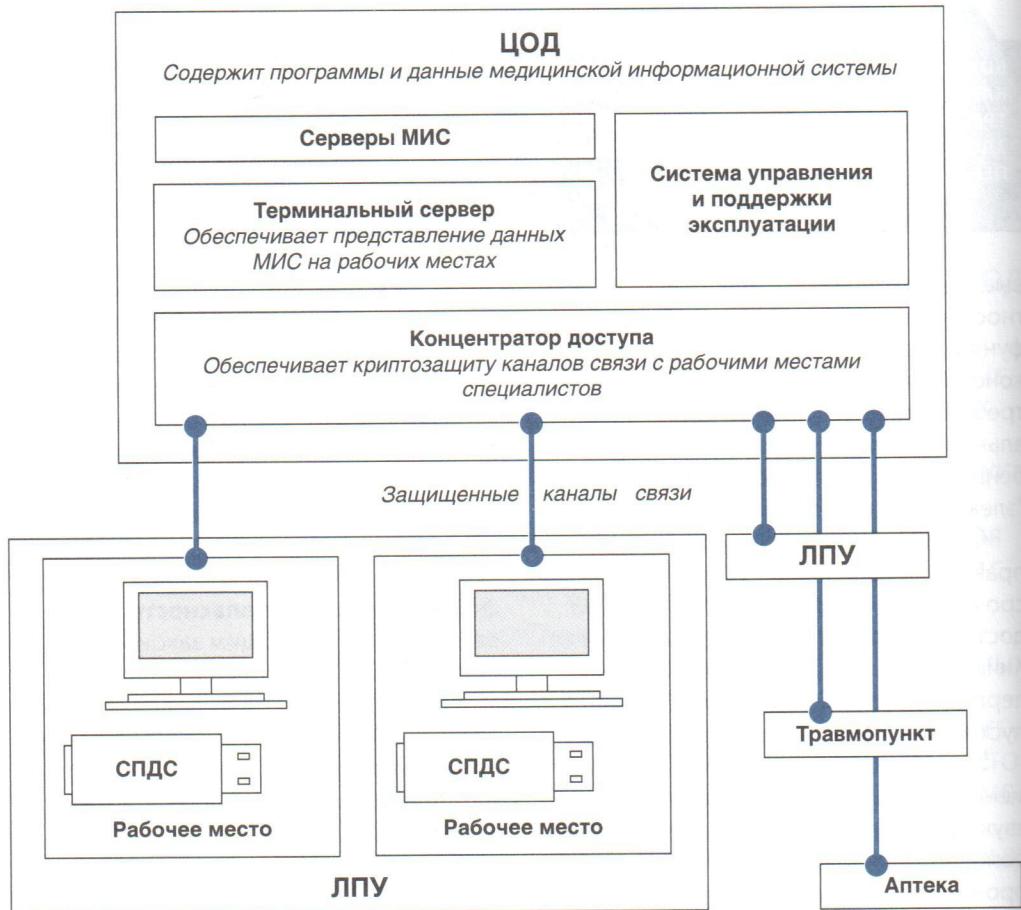
ПРИ ПОСМЕННОЙ РАБОТЕ СПЕЦИАЛИСТОВ, ИСПОЛЬЗУЮЩИХ ДЛЯ ВЕДЕНИЯ ДОКУМЕНТАЦИИ ОДИН КОМПЬЮТЕР, РАЗМЫВАЕТСЯ ОТВЕТСТВЕННОСТЬ ЗА ЗАЩИТУ ИНФОРМАЦИИ



ПОРАЖЕНИЕ КОМПЬЮТЕРИЗОВАННОГО РАБОЧЕГО МЕСТА ВИРУСАМИ ПРИ УСТАНОВЛЕНИИ ПОЛЬЗОВАТЕЛЕМ ПОСТОРОННИХ СЕТЕВЫХ СОЕДИНЕНИЙ



ОТСУСТВИЕ У МЕДИЦИНСКОГО ПЕРСОНАЛА КОМПЕТЕНЦИЙ, НЕОБХОДИМЫХ ДЛЯ ЭКСПЛУАТАЦИИ ЗАЩИЩЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ И СРЕДСТВ КРИПТОГРАФИИ



бочих мест, надежное хранение, возможность перераспределения ресурсов системы пропорционально запросам пользователей и значительную экономию средств при эксплуатации системы.

Для работы пользователей в системе применяется технология среды построения доверенного сеанса (далее – СПДС).

**Важно** Использование технологии СПДС необходимо для предотвращения утечек информации как по сети, так и из-за уязвимостей рабочего места специалиста ■

Необходимость применения технологии доверенного сеанса продиктована тем, что при доступе в медицинскую ин-

формационную систему со стационарного компьютера в кабинете врача практически невозможно обеспечить защиту информации:

- при посменной работе специалистов на одном и том же рабочем месте исчезает "хозяин", ответственный за его состояние;
- большой поток посетителей и персонала, ежедневно проходящий через кабинет, несет неконтролируемые угрозы;
- возможна компрометация рабочего места за счет вирусопоражения при установлении посторонних сетевых соединений и т.п.;
- не исключено безответственное пове-

дение персонала (по окончании смены не завершают сеанс, оставляют кабинет открытым и пр.);

- отсутствие у медицинского персонала компетенций, необходимых для эксплуатации защищенной информационной системы и средств криптографии, создает дополнительные угрозы информационной безопасности системы. Устранить эти угрозы можно следующим образом. Каждое рабочее место оснащается унифицированным оборудованием. Оптимальный выбор – бездисковая рабочая станция, исключающая загрузку любой операционной среды, кроме СПДС. Нарушитель безопасности, например случайный посетитель, не может ее как-либо атаковать, потому что не сможет ее загрузить, а даже если бы смог – то не нашел бы в ней информационных объектов для атаки.

“Личное” информационное наполнение каждого рабочего места каждый специалист носит с собой на специальном защищенном USB-носителе. Придя на работу, специалист устанавливает носитель СПДС в USB-порт, вводит уникальную комбинацию символов (PIN-код) и загружает персональную среду функционирования – операционную систему, специально подготовленную и снабженную криптографическими средствами для аутентификации, защиты данных и защиты канала связи.

**Важно** Носитель СПДС защищен от хищения и неправомерного использования посторонними лицами. При пятикратном введении неверного PIN-кода устройство блокируется ■

При этом для каждого специалиста выпускается индивидуальный носитель, содержащий его “личный” состав приложений. Тем самым для каждого пользователя создается персонализированная рабочая среда. Состав приложений будет

## ШИРОКОЕ ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАКТИКУ АПУ ТРЕБУЕТ БОЛЕЕ ПРИСТАЛЬНОГО ВНИМАНИЯ К ВОПРОСАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

различным, например, для сотрудника регистратуры и для врача-специалиста. Рабочее место врача-терапевта может отличаться от рабочего места врача-хирурга. В то же время врач-терапевт, работая временно в кабинете врача-хирурга, получит на “чужой” рабочей станции свой личный состав приложений.

**Важно** Среда сохраняет свое состояние между сеансами: при входе в систему ее состояние то же, что и при завершении работы в предыдущем сеансе ■

При этом унификация и типизация рабочих мест не ограничивает применения неунифицированной, специализированной периферии. Так, для решения простых задач (работа регистратуры, ведение учета, доступ к информационным приложениям и справочникам) в рабочей среде могут использоваться веб-приложения, хранящиеся в ЦОД. Но если специалистам для работы требуется определенный набор приложений и оборудования, например, экран повышенного разрешения, подключение аппарата УЗИ, цветного принтера, кардиоридера и т. д., то на рабочее место устанавливается требуемое оборудование и необходимые для его работы программы включаются в состав среды функционирования.

Рабочее место специалиста связано с ЦОД защищенным каналом. Это обеспечивает полную сетевую изоляцию рабочей среды врача. Данные, передаваемые по сети, не подвержены перехвату и искаражению. Также исключены контакты с посторонними сайтами, с которых в ме-

дицинскую информационную систему могут поступать опасные объекты (вирусы, черви) или осуществляться иные атаки.

Архитектура открыта для применения медицинской электронной карты пациента (при наличии кард-ридера).

**Важно** Технологически продукты СПДС готовы к работе с "электронной историей болезни", и в случае принятия соответствующих отраслевых стандартов все инвестиции в защищенную инфраструктуру будут сохранены ■

В основе всех средств защиты СПДС – сертифицированные российские криптографические алгоритмы, рекомендованные к применению в информационных системах обработки персональных данных до высшего класса К1 включительно.

Интересным дополнительным преимуществом СПДС как технологии безопасности является простота эксплуатации. Важнейшие информационные компоненты системы сосредоточены в двух местах: в ЦОД и составе среды на специальном но-

сителе. Ресурсы ЦОД поддерживает квалифицированный персонал ЦОД. Полный комплекс сопровождения персонализованных носителей, включая замену криптографических ключей и обновление программного обеспечения, обеспечивается в автоматическом режиме дистанционно с централизованной платформы, например, из того же ЦОД.

Эта функциональность обеспечивает возможность разделения полномочий между разными организациями. Так, одна компания может отвечать за функционирование ЦОД, а другая (например, специализированный сервис-провайдер) предоставлять услуги защищенной связи, поддержки жизненного цикла ключевых документов, управления и мониторинга, подготовки и сопровождения парка используемого оборудования (бездисковые рабочие станции, продукты СПДС).

Сервисная модель экономически эффективна, она снимает с медицинского учреждения нагрузку по содержанию оборудования и избыточного персонала эксплуатации, а также избавляет от необходимости получения лицензии ФСБ России на услуги по шифрованию данных.