Евгений Жарчинский:

Здравоохранению необходимы унифицированные и простые решения

Как защитить персональные данные граждан в медицинских учреждениях? Об этом в интервью CNews рассказал Евгений Жарчинский, руководитель департамента продаж «С-Терра СиЭсПи».

CNews: Насколько, по вашему мнению, изменилась ситуация в области информатизации здравоохранения в последнее время? Появился ли у медицинских организаций реальный интерес к ИТ-решениям?
Евгений Жарчинский: Развитие систем информатизации, в частности, с целью обеспечения здоровья граждан и решения задач здравоохранения, определяется сегодня многими стандартами и нормативами, в основу которых закладываются потребности и интересы медицинских учреждений.
Медицинские учреждения проявляют реальный интерес к ИТ-решениям. В последнее время проводятся сотни конкурсов по информатизации учреждений здравоохранения Российской Федерации, при этом выделяются сотни миллионов рублей для реализации проектов в сфере ИТ.

CNews: Значительная часть информации, с которой работают учреждения здравоохранения, является персональными данными граждан. Как вы оцениваете их готовность к обеспечению безопасности этих сведений в настоящее время?
Евгений Жарчинский: С уверенностью можно сказать, что все учреждения системы здравоохранения относятся к операторам персональных данных. Они оперируют сведениями, относящимися к врачебной тайне, большая часть которых позволяет идентифицировать человека. Такой вывод основывается на положениях Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных». Согласно ст. 3 закона, персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). А оператором является государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и/или осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия, совершаемые с персональными данными.
Развитие сотрудничества с учреждениями системы здравоохранения, компаниями-разработчиками медицинских информационных систем (МИС), привело к пониманию того, что решения сетевой защиты, предлагаемые в медицинские учреждения, должны отличаться рядом особенностей. Прежде всего, необходимо унифицированное и типизированное решение, которое, к тому же, является простым в пользовании и эксплуатации.

При этом стоит учитывать специализацию медицинских работников. В кабинете врача, в рентгенкабинете, в аптеке, в салоне «скорой помощи» требуются разные средства информатизации. Практика использования МИС приводит к централизации системы. Необходимо избежать накладок и потери данных, важно не потерять целостность истории болезни пациента. Выдвигаются повышенные требования надежности – экстренная медицина не терпит отказа средств информатизации, требования мультимедийности – телемедицина становится повседневной практикой, требования персонализации – у разных специалистов своя рабочая среда и своя зона ответственности.

Одно из непростых требований, которое предъявляется к решениям – сервисопригодность. Как правило, учреждения медицины не имеют специализированых подразделений ИТ, ИТ-услуги они получают от внешних компаний. А это также составляет особый набор технических требований.

CNews: Какие меры, по вашему мнению, необходимы, чтобы обеспечить безопасность персональных данных в медучреждениях?
Евгений Жарчинский: Мы исходили из того, что рабочее место врача в определенном смысле бесхозно. В кабинетах многих медицинских учреждений организована посменная работа. Информационную поддержку врача часто выполняет медсестра или его ассистент. Между сменами кабинет не всегда заперт. В нем могут бывать самые разные люди, от штатных медицинских работников до случайно заглянувших пациентов. В этих условиях трудно защитить рабочее место даже от непреднамеренных нарушений. При этом нельзя исключать действия, которые может предпринять проникший в кабинет врача злоумышленник.
Медицинские работники, как правило, не обладают квалификацией для корректной эксплуатации защищенной информационной системы. Их ошибки могут привести к нарушению функциональности и защищенности. Возникает необходимость упрощения их рабочей среды.

Необходимо учесть, что сетевая среда рабочего места врача может быть незамкнута. При этом могут быть установлены опасные посторонние соединения. Это создает угрозу вирусопоражения, руткитов и внедрения закладок, а после их установки - осуществления атаки на медицинскую информационную систему в целом. Безусловно, не обойтись без организационных мер обеспечения безопасности информации. Здесь всё известно – нужно разграничение уровня доступа, назначение ответственных лиц, персональная ответственность каждого специалиста, регламентированный порядок хранения документации и т.д.

Вместе с тем, только организационные меры не могут гарантировать требуемый уровень обеспечения безопасности информации. Необходимо применение специализированных технологий и средств. Использование технологии среды построения доверенного сеанса (СПДС), на базе которой работает наш продукт СПДС «ПОСТ», позволит обезопасить персональные данные при их обработке сотрудниками медицинских организаций.

CNews: Расскажите подробнее об этой технологии.
Евгений Жарчинский: Суть данной технологии заключается в следующем.
Каждый врач-специалист, имеющий доступ в медицинскую информационную систему, снабжается персональным USB-носителем, на котором уже сформирована его рабочая среда. В начале работы врач-специалист производит загрузку своего рабочего места с этого носителя. Процесс загрузки защищен.

Специальный загрузочный носитель (СЗН) до ввода PIN-кода пользователя представляется устройством для загрузки операционной системы, но предъявляет неопознанному субъекту далеко не всю среду загрузки. Основные данные надежно защищены, а ключевая информация «упакована» дважды: внутри СЗН находится специализированная микросхема-токен отечественного производства.

До загрузки полной операционной системы «верхняя» часть модуля доверенной загрузки спрашивает у пользователя PIN-код. Среда функционирования и данные пользователя в это время еще находятся в закрытой защищенной зоне носителя и не доступны. После ввода правильного PIN-кода скрытая зона памяти носителя открывается в режиме «только для чтения» и на рабочее место пользователя загружается среда функционирования – операционная система, специально подготовленная и снабженная криптографическими средствами для аутентификации, защиты данных и защиты канала связи.

В этой операционной системе запускается, в зависимости от требований к рабочему месту специалиста, веб-браузер или терминал. От рабочего места специалиста к центру обработки данных (ЦОД) устанавливается защищенный VPN-канал. Он обеспечивает полную изоляцию среды доступа врача по сети: открытые соединения с недоверенными сайтами невозможны, поток данных шифрован, не допускает искажения данных и примешивания посторонней информации, даже повторного приема ранее принятых защищенных данных.

Таким образом, программы и данные концентрируются в центре обработки. Специалист «приходит» в ЦОД и получает персонализированную единообразную рабочую среду с какого бы рабочего места он не получал доступ. Более того, среда «умеет» сохранять свое состояние между сеансами: вход в систему приводит специалиста в «свое приложение», находящееся строго в том состоянии, в котором он завершил работу в предыдущем сеансе.

Рабочие места унифицируются. С точностью до периферии на рабочих местах применяется унифицированное оборудование.

Инфраструктура решения обеспечивает сквозную защиту доступа от рабочего места пользователя до его приложения. Здесь мы применяем технологию построения доверенного сеанса и инновацию, подсказанную нам пользователями из медицинских учреждений – комплект доверенного сеанса (КДС).

CNews: Как обеспечить баланс между соблюдением необходимого уровня безопасности и принципом доступности данных о здоровье пациента в случае необходимости?

Евгений Жарчинский: Чтобы ответить на данный вопрос, необходимо немного остановиться на доступных для пользователей вариантах исполнения СПДС «ПОСТ». Это две стандартных модификации – терминальная и веб.
Веб-приложения СПДС рекомендуются, прежде всего, для наиболее простых задач: работы регистратуры, учета, информационных приложений и справочников.

В случае применения более сложных систем привлекательным представляется терминальное решение. Оно позволяет установить для каждого специалиста сколь угодно сложный набор индивидуальных приложений, связать их с локальной периферией. Традиционные задачи эксплуатации массы индивидуальных рабочих мест – антивирусная защита, техническое обслуживание, резервное копирование и восстановление программ и данных – уходят в центр. В этом режиме доступна и видеоконференцсвязь для нужд телемедицины.

Взаимодействие с лечебно-профилактическими учреждениями привело нас также и к модернизации клиентского рабочего места. Для централизованной архитектуры идеально подходит тонкий аппаратный клиент, бездисковая рабочая станция. Безусловно, при этом требуется для специалистов различного профиля дифференцировать платформы по составу и качеству периферии (графический экран повышенного разрешения для врача, анализирующего изображения, подключение специализированной периферии, например, аппарата УЗИ, цветного принтера, кард-ридера для медицинской электронной карты пациента). На рынке в сегмент рабочих мест врача несколько производителей активно предлагают так называемые защищенные терминалы, которые обеспечивают аутентификацию пользователя и построение защищенного канала от рабочего места пользователя до терминального сервера. Мы пошли на некоторую модернизацию этого дизайна и предлагаем комплект доверенного сеанса. Он состоит из бездисковой рабочей станции, BIOS которой модернизирован таким образом, что исключает загрузку любой операционной среды, кроме СПДС «ПОСТ».

Для каждого пользователя выпускается индивидуальный носитель, содержащий его «личный» состав приложений. На одной и той же бездисковой станции в одну смену в полном составе функциональности разворачивается рабочее место ортопеда, в другую – терапевта.

В сравнении с традиционной архитектурой защищенного терминала мы получаем при этом три преимущества. Рабочее место в принципе не может активизировать никто, кроме зарегистрированного пользователя, для постороннего оно – «мертвое», незагружаемое железо. Бездисковая рабочая станция вообще не содержит программного обеспечения для загрузки. Всякий специалист уносит свое рабочее место с собой. Из этого свойства системы вытекает также удобство удаленной поддержки рабочих мест. Для любой операции технической поддержки достаточно провести обновление содержимого на специальном загрузочном носителе, не перепрошивая защищенный терминал.

Таким образом, достигается сочетание, при котором доступ к информационной системе является одновременно защищенным, быстрым и сравнительно простым. То есть соблюдаются оба принципа, как безопасности, так и доступности данных.

CNews: Известно, что в медучреждениях, как правило, нет собственных высококвалифицированных ИТ-специалистов. Как обеспечиваются установка и функционирование предлагаемого вами решения?
Евгений Жарчинский: Развертывание системы на базе технологии СПДС выглядит следующим образом. Программное обеспечение рабочего места врача инициализируется в едином центре, например, администратором ЦОД. Все необходимые данные, включая сертификаты ключей, записываются на специальный загрузочный носитель. Далее специальные загрузочные носители передаются специалистам. Важно отметить, что распространение СЗН нет нужды осуществлять по доверенному каналу: носитель защищен PIN-кодом и только личный PIN-код необходимо передать специалисту в индивидуальном порядке. Последующий процесс обеспечения жизненного цикла СПДС может осуществляться строго в дистанционном режиме. Администратор своевременно получает сведения об истекающих сроках жизни сертификатов и может заблаговременно формировать им замену. Он имеет возможность подготовить пакетные задания на обновление программного обеспечения, политик безопасности среды функционирования и т.п. Далее пользователь получает уведомление о необходимости обновления рабочего места. Он подключается к сети, передает управление серверу технического обслуживания, который в краткое время проводит сеанс обновления рабочего места.

Обслуживание производится автоматически. Администратор, сформировавший пакет обновления, к обслуживанию не привлекается. При этом если применяются загрузочные носители достаточной емкости, старая среда функционирования не теряется. Она «откладывается» во временный буфер, после чего производится тест работоспособности решения в новой конфигурации. Если тест по каким-либо причинам не прошел, автоматически производится восстановление старой, заведомо работоспособной среды.

CNews: Каковы планы вашей компании в области информатизации здравоохранения на 2012 г.?

Евгений Жарчинский: Пока остается открытым вопрос о медицинской электронной карте пациента. Техническая база для этого вопроса есть в полном наборе, нужно просто интегрировать в среду СПДС тот или иной кард-ридер. Неопределенность с выбором базовой карты и с ее приложениями пока сдерживает развитие в этом направлении.
Вместе с тем, необходимо отметить, что у нас уже есть положительные результаты сотрудничества с несколькими производителями медицинских информационных систем. Совместные тестирования СПДС «ПОСТ» и нескольких МИС прошли успешно, о чем подписаны протоколы тестирования. Следующий шаг – это внедрение наших совместных с компаниями-производителями МИС решений в лечебных учреждениях. И этот шаг мы уже готовы сделать в текущем году.

CNews: Спасибо.