Ю.В. КОЗАДОЙ,
младший научный сотрудник, Федеральное государственное бюджетное учреждение науки Институт программных систем им. А.К. Айламазяна РАН, г. Переславль-Залесский, Россия, yvk@interin.ru
М.С. СМИРНОВ,
начальник отдела информационных технологий, Федеральное государственное бюджетное учреждение Поликлиника № 3 Управления делами Президента РФ, г. Москва, Россия, it@pudp.ru
М.И. ХАТКЕВИЧ,
заведующий лабораторией, Федеральное государственное бюджетное учреждение науки Институт программных систем им. А.К. Айламазяна РАН, г. Переславль-Залесский, Россия, mark@interin.ru

УПРАВЛЕНИЕ ДОСТУПОМ СОТРУДНИКОВ И ПАЦИЕНТОВ В ЛЕЧЕБНОМ УЧРЕЖДЕНИИ ПОЛИКЛИНИЧЕСКОГО ТИПА

УДК 61:658.011.56
Козадой Ю.В., Смирнов М.С., Хаткевич М.И. ***Управление доступом сотрудников и пациентов в лечебном учреждении поликлинического типа*** *(ФГБУН Институт программных систем им. А.К. Айламазяна Российской академии наук, г. Переславль-Залесский, Россия; ФГБУ Поликлиника № 3 Управления делами Президента РФ, г. Москва, Россия)*
Аннотация: В статье проводится анализ возможных подходов к управлению доступом сотрудников и пациентов в лечебном учреждении. Рассматриваются различия возможных решений, аспекты технической реализации и внедрения систем управления доступом. Описано решение, проходящее апробацию в крупном лечебном учреждении поликлинического типа.
Ключевые слова: *системы контроля и управления доступом, защита персональных данных, информационная безопасность, информационные системы, медицинские информационные системы, внедрение информационных систем, эпидемиология.*

UDC 61:658.011.56
Kozadoy Y.V., Smirnov M.S., Khatkevitch M.I. ***Patient and employee admission management for the out-patient clinic*** *(Program Systems Institute, RAS, Pereslavl-Zalessky, Russia; Clinic №3 of the President Administration, Moscow, Russia)*
Abstract: This article describes different approaches to the patient and employee admission management for the healthcare facility. An overview of the various technical solutions according to development and implementation processes. Detail explanation of the certain solution being implemented in a large out-patient clinic.
Keywords: *access control, personal records, personal data protection, information security, information systems, healthcare information systems, information system deployment, epidemiology.*

Введение

Требования по доступности объектов внутренней инфраструктуры, предъявляемые лечебно-профилактическим учреждением (ЛПУ), противоречивы. С одной стороны, необходимо обеспечить возможность пациенту беспрепятственно получить, а специалисту оказать своевременную и качественную медицинскую помощь, и в этом смысле ЛПУ должно быть максимально открыто.

С другой стороны, для ЛПУ можно выделить ряд факторов, создающих предпосылки для тех или иных ограничений:

• повышенными требованиями к чистоте и стерильности;

• эпидемиологическими соображениями (особенно в периоды распространения ОРЗ, ОРВИ и др.);

• юридическими соображениями (возможность предъявления исков, претензий и судебных разбирательств);

• экономическими соображениями (оказание платных медицинских услуг, необходимость строгого контроля взаиморасчетов с потребителями и с поставщиками);

• требованиями информационной безопасности (обработка персональных данных), необходимостью сохранения личной и врачебной тайны пациента;

• требованиями обеспечения безопасности, предъявляемыми к социально значимым объектам;

• выявлением и пресечением противоправных действий со стороны посетителей, облегчением процедуры «разбора» конфликтных ситуаций;

• требованиями и регламентами действий в случае возникновения чрезвычайных ситуаций (пожар, задымление и т.д.).

Для налаживания эффективной работы учреждения руководству ЛПУ приходится искать компромисс, оптимальное сочетание запретов и разрешений доступа с учетом приведенных выше соображений. Адекватные средства информатизации, позволяющие отслеживать движение и анализировать траектории перемещения сотрудников и пациентов по зданию ЛПУ, могут существенно упростить решение данной задачи и стать важным инструментом для руководителя ЛПУ.

В данной статье рассматриваются подходы к решению проблемы управления доступом, предлагаются средства информатизации и технические решения для организации подсистемы управления доступом (далее — Подсистемы или ПУД) в ЛПУ поликлинического типа, где эксплуатируется интегрированная медицинская информационная система.

Подходы к управлению доступом

Традиционно системы идентификации и управления доступом рассматриваются в двух ипостасях:

— Пропускной режим в здание и/или в различные «зоны» (корпуса, кабинеты, этажи и т.д.) в рамках общего «охраняемого периметра». Часто применяется в крупных престижных ЛПУ, пропуска (постоянные или временные), либо другие идентификационные документы имеют и сотрудники, и пациенты. Проверять право посетителя на вход в здание может вахтер или сотрудник охраны, их деятельность может быть поддержана использованием технического оснащения самой разной сложности и стоимости.

— Системы идентификации используемых медицинских информационных систем (МИС). Идентификации (различные идентификационные ключи при включении компьютера, имя и пароль в операционной системе, имя и пароль при входе в МИС) подлежат пользователи МИС. Идентификацию проходят и пациенты, оказываясь на приеме у врача или получая медицинские процедуры. Идентификационными документами при этом могут быть удостоверения личности, анкетные данные, номер полиса, медкарты и пр. Идентифицируется и медицинская карта пациента в МИС, чтобы записи о пациенте попали именно в его медкарту.

Развитие информационных технологий делает возможным интеграцию обеих в рамках одной подсистемы — ПУД. В этом случае идентификатор, используемый посетителем (сотрудник или пациент) для входа в здание ЛПУ, впоследствии используется и в качестве идентификатора местоположения (кабинет и АРМ), где тот или иной сотрудник ЛПУ в данный момент работает или где принимается данный пациент.При этом регистрируется считыватель, который считал идентификатор этого сотрудника на рабочем месте, после чего все идентификаторы, прошедшие указанный считыватель, определяют посещение

пациентами данного сотрудника.Идентификатор сотрудника может также использоваться и в качестве идентификатора пользователя МИС.Идентификатор пациента для входа в здание используется и для оказания ему медицинских услуг во врачебных кабинетах, и даже медицинская карта для записей о вошедшем в кабинет врача пациенте автоматически подбирается по идентификатору пациента. В свою очередь информация о пациенте или сотруднике, обрабатываемая в МИС, может оказывать непосредственное влияние на решение вопроса о его проходе в здание или помещение. Такое взаимопроникновение функционала приводит к качественному изменению системы управления доступом, она приобретает свойства, не присущие ранее ни одной из интегрированных схем идентификации.

В основе управления доступом лежит мониторинг: фиксация событий, связанных с проходом посетителей (как сотрудников ЛПУ, так и пациентов) к отдельным элементам инфраструктуры и сохранение в журналах сведений в объеме, достаточном для анализа и принятия решений при управлении доступом. Для фиксации перемещения посетителей по зданию ЛПУ используются различные считыватели идентификационной информации, размещенные не только при входе в здание, но и в ключевых точках по пути следования сотрудников или пациентов. Безусловно, все вышеозначенное интересно более всего для ЛПУ поликлинического типа, так как поток посетителей и интенсивность их перемещения там значительно выше, чем в стационарах.

Можно рассмотреть два подхода к организации доступа:

- мягкий контроль;
- жесткий контроль.

Мягкий контроль ограничивается мониторингом передвижения сотрудников и пациентов, при том, что ограничений на проход не предъявляется. Анализ накопленной информации позволяет выявлять источники проблем и «узкие места», вырабатывать управленческие решения и воздействовать на ситуацию постфактум. За счет такого подхода не происходит существенного изменения бизнес-процессов во всем ЛПУ одновременно. А также не допускаются приостановки бизнес-процессов в случае возникновения ситуации отказа в доступе, когда какой-то фактор не был предусмотрен в модели, вследствие чего доступ неоправданно оказался несанкционированным.

При жестком контроле сотрудник допускается только к тем элементам инфраструктуры, которые требуются ему в рамках исполнения его должностных обязанностей, а пациент допускается в помещения только в рамках маршрута, определенного целями его посещения ЛПУ.

При этом недоступность сегментов ЛПУ для посещения обеспечивается техническими средствами (турникеты, двери с идентификационными замками и пр.).

Такой подход предполагает разработку моделей поведения сотрудника и пациента для абсолютно всех возможных случаев и превентивно исключает любые действия, не заложенные в модель. Это позволяет обеспечить контроль доступа на высоком уровне, а также упорядочить процесс посещения ЛПУ. Однако затраты на поддержание контроля доступа посетителей при таком подходе существенно вырастают. Особенно проблематичным становится управление доступом в период ввода Подсистемы в действие. Любой возникший инцидент, не укладывающийся в имеющиеся модели посещения, блокирует бизнес-процессы задействованных подразделений ЛПУ, требуя вмешательства уполномоченных лиц, авторизующих нарушение данного бизнес-процесса до внесения уточнений в модель управления доступом. Разработать достаточную и непротиворечивую модель управления доступом в конкретном ЛПУ до начала внедрения ПУД, основываясь только лишь на теоретических выкладках, не пред-

ставляется возможным. Период разработки и уточнения таких моделей может занимать довольно длительное время, причем значительная его часть приходится на период промышленной эксплуатации ПУД. С учетом времени, требующегося для доводки модели управления доступомна действующей Подсистеме с часто возникающими неучтенными отклонениями, издержки внедрения могут оказаться неоправданно высокими.

Рабочий подход к проблеме управления доступом может являться некоторым компромиссом между описанными выше мягким и жестким подходами и представлять собой их комбинацию.

Комбинация подходов во многом зависит от реалий конкретного ЛПУ, в рамках данной статьи мы ограничимся лишь формулировкой самых общих рекомендаций:

— Жесткий контроль на входе-выходе и в ряде выделенных помещений внутренней инфраструктуры (это могут быть административные и технические помещения, в которых хранится и обрабатывается конфиденциальная информация, расположены узловые элементы инфраструктуры ЛПУ, хранилище бумажных амбулаторных карт, аптечный склад и др.).

— Мягкий контроль (идентификация и верификация) во всех объектах внутренней инфраструктуры ЛПУ.

— Контроль осуществляется на фоне мониторинга движения сотрудников и пациентов.

Поскольку с самого начала желательно предотвратить бесконтрольный и не подлежащий учету доступ к внутренней инфраструктуре, на входе в ЛПУцелесообразно использовать турникеты, проход через которые однозначно идентифицирует прошедшего.

Контроль доступа осуществляется по следующим направлениям:

- идентификация на основе постоянного пропуска,
- идентификация на основе документов (выдача временного пропуска),
- фотоверификация.

Контроль может проводиться на промежуточных точках (проходная, двери, рамки) и на конечных точках (кабинет специалиста). Использование бесконтактных средств идентификации повышает удобство контроля. Более детальный учет можно вести в случае применения таких средств (с достаточным радиусом действия), которые позволяют использовать бесконтактные рамки, что более комфортно для посетителей, чем открытие дверей по прикладыванию пропуска.Однако по первичным прикидкам данные решения либо не обеспечивают 100% идентификации, либо дороги в применении.

Тогда как контроль «вручную» (осуществляемый сотрудником ЛПУ) позволяет вести учет в полной мере (конечно, если исключить «человеческий фактор»), автоматизированные системы контроля (рамки, двери, турникеты и пр.) имеют некоторую погрешность, связанную с возможностью прохода через рамку одновременно нескольких посетителей либо с открытием двери по одному идентификатору и последующим проходом двух и более посетителей. Уменьшить данную погрешность в критических точках маршрута можно было бы посредством установки турникета типа «трипод», однако, удобство и применимость данного решения для ЛПУ весьма спорно.

Актуальные задачи управления доступом

Осуществление контроля ключевых точек маршрута при посещении ЛПУ позволяет решать следующие задачи:

- Выявлять в местах пересечения маршрутов и совпадения их участков области с высокой интенсивностью взаимодействия посетителей.Это является важным, например, для контроля эпидемиологической обстановки или для выявления и расширения «узких мест» (лифты, зоны ожидания перед наиболее посещаемыми кабинетами и пр.). Лучшего результата можно достичь с помощью установки бесконтактных рамок в ключевых позициях

(вход на этаж, переход между корпусами и т.п.).

• Обеспечить своевременную и оперативную реакцию персоанала в случае возникновения чрезвычайной ситуации. Например, информация о том, сколько людей находится на определенном этаже или в определенном здании, существенно облегчит эвакуацию при пожаре.

• Учитывать при организации пропускного режима сроки обслуживания (сроки действия медицинских полисов) пациентов.

• Выявлять и анализировать случаи нетипичного посещения ЛПУ: например, посещение с идентификацией только на проходной, тогда как ни в один кабинет посетитель не заходил.

• Выявлять нарушения условий предоставления медицинской помощи: например, верификация по фотографии на рабочем месте врача в случаях попытки получения пациентом медицинской помощи по чужому медицинскому полису.

• Вести учет оплаты оказанных медицинских услуг при системе оплаты постфактум

• За счет введения технических средств контроля повысить уровень полноты и своевременности оплаты оказанных пациенту медицинских услуг.

• Комбинировать данные ПУД и системы видеонаблюдения в случае с применением видеофиксации, что облегчает последующее использование видеоматериалов.

• Сокращать время на идентификацию пациента, а также минимизировать ошибки ввода при идентификации — в том функционале МИС, который поддерживает идентификацию пациента средствами ПУД.

• Поддерживать комплекс мероприятий, направленный на обеспечение информационной безопасности в соответствии с 152-ФЗ «О персональных данных» в части уточнения модели угроз и реагирования на возможные инциденты. При этом ПУД способна определить потенциальный круг лиц, допущенных к той или иной информации в указанный момент времени.

• Вести учет рабочего времени сотрудника, контролировать опоздания и простои.

Архитектура предлагаемого решения

Система, обеспечивающая функционирование технических средств контроля и управления доступом, довольно специфична в силу высокой степени взаимодействия с оборудованием, которое может быть самым разным (фото- и видео-техника, турникеты, двери, рамки, считыватели, контроллеры, и пр.), тогда как любая полнофункциональная интегрированная МИС обладает всей полнотой информации о субъекте контроля — посетителе ЛПУ (сведения о сотруднике или о прикреплении, анкетных данных, процессе лечения и плане посещения пациентом ЛПУ). С учетом разной направленности этих систем наиболее эффективным решением для организации интегрированного управления доступом является совместное использование двух отдельных специализированных систем — медицинской информационной системы (МИС) и системы контроля и управления доступом (СКУД). И те, и другие довольно часто используются в современных ЛПУ «по отдельности» (не взаимодействуя друг с другом). Объединение же столь различного функционала в рамках одной системы нецелесообразно, так как зависимость задач МИС и СКУД друг от друга в рамках одной системы снижает отказоустойчивость и производительность комплекса в целом *(рис. 1)*.

ПУД в рамках МИС пропускает через себя ряд информационных потоков между МИС и СКУД. Не все СКУД могут иметь интерфейс SOAP, для реализации которого, а также для расширения функциональных или мощностных характеристик СКУД целесообразно реализовать систему управления посещениями (СУП), которая в свою очередь будет непосредственно взаимодействовать со

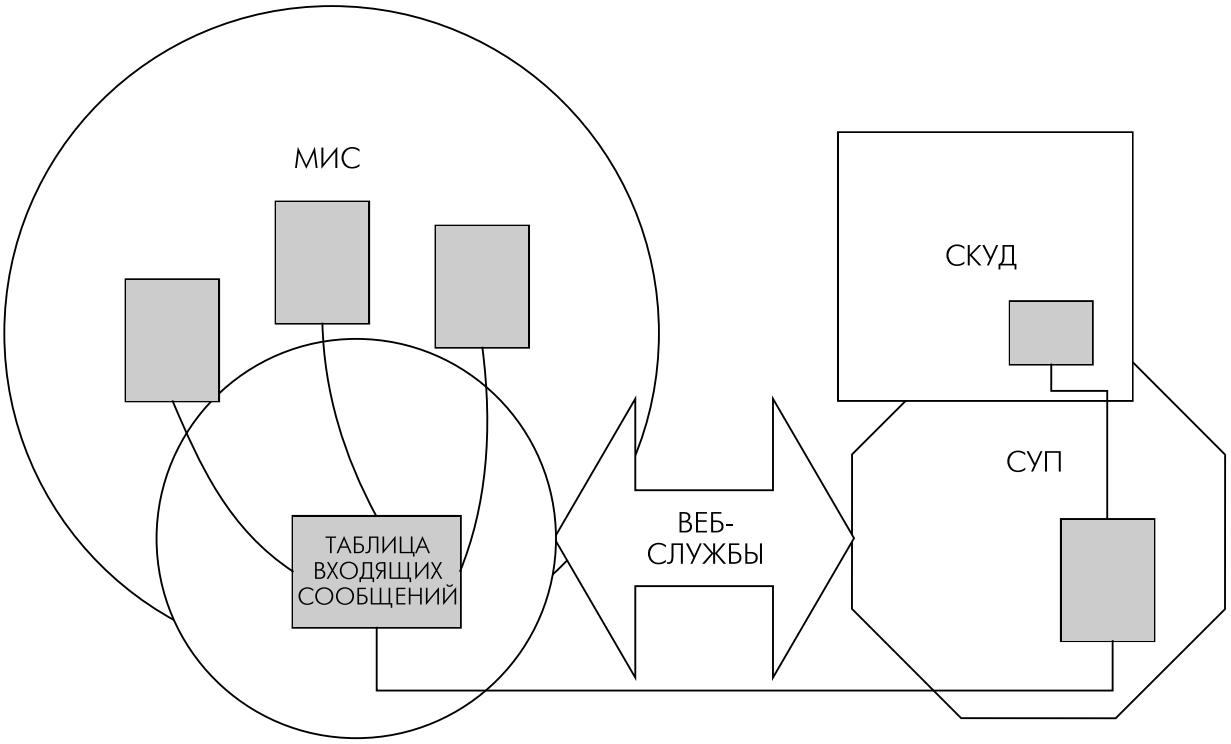

Рис. 1. **Принципиальная схема информационного взаимодействия МИС и СКУД**

СКУД. Для СКУД характерны информационные потоки, содержащие данные о фактах попыток прохода через определенную точку контроля, а также о результатах этих попыток. Например, передаются данные о прохождении посетителя на КПП с фиксацией результата («разрешен вход/выход» либо «прохождение было блокировано»), а также данные об идентификации пользователя МИС на том или ином рабочем месте или идентификации пациента на рабочем месте врача. На основе этих данных Подсистема подготавливает для МИС граф, связывающий специалистов ЛПУ и пациентов, который может быть использован для быстрой идентификации пациента на рабочем месте специалиста, а также для анализа движения посетителя в пределах контрольных точек. Для МИС же характерны информационные потоки, содержащие данные о пропусках, формируемые отделом кадров для сотрудников или отделами учета контингента ЛПУ для пациентов, сведения о месте работы медицинского специалиста — пользователя МИС и о цели посещения ЛПУ пациентом, а также различные управляющие сообщения для поддержки принятия решений в рамках СКУД. Примером таких сообщений могут служить сведения, которые необходимо передать пациенту при выходе с территории ЛПУ (например, о забытых им в кабинете врача вещах), а также сигнализирующие оператору на КПП о том, что пациент не выполнил намеченные в рамках его визита в ЛПУ действия, как то: не получил заказанные услуги, не оплатил полученные услуги, не получил результаты анализов или диагностических исследований и пр.

На основе данных, интегрированных подсистемой управления доступом, МИС получает возможность централизованно использовать информацию о местонахождении пациента или сотрудника.

Особенности реализации

Реализация комплекса, решающего задачи контроля доступа, зависит от специфики конкретного ЛПУ, используемых МИС и оборудования, однако, обладает описанными выше общими чертами. В качестве примера рассмотрим решение, которое построено на основе МИС «Интерин PROMIS» и СКУД «Parsec» в качестве основы системы учета посетителей.

На построение ПУД влияли также следующие технологические особенности:

- Часть пользователей МИС может работать через терминальный доступ, что осложняет использование считывателей, подключаемых непосредственно к рабочей станции.
- Рабочие места сотрудников различаются по техническому исполнению, что не всегда позволяет единым образом подключить считыватель непосредственно к рабочей станции.

С учетом этих особенностей предложен способ интеграции, когда считыватели средств идентификации составляют отдельную сеть, сигналы в которой обрабатываются исключительно системой учета посетителей. В таком режиме ПУД взаимодействует исключительно со специальной службой интеграции системы учета посетителей, которая централизованно оперирует сигналами со всех считывателей.

В МИС для каждого рабочего места регистрируется уникальный идентификатор считывателя, после чего работа пользователя МИС начинается с «открытия» сессии на определенном считывателе с помощью прикладывания сотрудником ЛПУ собственного пропуска во время авторизации.

Контроль доступа устроен таким образом, что система учета посетителей передает в подсистему управления доступом факт каждой идентификации посетителя на каждой точке контроля. На основе этих данных ПУД формирует для МИС готовую картину состояния рабочих мест сотрудников на данный момент: на рабочих местах авторизованы определенные сотрудники, в их кабинетах могут быть идентифицированы определенные пациенты. С помощью этих данных МИС способна решать задачи идентификации посетителей и их верификации прямо на рабочем месте врача.

В свою очередь сотрудники отделов учета контингента ведут выдачу пропусков пациентам. Впервые войдя на территорию ЛПУ по предъявлению документов с получением временного пропуска, пациент попадает в отдел учета контингента, где оператор фотографирует пациента, изымает временный пропуск и изготавливает постоянный пропуск с фотографией и данными пациента, указывая срок, в течение которого пропуск действителен (пациент может обслуживаться в ЛПУ). Данные об этом пропуске передаются в ПУД, которая направляет их в систему учета посетителей. Аналогичным образом происходит и аннулирование пропусков, если пациент утрачивает право на обслуживание в данном ЛПУ.

Также на своих рабочих местах пользователи МИС могут воспользоваться Подсистемой управления доступом для передачи сообщений, влияющих на проход пациента через проходную, — нужно ли сообщить какие-либо сведения пациенту, инициировать выполнение им каких-либо действий, или же проход осуществится в обычном режиме.

Технически реализация построена на асинхронном взаимодействии через передачу сообщений. Система учета посетителей передает сообщения в формате XML, записывая их в таблицу входящих сообщений в Подсистеме управления доступом. Сообщение содержит данные о считывателе, персоне, результате идентификации и ряд дополнительных данных — например, тип (сотрудник, пациент).

Подсистема управления доступом передает сообщения о пропусках: создании, аннулировании, изменении сроков, а также о сообщениях для пациента на входе или выходе из ЛПУ. Они передаются посредством вызова веб-службы системы учета посетите-

лей, где содержится набор методов, комбинации которых определяют требуемое действие.

В самой МИС реализована идентификация на основе данных пациента со считывателя с помощью информации от Подсистемы управления доступом. Таким образом, в автоматизированных рабочих местах врача, регистратора, сотрудника учета контингента и пр. можно идентифицировать пациента по его пропуску, исключая ручной ввод данных.

Практическое использование

В настоящий момент Подсистема управления доступом ЛПУ, реализованная с учетом концептуальных и технологических принципов, изложенных в данной статье, введена в опытную эксплуатацию в крупной ведомственной поликлинике и успешно проходит апробацию, что позволяет надеяться на успешный запуск системы в промышленную эксплуатацию и эффективное выполнение возложенных на нее задач на последующих этапах эксплуатации.

Ввод в действие ПУД, безусловно, требует от ЛПУ определенных затрат на дополнительное оборудование и его интеграцию с МИС. Однако эти затраты вполне посильны ведущим медицинским учреждениям, а Подсистема управления доступом может играть заметную роль в повышении качества оказания медицинской помощи, эффективности работы персонала и комфорта пациентов, что способствует повышению престижа ЛПУ.

ЛИТЕРАТУРА

1. *Смирнов М.С., Хаткевич М.И.* Опыт комплексной информатизации многопрофильного лечебно-профилактического учреждения на основе системы Интерин PROMIS. ФГБУ «Поликлиника № 3» УД Президента РФ//В кн. Кремлевская медицина, тематический выпуск: Первичная медико-санитарная помощь, к 30-летию ФГБУ «Поликлиника № 3» УД Президента РФ. — С. 85–89.
2. *Назаренко Г.И., Гулиев Я.И., Ермаков Д.Е.* Медицинские информационные системы: теория и практика//Под ред. Г.И. Назаренко, Г.С. Осипова. — М.: Физматлит, 2005. — 320 с.

IT-новости

КРУПНЕЙШИЙ МЕДИЦИНСКИЙ ПОРТАЛ ПОЯВИТСЯ В РУНЕТЕ

Венчурные фонды Runa Capital, Prostor Capital и Интернет-группа Fastlane Ventures объединяют ресурсы «ВитаПортал» и «ЗдоровьеОнлайн» и вложат 1,35 миллиона долларов для создания единого онлайн-сервиса в сфере здравоохранения, говорится в официальном сообщении этих компаний. Объединенный ресурс получит бренд «ВитаПортал».

Средства будут направлены на развитие технологии персонализации медицинских данных и разработку приложения для мобильных платформ.По словам Азамата Ульбашева, генерального директора и сооснователя сайта «ВитаПортал», основной целью проекта является формирование российского рынка медицинских онлайн-сервисов. В настоящее время число пользователей объединенного сервиса составляет более 700 тысяч, в 2014 году их число планируется увеличить до пяти миллионов.

Цифровая медицина относится к одному из наиболее быстро растущих Интернет-сегментов, общемировой объем инвестиций в стартапы в области здравоохранения составляет около 1,5 миллиарда долларов.

Источник: ria.ru