РОССИЙСКАЯ КОМПАНИЯ-РАЗРАБОТЧИК
КОМПЛЕКСНЫХ РЕШЕНИЙ IT-БЕЗОПАСНОСТИ «СМАРТ-СОФТ»

МЕТОДИЧЕСКОЕ ПОСОБИЕ

Информационная безопасность и соблюдение
законодательства РФ, регулирующего доступ
в Интернет, в учреждениях здравоохранения

2017

СОДЕРЖАНИЕ

АКТУАЛЬНЫЕ ЗАДАЧИ ИНФОРМАТИЗАЦИИ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ. ПРОБЛЕМЫ И РЕШЕНИЯ.....5

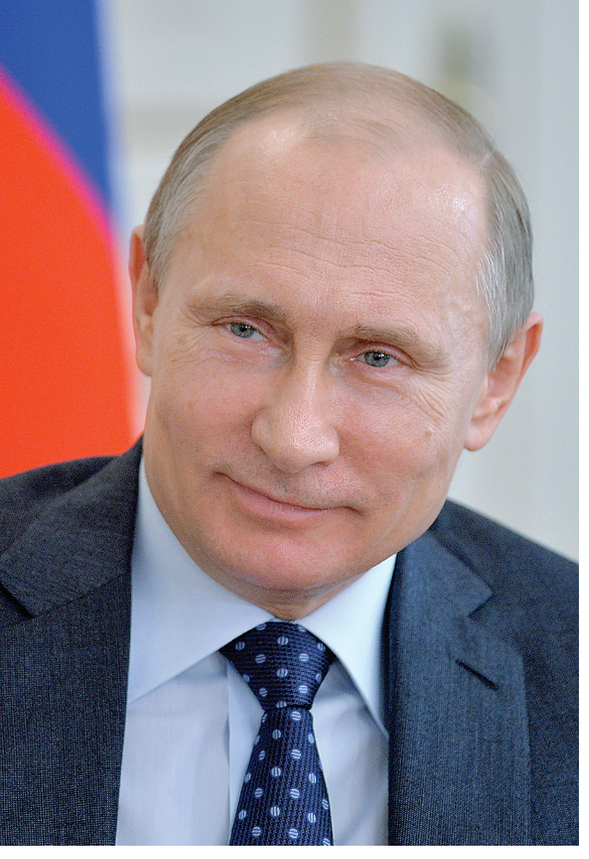
РАЗДЕЛ 1. ИНТЕРНЕТ В ЗАКОНЕ: ТРЕБОВАНИЯ, ОТВЕТСТВЕННОСТЬ, РЕШЕНИЯ.....7

РАЗДЕЛ 2. КЛИК ДУШИ: ЧЕМ БЕСПЛАТНЫЙ WI-FI В БОЛЬНИЦАХ МОЖЕТ ПОМОЧЬ ПАЦИЕНТАМ И ЧТО ОБЯЗАТЕЛЬНО ДОЛЖНЫ ЗНАТЬ О НЕМ ВРАЧИ.....12

РАЗДЕЛ 3. СЕТЬ БЕЗ ПРОБЛЕМ: КАК ОРГАНИЗОВАТЬ ИНТЕРНЕТ-ДОСТУП В МЕДИЦИНСКОМ УЧРЕЖДЕНИИ.....15

РАЗДЕЛ 4. ИСТОРИЯ УСПЕШНОГО ВНЕДРЕНИЯ: НУЗ «УЗЛОВАЯ БОЛЬНИЦА НА СТАНЦИИ ТИМАШЕВСКАЯ ОАО «РЖД».....18

РАЗДЕЛ 5. С ПОЛЬЗОЙ ДЛЯ ДЕЛА: РЕСУРСЫ ДЛЯ МЕДУЧРЕЖДЕНИЙ.....21



В течение ближайших двух лет предлагаю подключить к скоростному Интернету все больницы и поликлиники нашей страны.

Это позволит врачам даже в отдаленном городе или поселке использовать возможности телемедицины, быстро получать консультации коллег из региональных и федеральных клиник.

Президент РФ
Владимир Путин
Источник: ИТАР-ТАСС

Актуальные задачи информатизации медицинских учреждений

Программа информатизации российского здравоохранения стартовала в 2011 году. Среди ее целей: обеспечение безопасности пациентов, доступности и непрерывности медпомощи, повышение ее качества и другие. Часть мер уже исполнена, другая находится в стадии реализации. Так сегодня две трети российских поликлиник и больниц (более 60%) подключены к скоростному Интернету. Планируется, что оставшиеся медучреждения будут обеспечены услугами связи к концу 2018 года.

Преимущества интернетизации медицины очевидны: компьютерные и сетевые технологии позволяют организовать рабочее место специалиста, упростить взаимодействие между сотрудниками, обеспечить доступ к огромному объему справочной информации. Итогом ее должна стать полная компьютеризация процесса работы с пациентами, когда вся информация будет храниться и обрабатываться в электронном виде.

На современном этапе реализации программы одними из наиболее актуальных задач для медучреждений, в частности, являются:

- обеспечение комплексной информационной безопасности и защиты персональных данных в соответствии с ФЗ-152 «О персональных данных» в рамках реализации приоритетных проектов по внедрению телемедицины и упрощению доступа населения к высокотехнологичной медицинской помощи;
- обеспечение централизованного контроля и управления интернет-доступом географически распределенной филиальной сети;
- организация качественного Wi-Fi доступа для пациентов и персонала с учетом возрастных категорий;
- соблюдение законодательства, регулирующего доступ и использование Интернета.

Рассмотрим типичные проблемы, с которыми сталкиваются медучреждения при выполнении этих задач, и эффективные способы их решения.

Проблемы и решения

Делая выбор в пользу современных сетевых технологий, медицинские учреждения сталкиваются с типичными проблемами при:

- организации контролируемого доступа к сети Интернет;
- защите учреждения от взлома по Сети;
- соблюдении норм законодательства РФ в части использования сертифицированных межсетевых экранов;
- защите от вирусных атак и хакерских вторжений, которые могут парализовать работу учреждения;

- обеспечении конфиденциальной передачи данных в единый центр обработки;
- ограничении доступа сотрудников к нежелательным или запрещенным веб-ресурсам.

Избежать проблем при работе с сетью позволяет специальное программное обеспечение – универсальные шлюзы безопасности, устанавливаемые на границе локальной сети учреждения в месте ее подключения к Интернету. Подобное расположение позволяет обрабатывать весь трафик, которым пользователи локальной сети обмениваются с «внешним миром».
Как это программное обеспечение помогает минимизировать риски, рассмотрим на примере **Traffic Inspector** и **Traffic Inspector Next Generation** – продуктов компании «Смарт-Софт», которая более десяти лет является одним из лидеров отечественного рынка универсальных шлюзов безопасности.

Организация контролируемого доступа к сети Интернет
Продукты **Traffic Inspector** и **Traffic Inspector Next Generation** поддерживают концепцию идентификации пользователей в соответствии с их учетными записями. Только пользователи и компьютеры, успешно прошедшие процесс аутентификации, получают доступ к сети Интернет. Гостевые устройства более не смогут свободно и бесконтрольно выходить в Интернет.

Защита учреждения от взлома по Сети
Межсетевой экран, реализованный в продуктах **Traffic Inspector** и **Traffic Inspector Next Generation**, делает все TCP/UDP порты недоступными для подключения из Интернета. Кроме того, межсетевой экран автоматически отслеживает все сетевые подключения и разрешает входящий трафик, только если он является ответным на запросы компьютеров внутренней сети. Все остальные входящие запросы из Интернета полностью блокируются.

Соблюдение норм законодательства РФ
Продукты **Traffic Inspector** и **Traffic Inspector Next Generation** обладают сертификатами ФСТЭК по профилю МЭ тип Б класс 6 и тип А класс 4 соответственно. Использование продуктов компании «Смарт-Софт» позволит соблюсти нормы законодательства РФ в части использования сертифицированных сетевых экранов в государственных учреждениях.

Защита от вирусных атак, которые могут парализовать работу учреждения
В состав продуктов **Traffic Inspector** и **Traffic Inspector Next Generation** входят модули антивирусной защиты, которые обеспечивают сканирование веб-трафика, скачиваемого пользователями локальной сети. Модули дезинфицируют инфицированные файлы или блокируют скачивание вредоносных файлов, не поддающихся лечению.

Обеспечение конфиденциальной передачи данных в единый центр обработки
Продукты **Traffic Inspector** и **Traffic Inspector Next Generation** поддерживают технологии VPN и позволяют настроить конфиденциальное взаимодействие между географически разнесенными сетями или обеспечить безопасное подключение удаленных пользователей к офису учреждения.
Traffic Inspector Next Generation можно интегрировать с сертифицированным средством криптографической защиты информации «МагПро Криптопакет», которое соответствует ГОСТ 28147-89, ГОСТ Р 34.10 2001, ГОСТ Р 34.10-94 и требованиям ФСБ России к СКЗИ по классам КС1 и КС2. Сертификат ФСБ N СФ/124-2767 от 5 февраля 2016 г. Вы сможете использовать наш межсетевой экран для организации шифрованных по ГОСТ VPN-каналов между своими филиалами или партнерскими организациями.

Ограничение доступа сотрудников к нежелательным или запрещенным веб-ресурсам
Продукты **Traffic Inspector** и **Traffic Inspector Next Generation** принимают решение о том, следует ли разрешить или заблокировать сетевой трафик в соответствии с определенными в программе политиками веб-доступа для пользователей и групп пользователей. Политики веб-доступа основываются на правилах межсетевого экрана и правилах для веб-прокси сервера.

Контроль за сетевой активностью, осуществляемой из компьютерной сети учреждения
Продукты **Traffic Inspector** и **Traffic Inspector Next Generation** собирают статистику сетевого доступа и предоставляют ее в виде удобных и гибких отчетов. Поддерживаются разнообразные отчеты: сетевая статистика, отчет по прокси, использование полосы пропускания, отчет по письмам, отчет по работе антивируса и другие.

1. ИНТЕРНЕТ В ЗАКОНЕ: ТРЕБОВАНИЯ, ОТВЕТСТВЕННОСТЬ, РЕШЕНИЯ

Администрациям медицинских учреждений важно знать правила и стандарты подключения к Интернету, которые сегодня регламентируются следующими законами:
- ФЗ-152 «О защите персональных данных»;
- ФЗ-13 от 7.02.2017 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»;

- ФЗ-149 «Об информации, информационных технологиях и о защите информации»;
- ФЗ-188 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации».
- Постановление Правительства №758;
- ФЗ-436 «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- ФЗ-139 «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию».

Рассмотрим подробнее требования закона и решения, которые помогут администрации учреждений здравоохранения их соблюсти и тем самым избежать наказания.

ФЗ-152 «О защите персональных данных»

Требование. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Ответственность при нарушении норм, регулирующих обработку и защиту персональных данных работника: если у оператора будет выявлено 50 нарушений, каждое из них может быть квалифицировано отдельно, по каждому составлен протокол и за каждое наложен штраф от 25 тыс. до 50 тыс. рублей.

Решение. Использовать средства защиты – межсетевые экраны, сертифицированные ФСТЭК РФ по новым требованиям, вступившим в силу 1 декабря 2016 года.
В новых требованиях выделены следующие типы межсетевых экранов:

- межсетевой экран уровня сети (тип А) – применяется на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы;
- межсетевой экран уровня логических границ сети (тип Б) – применяется на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы;
- межсетевой экран уровня узла (тип В) – применяется на узле (хосте) информационной системы;
- межсетевой экран уровня веб-сервера (тип Г) – применяется на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера);

- межсетевой экран уровня промышленной сети (тип Д) – применяется в автоматизированной системе управления технологическими или производственными процессами.

Для дифференциации требований к функциям безопасности межсетевых экранов выделяется шесть классов защиты: от 6-го (низкий) до 1-го (высокий).

Межсетевые экраны, соответствующие 6-му классу защиты, применяются в государственных информационных системах 3-го и 4-го классов защищенности, в автоматизированных системах управления производственными и технологическими процессами 3-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3-го и 4-го уровней защищенности персональных данных.

Межсетевые экраны, соответствующие 5-му классу защиты, применяются в государственных информационных системах 2-го класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2-го уровня защищенности персональных данных.

Межсетевые экраны, соответствующие 4-му классу защиты, применяются в государственных информационных системах 1-го класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1-го уровня защищенности персональных данных, в информационных системах общего пользования 2-го класса.
Межсетевые экраны, соответствующие 3, 2 и 1-му классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

ФЗ-13 от 7.02.2017 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»

Требование. Закон описывает семь составов правонарушений и устанавливает соответствующие им штрафы с самым высоким из них (для юридических лиц) – 75 тыс. рублей.

Ответственность. Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством РФ сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ,

если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния.
Новая конструкция статьи 13.11 с семью составами правонарушений может привести к принципиальному изменению надзорной практики. Теперь, если у оператора будет выявлено 50 нарушений, каждое из них может быть квалифицировано отдельно, по каждому – составлен протокол и наложен штраф, суммарно весьма внушительный и фактически неограниченный.

Решение. Использовать средства защиты – межсетевые экраны, сертифицированные ФСТЭК РФ по новым требованиям, вступившим в силу 1 декабря 2016 года.

ФЗ-149 «Об информации, информационных технологиях и о защите информации»

Требование. Любая организация, предоставляющая доступ в Интернет, обязана блокировать ресурсы в соответствии с черным списком Роскомнадзора. У разных интернет-провайдеров обновление списков проходит не всегда своевременно, а ответственность ложится на компанию – организатора раздачи Интернета.

Ответственность. Нарушение требований настоящего закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность согласно законодательству Российской Федерации.

Решение. Использовать программное обеспечение для регулярной фильтрации по спискам Роскомнадзора. Как это сделать, вы можете узнать здесь: http://www.smart-soft.ru/documents-useful-materials/roscomnadzor.pdf.

ФЗ-188 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»

Требование. С 1 января 2016 года введен запрет на приобретение иностранного программного обеспечения для нужд государственных учреждений, за исключением тех случаев, если ПО соответствующего класса нет в едином реестре российских программ для ЭВМ и баз данных.

Ответственность. Отказ в праве проводить конкурс.

Решение. Работать с реестром отечественного ПО: https://reestr.minsvyaz.ru/reestr.

Постановление от 31 июля 2014 г. № 758 об идентификации пользователей Wi-Fi и законопроект «О внесении изменений в Федеральный закон «О связи»

Требование. Предоставление доступа к сети Интернет в общественных местах осуществляется после идентификации оператором пользователей услуг связи и их оконечного оборудования. Идентификация может производиться по паспорту, учетной записи на сайте госуслуг или с помощью СМС-сообщения при авторизации.

Ответственность. Нарушение требований настоящего закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность согласно законодательству Российской Федерации.

Решение. Использовать программное обеспечение для идентификации пользователей по паспорту, учетной записи на сайте госуслуг или посредством авторизации с помощью СМС-сообщений.

ФЗ-139 и ФЗ-436 «О защите детей от информации, причиняющей вред их здоровью и развитию»

Требование. Российское законодательство обязывает администраторов точек публичного интернет-доступа использовать средства фильтрации, ограждающие детей от посещения ресурсов с опасным, экстремистским и порнографическим контентом.

Ответственность. При нарушении закона накладывается административный штраф: на граждан – от 2000 до 3000 рублей с конфискацией предмета административного правонарушения; на должностных лиц – от 5000 до 10 тыс. рублей; на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, – от 5000 до 10 тыс. рублей с конфискацией предмета административного правонарушения или административное приостановление деятельности на срок до 90 суток; на юридических лиц – от 20 тыс. до 50 тыс. рублей с конфискацией предмета административного правонарушения или административное приостановление деятельности на срок до 90 суток.

Решение. Блокировать ресурсы, не предназначенные для просмотра детьми. Это сайты, на которых пропагандируются наркотики, отрицаются семейные ценности, содержится нецензурная брань, информация порнографического характера, и другие ресурсы, указанные в законах, регламентирующих информационную безопасность детей.

2. КЛИК ДУШИ: ЧЕМ БЕСПЛАТНЫЙ WI-FI В БОЛЬНИЦАХ МОЖЕТ ПОМОЧЬ ПАЦИЕНТАМ И ЧТО ОБЯЗАТЕЛЬНО ДОЛЖНЫ ЗНАТЬ О НЕМ ВРАЧИ

Во всех медицинских учреждениях Подмосковья в скором времени должен появиться бесплатный Wi-Fi. Пользоваться им без ограничения смогут как врачи, так и пациенты. Пока свободный доступ к Интернету в тестовом режиме получили лишь некоторые столичные клиники, однако в планах Министерства здравоохранения «опутать» сетью как можно больше лечебных заведений.

Кому это нужно?

1. Пациентам. Безлимитный доступ к Интернету позволит постоянно поддерживать связь с родственниками, своевременно получать отзывы о работе врачей, при необходимости самостоятельно расшифровать анализы, дистанционно учиться или работать при длительном пребывании в стационаре. Ну и, конечно, развлечь себя любимым фильмом или давно отложенной в закладки книгой.

2. Врачам. Для развития медицинских технологий, ведения электронной истории болезни пациента и оперативного получения результатов обследований в любом медучреждении, проведения совещаний и консилиумов в режиме видеоконференции, а также для скорейшего выздоровления больных. Ведь беспроводная связь, по мнению экспертов, поможет пациентам не чувствовать себя оторванными от внешнего мира.

Одними из первых получили доступ к Wi-Fi посетители консультативно-диагностических центров, то есть поликлиник Московского областного научно-исследовательского институт имени М. Ф. Владимирского (МОНИКИ).

«Видя табличку с надписью «Wi-Fi free», как в метро, пациенты бывают очень довольны, – говорит Д. Жернов, руководитель службы информационных технологий МОНИКИ. – Сегодня Wi-Fi входит в список обязательных пунктов, рекомендованных губернатором Московской области для повышения комфортности пребывания в больнице. Это так же важно, как удобная автомобильная парковка, помещение для детских колясок, доступная среда

и наличие таких приятных вещей, как кулер, кафе, телевидение, инфомат для электронной записи к врачу и определения своего места в очереди».

Коротко о главном

Ученые Калифорнийского университета в Дэвисе уверены, что общение пациентов с родными и друзьями – не просто развлечение, но и часть лечебного процесса. 367 детей, госпитализированных в больницу при университете, приняли участие в эксперименте американских врачей. Результаты подтвердили: видеосвязь с родными с помощью iPad способствовала скорейшему выздоровлению маленьких пациентов в отличие от сверстников, лишенных этой возможности. Все дело в положительных эмоциях. И подобных исследований на сегодня немало.

Взрослые больные все равно что дети. Такие, на первый взгляд, мелочи, как узкое оконце в палате или равнодушный взгляд медсестры, могут ухудшить их самочувствие. Грамотные врачи знают, что выздоровление начинается с победы над депрессией. Зависимость физического состояния от психологического ярко иллюстрирует эффект плацебо, когда «пустая таблетка» способна существенно повлиять на биохимию человека только из-за веры в ее полезные свойства. В этой ситуации необъятные возможности глобальной сети смогли бы сослужить эскулапам хорошую службу хотя бы по причине ее развлекательной функции. Но лишь при одном условии – выход в интернет-пространство должен быть максимально комфортным для пациента.

Головная боль для главных врачей

Но информатизация больниц грозит обернуться головной болью для главных врачей.

Сотрудники одной из ведущих российских компаний в области разработки комплексных средств информационной безопасности, организации и контроля интернет-доступа – «Смарт-Софт» предупреждают о «побочных эффектах», которые могут возникнуть в связи с тотальным оснащением публичными сетями Wi-Fi медицинских учреждений.

1. Сбои из-за некачественной раздачи интернет-доступа в связи с чрезмерной нагрузкой на сеть Wi-Fi. К примеру, кто-то из пациентов решил скачать фильм, а врач в это время не может получить важные сведения о состоянии больного. Более того, соседи по палате начинают нервничать из-за того, что их неплохой вроде бы смартфон завис (как сказываются на здоровье пациентов негативные эмоции, мы уже знаем). Сбои в основном происходят, если не подключены функции мониторинга и контроля пользовательского доступа. И разобраться в данном вопросе под силу только высококлассным IT-специалистам.

2. Не работает система идентификации пользователей по СМС, за что начнут штрафовать уже с 2016 года. Вряд ли у главных врачей есть время, чтобы изучать тонкости интернет-законодательства.

3. А еще руководителей медицинских учреждений могут обвинить в причинении вреда здоровью и развитию детей по причине отсутствия контентной фильтрации. Говоря проще, если больница, в которой могут находиться несовершеннолетние, наряду с полезными сервисами раздает и доступ к запрещенным ресурсам, она нарушает ФЗ-436 о защите детей от вредной информации. Данное обстоятельство влечет наложение солидных штрафов. Кстати говоря, прецеденты уже имеются: в Барнауле, к примеру, оштрафовали сеть пиццерий.

Что делать?

Избавить от этих и других проблем сможет комплексное программное обеспечение для организации комфортного и безопасного доступа в Интернет сотрудникам и пациентам больниц. Двенадцатилетний опыт разработки собственных систем комплексной IT-защиты позволил «Смарт-Софт» создать специальную версию ПО для организации интернет-подключения в медучреждениях.

Центр восстановительной терапии им. М. А. Лиходея – один из первых, кто воспользовался Traffic Inspector.

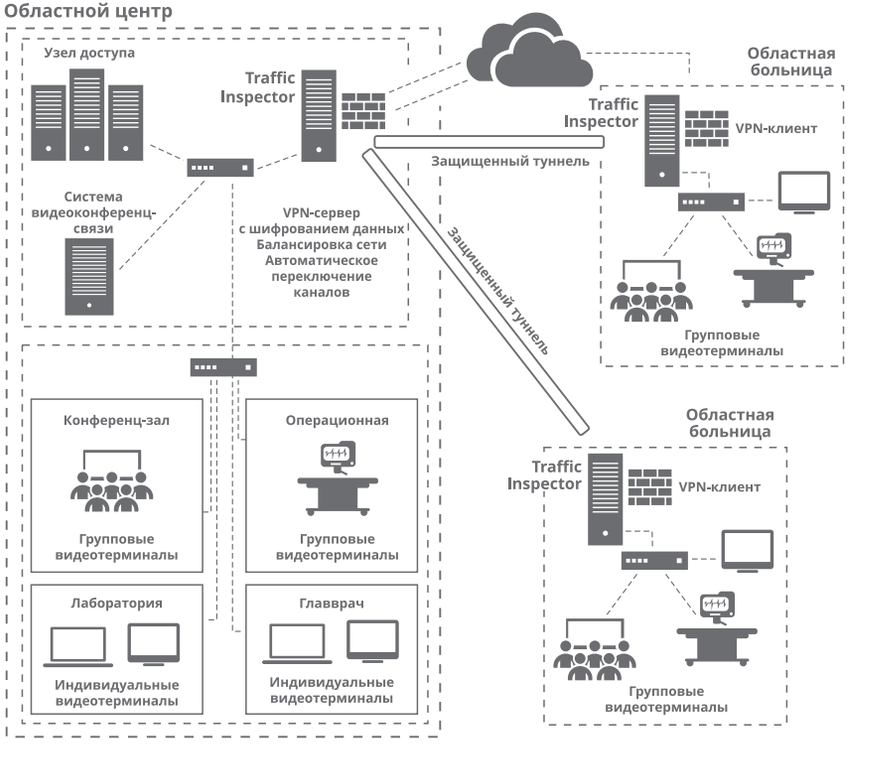
– Программное обеспечение отлично работает, пациенты довольны, – рассказал инженер-программист медицинского учреждения Э. Байдаков.

А в городе Коломне все еще ломают голову, как правильно организовать раздачу бесплатного Wi-Fi для пациентов местных больниц.

О. Трипутень, начальник отдела информационных технологий Коломенской ЦРБ:
– Организовать грамотную раздачу Wi-Fi в поликлиниках – задача технически сложная. Не допустить утечку персональных данных, равномерно распределить беспроводной Интернет по всей огромной территории, защитить сеть от несанкционированного доступа – все эти вопросы под силу решить только специалистам в области IT-технологий.

3. СЕТЬ БЕЗ ПРОБЛЕМ: КАК ОРГАНИЗОВАТЬ ИНТЕРНЕТ-ДОСТУП В МЕДИЦИНСКОМ УЧРЕЖДЕНИИ

Задачи по организации сети медучреждения в соответствии с законодательством РФ можно решить разными способами. Покупать отдельные программы, оборудование, тратить время на их интеграцию, настройку, поддержание работоспособности. Или приобрести комплексное решение Traffic Inspector, проверенное временем и клиентами, имеющее необходимые сертификаты, понятную документацию и обеспеченное технической поддержкой компании-разработчика.



Типичная схема локальной сети

TRAFFIC INSPECTOR

Отзывы пользователей о работе с Traffic Inspector

Каждый пользователь Traffic Inspector, несмотря на то, что находится на значительном удалении от центральной поликлиники, надежно защищен от внешних угроз. Пациенты также могут не беспокоиться об утечке персональных данных, ведь программа сертифицирована ФСТЭК России по самому высшему классу К1 ИСПДн. Успешный трехлетний опыт использования решения Traffic Inspector от «Смарт-Софт» позволяет рекомендовать продукт другим организациям здравоохранения как лучший в своем классе для обеспечения эффективного и безопасного интернет-доступа в лечебных учреждениях».

Пигарева А. Л., главный врач,
МУЗ «Коломенская ЦРБ»

В корпоративной сети санатория 80 пользователей, которые ежедневно используют внутреннюю сеть и Интернет, а качественный межсетевой экран – залог эффективной и безопасной работы всей организации. К тому же Traffic Inspector простой, удобный в настройке и работе. Администрация санатория выражает благодарность разработчику и рекомендует российское программное обеспечение Traffic Inspector – качественный и надежный продукт».

Мосиенко С. В., директор
ФБЛПУ «Санаторий «Эллада» ФНС России»

За последние 2 года использования продукта проблем с информационной безопасностью не возникало. Выражаем благодарность компании «Смарт-Софт» за стабильность решения и рекомендуем Traffic Inspector для использования в учреждениях здравоохранения».

Овечкин П. Г., главный врач,
Ханты-Мансийская клиническая станция

4. ИСТОРИЯ УСПЕШНОГО ВНЕДРЕНИЯ: НУЗ «УЗЛОВАЯ БОЛЬНИЦА НА СТАНЦИИ ТИМАШЕВСКАЯ ОАО «РЖД»

Попробуйте представить современное предприятие без должного технического оснащения? Например, медицинское учреждение, в котором нет коек, кардиографа, рентгена и необходимого минимума для обслуживания пациентов. На счету каждая минута, а оперативность и своевременная диагностика – залог успешного лечения больного.

С появлением компьютерных сетей прогресс всей медицинской сферы продвинулся сразу на несколько десятилетий вперед. Ведь теперь вместо изнурительного путешествия по кабинетам в поисках нужного врача и очередей для получения результатов анализов достаточно нажать всего несколько клавиш.

Но в Сети, как и в медицине, нужно точно знать, какие методы использовать и какое решение будет максимально эффективным.

Понимая это, руководство НУЗ «Узловая больница на станции Тимашевская ОАО «РЖД» приняло решение о необходимости реорганизации сетевого доступа в пределах частной сети. Выбор пал на комплексное решение информационной безопасности Traffic Inspector.

Опасения руководства

Современный человек без Интернета чувствует себя некомфортно. Доступ к глобальной Паутине вполне можно сравнить с кислородом. Именно поэтому табличка с указанием «Бесплатный Wi-Fi» подсознательно успокаивает нашу суетливость и волнение: «Здесь меня точно ждут. Здесь уютно, и время ожидания пролетит незаметно», ведь здесь есть выход в Сеть.

Правила оказания услуг связи по передаче данных посредством общественных сетей Wi-Fi имеет несколько специфический характер. Регламентируется такая услуга так называемым Федеральным законом о Wi-Fi. Согласно принятому Правительством РФ Постановлению № 758 от 31 июля 2014 года и Постановлению № 801 от 12 августа 2014 года, все владельцы бесплатных точек доступа Wi-Fi в обязательном порядке должны выдавать

авторизованному в сети пользователю идентификатор – т. е. системный администратор в любой момент времени обязан знать, какой из выданных MAC-адресов принадлежит работнику больницы, а какой – пациенту или гостю.

Более того, предоставление доступа в Интернет без надлежащего контроля чревато самыми неблагоприятными последствиями. Используя незащищенную Wi-Fi-сеть, можно не только скрасить свой досуг, но и получить доступ к ресурсам, не допускающим анонимности.

Задачи, которые предстояло решить

В Узловой больнице на железнодорожной станции Тимашевская работает около 100 сотрудников. Учитывая, что в частной клинике есть и стационар, и физиотерапевтическое отделение, и сама поликлиника, организация сети несколько усложнялась. Перед специалистами-сетевиками и сетевым экраном Traffic Inspector стоял следующий перечень приоритетных задач:

- интегрировать возможность идентификации каждого пользователя частной сети;
- установить глобальный контроль корпоративной сети с возможностью фильтрации трафика и удаленного отключения как привязанных, так и гостевых MAC-адресов;
- ограничить доступ пользователей к определенным ресурсам;
- настроить фильтрацию веб-трафика согласно установленным руководством критериям.

И весь этот спектр запросов необходимо было развернуть на интуитивно понятном и доступном интерфейсе, не требующем долгосрочного обучения системного администратора и штудирования узкопрофильных документаций.

Правильный выбор и безграничные возможности

«Ну наконец-то они начали работать, а не сидеть в социальных сетях!» – Лазоркин Виктор Александрович, врач высшей категории.

С 2001 года возглавляет НУЗ «Узловая больница на ст. Тимашевская ОАО «РЖД». В понимании корпоративных сетей НУЗ «Узловая больница на станции Тимашевская ОАО «РЖД» относится к сетям среднего уровня сложности. Критерий для соответствующего оборудования – универсальный продукт с гибкой функциональностью, но без лишней опциональной перегрузки.

В качестве сетевого экрана был выбран отечественный продукт Traffic Inspector от компании «Смарт-Софт». Сочетая в себе сразу несколько преимуществ перед конкурентами, Traffic Inspector решил целый комплекс задач:

- идентификация пользователей – разработанный компанией «Смарт-Софт» сетевой экран позволил в полной мере удовлетворить требования Федерального закона «Об информации, информационных технологиях и о защите информации». Предоставление доступа к публичной Wi-Fi-сети в рамках НУЗ теперь осуществляется строго с идентификацией пользователя;
- активная защита трафика – Traffic Inspector позволил контролировать входящий трафик с предварительной очисткой от спама и вирусов;
- почтовый шлюз – в рамках больницы стало возможным построение собственного почтового сервера, на котором хранится вся корпоративная переписка и базы пациентов клиники;
- ограничение доступа – руководство получило возможность внутрисетевой блокировки социальных сетей и отдельных ресурсов, пользующихся особой популярностью среди персонала, но не имеющих прямого отношения к работе;
- гибкая маршрутизация – в режиме реального времени системный администратор может контролировать количество активных пользователей Сети, а также следить за категориями подключенных устройств с возможностью моментального отключения;
- доступный интерфейс – сетевой экран Traffic Inspector работает под управлением любой операционной системы Windows, начиная с седьмой версии. Учитывая уже установленный в поликлинике Windows-совместимый сервер, выбор был очевиден.

На проектирование сети специалисты потратили минимум времени, а сделать пришлось не так мало: от индивидуальной настройки каждого персонального компьютера до внедрения блокировки посредством прокси-серверов. Уже через две недели со дня подписания договора сетевой экран Traffic Inspector встал на страже безопасности корпоративной сети НУЗ «Узловая больница на станции Тимашевская ОАО «РЖД».

Разумная экономия

Компания «Смарт-Софт» сумела обеспечить целостность Сети в рамках Узловой больницы на станции Тимашевская. В настоящее время настроена блокировка посторонних интернет-ресурсов, за счет чего была существенно разгружена нагрузка на Сеть. Пропорционально этому выросла и скорость.
Руководству НУЗ «Узловая больница на станции Тимашевская ОАО «РЖД» был предложен оптимальный вариант сетевого мониторинга, а продукт

Traffic Inspector помог сэкономить не одну тысячу рублей. Учитывая гибкость настройки Traffic Inspector, дальнейшее совершенствование и надстройка дополнительных опций может проходить уже без вмешательства специалистов компании «Смарт-Софт».

5. С ПОЛЬЗОЙ ДЛЯ ДЕЛА: РЕСУРСЫ ДЛЯ МЕДУЧРЕЖДЕНИЙ

Медицина и право

http://med-pravo.ru/

Сборник законов, постановлений в сфере медицины и фармацевтики.

Медицинский вестник

http://medvestnik.ru/

Портал российского врача.

Федеральная электронная медицинская библиотека

http://feml.scsml.rssi.ru/

Федеральная электронная медицинская библиотека (ФЭМБ) входит в состав единой государственной информационной системы в сфере здравоохранения в качестве справочной системы.

Федеральная служба по надзору в сфере здравоохранения

http://rosminzdrav.ru/

Телефон «горячей линии»: **8 (800) 200-03-89.**

О КОМПАНИИ «СМАРТ-СОФТ»

«Смарт-Софт» сегодня – это:

2500 ПАРТНЕРОВ

Более 2500 партнеров на российском и международном рынках

4 500 000 ЧЕЛОВЕК

4 500 000 человек работают в сетях, где установлены наши решения

14 ЛЕТ

14 лет на рынке информационной безопасности

3 АССОЦИАЦИИ

Экспертное членство в трех ассоциациях: АРПП «Отечественный софт», «Руссофт», Некоммерческое партнерство «Союз защитников информации»

КОНТАКТЫ

Звоните: +7 (495) 77-55-991.
Пишите: info@smart-soft.ru.
Заходите: www.smart-soft.ru.