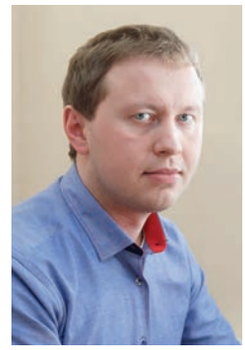
УДК 004.724.2:614.2

Мобильный доступ к медицинской информации и бесконтактная идентификация пациентов

В статье рассматриваются вопросы удаленного доступа к данным медицинских информационных систем (МИС). Для идентификации пациентов при доступе медицинских работников к электронным медицинским картам предлагается использовать технологию беспроводной передачи данных Near Field Communication (NFC), применимую к условиям медицинских учреждений Республики Беларусь. Предлагаемый подход упрощает процесс идентификации, повышает его быстродействие и надежность.



Е.А КАРШАКЕВИЧ,
аспирант факультета информационных технологий и робототехники БНТУ, инженер-электроник УЗ «19-я центральная районная поликлиника Первомайского района г. Минска»

Ключевые слова:
сети передачи данных, электронное здравоохранение, медицинские информационные системы, идентификация пациентов.

Введение. Одной из насущных задач современной системы здравоохранения является организация удаленного и мобильного доступа к данным МИС. Эти системы обеспечивают работоспособность широкого спектра специфичных процессов и средств (медицинские электронные карты и рецепты, электронная запись на прием, дистанционная диагностика и пр.). Необходимость решения упомянутой задачи вытекает из «Концепции развития электронного здравоохранения Республики Беларусь до 2022 г.». Актуальность данной тематики обусловлена также запланированным переходом в 2020 г. амбулаторно-поликлинических учреждений г. Минска на работу по принципу врача общей практики, тенденцией расширения приема и медицинского ухода на дому, эпидемиологической обстановкой, вызванной коронавирусной инфекцией.

Основная часть. Анализ практики удаленной работы с локальными МИС выявил необходимость совершенствования имеющейся схемы идентификации пациентов. Возникают ситуации, когда невозможно быстро и однозначно идентифицировать пациента в системе, например при частичном совпадении идентификационных данных (ФИО, адрес и т. д.) или когда пациент находится в бессознательном состоянии. В результате возможны случаи ошибочного ввода информации в электронные карты других пациентов или отсутствует возможность оперативного получения анамнеза пациента для выбора тактики лечения.

Проблема частично решается внедрением в обращение персональных карт для медицинского обслуживания (ПКМО). Это позволяет каждому пациенту присвоить персональный идентификатор, который нанесен на карту в виде штрих-кода, и использовать его для поиска пациента в МИС. Однако тенденции расширения сферы удаленной работы с МИС при помощи мобильных устройств требуют дополнительных решений, обеспечивающих скорость, надежность и удобство получения информации.

В статье предлагаются вариант организации удаленной работы с МИС и альтернативный существующему способ идентификации пациента.

Для доступа к электронной медицинской карте пациента (далее – ЭМК) предлагается идентификация по NFC-метке. Near Field Communication (NFC – коммуникация ближнего поля) это технология беспроводной передачи данных малого радиуса действия между устройствами, находящимися на расстоянии до 10 сантиметров. По сути, NFC это частный случай RFID (Radio Frequency Identification Data) – механизма радиочастотного обмена данными, хранящимися в так называемых транспондерах, или метках, который основан на

стандартах ISO/IEC 18092 NFC IP-1, JIS X 6319-4 и ISO/IEC 14443 для бесконтактных смарт-карт [1].

NFC-устройство работает на частоте 13,56 МГц и состоит из считывателя (ридера) и антенны или из метки и антенны (рис. 1) [2]. Ридер генерирует радиочастотное поле, которое может взаимодействовать с меткой или с другим ридером. Ридер – это устройство NFC, работающее в режиме активной коммуникации. Метка – устройство NFC, которое работает в режиме пассивной коммуникации.

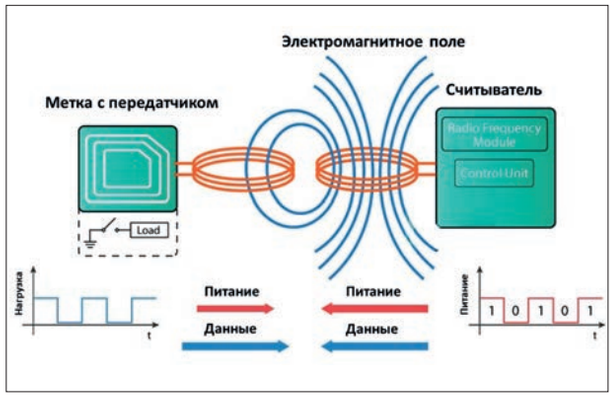


Рисунок 1 – Схема бесконтактной передачи данных NFC

NFC-метки нашли свое применение в различных сферах жизнедеятельности человека. Их используют в банковских картах, проездных билетах, картах лояльности, IoT («интернете вещей»), системах идентификации и контроля доступа, гостиничном бизнесе, маркетинге и рекламных предложениях, контроле подлинности товаров.

В медицине NFC-метки представлены браслетами и картами, на которых хранятся личные данные и важная информация о здоровье, заболеваниях и аллергиях. Данные можно считать телефоном с поддержкой NFC. Также браслеты помогают в повседневных ситуациях людям с опасными для жизни состояниями, такими как диабет, астма, аллергия на продукты питания или лекарства. Медицинские NFC-браслеты, также позволяют отслеживать перемещение пациентов, сотрудников, что больше относится к идентификации в системе контроля доступа, чем к здравоохранению.

Электронные данные нуждаются в такой же защите от несанкционированного доступа, как и физические бумажные документы. Поэтому использование NFC для управления доступом к МИС – удобный и более безопасный способ доступа к данным. Для реализации такого доступа к МИС необходимо выстроить определенную инфраструктуру, учитывая особенности оборудования, технических решений и требований информационной безопасности (рис. 2).

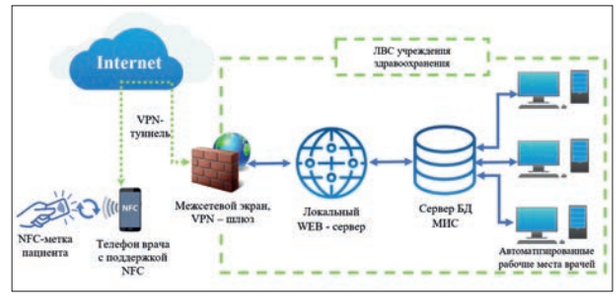


Рисунок 2 – Схема обмена информацией при удаленной работе врачей с МИС через мобильное устройство с поддержкой NFC

Ключевую роль в предложенной схеме обмена играют несколько технических решений. Во-первых, это наличие защищенного канала связи между мобильным устройством врача и локальной сетью учреждения. Получить закрытый канал связи можно через VPN-соединение (англ. Virtual Private Network виртуальная частная сеть) — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, интернета) [3]. Наибольшее практическое применение нашли UTM-системы (Unified Threat Management, шлюз безопасности) – аппаратное и программное обеспечение, которое обеспечивает защиту локальной сети. UTM-система включает следующие функциональные блоки: межсетевой экран уровня приложений, подсистему обнаружения и предотвращения вторжений, встроенный VPN-сервер, подсистему антивирусной защиты, модуль управления полосой пропускания, модуль поддержки.

Используя VPN-соединение, пользователь получает полноценный доступ к локальным ресурсам сети учреждения [4]. Для дополнительной защиты передаваемых данных может быть использовано программное средство канального шифрования. Таким образом, можно обеспечить шифрование и контроль целостности сетевого трафика, аутентификацию сторон и выработку общего сеансового ключа [5].

Во-вторых, наличие веб-сервера, который позволяет реализовать процесс авторизации пользователей в системе и обеспечивает прием и обработку http-запросов к серверу МИС, выдает http-ответы в удобном виде.

В-третьих, поддержка технологии передачи данных NFC на мобильном устройстве врача для прочтения NFC-метки пациента. В данном случае доступ к данным о пациенте будет основан на связке «метка – ридер». Метка может быть использована в любом форм-факторе (брелок, карта, браслет, наклейка) и даже записана на мобильное устройство пациента. На NFC-метку записывается http-запрос (ссылка) по персональному идентификатору

к электронной карте пациента на локальном веб-сервере. На метку кроме ссылки, дополнительно может быть записана важная информация о здоровье и личные данные. Дополнительная информация на метке позволит получить базовую информацию о пациенте в случае отсутствия связи с сервером МИС.

Ссылку на медицинские данные в локальной МИС можно интерпретировать в QR-код, который, как и NFC-метка, предоставит доступ к информации о пациенте при условии наличия VPN-соединения с сервером.

Если применить единый, универсальный подход при построении системы обмена данными мобильных устройств с локальным web-сервером организации здравоохранения и определить правило построения пути (ссылки) в системе на основе персонального идентификатора, то еще на этапе выпуска ПКМО можно записать нужную ссылку в NFC-метку и нанести QR-код со ссылкой на карту пациента. Защита от записи и копирования NFC-меток дополнительно повысит надежность идентификации. При масштабировании архитектуры системы здравоохранения в региональные МИС может быть применена аналогичная схема работы по VPN и идентификации пациентов по NFC на региональном сервере. В перспективе возможно использование мобильных телефонов пациентов с поддержкой NFC для эмуляции метки доступа к ЭМК.

Заключение. Работа с медицинскими данными с применением NFC-меток позволяет однозначно идентифицировать пациентов, сделав этот процесс быстрым и безошибочным. Предложенный метод идентификации хорошо интегрируется в существующую систему информатизации здравоохранения. Безопасность метода обусловлена наличием ряда технических решений при реализации: VPN-туннель на считывающем устройстве врача с сетью медучреждения, поддержка NFC, авторизация пользователей в МИС на веб-сервере. Каждое техническое решение по-своему защищает данные от несанкционированного доступа. Описанные методы организации информационного взаимодействия с помощью VPN-соединений [4] и защитой интернет-соединения с применением канального шифрования данных активно используются в работе УЗ «19-я центральная районная поликлиника Первомайского района г. Минска».

Таким образом, перед врачами открывается возможность удаленной работы с информацией о пациенте в пределах их компетенции и упрощается процесс идентификации пациентов. Применение NFC в работе с МИС позволит сократить время контакта врача и пациента, что особенно актуально в период пандемии.

ЛИТЕРАТУРА

1. NFC от «А» до «Я» подробно рассказываем что такое, и как NFC в телефоне изменит жизнь каждого // securityrussia.com [Электрон. ресурс]. – 2020. – Электронные данные. – Режим доступа: ttps://securityrussia.com/blog/nfc.html – Дата доступа: 20.04.2020.
2. Что такое NFC // prom-tex.org: [Электрон. ресурс]. – 2020. – Электронные данные. – Режим доступа: https://www.prom-tex.org/solutions/mnogokanalnyy-sbor-dannykh/nfc-telemetriya-i-sensornye-seti/ – Дата доступа: 22.05.2020.
3. VPN - Wikipedia // wikipedia.org: [Электрон. ресурс]. – 2020. – Электронные данные. – Режим доступа: https://ru.wikipedia.org/wiki/VPN – Дата доступа: 11.05.2020.
4. **Каршакевич Е.А.** Организация удаленной работы врачей с медицинскими информационными системами // Каршакевич Е.А. // Вестник Связи. – 2018. – № 5 (151). – с. 53–56.
5. itVPN - Программное средство канального шифрования // ittas.by [Электрон. ресурс]. – 2020. – Электронные данные. – Режим доступа: https://www.ittas.by/solutions/itvpn/. – Дата доступа: 22.04.2020.

The article describes the scheme of remote work of doctors with a medical database using mobile devices. Author Suggests using NFC to quickly and correctly identify patients. Remote access to the medical information system is organized using VPN technology. The proposed option of remote work can simplify the process of patient identification, make it quick and error-free.

Key words: *e-health, medical information systems, patient identification.*

Получено 22.06.2020.