находится у нас в распоряжении, оно не принадлежит нам, в этом и заключается проблема. Это досье скажет о нас больше, чем мы сами, так как вы не помните и половины всех событий, что происходили с вами до этого момента. Есть компании, которые занимаются созданием персональных черных ящиков, подобных вашему виртуальному досье. Ваш персональный цифровой профиль хранит и дополняет всю эту информацию и ее можно монетизировать. Суть этого в том, что это также помогает защищать личные данные. А если мы стремимся к свободному обществу, то стоит начать с защиты доступа к личным данным.

Большинство контентмейкеров получают несправедливо мало, потому что система интеллектуальной собственности несовершенна. На примере музыкантов видно, что их записи слушают миллионами, но при этом исполнитель по большей части получает деньги не с продажи своей музыки, а с концертов. Певица Imogen Heap сегодня выкладывает песни в среду blockchain. Музыка находится под защитой, интеллектуальная собственность находится под защитой. Прослушать песню вы сможете либо прослушать бесплатно, либо необходимо заплатить некоторую криптовалюту, которая переведется на цифровой счет. Хотите, чтобы песня была в вашем фильме – придется следовать условиям, прописанным в коде. Поставить песню на рингтон – другие условия. Все эти права специально оговорены. Песня будто становится самостоятельной, все деньги, которые переводятся на счет песни, идут непосредственно к музыканту, таким образом музыканту остается только отправить песню в реестр, а в дальнейшем получать с нее прибыль.

Если вы еще не поняли, что же такое blockchain, то есть один пример. Представьте, что есть какой-то остров, где живет небольшое племя. Их валюта - это большие камни, которые они не могут передвинуть. Назовем такой камень стоун. Они лежат в разных точках острова, но все жители об этом знают. Если кто-то из жителей хочет заплатить другому за какую-либо услугу, то собирается все племя и все узнают о том, что этот bitcoin теперь принадлежит другому жителю. Такая система лучше, так, как если бы учетом этих стоунов занимался один житель, то тут влиял бы еще и такой фактор, как честность. Если этот житель по какой-либо причине исчезнет, то весь учет пропадет. И тут снова будет играть роль фактор честности. Найдутся те жители, которые захотят приобрести себе чей-то стоун обманом. Вернемся к предыдущей системе. В случае, если один из жителей пропадет. Учет останется, так как каждый из жителей знает о том, кому принадлежит определенный стоун. Даже если вдруг один из стоунов скатится в море, жители могут запомнить, что у этого жителя есть этот стоун, но он не находится на суше.

Таким образом можно провести аналогию с blockchain'ом. Жители – это компьютеры майнеров. Когда проводится какая-то операция то множество этих компьютеров это фиксируют, при этом обеспечивая безопасность этой транзакции.

В последнее время выражалось много недовольства по поводу безопасности информации и по поводу защиты интеллектуальной собственности. Blockchain решит эти проблемы и сделает привычное еще проще. Blockchain будет способствовать развитию творчества, оно перестанет быть просто хобби, зарабатывать на своем таланте будет проще. Понимая принцип работы Blockchain'а, можно определить потенциал этой системы и то, на сколько изменится ваша жизнь.

Список используемых источников

1. Fleming, Stephen. Blockchain technology: Introduction to blockchain technology and its impact on Business Ecosystem/Stephen Fleming. – Stephen Fleming, 2017

2. Sean, Bennet. Blockchain: a guide to understanding blockchain/ Bennet Sean. – Cryptomasher via PublishDrive, 2017.

3.Описание технологии blockchain і [Электронный ресурс]. — Код доступа: https://www.investopedia.com/terms/b/blockchain. – Дата доступа: 05.03.2018.

СОСТОЯНИЕ ЗАЩИТЫ ПЕРСОНИФИЦИРОВАННЫХ МЕДИЦИНСКИХ ДАННЫХ В БЕЛАРУСИ В 2018 ГОДУ

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Ситник М.Ю.

Сечко Г.В. – доцент каф. ИСиТ, к.т.н,, доцент

Представлен анализ защиты персонифицированных данных в лечебных медицинских учреждениях

Анализируется терминология в области персональных данных пациента и предлагается именовать их персонифицированными медицинскими данными. На примере 29-й минской поликлиники анализируется состояние защиты персонифицированных медицинских данных в Беларуси в 2018 году. Показывается, что для минимальной защиты конфиденциальных персонифицированных медицинских данных, нужно полностью отказаться от всевозможных бумажных носителей медицинских данных и перейти на электронные, в том числе исключить хранение бумажных документов в регистратуре поликлиники. При исключении бумажной документации в медучреждении защиту данных в ЛВС медицинского учреждения традиционными методами (защита от несанкционированного доступа, защита от хакерских атак и т. д.)) можно считать достаточной, а, главное, дешёвой. Естественно, однако, что в этом случае стопроцентной гарантии исключения утечки данных для пациента через работников медучреждения нет. Для повышения уровня защиты персонифицированных медицинских данных состоятельных пациентов предлагается использовать белорусские биометрические средств контроля доступа к рассматриваемым данным.

Характер медицинской деятельности связан с использованием большого количества данных о здоровье пациента, истории его болезней, истории обращения к врачу и других данных. Эти данные содержатся в

медицинских документах, которые оформляются сотрудниками медицинских учреждений на каждого пациента или их группу. Медицинская документация – это документы установленной формы, предназначенные для регистрации результатов лечебных, диагностических, профилактических, реабилитационных, санитарно-гигиенических и других мероприятий. Примерами медицинских документов для Беларуси являются «Медицинская карта амбулаторного больного», «Медицинская карта стационарного больного» «Медицинская карта амбулаторного больного инфекциями, передаваемыми половым путем», «Медицинская карта больного грибковым заболеванием, чесоткой», «Медицинская карта амбулаторного больного кожным заболеванием», рецепт на лекарство и другие.

Однако, как следует из паспортной части, например, «Медицинской карты амбулаторного больного», в медицинских документах содержатся не только медицинские, но и персональные данные пациента. Согласно Федеральному закону Российской Федерации «О персональных данных» от 27.07.2006 N 152-ФЗ (статья 3, пункт 1) персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Ссылка на закон РФ сделана только потому, что аналогичный закон Беларуси готовится к принятию только в 2019 году.

Комплект персональных данных пациента вместе с его медицинскими данными будем именовать персонифицированными медицинскими данными (ПМД, название «персональные данные пациента» – синоним»). Именно эти данные – клад для мошенников [1]. Как утверждают независимые эксперты, на чёрном рынке ценность медицинской информации в 10 раз выше финансовой. Полученные незаконным методом сведения о здоровье могут использоваться в ущерб пациентов. Это и обман пенсионеров, когда им пытаются продать препараты-пустышки за баснословные суммы, и желание выручить деньги с угрозами обнародования диагнозов у известных личностей, и другие случаи [2]. Отсюда вытекает задача защиты персональных данных пациентов, которым такая защита нужна. Рассмотрим состояние защиты персонифицированных медицинских данных в Беларуси в 2018 году на примере сорока минских поликлиник для взрослых и, включая 13-ю военную и 33-ю студенческую, и 16 детских поликлиник, включая поликлинику Минского района в Боровлянах. Пациенту, обратившемуся в поликлинику, оформляют вручную «Медицинскую карту амбулаторного больного» и, при наличии в поликлинике нужного софта и указания главврача поликлиники, в регистратуре заполняют «Электронную медицинскую карту (ЭМК) [3, 4]» пациента, которая затем автоматически включается в электронную картотеку пациентов (часть базы ПМД поликлиники). Необходимый для заполнения ЭМК софт в Беларуси разрабатывают 5 основных организаций, крупнейшая из которых – ЗАО МАПСОФТ, чей софт работает в 36 из 56 взятых на рассмотрение поликлиник, что составляет 64 % от охваченных автоматизацией поликлиник. Программа для ЭМК в комплексе ПО для медицины ЗАО МАПСОФТ, называется «Регистратура», Если несмотря на наличие программы «Регистратура» в закупленном комплексе ПО для медицины в поликлинике нет или нет указания главврача поликлиники на её применение по причине, например, отсутствия финансирования, то в поликлинике остается только бумажный вариант «Медицинской карты амбулаторного больного». При этом в Беларуси никто не требует у пациента согласия на обработку его персональных данных из ПМД, что предусмотрено статьей 6 (пункт 1 подпункт 1.1) закона РФ «О персональных данных» от 27.07.2006 N 152-ФЗ.

В начале февраля 2014 года появилась информация [3], что в Минске на базе 29-й поликлиники начали тестировать работу ЭМК. Собственно ЭМК, как рассказала главный врач поликлиники Раиса Григорьевна Званец в интервью информационному агентству «Минск новости», представляет собой электронный вариант амбулаторной карты. Причем, по заверению врача, оцифрованы были медицинские карты всех 39 тысяч пациентов поликлиники. Финансировал работы госбюджет, затем эксперимент с белорусской ЭМК в 29-й поликлинике был заморожен до настоящего времени из-за отсутствия дальнейшего финансирования. База оцифрованных ЭМК при этом устарела.

Но, предположим, что база ПМД базе 29-й поликлиники, все 39 тысяч ЭМК, попадут в ЛВС поликлиники. Обеспечит ли поликлиника их надёжную защиту? Мы полагаем, что нет. Во-первых, регистратура поликлиники до сих пор хранит бумажные варианты «Медицинских карт амбулаторного больного». При существующей зарплате медрегистратора в 300 рублей в месяц нет гарантии в том, что за 10 рублей наличными он не представит доступ к любой карте любому злоумышленнику. Во-вторых, при отказе от всевозможных бумажных носителей ПМД и переходе на электронные стопроцентной гарантии исключения утечки данных для пациента через работников медучреждения нет. Действительно, традиционные методы защиты информации в ЛВС медицинского учреждения обеспечивают некоторый уровень защиты, но не исключают утечку данных для пациента через работников медучреждения нет. К числу таких работников относится системный администратор поликлиники, главврач, начмед и некоторые другие. Полагаем, что материально обеспеченные пациенты могут достичь более высокого уровня защиты своих ПМД аутентификацией за умеренную плату своей личности по радужке с помощью описанного в [5, 6] архиватора. Предварительный расчёт показал, что что при хранении в базе архививатора в течение трёх лет примерно 2000 изображений радужки стоимость аутентификации, включающая затраты на покупку и эксплуатацию архиватора, для одного пациента составит примерно 100 рублей

Воспользоваться аутентификацией по радужке могут и менее обеспеченные пациенты, если утечка информации может привести к значительным негативным последствиям для таких пациентов.

Следует отметить также, что обеспечение защиты ПМД в Беларуси даже после принятия белорусского Закона о персональных данных встретит ряд негативных моментов, имеющихся в России, которая опережает Беларусь в данной области (даже в части упомянутого Закона). Например, в [7] указано, что:

1. Даже если у врача на столе стоит компьютер с ЭМК, ему по привычке проще пользоваться бумажными документами.

2. Обычно в медицинских организациях нет выделенного человека и/или подразделения по информационной безопасности, а в небольших медицинских учреждениях нет даже своих системных администраторов. При этом основные пользователи информационных систем (врачи и младший медицинский персонал) часто имеют низкий уровень осведомленности и компьютерной грамотности.

3. Недостаток финансирования. Когда у главврача стоит дилемма, что купить: томограф или средства защиты информации, выбор всегда будет в пользу томографа, потому что именно это прибор позволяет

обеспечить основную функцию лечебно-профилактического учреждения – защиту здоровья граждан. Здесь надо искать компромисс. Надо, чтобы менеджеры от медицины осознали важность проблемы защиты персональных данных своих пациентов».

ВЫВОДЫ. 1. Чтобы минимально защитить конфиденциальные ПМД, нужно отказаться от всевозможных бумажных носителей медицинских данных и перейти на электронные. К сожалению, в части внедрения электронных медицинских карт Беларусь намного отстаёт от России. Отставание имеется и в части законодательства.

2. При исключении бумажной документации в медучреждении защиту ПМД в ЛВС медицинского учреждения традиционными методами (защита от несанкционированного доступа, защита от хакерских атак и т. д.)) можно считать достаточной, а, главное, дешёвой. Естественно, однако, что в этом случае стопроцентной гарантии исключения утечки данных для пациента через работников медучреждения нет.

3. Наиболее материально обеспеченные пациенты могут достичь более высокого уровня защиты своих ПМД аутентификацией за умеренную плату своей личности по радужке с помощью описанного в [5] архиватора. Воспользоваться аутентификацией по радужке могут и менее обеспеченные пациенты, если нарушение заданной характеристики безопасности ПМД, обрабатываемых традиционными методами, может привести к значительным негативным последствиям для таких пациентов.

Список использованных источников.

1. Защита персональных данных в медицинских учреждениях [Электронный ресурс]. – Режим доступа: www.bit-medic.ru/articles/zashita-personalnyh-dannyh/. – Дата доступа 25.03.2018.

2. О чём молчат сотрудники похоронных бюро? Беларускія навіны – [Электронный ресурс]. – Режим доступа: www.newsby.org/by/2011/08/11/text20890.htm. – Дата доступа: 25.03.2018.

3. Электронная медицинская карта. Введение в картотеку « e-Gov.by ... [Электронный ресурс]. – Режим доступа: e-gov.by/stroitelstvo-e-gov/elektronnaya-medicinskaya-karta-vvedenie-v-kartoteku. – Дата доступа 25. 03.2018.

4. Электронная медицинская карта (ЭМК) [Электронный ресурс]. – Режим доступа: swan-it.ru/elektronnoe_zdravoohranenie/elektronnaya_meditsinskaya_karta. – Дата доступа 25. 03.2018..

5. . Гивойно, А. А. Защита медицинских данных пациентов / А. А. Гивойно, В. Н. Ростовцев // Доклады БГУИР. – 2016. – № 7 (101). – С. 79–83.

6. Безопасное архивирование данных с помощью биометрических технологий / А. А. Гивойно, С. В. Нестерович, Г. В. Сечко, Т. Г., Таболич Т. Г. // Веснік сувязі. – 2013. – № 6 (122). – С. 25–28.

7. Обзор: ИТ в здравоохранении 2014, Денег на ИБ не хватает - CNews [Электронный ресурс]. – Режим доступа: www.cnews.ru/reviews/publichealth2014/articles/deneg_na_ib_ne_hvataet. – Дата доступа 25.03.2018.

МНОГОПОТОЧНОСТЬ В UNITY СРЕДСТВАМИ РЕАКТИВНЫХ РАСШИРЕНИЙ

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Соколов В.А. Скуратович Е.С.

Бакунова О.М., ст. преподаватель каф. ИСиТ, м.т.н.

В данной статье будут затронуты основные проблемы, возникающие при разработке многопоточных мобильных приложений на платформе Unity, а также способы их решения с использованием библиотеки и реактивных расширений UniRx.

С помощью языка C# можно создавать приложения, выполняющие несколько задач одновременно. Задачи, которые потенциально могут задержать выполнение других задач, выполняются в отдельных потоках; такой способ организации работы приложения называется многопоточностью или свободным созданием потоков. Приложения, которые используют многопоточность, более продуктивно реагируют на действия пользователя, так как пользовательский интерфейс остается активным, в то время как задачи, требующие интенсивной работы процессора, выполняются в других потоках. Многопоточные приложения на языке C# при использовании Mono разрабатываются с помощью ключевых слов: ThreadPool, Thread и асинхронных делегатов.

В качестве примера многопоточного приложения можно представить работу в ресторане. Предположим, что каждый сотрудник выполняет свои обязанности в одно время с другими сотрудниками. К примеру, один готовит еду, второй убирает столы и т.д. (и все это происходит одновременно). Это и есть наши потоки.

ThreadPool — реализация паттерна «пул объектов». Его смысл в эффективном управлении потоками: создании, удалении, назначении им какой-то работы. Возвращаясь к ресторанной аналогии, ThreadPool — это шеф-повар, который контролирует количество сотрудников на стройке и назначает каждому из них задания на день.

Класс, который позволяет создавать новые потоки внутри существующего приложения, называется Thread.

Асинхронные делегаты — асинхронный вызов метода с помощью делегата, который определен с такой же сигнатурой, что и вызываемый метод. Для асинхронного вызова метода необходимо использовать метод BeginInvoke. При таком подходе делегат берет из пула поток и в нем выполняет некоторый код.

Инструменты для синхронизации потоков