

Сравнительный анализ программного обеспечения Smartmed и Damumed

¹ЕСЕНГАЛИЕВА Жанна Сержановна, PhD, доцент, jannayess@gmail.com,

^{1*}КАСЫЛКАСОВА Камила Нуралиевна, докторант, Camilla.kas@mail.ru,

²КАСЫЛКАСОВА Айман Ошакбаевна, старший преподаватель, kasylkasova.ayman@bk.ru,

³КАСЫЛКАСОВ Рамзес Нуралиевич, магистр, ramzes.kas98@gmail.com,

¹Евразийский национальный университет имени Л.Н. Гумилева, Казахстан, Нур-Султан, ул. Сапиева, 2,

²НАО «Карагандинский технический университет имени Абылкаса Сагинова», Казахстан, Караганда, пр. Н. Назарбаева, 56,

³Карагандинский университет имени Е.А. Букетова, Казахстан, Караганда, ул. Университетская, 28,

*автор-корреспондент.

Аннотация. Целью исследования являются сравнение и анализ программного обеспечения SmartMed и DamuMed, предоставляющих медицинские услуги в сфере здравоохранения. В статье представлено обоснование сложности выбора среды разработки программного обеспечения. Рассмотрены основные факторы, которые определяют программную среду для разработки мобильного приложения. В результате исследования выявлены плюсы и минусы программ, среды разработки, проведено тестирование приложений DamuMed и SmartMed. Также приведено подробное описание алгоритма работы сеансового шифрования, которые мы использовали в процессе разработки программного обеспечения при онлайн-взаимодействии. Разрабатываемое программное обеспечение SmartMed и DamuMed схожи по услугам, функциям. При этом SmartMed ориентируется как карманная больница и нацелена на онлайн-помощь пациентам вне зависимости от геолокации. DamuMed больше ориентирована на граждан РК и взаимодействие с учреждениями, находящимися на территории Казахстана.

Ключевые слова: Encrypting data, Xamarin forms, Visual Studio, C#, тестирование, протокол SLL/TLS, RSA, здравоохранение, IOS/Android, шифрование сеансового ключа.

Введение

В современном мире важное место занимают мощные компьютеры, интегрированные в нашу жизнь. По исследованиям Comscore, около 77% населения в мире владеют смартфонами [1]. Согласно отчету исследования Нилсена, в среднем в месяц человек тратит на использование мобильных приложений 37 часов 28 минут [2]. Неудивительно, что самые популярные мобильные приложения – это те, которые обеспечивают взаимодействие пользователей через социальные сети, например Gmail, WhatsApp, Facebook и т.д. [2]. Ученые в своих исследованиях активно используют мобильные приложения. Одно из таких исследований проводилось нейробиологами Ратледжем Скандали и Даяном Доланом, в котором приняло участие свыше 60000 человек. Учеными было создано бесплатное программное обеспечение, которое способно предупредить болезнь Альцгеймера на ранних стадиях [3].

В работе Иесака Т.М и других описываются инновационные достижения современного мира посредством программного обеспечения. Специ-

алисты в области информационных технологий создают программное обеспечение, которое дает возможность для решения большого количества задач в жизни человека [4].

Особо важное значение в жизни человека занимает здравоохранение, от уровня развития которого зависит качество и продолжительность жизни населения. Внедрение информационных технологий и цифровизации в систему здравоохранения значительно поднимает уровень медицинского обслуживания. Оказавшись в сложной ситуации, пациент быстро сможет получить качественную помощь медицины, общаясь онлайн со специалистом [5]. Большое облегчение должны получить люди с ограниченными возможностями, имеющие трудности с посещением больницы.

В Казахстане внедрен продукт – DamuMed, который осуществляет взаимодействие населения с организациями здравоохранения. Такие программы особенно актуальны в период пандемии, тем более, что новые технологии и цифровизация переводят многие государственные услуги в формат онлайн [6].

В области здравоохранения время играет критическую роль, так как человек зачастую находится в ситуации смертельной опасности. Нет сомнений, что есть необходимость в качественном внедрении информационных технологий и цифровизации в существующую модель здравоохранения. Необходимость реализации альтернативного программного обеспечения SmartMed является существенным обоснованием в исследовании.

В статье проведено сравнение сильных/слабых сторон систем SmartMed и DamuMed.

В свете актуальных событий пришла идея создания мобильного приложения, которое дает возможность, не выходя из дома, посещать специализированные учреждения, обращаться за помощью в медицинские организации. Для этого началась разработка приложения «SmartMed», где пользователи могут не только обратиться к терапевту с обычными вопросами здравоохранения, но и получить рекомендации, полную информационно-аналитическую картину, записаться на прием к врачу и т.д. При использовании приложения не имеют значения гражданство, язык общения, наличие медицинской страховки.

Методы исследования

В первую очередь, исследование фокусируется на сравнении приложения DamuMed и SmartMed, созданные для платформы Android. Проводились исследования аналогичных приложений для того, чтобы проанализировать их сильные и слабые стороны, преимущества и недостатки.

DamuMed – программное обеспечение, которое создано для резидентов Республики Казахстан с целью получения доступа с мобильных приложений к определенным медицинским организациям, при этом существует возможность записи прикрепленных пациентов к участковому врачу, вызова врача на дом и другой необходимой помощи. В нашем исследовании взяты несколько ключевых критериев, представленных в таблице 1.

SmartMed – программное обеспечение, позволяющее пациенту записаться на полноценную онлайн-консультацию с врачом. Существует возможность обращения за помощью с любой точки мира. Онлайн-консультация совершается посредством видео/аудио звонка, чата в оговоренное для пациента времени. Есть возможность выбора нужного взрослого/детского доктора. К недостаткам и преимуществам SmartMed относятся показатели, представленные в таблице 2.

Важно правильно выбрать мобильное медицинское приложение, так как медицина является важной областью в жизни человека. В случае недомогания, всегда следует обратиться за консультацией к врачу. При традиционном способе обращения к узкопрофильному врачу в аналогичной ситуации предварительно следует записаться на прием к терапевту, при этом не всегда есть воз-

можность записи к специалисту, живые очереди до сих пор имеют место быть. Установив мобильное приложение SmartMed, которое предназначено для онлайн-доступа пациентов с любого уголка мира, пациент может выбрать опытного узкопрофильного специалиста по отзывам или рейтингу.

SmartMed имеет возможность обратиться к таким узкоспециализированным медицинским специалистам, как урологи, хирурги, невропатологи, кардиологи, онкологи и другие для взрослых и детей. Дети могут в формате онлайн получить помощь педиатров, логопедов, невропатологов, травматологов и т.д.

Посредством приложения появляется возможность оказания помощи жителям отдаленных поселений. Такой вид сервиса не является бесплатным, за одну консультацию необходимо провести оплату.

Если есть страхование, то для граждан РК услуги DamuMed бесплатны, но данное программное обеспечение не предоставляет бесплатные медицинские услуги нерезидентам РК.

Следует отметить, что независимость геолокации пациента является приоритетом, новым подходом к решению проблемы. SmartMed разрабатывается специально независимым продуктом, без привязки к медицинским учреждениям, странам, медицинским страховкам.

Результаты

В тестовом режиме для исследования запущено приложение. Интерфейс меню SmartMed представлен на рисунке 1.

Данное программное обеспечение написано на языке C# платформы Xamarin Forms, на которой создаются кроссплатформенные приложения под Android, iOS и Windows [8]. Фрагмент разработки в среде Visual Studio приложения SmartMed представлен на рисунке 2.

При выборе среды для создания ПО разработчики сталкиваются со следующими трудностями:

- различие в подходах построения графического интерфейса так или иначе влияет на разработку, разработчики вынуждены подстраивать приложение под требования к интерфейсу на конкретной платформе;

- разные API – различие в программных интерфейсах и реализациях тех или иных функциональностей также требует от программиста учета этих специфических особенностей;

- разные платформы для разработки. Например, чтобы создавать приложения для iOS нам необходима соответствующая среда – Mac OS X и ряд специальных инструментов, типа XCode. А в качестве языка программирования выбирается Objective-C или Swift. Для Android мы можем использовать самый разный набор сред – Android Studio, Eclipse и т.д. Но здесь для подавляющего большинства приложений применяется Java либо Kotlin. Для создания приложений под Windows используется Visual Studio, а в качестве языков –

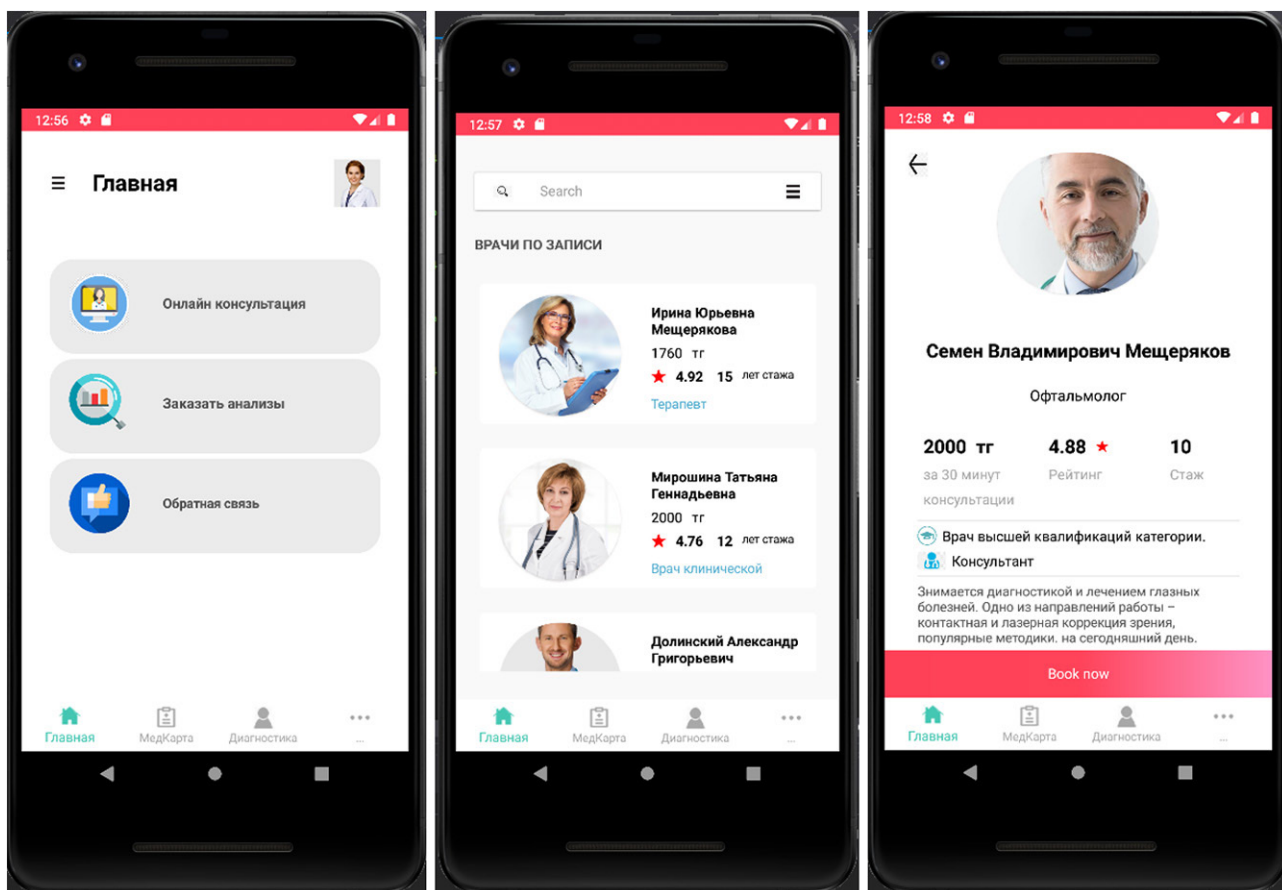


Рисунок 1 – Интерфейс SmartMed

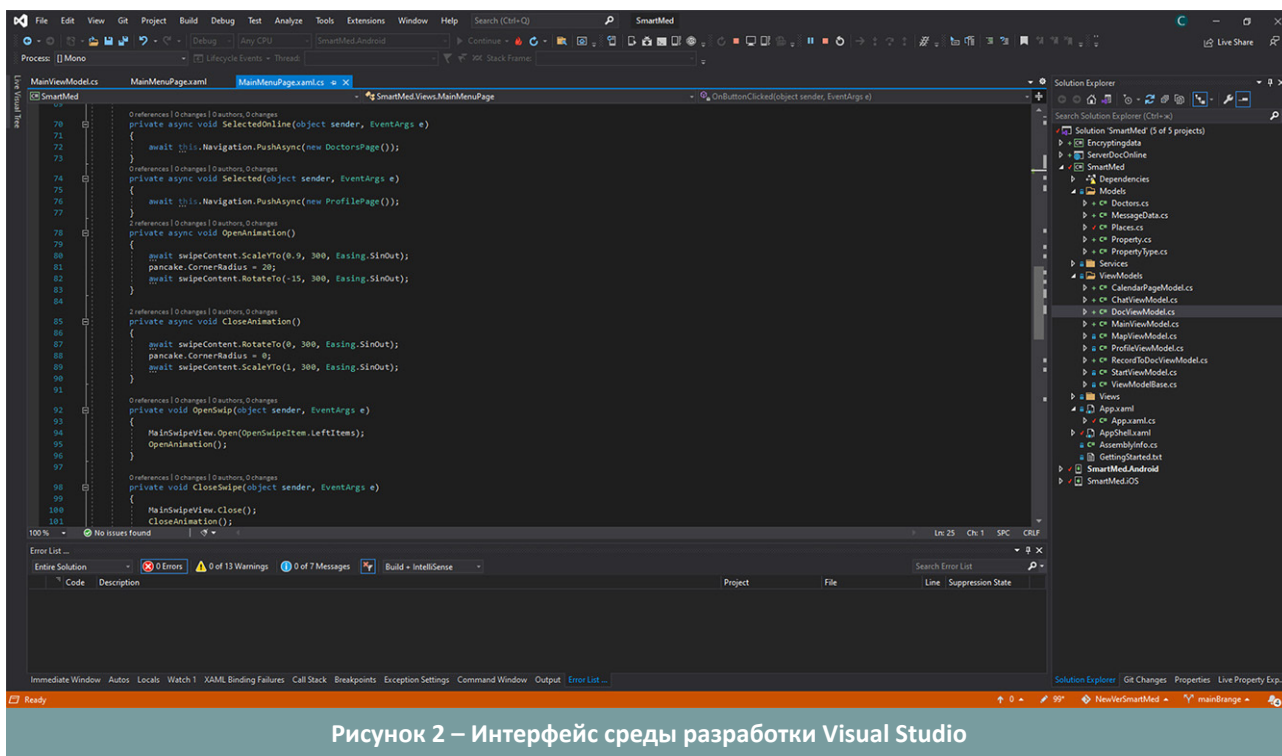


Рисунок 2 – Интерфейс среды разработки Visual Studio

C#, F#, VB.NET и C++[9].

Большое количество сред разработки и языков программирования не может положительно

влиять на сроки создания приложений и в итоге скажется негативно в денежных средствах, выделяемых на разработку. Будет намного эффектив-

нее иметь один инструмент, который позволяет легко и просто создавать приложения для всех платформ. В связи с этим мы выбрали в исследовании платформу Xamarin.

Преимущества использования Xamarin Forms:

- в процессе разработки создается единый код для всех платформ;
- Xamarin предоставляет прямой доступ к нативным API каждой платформы;
- при создании приложений мы можем использовать платформу .NET и язык программирования C# (а также F#), который является достаточно производительным, и в то же время ясным и простым для освоения и применения;
- Xamarin forms поддерживает несколько платформ.

Авторами был проведен социологический эксперимент среди населения. Ниже представлены отзывы о работе SmartMed:

1. Аида. Установив данную программу, я раз и навсегда решила проблему с неоднократными поездками в поликлинику. Все необходимые результаты сейчас получаю через медицинскую карту, есть возможность распечатки необходимой информации.

2. Тимур. Закажал бесплатную медицинскую консультацию для родителей, которые проживают в отдаленном населенном пункте. Родители получили рекомендации по лечению, не выходя из дома.

3. Алан. Я в восторге от этого приложения – экономит время, достаточно зайти в программу, и в разделе с виртуальной картой можно ознакомиться с записями. Виртуальная медкарта может быть использована и другими врачами в любой больнице.

4. Данил. Очень удобная программа, но есть недостаток, это то, что на экране мобильного телефона трудно рассмотреть присланные анализы, приходится загружать на компьютер или распечатывать файл. И SmartMed, и DamuMed очень достойные программы, просты в использовании, дают чувство комфорта пользователю и полностью удовлетворяют потребителя.

В программном обеспечении DamuMed не предусмотрены видеозвонки. На связь с пациентом выходит только терапевт по мобильной связи, а посетить узконаправленного специалиста можно после записи на очередь, которую осуществляет терапевт. Узконаправленные специалисты принимают пациентов только офлайн.

Однако врачи в программном приложении SmartMed принимают пациентов только в онлайн-формате. Поэтому в приложении применяется технология шифрования сеансового ключа.

Сеансовое шифрование (ключа) – это смешанный алгоритм асимметрического и симметрического шифрования [10]. Сначала используется асимметрическое шифрование (RSA), которое является криптографической системой, использует два различных ключа: открытый и секретный.

Открытый ключ передается по незащищенному транспортному каналу и с помощью него происходят шифрование данных и проверка электронной подписи. С помощью закрытого ключа (секретного) проводится дешифрование данных.

В программном обеспечении используется асимметрический алгоритм RSA в протоколе SSL/TLS. Два протокола транспортного уровня SSL/TLS разработаны специально для защищенной передачи данных в сети интернет [11].

В симметричном шифровании используется один приватный ключ, который позволяет как шифровать, так и дешифровать данные. Плюсом такого подхода обеспечивается возможность шифровать большие объемы данных. Для безопасной передачи данных по сети в программном обеспечении SmartMed сначала обмениваются асимметричными ключами, а затем уже симметричными – для непосредственно шифрования передаваемых данных [12].

Порядок шагов шифрования сеансового ключа. Рассмотрим открытый ключ (e, n) пользователя 1, для него генерируем случайный сеансовый ключ m , с помощью открытого ключа зашифровываем его согласно формуле:

$$(c = E(m) = m^e \bmod n). \quad (1)$$

Шифруем текст M_A с ключом симметрического алгоритма:

$$C = E_m(M_A). \quad (2)$$

Алгоритм расшифрования сеансового ключа – получить зашифрованный ключ пользователя 2, используем свой секретный ключ (d, n) для расшифровки сеансового ключа:

$$(m = D(c) = c^d \bmod n), \quad (3)$$

расшифровка текста C сеансового ключа:

$$(M_A = D_m(C)). \quad (4)$$

Шифруют и разбивают данные на блоки нужной длины, если сеансовый ключ больше, чем модуль n [13]. Алгоритм сеансового ключа показан на рисунке 3.

В DamuMed организации здравоохранения получают доступ к сервису после оплаты. Плюсом данной технологии является то, что обслуживание сервиса целиком занимается провайдер услуги, а пользователь – организация здравоохранения – только работает с нею. Данное программное обеспечение интегрировано во всех медицинских учреждениях Республики Казахстан. За использование данного продукта ежемесячно оплачивается небольшая абонентская плата.

Выводы

Изучено программное обеспечение DamuMed, при этом хотелось бы отметить, что отсутствует информация о языке написания программного обеспечения DamuMed.

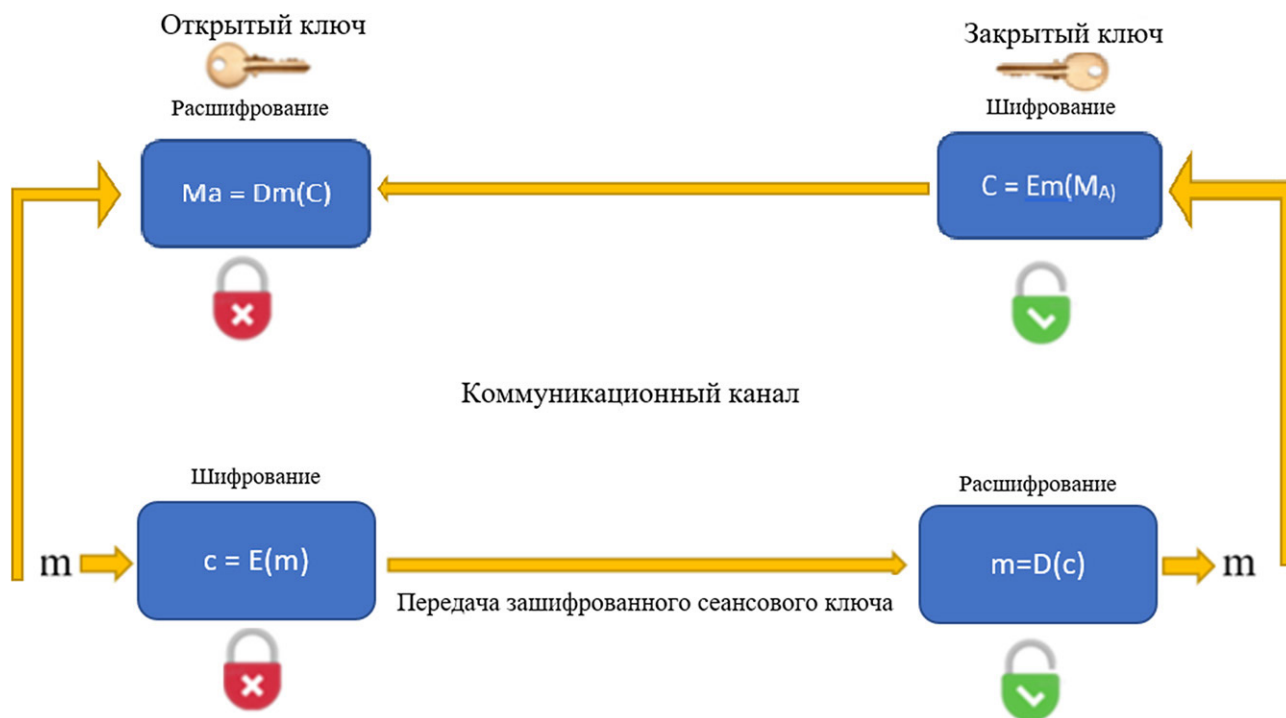


Рисунок 3 – Алгоритм шифрования сеансового ключа

Поэтому в данном исследовании мы рассматривали функционал данного ПО и провели тестирование на выявление багов приложения, нашли ошибки, перечисленные ниже:

- некорректное отображение специалистов/аптек на карте при поиске специалистов/лекарств/клиник;
- не разрешается записаться к специалисту онлайн (только к терапевту или психологу), что существенно снижает пользу от приложения;
- нет возможности связаться/созвониться с семейным/участковым врачом;
- больничные в приложении не подписываются, организации не принимают электронные больничные без подписей и печатей;
- нужен больший акцент (вывести на главный экран) на показатели здоровья в медкарте (давление, пульс, вес, сахар) и рекомендации к ним – геймификация, не сразу бросается в глаза изменения, более удобно использовать второстепенные приложения, такие как Google Fit, MiFit, Samsung Health.

Подводя итоги, можно сказать, что разрабатываемое программное обеспечение SmartMed и DamuMed схожи по услугам, функциям. Вероятно, выбор будет зависеть от личных предпочтений дизайна интерфейса, а также от количества функций, использующих то или иное приложение. SmartMed ориентируется как карманная больница и нацелена на онлайн-помощь пациентам, вне зависимости от геолокации. DamuMed больше ориентирована на граждан РК и взаимодействие с учреждениями, находящимися на территории Казахстана.

СПИСОК ЛИТЕРАТУРЫ

1. Fetzer T.; Graeber T. Does Contact Tracing Work? QuasiExperimental Evidence from an Excel Error in England. [Электронный ресурс] URL: <https://ssrn.com/abstract=3753893> (дата обращения 25.12.2020).
2. Toussaert S. Upping uptake of COVID contact tracing apps // Behav. – 2021. – P. 183.
3. Sturniolo S., Waites W., Colbourn T.; Manheim D., Panovska-Griffiths J. Testing, Tracing and isolation in compartmental models // PLoS Comput. Biol. – 2021. – 28 p.
4. Yasaka, T.M.; Lehigh, B.M.; Sahyouni, R. Peer-to-peer contact tracing: Development of a privacy-preserving smartphone app. – JMIR mHealth uHealth. – 2020. – P. 9.
5. How Tracing and Warning Apps Can Help during the Pandemic. [Электронный ресурс] URL: <https://echalliance.com/the-digital-economy-and-society-index-desi/> (дата обращения 25.05.2021).
6. Damumed – медицинская информационная система. [Электронный ресурс] URL: <https://oculi.kz/ru/patsientam/damumed-meditinskaya-informatsionnaya-sistema.html> (дата обращения 25.02.2021).
7. Медицинский недосмотр или Сюрпризы приложения DamuMed. [Электронный ресурс] URL: <https://rus.azattyq.org/a/damumed-kazakhstan-medical-insurance/30770878.html> (дата обращения 12.10.2021).

8. Что такое Xamarin? [Электронный ресурс] URL: <https://docs.microsoft.com/ru-ru/xamarin/get-started/what-is-xamarin> (дата обращения 25.08.2021).
9. Xamarin и кросс-платформенная разработка. [Электронный ресурс] URL: <https://metanit.com/sharp/xamarin/1.1.php> (дата обращения 26.08.2021).
10. Шнайер Б. Прикладная криптография. 2-е изд. Протоколы, алгоритмы и исходные тексты на языке C++ // Вильямс-2016 – С. 1024.
11. Асимметрическое шифрование. [Электронный ресурс] URL: <https://indeed-id.ru/blog/asimmetrichnoe-shifrovanie/> (дата обращения 12.09.2021).
12. Криптография в C# (RSA, DES, SHA1). [Электронный ресурс] URL: <https://studlearn.com/works/details/primery-kriptografii-na-c-rsa-des-sha1-575> (дата обращения 26.08.2021).
13. RSA. [Электронный ресурс] URL: <https://ru.wikipedia.org/wiki/RSA/> (дата обращения 21.10.2021).

Smartmed және Damumed бағдарламалық жасақтаманы салыстырмалы талдау

¹ЕСЕНГАЛИЕВА Жанна Сержановна, PhD, доцент, jannayess@gmail.com,

¹*КАСЫЛКАСОВА Камила Нуралиевна, докторант, Camilla.kas@mail.ru,

²КАСЫЛКАСОВА Айман Ошакбаевна, аға оқытушы, kasylkasova.ayman@bk.ru,

³КАСЫЛКАСОВ Рамзес Нуралиевич, магистр, ramzes.kas98@gmail.com,

¹Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қазақстан, Нұр-Сұлтан, Сәтпаев көшесі, 2,

²«Әбілқас Сағынов атындағы Қарағанды техникалық университеті» КеАҚ, Қазақстан, Қарағанды, Н. Назарбаев даңғылы, 56,

³Е.А. Бөкетов атындағы Қарағанды университеті, Қазақстан, Қарағанды, Университет көшесі, 28,

*автор-корреспондент.

Аңдатпа. Зерттеудің мақсаты – денсаулық сақтау саласында медициналық қызмет көрсететін SmartMed және DamuMed бағдарламалық жасақтамасыз ету бағдарламалық жасақтамаларын салыстыру және талдау. Мақалада бағдарламалық жасақтаманы әзірлеу ортасын таңдаудың күрделілігінің негіздемесі келтірілген. Мобильді қосымшаны әзірлеу үшін бағдарламалық ортаны анықтайтын негізгі факторлар қарастырылады. Зерттеу нәтижесінде бағдарламалардың, даму ортасының оң және теріс жақтары анықталды, DamuMed және SmartMed қосымшалары сыналды. Сондай-ақ, онлайн-өзара әрекеттесу кезінде бағдарламалық жасақтаманы әзірлеу процесінде қолданған сеанстық шифрлау алгоритмінің егжей-тегжейлі сипаттамасы келтірілген. Әзірленген SmartMed және DamuMed бағдарламалық жасақтамасы қызметтер мен функцияларға ұқсас. Бұл ретте SmartMed қалта ауруханасы ретінде бағдарланады және геолокацияға қарамастан пациенттерге онлайн көмек көрсетуге бағытталған. DamuMed ҚР азаматтары үшін және Қазақстан аумағындағы мекемелермен өзара іс-қимылға көбірек бағытталған.

Кілт сөздер: Encrypting data, Xamarin forms, Visual Studio, C#, тесілеу, SLL/TLS хаттамасы, RSA, денсаулық сақтау, IOS/Android, сеанс кілтін шифрлау.

Comparative Analysis of Smartmed and Damumed Software

¹YESSENGALIYEVA Zhanna, PhD, Assistant Professor, jannayess@gmail.com,

¹*KASSYLKASSOVA Kamila, doctoral student, Camilla.kas@mail.ru,

²KASSYLKASSOVA Ayman, Senior Lecturer, kasylkasova.ayman@bk.ru,

³KASSYLKASSOV Ramses, Master's Degree, ramzes.kas98@gmail.com,

¹L.N. Gumilyov Eurasian National University, Kazakhstan, Nur-Sultan, Satpayev Street, 2,

²NPJSC «Abylkas Saginov Karaganda Technical University», Kazakhstan, Karaganda, N. Nazarbayev Avenue, 56,

³Karaganda Buketov University, Kazakhstan, Karaganda, University Street, 28,

*corresponding author.

Abstract. The goal of the study is to compare and analyze SmartMed and DamuMed software, which provide medical services in the field of health care. The article presents a rationale for the complexity of choosing a software development environment. The main factors that determine the software environment for mobile application development are considered. The study identifies the pros and cons of the software and development environment, and tests the DamuMed and SmartMed applications. A detailed description of the session encryption algorithm that we used in the software development process for online interaction is also given. The SmartMed and DamuMed software under development are similar in terms of services and functions. However, SmartMed is oriented as a pocket hospital and aims at online patient care, regardless of geolocation. DamuMed is more focused on the citizens of Kazakhstan and interaction with institutions located in Kazakhstan.

Keywords: Encrypting data, Xamarin forms, Visual Studio, C#, testing, SLL/TLS protocol, RSA, healthcare, IOS/Android, encryption of the session key.

REFERENCES

1. Fetzer T.; Graeber T. Does Contact Tracing Work? QuasiExperimental Evidence from an Excel Error in England. [Elektronnyj resurs] URL: <https://ssrn.com/abstract=3753893> (data obrashcheniya 25.12.2020).
2. Toussaert S. Upping uptake of COVID contact tracing apps // Behav. – 2021. – P. 183.
3. Sturniolo S., Waites W., Colbourn T.; Manheim D., Panovska-Griffiths J. Testing, Tracing and isolation in compartmental models // PLoS Comput. Biol. – 2021, – 28 p.
4. Yasaka, T.M.; Lehigh, B.M.; Sahyouni, R. Peer-to-peer contact tracing: Development of a privacy-preserving smartphone app. – JMIR mHealth uHealth. – 2020. – P. 9.
5. How Tracing and Warning Apps Can Help during the Pandemic. [Elektronnyj resurs] URL: <https://echalliance.com/the-digital-economy-and-society-index-desi/> (data obrashcheniya 25.05.2021).
6. Damumed – medicinskaya informacionnaya sistema. [Elektronnyj resurs] URL: <https://oculi.kz/ru/patsientam/damumed-meditsinskaya-informatsionnaya-sistema.html> (data obrashcheniya 25.02.2021).
7. Medicinskij nedosmotr ili Syurprizy prilozheniya DamuMed. [Elektronnyj resurs] URL: <https://rus.azattyq.org/a/damumed-kazakhstan-medical-insurance/30770878.html> (data obrashcheniya 12.10.2021).
8. CHto takoe Xamarin? [Elektronnyj resurs] URL: <https://docs.microsoft.com/ru-ru/xamarin/get-started/what-is-xamarin> (data obrashcheniya 25.08.2021).
9. Xamarin i kross-platformennaya razrabotka. [Elektronnyj resurs] URL: <https://metanit.com/sharp/xamarin/1.1.php> (data obrashcheniya 26.08.2021).
10. SHnajer B. Prikladnaya kriptografiya. 2-e izd. Protokoly, algoritmy i iskhodnye teksty na yazyke C++ // Vil'yams-2016 – P. 1024.
11. Asimmetricheskoe shifrovanie. [Elektronnyj resurs] URL: <https://indeed-id.ru/blog/asimmetrichnoe-shifrovanie/> (data obrashcheniya 12.09.2021).
12. Kriptografiya v C# (RSA, DES, SHA1). [Elektronnyj resurs] URL: <https://studlearn.com/works/details/primery-kriptografii-na-c-rsa-des-sha1-575> (data obrashcheniya 26.08.2021).
13. RSA. [Elektronnyj resurs] URL: <https://ru.wikipedia.org/wiki/RSA/> (data obrashcheniya 21.10.2021).