3. RAPID7, Metasploit Framework. — URL: https://docs.rapid7.com/metasploit/quick-start-guide (date of the application: 26.05.2022). — Text : electronic.
4. Пост-эксплуатация с помощью Meterpreter — подсказка для Linux. — URL: https://ciksiti.com/ru/chapters/1260-post-exploitation-with-meterpreter--linux-hint (дата обращения: 26.05.2022). — Текст : электронный.
5. How to use a reverse shell in Metasploit | Metasploit Documentation Penetration Testing Software, Pen Testing Security. — URL: https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-a-reverse-shell-in-metasploit.html (date of the application: 27.05.2022). — Text : electronic.
6. How to exploit any android device using msfvenom and Metasploit Framework / Archana Tulsiyani. — URL: https://archanatulsiyani21.medium.com/how-to-exploit-any-android-device-using-msfvenom-and-metasploit-framework-9e90af4a4d7b (date of the application: 27.05.2022). — Text : electronic.

А. И. Левченко, А. С. Нестеров, М. С. Двинский, А. В. Широких
Тюменский государственный университет, г. Тюмень

УДК 004.056

РАЗРАБОТКА ЗАЩИЩЕННОГО ЛИЧНОГО КАБИНЕТА ДЛЯ ЧАСТНОЙ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

Аннотация. *В статье обсуждаются процесс разработки и средства для защиты данных пользователей личного кабинета частной медицинской организации. Приведено обоснование стойкости выбранных криптографических методов. Представлена демонстрация работы готового приложения.*

Ключевые слова: *цифровизация, разработка, безопасность, защита данных, ФСТЭК, Blowfish, bcrypt, Java, React.*

Введение. Актуальность темы обусловлена фактом того, что в современном мире происходит стремительная цифровизация и автоматизация бизнес-процессов, сфера здравоохранения при этом не исключение. Подтверждением данного факта является указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года» [1].

Согласно требованиям в указе, необходимо достигнуть «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления. Кроме того, следует увеличить до 95% доли массовых социально значимых услуг, доступных в электронном виде.

В связи с этим нам поступил заказ на разработку защищенного личного кабинета для частной медицинской организации, который поможет решить задачу цифровизации услуг здравоохранения, а также сделает более доступными получение данных услуг.

Тема цифровизации рассматривалась ранее в плане влияния на социально-экономические процессы [2], были проведены анализы цифровизации в экономике, и проблем, связанных с информационной безопасностью [3, 4]. Данные материалы в некоторой мере схожи с темой нашей статьи и послужили источником вдохновения.

Проблема исследования. Цель данной работы заключается в разработке приложения для частной медицинской организации, а также анализ существующих нарушителей и угроз, и обеспечение безопасности приложения в соответствии с анализом.

Исходя из поставленной цели, были сформулированы следующие задачи:

1) изучение и анализ законодательной и нормативно-правовой базы для обеспечения безопасности хранения и использования персональных данных;

2) разработка личного кабинета пользователя;

3) обеспечение безопасности приложения.

Материалы и методы. Применение практико-ориентированного подхода как метода, направленного на формирование практических умений и навыков в профессиональной деятельности. В рамках нашего проекта наиболее подходящим стеком технологий мы выбрали Java [5] в паре с фреймворком Spring Boot [6], React [7] в паре с TypeScript [8] и PostgreSQL [9]. Любое веб-приложение будет создано с использованием нескольких технологий, будь то фреймворки, библиотеки или базы данных. Следовательно, при создании

фуллстек приложения, необходимо продумать, как и на чем будет создаваться фронтенд часть, а также часть, которая будет отвечать за работу с сервером и базой данных.

Модель безопасности приложения

Для оценки безопасности приложения необходимо знать его инфраструктуру. Инфраструктура поможет правильно определить актуальность угроз и нарушителей, а также возможные вектора атаки злоумышленников. На рис. 1 представлена схема инфраструктуры приложения.

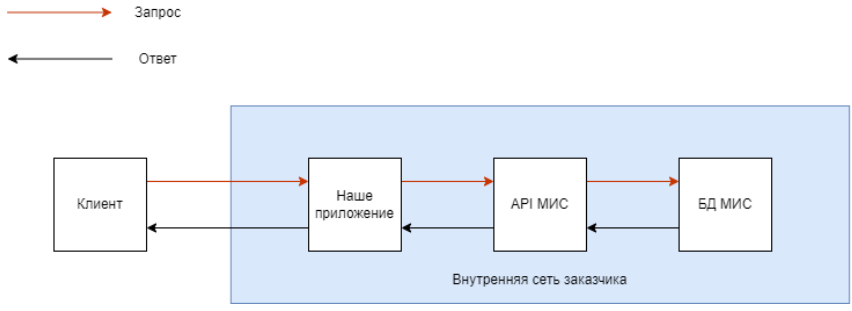

Рис. 1. Инфраструктура приложения

Для приложения был выделен отдельный виртуальный сервер, который находится во внутренней сети заказчика. Зоной нашей ответственности в данном случае является настройка внутреннего окружения для правильной работы приложения, все внешние настройки подконтрольны заказчику. Доступа к ним мы, соответственно, не имеем.

Исходя из наших полномочий и возможностей, мы составили модель нарушителя в соответствии с методическим документом «Методика определения угроз безопасности информации в информационных системах» от ФСТЭК [10], проанализировали банк данных угроз безопасности информации ФСТЭК [11] и составили адаптированный набор мер согласно приказу 21 ФСТЭК [12].

После выполнения требований к мерам нами были проанализированы актуальные рекомендации по обеспечению безопасности

веб-приложений от ФСТЭК и анализ новых уязвимостей от данной организации в паре с угрозами из базы данных OWASP [13].

В соответствии со всеми представленными анализами были предприняты необходимые меры для устранения и предотвращения уязвимостей, которые приводят к угрозам безопасности информации.

Обеспечение безопасности платформы

Для создания защищенных личных кабинетов пользователей необходимо обеспечить безопасность аутентификационных данных пользователей. В соответствии с рекомендациями ФСТЭК, для обеспечения безопасности аутентификационных данных пользователей необходимо использовать надежные хэш-функции и обеспечить безопасность передачи аутентификационных данных на сервер.

Для безопасной передачи данных на сервер используется HTTPS. В качестве TLS используется КриптоПРО JavaTLS версии 2.0.

Модуль spring-boot-starter-security [14] фреймворка Spring Boot содержит в себе большое количество функционала для обеспечения безопасности приложения. Класс BCrypt, который содержится в ранее представленном модуле, является реализацией адаптивной криптографической хеш-функции формирования ключа, называемой bcrypt [15], которая используется для хеширования паролей и последующей аутентификации пользователей. Данная хеш-функция выбрана не случайно, так как она является одной из самых надежных.

Bcrypt гарантирует безопасность хранения пароля, так как ее результат устойчив как к атаке нахождения прообраза, так и к атаке с помощью радужных таблиц. Вдобавок, безопасность хешированного пароля обеспечивается тем, что сложность функции адаптивна, в результате чего можно замедлить атаку простым перебором даже при большой вычислительной мощности злоумышленника [16].

Результаты. После завершения разработки мы хотели бы представить некоторый функционал нашего приложения.

В нашем приложении присутствует возможность простой аутентификации и аутентификация через ЕСИА. Для начала представим обычную аутентификацию.

Для входа в личный кабинет пользователя необходимо с главного экрана перейти на форму аутентификации нажатием на кнопку с иконкой «+» в правом верхнем углу главного экрана. Главный экран и кнопка представлены на рис. 2.

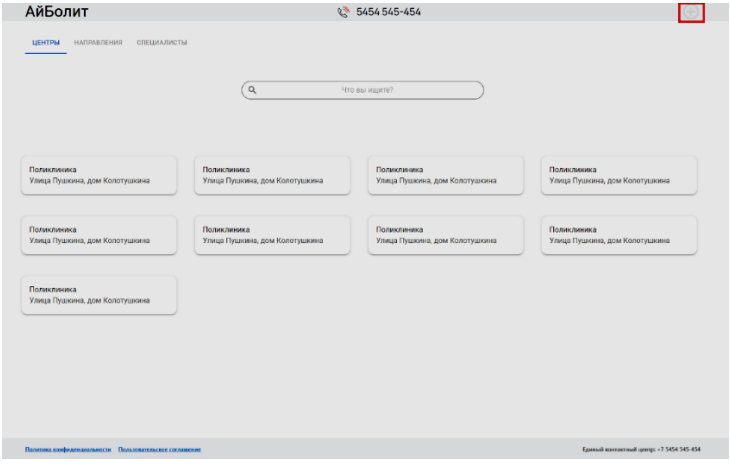

Рис. 2. Главный экран приложения

После нажатия на выделенную кнопку откроется форма аутентификации, которая представлена на рис. 3.

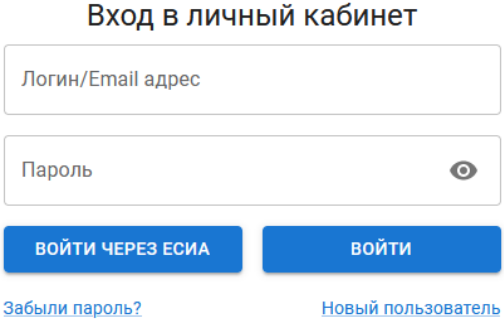

Рис. 3. Форма аутентификации

Далее, нужно ввести аутентификационные данные. Для аутентификации доступны логин или адрес электронной почты и пароль.

Введем данные от тестовой учетной записи и нажмем кнопку «Войти». После этого получим код подтверждения на привязанный номер телефона. После получения кода подтверждения на форме появится новое поле для ввода кода подтверждения. Форма с новым полем представлена на рис. 4.

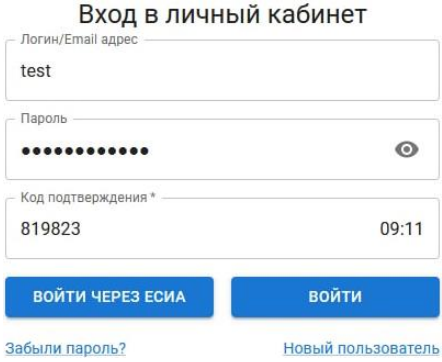

Рис. 4. Форма с кодом подтверждения

После ввода кода подтверждения нужно снова нажать «Войти». Таким образом попадем в личный кабинет нашего пользователя, который представлен на рис. 5.

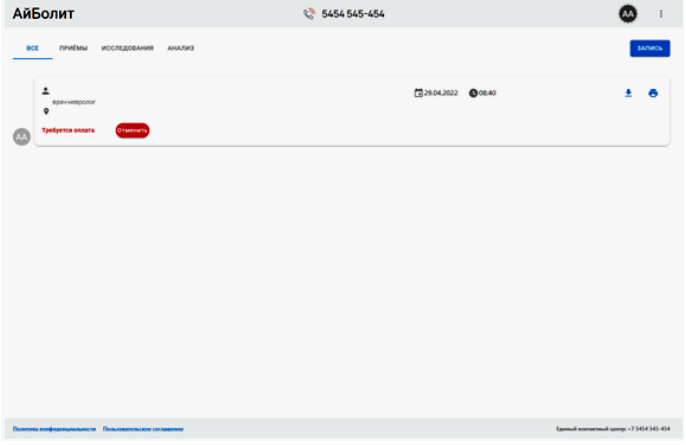

Рис. 5. Личный кабинет пользователя

Процесс аутентификации через ЕСИА во многом схож с процессом обычной аутентификации. На форме аутентификации, представленной на рис. 3, нужно нажать кнопку «Войти через ЕСИА». При первичном входе появится форма согласия на предоставление персональных данных нашему приложению от ЕСИА. Данная форма представлена на рис. 6.

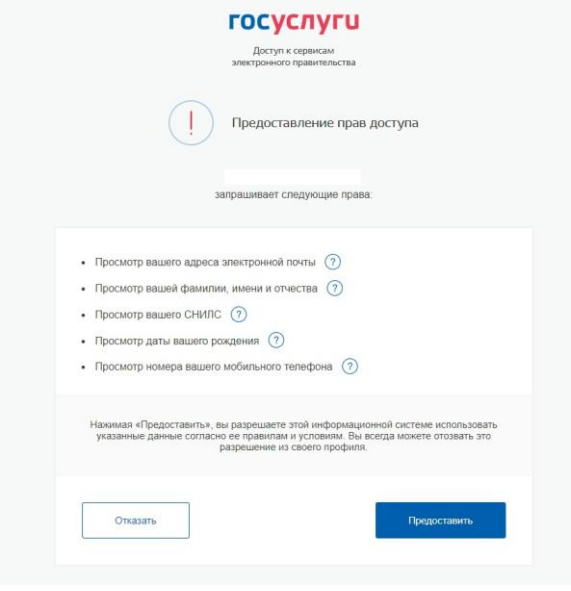

Рис. 6. Форма согласия ЕСИА

После соглашения пользователь попадет в свой личный кабинет, который был представлен на рис. 5.

Целевым функционалом приложения является возможность электронной записи к интересующим специалистам. Согласно бизнес-логике, записаться к врачу может как авторизированный, так и неавторизированный пользователь. Для начала рассмотрим процесс записи к врачу авторизированного пользователя.

Для перехода к началу процесса записи к врачу необходимо нажать на кнопку «Запись» из личного кабинета, который был представлен на рис. 5. После нажатия на кнопку «Запись» откроется

главная страница приложения, которая была представлена на рис. 2. На этой странице пользователю необходимо выбрать подходящий ему медицинский центр, после чего откроется экран выбора специальности врача, а также список всех врачей в выбранном медицинском центре, если пользователя интересует какой-то конкретный специалист. Экран выбора специальности представлен на рис. 7, экран выбора врачей представлен на рис. 8.

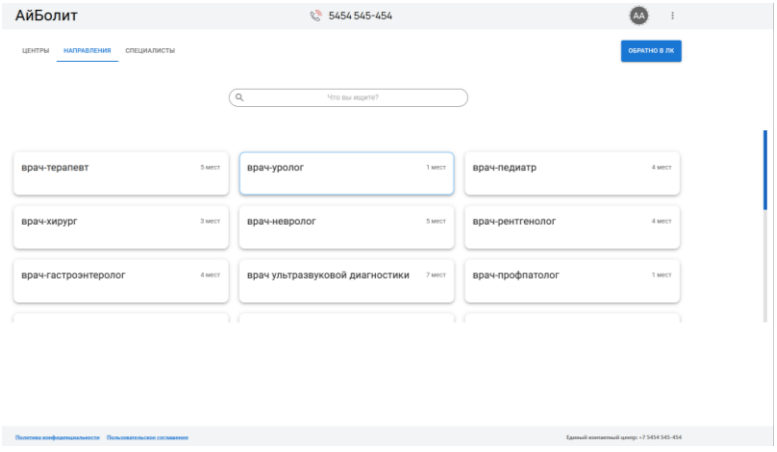

Рис. 7. Экран выбора специальностей

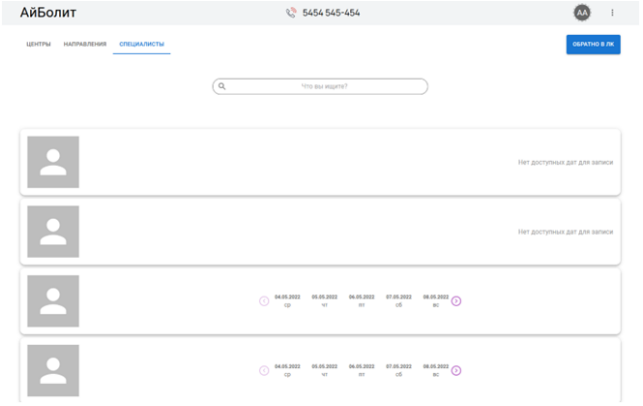

Рис. 8. Экран выбора врачей

После выбора интересующего врача и даты приема откроется выбор времени приема, представленный на рис. 9.

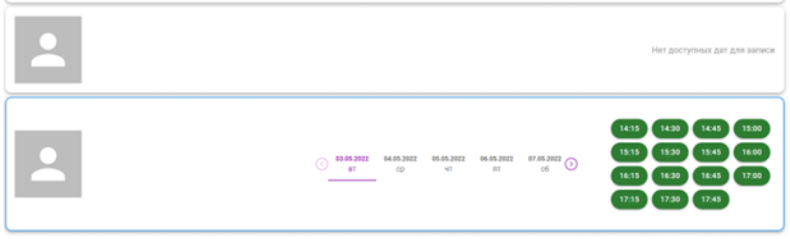

Рис. 9. Выбор времени приема

Для записи к специалисту необходимо выбрать время приема нажав на соответствующее время. После нажатия на кнопку, отображающую время приема, откроется форма подтверждения записи на прием, представленная на рис. 10.

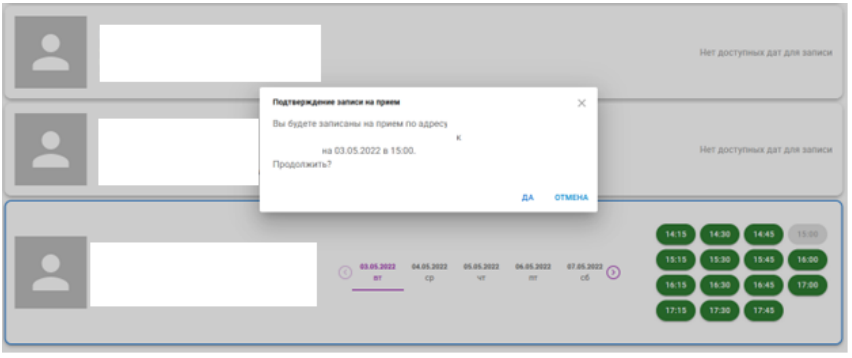

Рис. 10. Форма подтверждения записи на прием

После подтверждения записи на прием путем нажатия кнопки «Да» процесс записи будет завершен. Появится уведомление об успешном подтверждении записи, пользователь будет автоматически перенаправлен в личный кабинет, где он сможет увидеть новую запись. Новая запись показана на рис. 11.

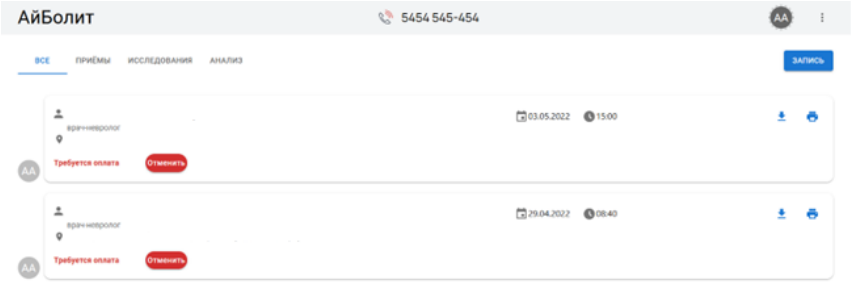

Рис. 11. Новая запись в личном кабинете

Авторизированный пользователь может посмотреть свои записи в личном кабинете, который был представлен на рис. 5. Записи имеют несколько типов, поэтому присутствует фильтрация для облегчения поиска записи нужного типа. Для просмотра талонов на прием нужно нажать на кнопку со стандартной иконкой «Скачать» напротив интересующей записи. После нажатия данной кнопки на ваше устройство будет скачан документ с информацией о приеме. Вид документа представлен на рис. 12.

«Сеть медицинский центров »

Талон на прием

Дата приема: **03.05.2022 г.**
Время приема: **15:00**
Врач:
Специальность: **врач-невролог**
Кабинет: **нет**
Адрес:
Код быстрого поиска: **нет**

Рис. 12. Талон на прием

Чтобы отменить запись, нужно нажать на кнопку «Отменить» под интересующей записью, которая находится в личном кабинете. После нажатия на кнопку откроется форма подтверждения отмены записи на прием. Данная форма представлена на рис. 13.

После подтверждения отмены записи появится уведомление об успешной отмене. Запись при этом пропадет из личного кабинета, а время, занятое пользователем, станет доступным для записи другим пользователям. Все это представлено на рис. 14.

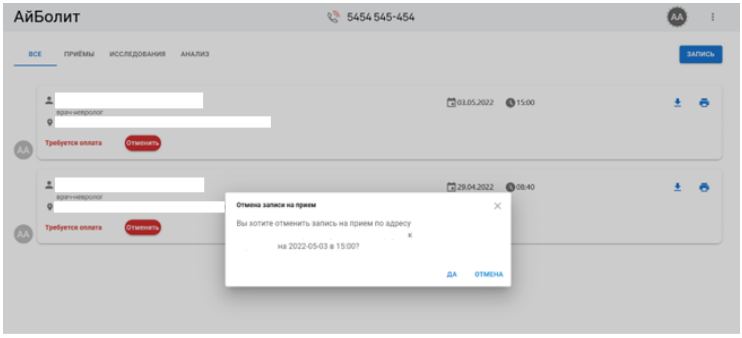

Рис. 13. Форма отмены записи на прием

Неавторизированный пользователь начинает работу с главного экрана приложения, который был представлен на рис. 2. С данного экрана можно начать процесс записи к специалисту. После выбора интересующего медицинского центра пользователю доступен выбор специальности и затем врача, либо же сразу выбор врача. Экраны выбора были представлены на рис. 7 и 8.

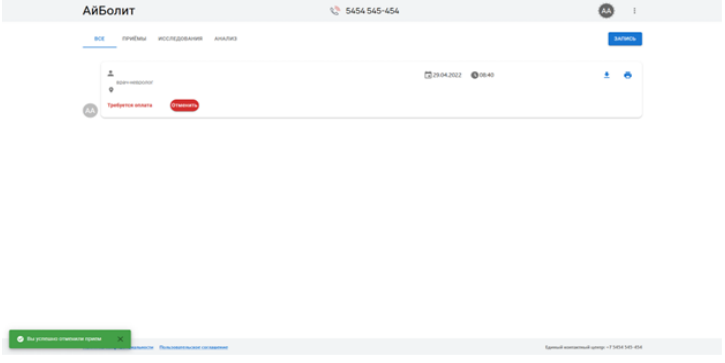

Рис. 14. Уведомление об успешной отмене и пропавшая запись

После выбора пользователем интересующего его специалиста, даты и времени записи, откроется окно подтверждения записи на прием, представленное на рис. 15.

Для подтверждения записи пользователю необходимо в течение десяти минут ввести код подтверждения в поле подтверждения кода.

Код подтверждения будет выслан на указанный номер мобильного телефона после нажатия кнопки «Получить код». Уведомление об успешной отправке кода и поле подтверждения также появится после того, как будет выслан код. Во избежание злоупотребления бронированием времени записи был реализован функционал бронирования длительностью десять минут. Форма подтверждения после ввода номера телефона и нажатия на кнопку получения кода представлена на рис. 16.

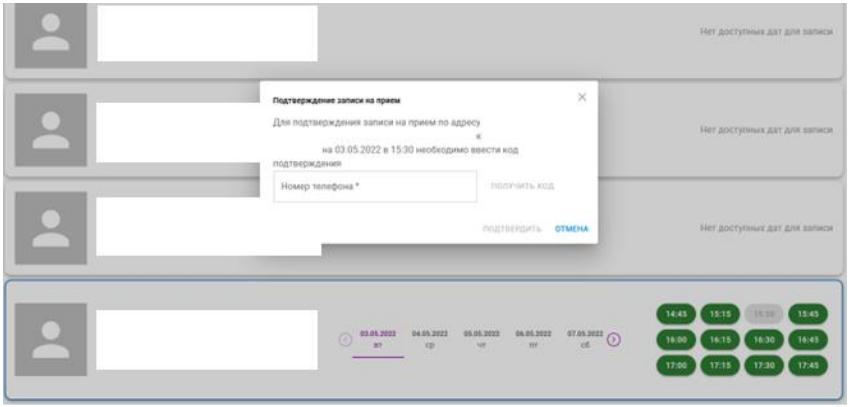

Рис. 15. Форма подтверждения на прием неавторизированного пользователя

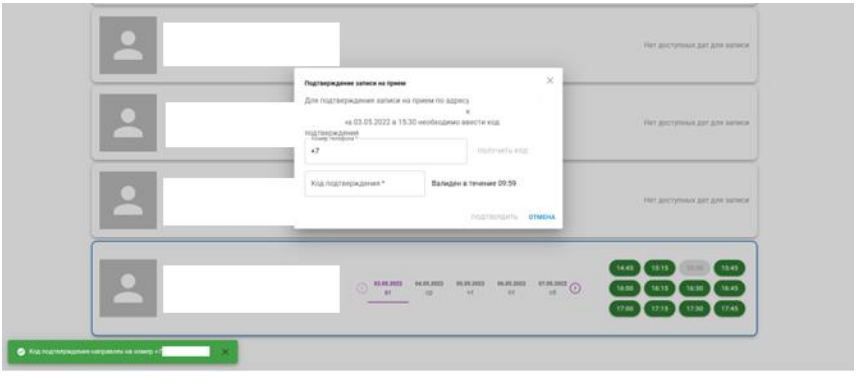

Рис. 16. Форма после ввода номера телефона

После ввода кода подтверждения и нажатия на кнопку «Подтвердить» появится уведомление об успешной записи на прием, а затем будет произведен переход на главный экран приложения. Успешная бронь записи представлена на рис. 17.

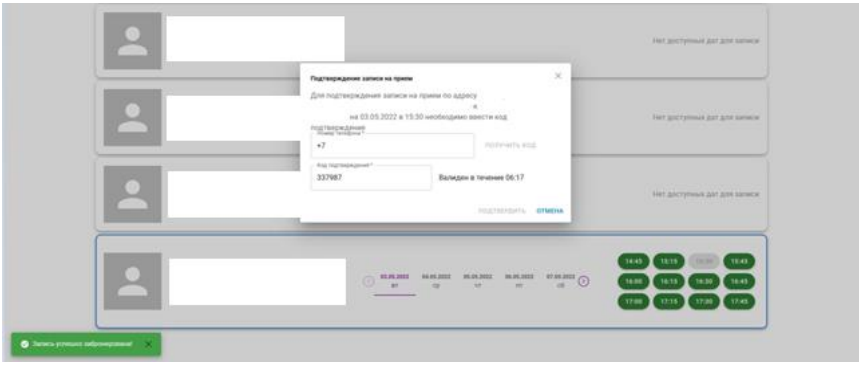

Рис. 17. Форма после ввода кода подтверждения

По прошествию пяти минут пользователю будет направлено СМС-уведомление с подробной информацией о приеме.

Заключение. В рамках статьи был представлен стек инструментов разработки, используемого для создания приложения, были проанализированы рекомендации и актуальные угрозы от ФСТЭК, был составлен адаптивный набор мер с последующим выполнением требований, представленных в мерах. Были представлены обоснования надежности выбранной нами хеш-функций. Была представлена демонстрация работы основного функционала приложения. Приложение было развернуто на сервере заказчика и отдано на тестирование.

СПИСОК ЛИТЕРАТУРЫ

1. О национальных целях развития Российской Федерации на период до 2030 года : Указ Президента РФ от 21.07.2020 № 474. — Текст: электронный // КонсультантПлюс.
2. Миткевич С. М. Цифровизация в экономике и инновациях: влияние на социально-экономические процессы / С. М. Миткевич. — Текст : электронный // Вузовское образование как новая реальность. —

2020. — № 1. — URL: elibrary_43802543_29643531.pdf (дата обращения: 19.03.2022).
3. Кривцова С. С. Цифровизация в экономике и информационная безопасность / С. С. Кривцова, Е. С. Ремесник. — Текст : электронный // Проблемы информационной безопасности социально-экономических систем. — 2021. — № 1. — URL: elibrary_44817301_37266992.pdf (дата обращения: 19.03.2022).
4. Фольмер К. В. Информационная безопасность и ее значение для современных предприятий / К. В. Фольмер. — Текст : электронный // Экономическая безопасность: правовые, экономические, экологические аспекты. — 2018. — № 1. — URL: elibrary_48030384_20921582.pdf (дата обращения: 19.03.2022).
5. New to Java Programming Center : сайт. — URL: https://www.oracle.com/topics/technologies/newtojava/programming-center.html (дата обращения: 20.03.2022). — Text : electronic.
6. Spring Boot : сайт. — URL: https://spring.io/projects/spring-boot (дата обращения: 21.03.2022). — Text : electronic.
7. React.js : сайт. — URL: https://ru.reactjs.org/ (дата обращения: 30.03.2022). — Text : electronic.
8. TypeScript : сайт. — URL: https://www.typescriptlang.org/ (дата обращения: 30.03.2022). — Text : electronic.
9. PostgreSQL : сайт. — URL: https://www.postgresql.org/about/ (дата обращения: 01.04.2022). — Текст : электронный.
10. ФСТЭК. Методика определения угроз безопасности информации в информационных системах: методический документ / ФСТЭК России. — Москва, 2015. — 43 с. — URL: https://fstec.ru/component/%20attachments/download/812 (дата обращения: 10.04.2022). — Текст : электронный.
11. Банк угроз безопасности информации : сайт. — URL: https://bdu.fstec.ru/threat (дата обращения: 10.04.2022). — Текст : электронный.
12. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ № 21 : [утвержден приказом ФСТЭК России от 18 февраля 2013 г. № 21]. — Текст : электронный // КонсультантПлюс.
13. OWASP Top Ten : site. — URL: https://owasp.org/www-project-top-ten/ (date of the application: 13.04.2022). — Text : electronic.

14. Spring Boot security : site. — URL: https://docs.spring.io/spring-boot/docs/current/reference/htmlsingle/#web.security (дата обращения: 21.04.2022). — Текст : электронный.
15. Provos N. A Future-Adaptable Password Scheme / N. Provos, D. Mazières. — Text : direct // Proceedings of 1999 USENIX Annual Technical Conference. — 1999. — P. 81-92.
16. Malvoni K. Are your passwords safe: energy-efficient bcrypt cracking with low-cost parallel hardware / K. Malvoni, S. Designer, J. Knezovic. — Text : direct // Proceedings of the 8th USENIX Conference on Offensive Technologies. — 2014. — P. 6.

А. И. Угренинов, А. М. Шабалин
Тюменский государственный университет, г. Тюмень

УДК 004.732

АВТОМАТИЗАЦИЯ СЕТЕВЫХ СЕРВИСОВ ПРЕДПРИЯТИЯ СРЕДСТВАМИ SDN

Аннотация. *В работе описан анализ различных протоколов, предназначенных для централизованного управления сетью. Представляются варианты использования автоматизации для решения различных задач по мониторингу, администрированию и обеспечению безопасности сети. Результатом работы стала модель компьютерной сети, решающая задачу проверки доступности сетевой среды средствами автоматизации.*

Ключевые слова: *автоматизация, программно-управляемые сети, SDN, Netconf.*

Введение. В связи с ежегодным ростом использования сетей возрастает и потребность в увеличении количества устройств, а с ними появляется и большое количество проблем, связанных с управлением и отслеживанием всех ее элементов [1]. Увеличиваются затраты на администрирование, а также шансы появления ошибок конфигурации, которые могут привести к проблемам безопасности и нестабильности сети в целом. Одним из решений этих проблем является внедрение автоматизации, которая используется для исключения выполнения однотипных операций и используемая в качестве инструмента автоматической конфигурации устройств, что позволяет избежать одной из самых частых причин — ошибок