Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри управління
інформаційною безпекою, д.т.н.,
полковник служби цивільного захисту

_____ Ростислав ТКАЧУК
“____” _____2021 року

ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему **Розроблення системи обробки та зберігання персональних даних у мобільному додатку**

Виконав:
здобувач IV курсу, групи КБ-41з
спеціальності (освітньої програми)
125 «Кібербезпека» (Управління інформаційною безпекою)
(шифр і назва спеціальності (освітньої програми))
Андрій ШКЛЯРУК
(прізвище та ініціали)
Керівник Наталія КУХАРСЬКА
(прізвище та ініціали)
Рецензент Анатолій КОСТЕНКО
(прізвище та ініціали)

Львів – 2021

АНОТАЦІЯ

Шклярук Андрій «Розроблення системи обробки та зберігання персональних даних у мобільному додатку». Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 59 сторінок, 29 рисунків, 5 таблиць, 31 джерела.

Об’єкт – процес розроблення системи обробки та зберігання персональних даних у мобільному додатку.

Предмет дослідження – система, на основі мобільного додатку, що виконує функції обробки та зберігання персональних даних з використанням криптографічного алгоритму *AES*.

Мета роботи – розробити систему, на основі мобільного додатку, що буде виконувати обробку та зберігання персональних даних з використанням криптографічного алгоритму шифрування/дешифрування.

У дипломній роботі бакалавра розглянуто питання захисту інформації у мобільних пристроях та додатках, криптографічні методи захисту інформації. Проаналізовано сучасні засоби розробки мобільних додатків, принцип роботи криптографічного алгоритму *AES*. Описано процес програмної реалізації криптографічного алгоритму *AES* на мові програмування *JavaScript* та процес розроблення мобільного додатку з використанням обраних технологій.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, КРИПТОГРАФІЯ, МОБІЛЬНІ ПРИСТРОЇ, AES, JAVASCRIPT, REACT NATIVE, FIREBASE.

ABSTRACT

Shkliaruk Andrii "Development of a system for processing and storing personal data in a mobile application." Thesis on the specialty 125 "Cybersecurity" consists of a text part containing 3 sections, 59 pages, 29 figures, 5 tables, 31 sources.

Object - the process of developing a system for processing and storing personal data in a mobile application.

The subject of research - a system based on a mobile application that performs the functions of processing and storage of personal data using the cryptographic algorithm AES.

The purpose of the work is to develop a system based on a mobile application that will process and store personal data using a cryptographic encryption / decryption algorithm.

In the bachelor's thesis the issues of information protection in mobile devices and applications, cryptographic methods of information protection are considered. Modern means of mobile application development, the principle of operation of the *AES* cryptographic algorithm are analyzed. The process of software implementation of the *AES* cryptographic algorithm in the *JavaScript* programming language and the process of developing a mobile application using selected technologies are described.

INFORMATION SECURITY, INFORMATION PROTECTION, CRYPTOGRAPHY, MOBILE DEVICES, AES, JAVASCRIPT, REACT NATIVE, FIREBASE.

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

У дипломній роботі для розроблення системи обробки та зберігання персональних даних створено крос-платформний мобільний додаток, в якому реалізовано функцію шифрування даних за допомогою криптографічного алгоритму *AES*.

У першому розділі описано основні проблеми захисту інформації у мобільних пристроях та додатках з урахуванням обмежень, що стосуються даних апаратів та їх програмного забезпечення, а саме: портативність, обмежений час роботи батареї, вбудовані датчики смартфону, що також зчитують інформацію та інші. Описано основні види мобільних додатків за функціоналом та за принципом розробки: нативні, веб-версії сайтів, гібридні (крос-платформні). Також розглянуто принципи, на яких базуються системи захисту у мобільних додатках. Описано основні методи криптографічного захисту даних.

У другому розділі проведено аналіз принципу роботи криптографічного алгоритму для шифрування та дешифрування даних *AES*, з описанням кожного етапу реалізації. Розглянуто технічні засоби, що були обрані для програмної реалізації мобільного додатку з функцією шифрування/дешифрування даних, а саме: фреймворк для розробки крос-платформних додатків *React Native*, технологію для спрощеного розгортання додатків *Expo*, мову програмування *JavaScript*, сервіс для створення баз даних *Firebase* та середовище розробки *Visual Studio Code*.

У третьому розділі описано структуру проєкту мобільного додатку «Персональні дані». Розглянуто етап проєктування інтерфейсу користувача додатку. Описано програмну реалізацію основних функцій криптографічного алгоритму *AES* та процес створення віддаленої бази даних на основі сервісу *Firebase*. Проведено опис програмної реалізації основних компонентів мобільного додатку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адаменко Михаил. Основы классической криптологии. Секреты шифров и кодов. / Адаменко Михаил – ДМК Пресс, 2012. – 256 с.

2. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С.121-124).

3. Вайк А. JavaScript. Энциклопедия пользователя / А. Вайк, Р. Вагнер – М: ДиаСофт, 2001 – 480с.

4. Вейл Э. Разработка приложений для мобильных устройств. / Вейл Э. – СПб.: Питер, 2015 – 480с.

5. Вербіцький О. В. Вступ до криптології. / Вербіцький О. В. — Л. : ВНТЛ, 1998. — 248 с.

6. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України. Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів “Проблеми та перспективи розвитку системи безпеки життєдіяльності” (м. Львів, 23-24 березня 2017 р.). [в 2 ч.]. Ч. 2. – Львів: ЛДУ БЖД, 2017. С. 11–12.

7. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція “Інформаційна безпека в сучасному суспільстві” (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24.

8. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп’ютерних технологій. – Запоріжжя: Просвіта, 2001. – с.120-174.

9. Довганич М. О. Методи та засоби захисту персонального інформаційного простору в контексті мережевої розвідки / М. О. Довганич, В. І. Ящук // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С. 79-81).

10. Используйте Firebase, единый кроссплатформенный SDK от Google, чтобы улучшить приложения. [Електронний ресурс] // Android – Режим доступу до ресурсу: https://developer.android.com/distribute/best-practices/develop/build-with-firebase?hl=RU

11. Кухарська Н.П., Полотай О.І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13), pp. 126-136.

12. Маккоу А. Веб-приложения на JavaScript. / Маккоу А. – СПб.: Питер, 2012 – 288с.

13. Полотай О., Деменко В. Особливості оцінки ризиків загроз інформаційної безпеки. Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. (Київ, 18 березня 2016 року) : у2 ч. Ч. 2. – Київ: Нац. акад. СБУ, 2016. – С. 204-205.

14. Полотай О.І. Аналіз програмного забезпечення захисту систем керування базами даних. Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: збірник тез доповідей Всеукраїнської науково-практичної Інтернет-конференції. – Черкаси: ЧНУ ім.. Богдана Хмельницького, 2016, С. 75-76.

15. Полотай О.І., Крепак В. Способи захисту інформації баз даних MYSQL. Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції. – Черкаси, 2017. - С. 60-61.

16. Про захист персональних даних. [Електронний ресурс] // rada.gov.ua – Режим доступу до ресурсу: http: //zakon4.rada.gov.ua/laws/show/2297-17

17. Упростите вход с помощью быстрой и надежной аутентификации Firebase. Електронний ресурс] // Android – Режим доступу до ресурсу: https://developer.android.com/distribute/best-practices/develop/firebase-authentication?hl=RU

18. Хансен Г. Дж. Базы данных: разработка и управление / Г.Дж. Хансен. – М.: БИНОМ, 2010. – 704 с.

19. Хорошко В.О., Огаркова І.М., Чирков Д.В., Голего А.Г., Горохова Т.Б. Термінологічний довідник з питань технічного захисту інформації. / За ред. проф. Хорошка В.О. – К.: Ей-Бі-Сі, 2002.

20. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).

21. Adam Boduch, Roy Derks. React and React Native: A complete hands-on guide to modern web and mobile development with React.js, 3rd Edition. Packt Publishing Ltd / Adam Boduch, Roy Derks, 2020 - Computers - 526 p.

22. Andress, J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. / Andress, J. – Syngress, 2014. – 240 p.

23. Bonnie Eisenman. Learning React Native. / Bonnie Eisenman. – O'Reilly Media, Inc., 2015. – 272 p.

24. Dowkin Morris. Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption. [Електронний ресурс] // NVPUBS – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38G.pdf.

25. Firebase. [Електронний ресурс] // BMSTU – Режим доступу до ресурсу: https://ru.bmstu.wiki/Firebase

26. Learning React Native. [Електронний ресурс] // O'Reilly – Режим доступу до ресурсу: https://www.oreilly.com/library/view/learning-react-native/9781491929049/ch01.html

27. Martin Fowler — GUI Architectures. Часть 2. [Електронний ресурс] // Habr – Режим доступу до ресурсу: https://habr.com/post/53536/.

28. OS Statistics. [Електронний ресурс] // W3C – Режим доступу до ресурсу: http://www.w3schools.com/browsers/browsers_os.asp

29. React Native official page. [Електронний ресурс] // GitHub – Режим доступу до ресурсу: https://facebook.github.io/react-native/

30. UX – это не UI [Електронний ресурс] // cmsmagazine.ru – Режим доступу до ресурсу: http://www.cmsmagazine.ru/library/items/usability/ux-is-not-ui/

31. Visual Studio Code web page. [Електронний ресурс] // Visual Studio – Режим доступу до ресурсу: https://code.visualstudio.com/