

АНАЛІЗ БЕЗПЕКИ ДАНИХ В ОНЛАЙН-СЕРВІСІ ДЕРЖАВНИХ ПОСЛУГ «ДІЯ»

Запара М. О.

Національний аерокосмічний університет ім. М. Е. Жуковського
«ХАІ» Науковий керівник Цуранов М. В.

Актуальність. З розвитком цифрових технологій ціна на мобільні пристрої суттєво зменшилася, що призвело до росту кількості користувачів. Через пандемію коронавірусу збільшився попит на різноманітні онлайн сервіси. Це призвело до прискорення цифрової трансформації, завдяки якій різноманітні структури почали створювати онлайн сервіси. На відміну від фізичних офісів, онлайн сервіси відкриті цілодобово та без вихідних. У зв'язку з цим, чимала кількість країн почали розробляти проекти у цій сфері. Найбільш успішними з них є: Польща, Китай, Естонія, ОАЄ та Великобританія — які запустили свої проекти впродовж 2019-го року [1]. Також до цього списку, у лютому 2020-го року, приєдналась Україна, у рамках проекту «Держава у смартфоні».

Метою цієї роботи є проведення аналізу безпеки даних в онлайн-сервісі державних послуг «Дія». В рамках цієї роботи буде проведено аналіз мобільного застосунок «Дія».

Основні положення. «Держава і Я» — український електронний сервіс державних послуг, розроблений Міністерством цифрової трансформації, в рамках проекту «Держава у смартфоні». Розглянемо складові даного сервісу: Портал — онлайн-сервіс державних послуг. [2] Застосунок — мобільний застосунок з електронними документами. Освіта — портал з онлайн-курсами. Бізнес — портал з допомоги малому та середньому бізнесу. Дія City — спеціальний правовий режим для IT-індустрії.

В даний час користувачу доступні наступні цифрові документи: водійські права, свідоцтво про реєстрацію транспортного засобу, поліс страхівки авто, закордонний паспорт, ID-картка, Цифровий студентський, картка платника податків. Таким чином станом на 17 серпня 2021 року кількість активних користувачів онлайн-сервісу державних послуг «Дія» перевищила 6 млн осіб [3].

Для того, щоб скористатися цифровими документами користувач повинен пройти процес ідентифікації. Для цього у додатку існують наступні варіанти авторизації з використанням: BankID, технології NFC та ЕЦП. Перший варіант є основним, оскільки авторизація з NFC є

неможливо у випадку, якщо у користувача немає ID картки, а ЕЦП має лише незначна кількість користувачів.

Авторизація за допомогою BankID для користувача доволі зручна, оскільки він проходить цей процес використовуючи свої дані для авторизації у банківському клієнті.

У подібних застосунках інших держав основними засобами ідентифікації є Mobile-ID. Mobile-ID – це рішення цифрового підпису на базі SIM-карти (для якого необхідна спеціальна SIM картка) [4]. Такий ідентифікатор є надійним завдяки тому, що це ЕЦП яке зберігається на спеціальній SIM картці контрактних абонентів.

Останнє оновлення надало можливість зробити знімок екрану, який дозволяє надати інформацію зі своїх документів іншій людині. Але таким чином виникає неконтрольоване поширення персональних даних.

Висновки. Додаток «Дія» на даний момент продовжує розроблятися та оновлюватися, оскільки, має чи малу кількість недоліків відносно світових аналогів. До цих недоліків відноситься: використання менш надійного BankID замість Mobile-ID; відсутність технічної документації та закритість системи. Значно зменшити кількість недоліків можна лише за умови проведення аудиту незалежними експертами.

Список літератури

1. Ukraine's digital revolution continues with enhanced legal status for e-passports. *Atlantic Council*. URL: <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-digital-revolution-continues-with-enhanced-legal-status-for-e-passports/> (дата звернення: 23.10.2021);
2. Державні послуги онлайн. *Дія*. URL: <https://plan2.diia.gov.ua/> (дата звернення: 23.10.2021);
3. Телеграм канал «FEDOROV». *Telegram*. URL: <https://t.me/zedigital/766> (дата звернення: 23.10.2021);
4. «Smart-ID» — интеллектуальный способ идентификации личности. Как пользоваться Mobile-ID для регистрации учетной записи Smart-ID. *Smart-ID*. URL: <https://www.smart-id.com/ru/spravka/voprosy-otvety/registratsiya/kak-polzovatsya-mobile-id-dlya-registratsii-uchetnoj-zapisi-smart-id/> (дата звернення: 30.10.2021).

Відомості про авторів

Запара Михайло Олександрович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 050-555-16-08, m.zapara@student.csn.khai.edu

Цуранов Михайло Віталійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, m.tsuranov@csn.khai.edu