

Секція 1

## АНАЛІЗ ТА ФОРМУВАННЯ ОСНОВНИХ РИЗИКІВ ДЛЯ БЕЗПЕКИ ДАНИХ КОРИСТУВАЧІВ ДЕРЖАВНОГО ЗАСТОСУНКУ «ДІЯ»

Зміївський В.С

Національний аерокосмічний університет ім. М.С. Жуковського «ХАІ»  
Науковий керівник Шевченко І.В.

**Актуальність.** Безумовним є те, що сучасний світ ІТ невпинно розвивається, роблячи наше повсякденне життя максимально комфортним. Наша держава на сьогодні є однією з найбільш прогресивних та сучасних країн Європейського континенту з точки зору діджалізації життя суспільства. Український уряд спрямовує значні ресурси на розвиток цільової галузі та процесу діджалізації, розуміючи, що саме за цим буде майбутнє. Одним з доказів цього є створення державного застосунку «ДІЯ» [1], який був впроваджений у користування українських громадян. Але, чи є цей застосунок безпечним з точки зору зберігання даних?

**Мета роботи:** полягає у аналізі та виділенні основних ризиків, які можуть призвести до порушення безпечності зберігання, а отже до «витікання» даних користувачів.

**Основні положення.** Дія (скорочення від «Держава і я») – мобільний застосунок і офіційний веб-сервіс для отримання державних онлайн-послуг, розроблений Міністерством цифрової трансформації України, який дозволяє працювати з цифровими документами та публічними послугами.

Встановивши Дію користувач отримує можливість отримати електронні документи в смартфоні, а також передавати їхні копії при отриманні державних послуг. Також користувач може скористатися послугами отримання різних за типом і призначенням довідок. Станом на травень 2022 року застосунком і веб-сервісом користується вже понад 17 млн людей, у веб-сервісі доступно вже 72 послуги, а у застосунку – 9 послуг та 15 цифрових документів, в планах уряду до 2024 року перевести 100 % державних послуг у Дію [2].

Аналізуючи проблему безпечності даних в Дії було виділено ряд ризиків, які можуть нести інформаційну небезпеку для зберігання даних користувачів:

Ризик 1. Порушення розмежування інструментів ідентифікації за рівнями довіри. Потрібно розуміти, що можливість ідентифікації особи через програмний інструмент BankID, яку надає Дія, є сумнівною для такого рівня важливості документів, які зберігаються у Дії.

Ризик 2. Дія збирає, опрацьовує та зберігає дані користувача. Як і будь-який програмний застосунок, Дія збирає, опрацьовує та зберігає дані, про що прямо написано на офіційному сайті «Дії» та у розділі

«Меню/Повідомлення про обробку персональних даних» мобільного додатка.

Ризик 3. Вхідна аутентифікація за допомогою пароля-кода. Звичайно, що код – це найпростіший у запам'ятовуванні та введенні вид аутентифікації, але також і найпростіший у підборі та взламуванні. До речі пароль-код у Дії складається всього з 4 цифр.

Ризик 4. Дані зберігаються на смартфоні чи гаджеті, на якому встановлено застосунок. Згідно з заявами розробників програми «Дія», програма не зберігає електронні документи громадян, при цьому зображення з даними документа зберігаються у смартфоні. При втраті смартфона даними з застосунку можна неправомірно користуватися.

Ризик 5. Незрозумілість порядку використання та «підтягування» даних сторонніми організаціями. Немає чіткого роз'ясненого порядку використання електронної версії паперів у державних організаціях. Є ризики, що електронна версія може бути використана без дозволу власника [3].

**Висновки.** В результаті проведеного аналізу було виділені основні ризики, які можуть нести інформаційну небезпеку для зберігання даних користувачів Дії. На основі відгуків користувачів був проаналізований їх практичний досвід використання Дії, а також він був порівняний з власним досвідом автора. Отримані результати будуть використані для вирішення проблеми підвищення рівня довіри до державної цифрової програми на прикладі Дії.

### Список літератури

1. Дія. *Wikipedia*. URL: <https://ru.wikipedia.org/wiki/Дія> (дата звернення: 27.10.2022);
2. Оформлення субсидій у Дії та перепис населення з Apple - Михайло Федоров про цифрові плани України. *Surl*. URL: <http://surl.li/dsdmj> (дата звернення: 27.10.2022);
3. Як працює «Дія» та звідки беруться данні. *Surl*. URL: <http://surl.li/dsdlm> (дата звернення: 29.10.2022).

### Відомості про авторів

Зміївський Володимир Сергійович, студент кафедри інженерії програмного забезпечення, м.т. 0971718829, [vovazmievskoy2003@gmail.com](mailto:vovazmievskoy2003@gmail.com)

Шевченко Ілона Володимирівна, доцент кафедри інженерії програмного забезпечення, к.т.н., доцент, [i.shevchenko@khai.edu](mailto:i.shevchenko@khai.edu)