УДК 004.492

Ігор Володимирович Кобзев,
кандидат технічних наук, доцент, доцент кафедри природознавчих наук Харківського національного університету радіоелектроніки

Катерина Костянтинівна Петрова,
студентка групи ВПС 17-1
Харківського національного університету радіоелектроніки

Кібербезпека та відкриті дані

Відкриті дані (або open data) – підхід до зберігання інформації, згідно з яким набір даних має бути у вільному доступі, вільно використовуватися та розповсюджуватися. При цьому такі дані можуть використовувати як неприбуткові організації, так і комерційні установи [1].

Відповідно до Закону України «Про доступ до публічної інформації» публічна інформація у формі відкритих даних (відкриті дані) оприлюднюється для вільного та безоплатного доступу до неї. Відкриті дані дозволені для їх подальшого вільного використання та поширення [2].

У 2016 році Україна взяла на себе зобов'язання виконувати принципи Хартії відкритих даних: перш за все, робити урядові дані відкритими за замовчуванням. Відповідальним органом стало Державне агентство з питань електронного уряду.

В процесі реформування державні органи України публікують все більше відкритих даних з різних сфер діяльності. І ці дані допомагають зробити державний апарат прозоріше і посилити економіку країни.

Згідно з рейтингом Global Open DataIndex, який становить неурядова організація Open Knowledge International, в 2018 году Украіна зайняла 31 місце (на 23 позиції вище в порівнянні з 2016-м) [4]. У рейтингу Open Data Barometer від World Wide Web Foundation Україна посіла 17 місце за 2017 рік, які підписали Міжнародну хартію відкритих даннях [3].

Для функціонування будь-якого сервісу необхідні дані. Велика кількість даних знаходиться у власності у держави, і держава не завжди поспішає ними ділитися.

Не все просто і з питаннями кібербезпеки відкритих даних. На жаль, сучасні цифрові технології розвиваються настільки стрімко, що архі-

тектори і розробники забувають пропрацювати ризики кібербезпеки і впровадити ефективні заходи їх зниження.

У звіті з кібербезпеки від компанії Cisco відзначається що хакери та держави створюють зловмисне програмне забезпечення із безпрецедентним рівнем складності та впливу; відбувається використання у військових цілях та на користь спецслужб хмарних сервісів та інших технологій, що використовуються зазвичай для законних цілей; для деяких творців шкідливого програмного забезпечення завдання полягає не в отриманні фінансової вигоди, а у руйнуванні інфраструктури та блокуванні систем цілих держав [1].

Фізично можливо два варіанти архітектури: Semi-automatic- дані завантажуються на портал відкритих даних вручну (через веб-інтерфейс) та Real-time – дані динамічно завантажуються з порталів відкритих даних органів державної влади або з інших веб-сервісів.

Архітектура Semi-automatic зазнає трьох ризиків:

- фальсифікація відкритих даних – зламавши портал, зловмисник може підробити відкриті дані, вплинувши тим самим на роботу цифрових сервісів, котрі їх використовують;

- підробка порталів – зловмисники можуть створити підробки порталів відкритих даних, представившись довіреним джерелом даних для цифрових сервісів.

- атака на бренд «відкриті дані» – розсилка спаму з пропозиціями отримати доступ до «розширених відкритих даних» в рамках «бета-тесту» або за невелику плату. Насправді листи міститимуть віруси і експлойти.

Архітектура Real-time зазнає трьох вищеописаним і двом специфічним ризикам:

- DDoS-атаки – відмова в обслуговуванні може привести до недоступності цифрових сервісів;

- комплексні цільові атаки – веб-сервіс може бути використаний як «точка входу» (entry point) в IT-інфраструктуру органу влади.

Вищеописані ризики можуть призвести до значних негативних соціальних і фінансових наслідків. Це може привести до нелегітимного використання відкритих даних в неправомірних цілях.

Сама наявність відкритих даних дозволяє бізнесу і суспільству звіряти новинні публікації і дослідження з незалежним офіційним джерелом, що істотно підвищує інформаційну безпеку.

Відсутність в відкритому доступі відомостей про архітектуру кібербезпеки відкритих даних не означає, що система заснована на відкритих даних цифрових сервісів може бути скомпрометована, а відповідні можливості для економічного зростання країни – втрачені.

Список бібліографічних посилань

1. Що таке відкриті дані та як ними користуватися. *Na chasi* URL: https://nachasi.com/2018/06/12/vidkryti-dani/ (дата звернення: 08.10.2019).
2. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 08.10.2019).
3. Україна вийшла на 17 місце в рейтингу відкритості даних // Українська правда : сайт. 21.09.2018. URL: https://www.pravda.com.ua/news/2018/09/21/7192760/ (дата звернення: 08.10.2019).
4. Place overview // Global Open Data Index. 2018. URL: https://index.okfn.org/place/ (дата звернення: 08.10.2019).

Одержано 10.10.2019