Тарасенко Олег Сергійович,
кандидат юридичних наук, доцент кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ

ПРОТИДІЯ КІБЕЗЛОЧИНАМ: ДОСВІД БРАЗИЛІЇ

За останні кілька років велика кількість бразильців отримали доступ мережі Інтернет за допомогою до комп'ютерів, мобільних пристроїв тощо, причому державні та приватні сектори сприяють тому, щоб ці технології стали більш доступними та доступними для населення. Поряд з цим,

більшість населення Бразилії не вживають необхідних заходів для забезпечення захисту особистих та конфіденційних даних [1].

Здебільшого, користувачі службових, приватних пристроїв під час налаштування мережі Інтернет використовують стандартні паролі. Як наслідок, бразильська арена кіберзлочинності є лідером у сфері Інтернет-зловживань. Бразилія перебуває на другому місці за кількістю шахрайств онлайн-банкінгу та фінансових Інтернет-шахрайств [2]. Як правило, кіберзлочинці такі засоби вчинення як троян, фішинг на основі зображення або фальшивого браузера, велика кількість векторів атак тощо. У свою чергу, користувачі глобальної мережі не видаляють незрозумілі електронні листи, підключаються до незахищених загальнодоступних бездротових мереж, як наслідок шість із десяти користувачів Інтернету стали жертвами кіберзлочинів [1].

Поряд з великою кількістю вчинення злочинів з використанням мережі Інтернет, в Бразилії не прийнято окремого Закону, який регулювалося протидія кіберзлочинності та кібербезпеці. Поряд з цим, окремі положення щодо протидії даним злочинам регламентуються кримінальним, споживчим кодексами та Законом про Інтернет.

У той же час, на відмінну від України, законодавством Бразилії значна законодавча робота проведена в напрямку захисту персональних даних. В першу чергу, передбачено законодавчі положення на захист персональних даних. Так, Цивільний кодекс визнає і закріплює принцип незалежності особистого та приватного життя і закріплює, що особисте життя людини є недоторканим; Кодекс споживачів закріпив захист конфіденційних даних особи при виникненні відносин між споживачами; Закон про Інтернет встановлює інші принципи та правила стосовно конфіденційності та захисту персональних даних користувачів Інтернету, а саме, правила збирання, зберігання та обробки особистої інформації через Інтернет-послуги та програми [3].

Також необхідно відзначити, що законодавчими актами Бразилії передбачено відповідальність за незаконне використання персональних даних особи. Перш за все, кодекс Споживача передбачає кримінальну відповідальність (від шести до дванадцяти місяців позбавлення свободи) за певні дії, які можуть кваліфікуватися як правопорушення, хоча кримінальна відповідальності за порушення законів про кібербезпеку та захист даних застосовується дуже рідко. В будь-якому випадку штраф може бути накладений на організацію, яка не дотримується законів про конфіденційність або у разі порушень даних. По-друге, Законом про Інтернет встановлено штраф у розмірі до 10% від економічного обігу коштів в Бразилії за попередній фінансовий рік або призупинення чи заборона на ведення бізнесу в Бразилії [3].

Також, Кримінальним кодексом Бразилії [4] закріплено основні положення щодо відповідальності за кіберзлочини. Так, Розділ III «Злочини проти нематеріальної власності», містить «Главу I «Злочини проти інтелектуальної власності та порушення авторських прав», в якій закріплено відповідальність за: порушення авторського права, шляхом передачі програмного продукту (медіа) з повним або частковим відтворення, з прямою або непрямою метою отримання вигоди, *будь-якими засобами або способами*, без спеціального дозволу (ч. 1 ст. 184 КК Бразилії), а також надання такого матеріалу за допомогою кабелю, волоконно-оптичних, супутникових, хвиль або будь-якої іншої системи (ч. 2 ст. 184 КК Бразилії); публічні звинувачення за допомогою технічних засобів у вчиненні злочину (ч. 2 ст. 186 КК Бразилії), у т.ч. органи влади та управління (ч. 3 ст. 186 КК Бразилії). Наступне положення закріплене Главою I Злочини проти державних посадових осіб, проти управління, в цілому казнокрадство» Розділу XI «Злочини проти державного управління», а саме: ст. 313-А, передбачає відповідальність за включення помилкових даних, підробки або видалення правильних даних, а також зміна даних в комп'ютерних системах та базах даних державного управління з метою отримання неправомірної

вигоди для себе чи інших осіб або здійснення дій, що завдають шкоду; ст. 313-В, закріплює відповідальність за заміну або зміну офіційну, інформаційну систему або комп'ютерну програму без дозволу або клопотання уповноваженого органу.

Отже, поряд з великою кількістю вчинення злочинів з використанням мережі Інтернет, окремого закону направленого на протидії кіберзлочинності у Бразилії не закріплено. Проте, значні кроки зроблені щодо захисту персонального захисту осіб, при цьому передбачаються жорсткі санкції до фізичних та юридичних осіб.

Список використаних джерел

1. Teixeira M. Largest Cybercrime Threats in Brazil. Published: 8 Apr 2015 https://techinbrazil.com/largest-cybercrime-threats-in-brazil.

2. Going for Gold: Cybercrime and the Brazilian Threat Landscape. July 21, 2016. https://securityintelligence.com/going-for-gold-cybercrime-and-the-brazilian-threat-landscape/.

3. Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados. Data Security & Cybercrime in Brazil. https://www.lexology.com/library/detail.aspx?g=a1b949b5-5644-4941-858e-96c983ca7e42.

4. Código Penal Decreto-Lei n° 2.848, de 7 de dezembro de 1940. http://www.wipo.int/wipolex/ru/text.jsp?file_id=226393.