2. Roger R. Dube, Hardware-based Computer Security Technicas to Defeat Hackers: From Biometrics to Quantum Cryptography, 2021. 205 p.
3. Luther Martin, Introduction to Identity-Based Encryption (Information Security and Privacy Series), 2008. 245 p.

УДК 004.8

Ярош О.Л., студент 4 курсу спеціальності 122 «Комп'ютерні науки»
Потапова Н.А., к.е.н, доцент, доцент кафедри інформаційних технологій

ЗАХИСТ ОСОБИСТИХ ДАНИХ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

Донецький Національний університет імені В. Стуса, м. Вінниця

На сьогоднішній день збір та обробка даних знайшли широке використання в найрізноманітніших сферах. Їх обробка не тільки допомагає в виконанні повсякдених задач, але й може слугувати інструментом порушення права на приватність людини. У зв'язку з цим одним із найбільш актуальних завдань є розробка систем захисту персональних даних. Створення дієвої системи захисту персональних даних належить до міжнародних зобов'язань України, в тому числі пов'язаних із європейською інтеграцією нашої держави. Зокрема, саме від виконання цього зобов'язання значною мірою залежать євроінтеграційні прагнення української держави.

Проблема, як виток персональних даних громадян України із автоматизованих систем державних органів та приватних компаній стає пріоритетом діяльності злочинів. Ситуація стає все більш складнішою, оскільки з'являються нові форми приховування злочинцями не лише своїх комунікацій (в т.ч. із використанням можливостей Darknet та Deepweb), але й інструментів виведення коштів (кріптовалюти).

На сьогоднішній день органи державної влади стикаються із низкою загроз та викликами в сфері кібербезпеки. В Україні існує понад 100 державних та єдиних реєстрів, які містять конфіденційну інформацію. Більшість з них використовує авторизацію за допомогою логіну та паролю, що в свою чергу має певні вразливості. Зокрема, у такий спосіб не можливо достовірно ідентифікувати особу, яка отримує інформацію з реєстру [2].

В сучасних умовах гостро стоїть проблема із захистом інформації, яка зберігається у розпорядників (держателів) реєстрів. Здебільшого мережева інфраструктура має застаріле та вразливе програмне забезпечення. Переважно користувачі, а деколи і адміністратори поряд з доступом до реєстрів мають

доступ в мережу інтернет, що в рази збільшує ризики зовнішнього ураження та подальшої кібератаки на системи зберігання інформації.

За період незалежності України, переважна більшість інформації накопичена на паперових носіях. З метою її цифрової трансформації залучаються приватні компанії. Вони тимчасово отримують доступ до інформації, що містить персональні данні. Тобто в рази зростають ризики витоку конфіденційних даних. На противагу, накопичення, обробка та зберігання більшої кількості інформації потребує збільшення цифрової інфраструктури (сервери, мережі, дата центри), а їх збільшення та розростання потребує підвищеної уваги до забезпечення безпеки цих об’єктів [1].

Збирання, опрацювання та накопичення даних в реєстрах вимагає реалізації принципу прозорості. Будь-яка інформація та опрацювання персональних даних повинні бути доступними і зрозумілими. Спеціальні цілі опрацювання конфіденційної інформації на момент їх збирання мають бути прямо вираженими, означеними та законними. В той же час, персональні дані повинні бути достатніми, відповідними та обмежуватися досягненням мети, для яких їх збирають. Крім цього, період, протягом якого зберігаються персональні дані, має бути скорочений до абсолютного мінімуму, з метою реалізації принципу «дані не зберігаються довше, ніж це необхідно». Чітко визначений період зберігання та знищення, убезпечить від несанкціонованого витоку інформації [1].

Національною поліцією встановлено, що на спеціальних форумах та у закритих спільнотах циркулюють різні бази даних. Деякі дійсно актуальні та постійно оновлюються, інші мають застарілий характер, однак містять персональну інформацію. Наявність такої циркулюючої інформації, створює підґрунтя для вчинення протиправних дій у кіберпросторі метою, яких є отримання прибутку від продажу персональних даних. Злочинці створюють спеціальні сервіси для перевірки інформації чи безпосереднього продажу баз даних.

Більш широка сфера – шахраї. Вони під приводом продажу інформації, баз даних здійснюють заволодіння коштами. Великий суспільний розголос, а також інше привертання уваги до будь-яких витоків інформації активізує злодіїв. Латентність таких злочинів значна, а їх розслідування переважно не розпочинається з заяви потерпілої сторони, більшість таких фактів розкривається ґрунтуючись на оперативній інформації [2].

Національною поліцією на постійній основі забезпечено відслідковування активності учасників російськомовного сегменту хакерської спільноти. Зокрема, на закритих онлайн майданчиках «darknet», «tor», на закритих каналах «skype», «telegram». Відслідковуються публікації приватних дослідників з інформаційної безпеки щодо витоку персональних даних громадян України із автоматизованих систем державних органів та приватних компаній. За наявною інформацією, такі витоки відбуваються щонайменше раз на 2 місяці.

Найпопулярнішими серед таких майданчиків є закриті веб-форуми «exploit.in», «phreaker.pro», «peers.fm» та «xss.io» доступ до участі в яких здійснюється на підставі численних перевірок кандидатів. Наявності в них хакерських навичок та поручителів, а також за вступними внесками, що в деяких випадках перевищують 150 доларів США.

У Національній поліції зазначений напрямок роботи забезпечується системними заходами особистого пошуку, які здійснюються найдосвідченішими працівниками, агентурною роботою з учасниками хакерської спільноти, роботою із власними оперативними обліками, які напрацьовані у ході збору вмісту закритих онлайн майданчиків «darknet», «tor», та у тому числі завдяки активній участі поліції у співпраці із правоохоронцями інших держав. Крім цього, Національною поліцією уживається комплекс заходів, спрямованих на викриття кримінальних правопорушень у сфері використання високих інформаційних технологій.

Таким чином, сьогодні загострюється проблема неправомірних дій різних суб'єктів, які використовують засоби електронно-інформаційного середовища. Активність у формуванні баз даних, обробка та поширення відомостей про осіб без їх відома призвели до виникнення глобальної за своїми масштабами у часі та просторі проблеми інформаційної безпеки людини, суспільства і держави щодо захисту персональних даних.

Список літературних джерел.

1. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. *Київ: К.І.С,* 2015. 220 с.
2. Інтеграція України в Європейське інформаційне суспільство: виклики та завдання / упор. А. В. Пазюк; рец. О. О. Гріненко, О. В. Олійник. *Київ: ФОП Клименко,* 2014. 221 с.
3. Петров О. С. Основи безпеки інформаційних систем. *Луганськ: Вид-во СНУ ім. В. Даля*, 2004. 148 с.