УДК 007:004.56:351.824.11(824.11(477) DOI 10.33042/2522-1809-2020-6-159-181-190

В.Д. Бойко, М.Д. Василенко

Національний університет «Одеська юридична академія», Україна

КІБЕРБЕЗПЕКА РОЗУМНИХ МІСТ: СОЦІАЛЬНІ АСПЕКТИ, РИЗИКИ ДЕАНОНІМІЗАЦІЇ І ДОКСІНГУ

У статті аналізується поняття та схема здійснення доксінгу, розкривається сутність деанонімізації та виявляються пов'язані з цими процесами загрози приватності і безпеці мешканців розумних міст. Пропонується комплекс заходів для захисту персональних даних, що зберігаються в інформаційних системах, які дозволять знизити ризики зламу таких даних та мінімізувати шкоду від деанонімізації та доксінгу.

Ключові слова: *розумне місто, деанонімізація, доксінг, персональні дані, кібербезпека, ризики.*

Постановка проблеми

Кількісне збільшення насиченості міської інфраструктури інформаційними технологіями (IT) в недалекому майбутньому призведе до якісного переходу: від розрізнених "цифрових островів" до "цифрових кластерів", а від них – до "розумних міст" [1]. Нині перехід не скрізь здійснюється планово. Найчастіше все відбувається "самопливом", без централізованої стратегії, або з недостатньо вибудуваною, декларативною стратегією, з некваліфікованим персоналом, без аналізу довгострокових наслідків [2, 3]. Стандарти, покликані підвищити ефективність і безпеку планування розвитку розумних міст, на жаль, ще не досягли достатньої зрілості і не позбулися "дитячих хвороб" [4].

Недолік організації й планування тягне за собою ризики вже на стадії розгортання розумних міст. Попередня частина роботи (див. [5]) була присвячена в основному технічним аспектам, однак забезпечення кібербезпеки вимагає комплексного підходу – і крім технічних ризиків існують ризики соціальні.

Небезпеку представляє не тільки фізичний злом систем і його наслідки, але і крадіжка персональних даних і деанонімізація користувачів міської інформаційної екосистеми. Збиток від такої крадіжки даних, яка часто може бути здійснена без технічного злому інформаційних систем взагалі, буває часто більшим, ніж від фізичного злому [6, 7]. Іноді розкриття конфіденційної інформації може породжувати ризики і завдавати шкоди, яка є більшою або сумірною зі шкодою від перехоплення контролю або виведення з ладу інформаційно-комунікаційної системи в результаті хакерської атаки.

У сучасній мові для такого процесу деперсоналізації існує окремий неологізм – "доксінг" (калька від англійського dox, doxxing [8]), який позначає процес навмисної публікації персональних даних, коли зловмисник розкриває конфіденційну та/або особисту інформацію. Термін походить від неформального прочитання терміна docs (документи) і використовувався в стійкому виразі dropping dox, яке позначало спосіб помсти комусь-небудь шляхом порушення його анонімності. Хоча це не єдиний ризик, пов'язаний з проблемою конфіденційності, він є одним з ключових у проблемі соціального аспекту кібербезпеки, оскільки тягне за собою ризик фізичної шкоди [9]. Опубліковані дані можуть включати таку особисту інформацію, як ім'я, адреса, номер телефону. Жертва доксінгу може піддаватися погрозам, переслідуванням, в сучасних умовах – насильству і соціальному тиску. Також доксінг може випереджати інші, складніші схеми завдання збитку, наприклад, бути частиною соціальної інженерії.

Без прийняття спеціальних заходів технічного, організаційного та законодавчого характеру практика доксінгу буде продовжувати зростати. Можна виділити дві головні причини цього.

Перша полягає в повсюдному впровадженні цифрових технологій і стосується безпосередньо розвитку міської інформаційної екосистеми на шляху до "розумних міст". Такий процес тягне за собою різке зростання збору і зберігання персональної інформації. Вже зараз основні учасники цифровізації міського середовища збирають велику кількість персональної інформації про користувачів. Інакше кажучи, сучасний мешканець інформаційного простору залишає помітний "цифровий слід", що складається з різних фрагментів інформації, що зберігаються в різних

 © Бойко В.Д., Василенко М.Д.

базах даних [10]. Чим ближче до "розумного міста", тим більш розвиненою і інтегрованою буде інформаційна система, що зберігає в собі персональні дані, тим більше "цифрових слідів", тим простіше отримувати потрібні дані, тим вище ризик доксінгу.

Друга причина полягає в зростанні громадянської активності в інфопросторі. Таке зростання пов'язане з поширенням цифрових технологій і усвідомленням їх можливостей, в тому числі для "хактівізму" (поєднання термінів "хакінг" і "активізм", що описує форму ненасильницького цифрового активізму, де мотивом не є особиста фінансова вигода), "мережевого вігілантізма" (переслідування в інфопросторі осіб, які є, на їхню думку, злочинцями) або навіть "netilantism", що набув поширення після широкої кампанії руху учасників протестів в Гонконзі проти законопроєкту про екстрадицію з публікації персональних даних офіцерів поліції й чиновників, які брали участь в придушенні заворушень [11]. Детально зростання і становлення "хактівізма", який найбільшу активність отримав з початку 2010-х років, описані в [12]. Тут ми відзначимо, що рухи, подібні Anonymous, продовжують рости й залучати до процесу деанонімізації все нових учасників.

Аналіз останніх досліджень та публікацій

Як було показано вище, проєктування розумних міст тісно пов'язане зі збором інформації, що створює ризики для конфіденційності та збереження персональних даних.

У роботі [13] показано, що урбанізація в найближчому майбутньому буде тісно пов'язана з трьома основними темами: розумні міста, використання великих даних і захист персональної інформації та конфіденційності. У цьому дослідженні детально розглядається використання великих даних, геоданих і даних, що збираються в розумному місті, а також вплив європейських і голландських директив щодо захисту конфіденційності та регулювання використання даних, зокрема – GDPR. Автори виявляють труднощі із забезпеченням конфіденційності та захисту персональних даних і показують, що частково вони обумовлені сформованою практикою розробки, частково – сучасними тенденціями в поширенні інформаційних технологій.

У статті [14] розглядається співвідношення між конфіденційністю і ефективним управлінням комунальними послугами, план управління якими є ключовим аспектом при проєктуванні розумних міст. Показано, що переваги інтелектуальної обробки даних в контексті розумного міста створюють ризики для конфіденційності, пов'язані з посиланням частих вимірювань з великим об'ємом даних.

Робота [15] представляє широкий огляд проблем, пов'язаних з безпекою, в контексті розумних міст. Показано, що на поточному етапі, розвиток розумних міст пов'язаний з такими тенденціями, як надмірна кількість даних, ускладнений і слабко впорядкований збір даних. Так само для сучасних технологій характерні розмиття кордонів між різними базами даних і індустріалізація, широке поширення хакінгу і технологій злому систем. Показано, що безпеку даних можна розглядати як чотирирівневу структуру з елементами, які вважаються критично важливими для роботи розумного міста: розумні речі, розумні простори, розумні системи і розумні громадяни (smart things, smart spaces, smart systems and smart citizens).

Викрадення персональних даних з інтегрованих інформаційно-комунікаційних систем і проблеми деанонімізації і доксінгу тепер набули глобальних масштабів.

У доповіді "Data breaches in Europe: Reported breaches of compromised personal records in Europe, 2005–2014" [16] наводяться такі цифри: персональні дані компрометуючі у 43 осіб зі 100 в Євросоюзі і у 56 зі 100 користувачів інтернету. Дослідження відноситься до 2014 року, зараз обсяг витоків набагато більший. Всього в доповіді розглянуто 229 інцидентів, пов'язаних з витоком даних, які в глобальному масштабі призвели до втрати близько 645 мільйонів записів. З них підтвердилось 200 випадків, пов'язаних з людьми в Європі, і 227 мільйонів записів, втрачених в результаті порушень, пов'язаних з Євросоюзом.

Як згадувалося вище, доксінг як масове явище відбувався під час "революції парасольок" в Гонконзі [11]. 9 червня 2019 року там почалися протести проти законопроєкту про екстрадицію. Управління уповноваженого з питань конфіденційності особистих даних (PCPD) в Гонконгу повідомило, що під час протестів з 14 червня по 28 серпня 2019 року було зареєстровано і виявлено 683 випадки доксінгу, з яких 72 відсотки стосувалися співробітників поліції. Решта були націлені на державних чиновників, громадських діячів, законодавців, медичний персонал, які протестують проти законопроєкту про екстрадицію і родичів поліцейських [17]. Одна з характерних справ: 3 листопада 2020 року 32-річний технік телекомунікаційної компанії був засуджений до двох років тюремного ув'язнення за доксінг щодо 3 громадських діячів, 20 поліцейських і 6 членів сімей поліцейських, інформацію про яких він розмістив в додатку Telegram [18].

У роботах [19, 11, 20] продемонстровано, що кількість витоків даних, їх використання для доксінгу і загальний матеріальний збиток виявляють тенденцію до зростання і в видимому майбутньому можуть досягти разючих величин.

У статті [19] показано, що обсяг персональних даних, доступних в онлайні, постійно зростає. "Поверхня атаки", що оточує ці дані, стає все більшою, і її все складніше захистити. Крім того, інформація, отримана в результаті самих різних зломів, поширюється і накопичується в руках кіберзлочинців ("сірі бази даних"), що призводить до кумулятивної ерозії конфіденційності. У роботі проведено дослідження статистики зломів з 2000 по 2015 рік. Прогнози показують, що загальний обсяг зломів подвоїться з двох до чотирьох мільярдів елементів протягом наступних п'яти років, перевищуючи кількість користувачів Інтернету.

Таким чином, загальне масове і неконтрольоване поширення персональних даних буде являти собою серйозний аспект кібербезпеки в контексті розвитку розумних міст.

Мета статті полягає в аналізі і виробленні рекомендацій з купірування або ослаблення можливих ризиків і загроз, породжуваних в процесі переходу від сучасних міст до розумних міст. Соціальний аспект кібербезпеки розумного міста бачиться насамперед у збільшенні ризиків розкриття приватності, які можуть привести до деанонімізації, яка надалі може бути використана для доксінгу, кібербулінгу, шантажу або в схемах соціальної інженерії.

Виклад основного матеріалу дослідження

Загальна схема доксінгу

Як здійснюється доксінг? Аналізуючи випадки деанонімізації і доксінгу, можна виділити три основні стадії:

• цільова установка, вибір "мішені" або "жертви";

• формування досьє: послідовний ітераційний процес пошуку і обробки даних;

• публікація отриманих джерел.

Весь ланцюжок дій є важливим для розуміння процесу, і при впровадженні систем захисту персональної інформації повинний розглядатися в цілому. Зокрема, від вибору мішені і цільової установки (як буде використовуватися інформація? Буллінг і соціально-суспільний тиск? Шантаж? Підготовчий етап для соціальної інженерії?) залежить від дій з отримання "досьє". Вибір платформи публікації "досьє" (третя стадія) – соціальна мережа, darknet, новинний сайт, навмисне поширення інформації в ЗМІ – визначає, ризики, можливий ступінь шкоди для жертви і заходи купірування щодо запобігання або скорочення збитків.

У сучасному світі неможливо повністю виключити ризики деанонімізації і доксінгу. Цьому сприяє розподілена і частково анонімна природа сучасних інформаційних мереж. У більшості випадків можна знайти місце, яке виявиться поза досяжністю для правових санкцій, заборон, цензури чи силового тиску.

Приклад WikiLeaks, як екстремальний варіант розвитку подій, показує що навіть спільні зусилля національних держав, кримінальними переслідуваннями і діями кількох мережевих гігантів (Amazon, PayPal, Visa, MasterCard) не привели до успіху спроб закриття розповсюджуваних даних. У деяких випадках прямі спроби перешкодити поширенню незручної інформації можуть призвести до протилежного результату, викликавши лавиноподібне тиражування даних по всій інформаційній мережі – ефект Барбари Стрейзанд.

Однак, для даної теми (захист персональних даних в "розумному місті") має значення аналіз дії зловмисника на другому етапі (збір та формування "досьє").

Такий збір інформації, як було сказано вище, може бути активним чи пасивним. Активне отримання даних має на увазі використання явно протизаконних дій для отримання інформації: соціальна інженерія, контакт з жертвою або з її оточенням, злом комп'ютера жертви, злом хмарних систем. Він не входить до розгляду в даній роботі, хоча його вплив все одно позначається, оскільки навіть при пасивному пошуку інформації може використовуватися "сіра інформація" – нелегальні джерела даних, отримані третіми особами, наприклад база даних мобільних телефонів з іменами і адресами користувачів.

Пасивне отримання даних передбачає роботу з безліччю ітерацій, в якій послідовно виконуються два основних етапи: збір інформації з відкритих (іноді "сірих") джерел інформації, аналіз отриманої інформації і постановка задачі на повторення збору інформації, але вже з іншим, більш точним запитом, з пошуком в альтернативному джерелі даних і так далі.

Як джерела для збору інформації зазвичай виступають публікації в соціальних мережах і на форумах, по-різному отримані геодані (дані геопозиціювання, позиціювання за сигналами мобільних вишок і по пеленгу локальних точок доступу WiFi), легальні бази даних – онлайнові карти і аерофотознімки (OpenStreetMap, WikiMapia, Google Earth, Bing), бази даних з панорамними оглядами (Mapillary, Google Street View), довідники різного роду, в тому числі інформація з різних реєстрів

(наприклад, єдиний державний портал відкритих даних в Україні).

Після отримання даних здійснюється їх аналіз. При цьому може використовуватися технологія, що нагадує фасетний пошук (перетин різних категорій інформації з метою відфільтрувати незначущі випадки), можуть вибудовуватися графи різного роду, зокрема, в роботі [21] показано, як будується соціальна графа жертви на основі її виявлених контактів.

Як приклад роботи по деанонімізації можна привести класичне використання бази даних переміщення мобільного телефону користувача. У первісному вигляді таке переміщення виходило шляхом аналізу присутності телефону в полі зору мобільних вишок, однак, зараз такі дані можуть бути отримані менш екзотичним шляхом, оскільки більшість смартфонів відкрито або закрито збирають геодані і зберігають їх як на телефоні, так і на сайтах різних постачальників даних.

Наприклад, згідно з [22], починаючи з операційної системи iOS 4, в смартфоні був виявлений файл consolidated.db, який становить базу даних sqlite з таблицями під промовистими назвами «CellLocation», «CdmaCellLocaton» і «WifiLocation» (тобто розташування GSM-сот, CDMA-сот і точок доступу Wifi).

Процес з'ясування особи при наявності такої бази даних займає кілька послідовних ітерацій. На першій ітерації маршрут користувача телефону наноситься на карту. На другій ітерації серед переміщень користувача з'ясовуються можливе місце роботи та можливе місце проживання. Якщо такий пошук приніс успіх, наступна ітерація полягає в складанні списку жителів в місці проживання і списку співробітників на місці роботи. Іноді місце проживання може бути приватним будинком, і лише це вже може сильно скоротити пошук. На наступному етапі відбувається "фасетна фільтрація": особистість власника телефону з'ясовується шляхом перетину списків співробітників і списку мешканців.

Слід розуміти, що тенденції і тренди, описані вище, не поліпшаться в доступному для огляду майбутньому. Широке поширення екосистеми "розумних міст" неминуче призведе до насичення міського середовища високотехнологічними пристроями і появи великого класу програмного забезпечення. Майбутній мешканець "розумного міста" буде широко використовувати мобільний телефон, частіше смартфон, в якому включена геолокація, камера, встановлено кілька соціальних додатків. При цьому користувач змушений покладатися на сумлінність виробника апаратного забезпечення і постачальника програмного забезпечення, які, як свідчать приклади з [23], далеко не невинні.

Так само мешканці "розумного міста" будуть широко використовувати розумну переносну електроніку і різні сервіси, засновані на геолокації. Примітно, що саме використання сервісів геолокації навіть без зовнішньої атаки може бути використано для отримання персональних та інших особистих даних [24–26].

Особливо показове поширення схем отримання даних за відкритими або відносно відкритими джерелами геоданих. Один з показових випадків – розкриття і локалізація місцеперебування кількох військових баз різних країн в Афганістані, Сирії, Туреччині за допомогою відстеження відкритих даних в сервісі відстеження активності спортсменів за допомогою мобільних пристроїв Strava.

Армійські положення зазвичай забороняють використання на території військових частин пристроїв, які допускають можливість стільникового зв'язку, WiFi, фото- і відеознімання, запису звуку і т.д. Однак, використання фітнес-трекерів, які часто мають тільки GPS і Bluetoth-зв'язок (а іноді просто таких, що скидають дані по USB), не підпадає під ці заборони і зазвичай дозволяється. Однак з'ясувалося, що дані тренувань (GPS-треки), які ці трекери вивантажують в онлайнову "соціальну мережу для спортсменів" Strava, дозволяють досить швидко вираховувати місцеперебування військових баз [27, 28].

В екосистемі "розумного міста" широке поширення отримають приватні і громадські відеокамери, які використовуються для підвищення безпеки, контролю дотримання правил дорожнього руху, таргетованої реклами контролю за ланцюгами постачання й т.д. Сучасні камери, особливо нижнього цінового сегмента, часто дуже погано захищені від витоку даних і при установці часто конфігуруються без урахування налаштувань безпеки даних. Часто на таких системах не скинутий пароль виробника, встановлений за замовчуванням. Такі камери часто стають частиною ботнетів і беруть участь в поширенні шкідливого коду і в DDOS-атаках [29–32].

Забезпечення безпеки персональних даних

Вимоги до обліку контексту захисту

При плануванні захисту персональних даних в системах розумного міста слід враховувати, що таке планування відбувається в контексті загальної інформаційної системи міста, тому завжди слід встановлювати пріоритети захисту даних, визначати загрози, заходи і механізми їх реалізації та дії при виникненні інцидентів, пов'язаних з витоком даних [33].

Можна виділити два основних підходи в цьому напрямку: "конфіденційність як політика" і "конфіденційність як архітектура" [34]. В основі першого

підходу лежить реалізація принципів повідомлення про збір персональної інформації і вибору "гри з чесними правилами" з використання персональних даних. Підхід на основі вибору архітектури забезпечення конфіденційності покликаний мінімізувати збір персональних даних і робить наголос на знеособленні, анонімізаціх даних, що зберігаються на серверній стороні і по можливості перенесенні зберігання і обробки даних на клієнтську сторону, де вони будуть менш уразливі.

При впровадженні перерахованих підходів слід враховувати такі особливості:

• захист персональних даних не повинний створювати складності для управління містом (в тому числі для отримання цих даних за запитами різних служб);

Якщо система створює більше проблем, ніж вирішує, нею не будуть користуватися. Це характерно для більшості систем безпеки. Розробник кожен раз змушений балансувати між безпекою системи і зручністю її використання [35].

• відкриті дані слід піддавати процесу санації;

Наші рекомендації з санації даних перераховані нижче, тут же хотілося б зупинитися на можливостях ненавмисного витоку даних – у вигляді EXIF-інформації в файлах фотографій (в організації обов'язково повинен бути передбачений автоматичний санітайзер, який прибирає зайву інформацію), можливості документів деяких текстових процесорів (зокрема, Microsoft PowerPoint) зберігати історію редагування, а отже потенційну можливість відновити дані, які були видалені перед публікацією документу в інформаційному просторі.

У більшості випадків така санація може здійснюватися в повністю автоматизованому режимі і не вимагає інших витрат, крім розгортання та оновлення. Наприклад, згадане вище видалення EXIF-тегів фотографій, що публікуються, зазвичай проводиться засобами пакету imagemagick (в поєднанні, наприклад, з модулем PHP Imagick::getImageProfiles), або пакету ExifTool, або написаний самостійно. Більшість мов програмування і інструментів веброзробки підтримують роботу з EXIF і зображеннями, наприклад, бібліотека PIL / Pillow для мови Python. Будучи один раз розгорнутим, такий інструмент всю подальшу роботу буде здійснювати на стадії передпублікаційної обробки зображення. Однак, на практиці така санація проводиться далеко не завжди, а часто її здійснюють в "ручному режимі", що не тільки може привести до помилок, але і підвищує навантаження на персонал.

• в завдання для служб інформаційної безпеки, "білих хакерів", команд пентестінга та інших підрозділів, залучених для захисту інформаційної інфраструктури розумного міста, слід включати не тільки злом і викрадення даних, але і аналіз вже доступних відкритих даних на ризик деанонімізація;

Для служби інформаційної безпеки, за нашим досвідом, характерно зосереджуватися на технічній частині, в основному в ракурсі недопущення злому системи. Це робить тим більш важливим запит на роботу з безпеки персональних і критичних даних і розгляд можливих схем деанонімізації, оскільки це питання не є очевидним і, відповідно, не завжди потрапляє в поле зору відповідальних за інформаційну безпеку осіб [36].

• апаратне і програмне забезпечення слід піддавати перевіркам на наявність прихованих можливостей збору інформації (приклад Apple і Google, які впроваджують в мобільні додатки такі "недокументовані можливості" як збір інформації про переміщення користувача і його дії [23], показує, що це цілком імовірна можливість).

Це також не завжди є очевидним. Якщо в проєкті залучене програмне забезпечення з закритим кодом, завжди має сенс або звернутися до розробника з прямим питанням, або досліджувати такі продукти самостійно.

• слід розробляти плани на випадок витоку даних, який вже стався: як, де і хто буде діяти для мінімізації втрат.

Як було сказано вище, ніяка найдосконаліша система забезпечення безпеки не може дати стовідсоткової гарантії. При цьому наявність плану зі зменшення шкоди інцидентів безпеки дозволяє істотно скоротити, а іноді і усунути таку шкоду в цілому [37]. Слід враховувати, що чим раніше зацікавлені особи будуть поінформовані про інцидент, тим менша ймовірність істотного збитку. Наприклад, при витоках баз даних, що зберігають паролі, при оперативному реагуванні можна встигнути замінити паролі, перш ніж це призведе до більш серйозних інцидентів.

Як приклад успішної роботи з особистими даними можна привести організацію такої роботи в системах банкінгу. Така організація, якщо говорити в цілому, характеризується такими рисами:

• існує централізований стандарт безпеки – Payment Card Industry Data Security Standard (PCI DSS) та робота з персональними даними відбувається в його рамках;

• всюди виділені чіткі стандарти безпеки і ключова інформація, яка не повинна потрапити в треті руки;

• процедури роботи і обміну інформацією спрямовані на принцип найменших привілеїв: коли співробітники і клієнти мають доступ тільки до тієї інформації, яка потрібна для роботи і не мають доступу до іншої інформації;

• однією з вимог стандарту є забезпечення шифрування даних власників карток при їх передачі через загальнодоступні мережі;

• ведеться цілеспрямована робота з користувачами, при цьому акцент робиться на збереженні ключової конфіденційної інформації і недопущенні попадання цієї інформації до третіх осіб ("наші співробітники ніколи не будуть питати у вас пароль до аккаунту").

Слід зазначити, однак, що навіть така розвинена система не завжди працює, про що свідчить статистика численних зломів систем банкінгу, істотну частку яких складають призначені для користувача помилки й схеми соціальної інженерії. Хорошим прикладом останніх витоків є злом American Bank Systems (ABS), коли в результаті атаки шкідливого ransomware Avaddon стався витік корпоративних даних розміром в 50 Гб. Цей витік охоплює файли з кредитними документами, діловими контрактами, електронним листуванням, облікові дані для загальних мережевих ресурсів і іншу конфіденційну інформацію [38]. Показово, що велика частина цих даних зберігалася у відкритій формі.

Основні рекомендації щодо захисту даних

На основі аналізу рекомендацій Національного інституту стандартів і технологій США – SP 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" [39] та інших праць (наприклад: [40, 41, 10]) були вироблені наступні додаткові рекомендації щодо захисту персональних даних в інформаційних системах "розумних міст".

Персональні дані не тільки повинні бути захищені надійними криптографічними і технічними засобами, а й там, де це допускають робочі завдання, специфічно або частково знеособлені. Наприклад, виходячи з рекомендацій [39] можна використовувати такі методи:

• Генералізація й узагальнення даних, що зберігаються, наприклад, зберігання результатів розрахунку, а не повної групи даних, за якими виконувався цей розрахунок;

• Придушення даних – пряме видалення записів або групи записів (після виконання необхідних дій);

• Додавання шуму і перешкод в дані – додавання невеликих порцій шуму або випадкових варіативних змін в обрані дані (наприклад, зашумлення чутливих для деанонімізації даних про геопозиції);

• Усереднення даних по вибірці – після аналізу по групі часто можна замінити всі її значення на середнє;

• Перестановки та роздільне зберігання даних, наприклад, зберігання адрес і користувачів в різних, але зв'язаних таблицях в різних частинах системи. Таким чином, якщо буде зламаний захист однієї з підсистем, отримані зловмисником дані все одно не будуть представляти небезпеки.

Хорошим прикладом системи роздільного зберігання даних є роздільне зберігання біометричних даних (фотографії і записи голосу) з прив'язкою користувача по цифровому ідентифікатору до його профілю в базі даних. Таким чином, при зломі бази даних із зразками голосів і фотографіями, зловмисник не отримає доступ до персональних даних, що зберігаються в базі людей (тільки до їх ідентифікаторів), а при зломі бази даних з персональними даними – отримає доступ до персональних даних, але не до зразків голосів і фотографій.

Так само на основі аналізу рекомендацій [39] можна рекомендувати список можливих рекомендацій щодо захисту персональних даних:

• обов'язкове використання систем розмежування ролей і прав доступу;

• в рамках таких систем – поділ привілеїв і обов'язків доступу до даних;

• принцип найменших привілеїв: доступ до даних, які є сторонніми щодо виконуваних обов'язків, повинен бути суворо обмежений;

• модель поділу доступу і прав (і найменших привілеїв) повинна поширюватися і на суміжні служби, з якими здійснюється співпраця;

• поширення принципу ролей і прав не тільки на основну інформаційну систему, а й на мобільні пристрої (ноутбуки, планшети, мобільні телефони), що використовуються співробітниками для віддаленої роботи. Інформація не повинна залишатися відкритою, і тим більше до неї не повинен отримати доступ потенційний викрадач службового пристрою;

• захист або блокування віддаленого доступу – в залежності від цільової установки використання даних, що зберігаються;

• система повинна збирати інформацію, що дозволяє проводити аудит подій, пов'язаних з персональними даними (наприклад, спроба несанкціонованого доступу до даних, спроба підбору пароля і т.д.);

• всі користувачі системи повинні однозначно ідентифікуватися, їх дії повинні зберігатися для аудиту;

• апаратне забезпечення для накопичення, зберігання, транспортування та обробки даних і схеми його використання також має проходити тестування на можливі витоки даних (наприклад, дані не повинні зберігатися на жорстких дисках в незашифрованому вигляді);

• повинна бути передбачена система виявлення та оповіщення про витоки персональних даних, оскільки тільки своєчасним оповіщенням можна досягти мінімізації шкоди від деанонімізації.

Висновки

Розглянуті вище факти та виведені з них схеми деанонімізації можна підсумувати наступним чином. Деанонімізація є послідовним процесом зламу, а доксінг – зламу і публікації приватної інформації. Така інформація може бути отримана шляхом збору та аналізу відкритих ("білих"), викрадених ("чорних") і викрадених третіми особами, але таких, що знаходяться в умовно-вільному доступі ("сірих") джерел інформації. З розвитком інфраструктури "розумних міст" буде рости кількість інформації, що збирається, зберігається і обробляється. Це призведе до збільшення "цифрових слідів" кожного користувача інформаційних систем, тобто практично кожного, хто проживає в місті.

Заходи щодо захисту від деанонімізації повинні бути спрямовані на максимальне ослаблення кожної з можливих ланок ланцюжка деанонімізації. Якщо розглядати загальну схему доксінгу (вибір мети – отримання даних – публікація даних), то основною ланкою впливу в контексті кібербезпеки "розумного міста" буде захист приватних персональних даних, що зберігаються в інформаційній системі. Наведені в статті рекомендації дозволять значно знизити ризик доступу до персональних даних третіх осіб і дозволять знизити можливі збитки від деанонімізації й доксінгу.

Література

1. Deakin M., Waer H.A. From intelligent to smart cities // Intelligent Buildings International. — Taylor & Francis, 2011. — Vol. 3, no. 3. — P. 140–152.

2. Caird S.P., Hallett S.H. Towards evaluation design for smart city development // Journal of Urban Design. — Routledge, 2019. — Vol. 24, no. 2. — P. 188–209.

3. Yigitcanlar T. Smart cities: An effective urban development and management model? // Australian Planner. — Routledge, 2015. — Vol. 52, no. 1. — P. 27–34.

4. Bastidas V., Helfert M., Bezbradica M.A Requirements framework for the design of smart city reference architectures / Proceedings of the 51st hawaii international conference on system sciences. — 2018. https://pdfs.semanticscholar.org/b01d/7901f131540cf7f0d03041a03f5e2f8589a8.pdf

5. Boyko V., Vasilenko N. Smart city in the context of cybersecurity: Incidents, risks, threats // Municipal economy of cities. — 2020. — Vol. 4, no. 157. — P. 184–191.

6. Cross M. Social media security: Leveraging social networking while mitigating risk. — Newnes, 2013, 346 p.

7. Study Shows Risks of Information Leaks in Financial Institutions. — https://www.bankinfosecurity.com/study-shows-risks-information-leaks-in-financial-institutions-a-484, 2020.

8. Dox | definition of dox by merriam-webster. — https://www.merriam-webster.com/dictionary/dox, 2020.

9. Boardman M. (2019). Doxing: An increased (and increasing) privacy risk. https://blogs.ischool.berkeley.edu/w231/2019/02/26/doxing-an-increased-and-increasing-privacy-risk/.

10. Peters F., Hanvey S., Veluru S., Mady A.E., Boubekeur M., Nuseibeh B. Generating privacy zones in smart cities / 2018 ieee international smart cities conference (isc2). — 2018. — P. 1–8.

11. Chang L.Y., Zhu J. Taking justice into their own hands: Predictors of netilantism among cyber citizens in hong kong // Frontiers in Psychology. — Frontiers Media SA, 2020. — Vol. 11. — P. 1–8.

12. Coleman G. Anonymous in context: The politics and power behind the mask. — 2013. No 3. https://www.cigionline.org/sites/default/files/no3_8.pdf.

13. Kerk I. van de. Data use versus privacy protection in public safety in smart cities: Master's thesis. — 2015. https://dspace.library.uu.nl/handle/1874/318131

14. Rebollo-Monedero D., Bartoli A., Hernández-Serrano J., Forné J., Soriano M. Reconciling privacy and efficient utility management in smart cities // Transactions on Emerging Telecommunications Technologies. — Wiley Online Library, 2014. — Vol. 25, no. 1. — P. 94–108.

15. Popescul D., Genete L.-D. Data security in smart cities: Challenges and solutions // Informatica Economică. — 2016. — Vol. 20, no. 1. — P. 29–39.

16. Howard P.N., Gulyas O. Data breaches in europe: Reported breaches of compromised personal records in europe, 2005-2014 // Available at SSRN 2554352. — 2014, 22 p.

17. Nicola C. Almost 700 doxxing cases reported since june, majority directed at hong kong police. — https://www.scmp.com/yp/discover/news/hong-kong/article/3066122/almost-700-doxxing-cases-reported-june-majority-directed, 2020.

18. 32-year-old male technician sentenced to 2 years in prison for doxxing – dimsum daily. — https://www.dimsumdaily.hk/32-year-old-male-technician-sentenced-to-2-years-in-prison-for-doxxing/, 2020.

19. Wheatley S., Maillart T., Sornette D. The extreme risk of personal data breaches and the erosion of privacy // The European Physical Journal B. — Springer, 2016. — Vol. 89, no. 1. — P. 1–12.

20. Eling M., Wirfs J. What are the actual costs of cyber risk events? // European Journal of Operational Research. — 2019. — Vol. 272, no. 3. — P. 1109–1119.

21. Qian J., Li X.-Y., Zhang C., Chen L. De-anonymizing social networks and inferring private attributes using knowledge graphs / IEEE infocom 2016-the 35th annual ieee international conference on computer communications. — IEEE, 2016. — P. 1–9.

22. Alasdair A., Pete W. Got an iPhone or 3G iPad? Apple is recording your moves – o'Reilly radar. — http://radar.oreilly.com/2011/04/apple-location-tracking.html, 2020.

23. Abalenkovs D., Bondarenko P., Pathapati V.K., Nordbø A., Piatkivskyi D., Rekdal J.E., Ruthven P.B. Mobile forensics: Comparison of extraction and analyzing methods of ios and android // Gjovik University College, Gjovik, Norway. — 2012. https://www.semanticscholar.org/paper/Mobile-Forensics-%3A-Comparison-of-extraction-and-of-Abalenkovs-Bondarenko/ed402e51fdc47b5459ec804f6bdbeb05cd75d96e.

24. Beltramelli T., Risi S. Deep-spying: Spying using smartwatch and deep learning // CoRR. — 2015. — Vol. abs/1512.05616. https://www.researchgate.net/publication/287249444_Deep-Spying_Spying_using_Smartwatch_and_Deep_Learning/link/572ceb7008aee02297598033/download.

25. Souza A., Pereira J., Batista T., Cavalcante E., Cacho N., Lopes F., Almeida A. A geographic-layered data middleware for smart cities / Proceedings of the 24th brazilian symposium on multimedia and the web. — 2018. — P. 411–414.

26. Mazhelis O., Hämäläinen A., Asp T., Tyrväinen P. Towards enabling privacy preserving smart city apps / 2016 ieee international smart cities conference (isc2). — 2016. — P. 1–7.

27. Strava data heat maps expose military base locations around the world. — https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/, 2020.

28. Strava suggests military users 'opt out' of heatmap as row deepens | technology. — https://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban, 2020.

29. Why was it so easy for hackers to take down the internet – cnet. — https://www.cnet.com/how-to/ddos-iot-connected-devices-easily-hacked-internet-outage-webcam-dvr/, 2020.

30. Lizard Squad hacked thousands of cameras to attack websites — https://www.engadget.com/2016-07-03-lizard-squad-creates-botnet-from-thousands-of-cameras.html, 2020

31. Peeping into 73,000 unsecured security cameras via default passwords | cso online. — https://www.csoonline.com/article/2844283/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html, 2020.

32. Marketer of internet-connected home security video cameras settles ftc charges it failed to protect consumers' privacy | federal trade commission. — https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles, 2020.

33. Beckers K. Comparing privacy requirements engineering approaches / 2012 seventh international conference on availability, reliability and security. — 2012. — P. 574–581.

34. Spiekermann S., Cranor L. F. Engineering privacy // IEEE Transactions on Software Engineering. — 2009. — Vol. 35, no. 1. — P. 67–82.

35. Yang M., Yu Y., Bandara A.K., Nuseibeh B. Adaptive sharing for online social networks: A trade-off between privacy risk and social benefit / 2014 ieee 13th international conference on trust, security and privacy in computing and communications. — 2014. — P. 45–52.

36. Ye X., Zhu Z. Privacy compliance engineering process / 2009 second international symposium on electronic commerce and security. — 2009. — Vol. 1. — P. 255–259.

37. El Masri A.A., Sousa J.P. Limiting private data exposure in online transactions: A user-based online privacy assurance model / 2009 international conference on computational science and engineering. — 2009. — Vol. 3. — P. 438–443.

38. American bank systems hit by ransomware attack, full 53 gb data dump leaked – security report. — https://securityreport.com/american-bank-systems-hit-by-ransomware-attack-full-53-gb-data-dump-leaked/ , 2020.

39. McCallister E., Grance T., Scarfone K.A. Sp 800-122. Guide to protecting the confidentiality of personally identifiable information (pii). — National Institute of Standards & Technology, 2010. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

40. Jutla D.N., Bodorik P. PAUSE: A privacy architecture for heterogeneous big data environments / 2015 ieee international conference on big data (big data). — 2015. — P. 1919–1928.

41. Solomon M.G., Sunderam V., Xiong L., Li M. Enabling mutually private location proximity services in smart cities: A comparative assessment / 2016 ieee international smart cities conference (isc2). — 2016. — P. 1–8.

References

1. Deakin M., Waer H.A. (2011). From intelligent to smart cities. *Intelligent Buildings International*. — Taylor & Francis, Vol. 3, no. 3. P. 140–152.

2. Caird S.P., Hallett S.H. (2019). Towards evaluation design for smart city development. *Journal of Urban Design*. — Routledge, Vol. 24, no. 2. P. 188–209.

3. Yigitcanlar T. (2015). Smart cities: An effective urban development and management model?. *Australian Planner*. — Routledge, Vol. 52, no. 1. P. 27–34.

4. Bastidas V., Helfert M., Bezbradica M. (2018). A requirements framework for the design of smart city reference architectures. Proceedings of the 51st hawaii international conference on system sciences. Retrieved from https://pdfs.semanticscholar.org/b01d/7901f131540cf7f0d03041a03f5e2f8589a8.pdf

5. Boyko V., Vasilenko N. (2020). Smart city in the context of cybersecurity: Incidents, risks, threats. *Municipal economy of cities*. Vol. 4, no. 157. 184–191.

6. Cross M. (2013). Social media security: Leveraging social networking while mitigating risk. — *Newnes*, 346.

7. Pahwa N. Individuals' rights at risk in the digital age. *Digital Debates*. — P. 12.

8. Dox | definition of dox by merriam-webster (2020). Retrieved from https://www.merriam-webster.com/dictionary/dox.

9. Boardman M. (2019). Doxing: An increased (and increasing) privacy risk. Retrieved from https://blogs.ischool.berkeley.edu/w231/2019/02/26/doxing-an-increased-and-increasing-privacy-risk/.

10. Peters F., Hanvey S., Veluru S., Mady A. E., Boubekeur M., Nuseibeh B. (2018). Generating privacy zones in smart cities. 2018 ieee international smart cities conference (isc2). 1–8.

11. Chang L. Y., Zhu J. (2020). Taking justice into their own hands: Predictors of netilantism among cyber citizens in hong kong. *Frontiers in Psychology*. — Frontiers Media SA, Vol. 11. 1–8.

12. Coleman G. (2013). Anonymous in context: The politics and power behind the mask. No 3. Retrieved from https://www.cigionline.org/sites/default/files/no3_8.pdf

13. Kerk I. van de. (2015). Data use versus privacy protection in public safety in smart cities: Master's thesis.

Retrieved from https://dspace.library.uu.nl/handle/1874/318131

14. Rebollo-Monedero D., Bartoli A., Hernández-Serrano J., Forné J., Soriano M. (2014). Reconciling privacy and efficient utility management in smart cities // Transactions on Emerging Telecommunications Technologies. — Wiley Online Library, Vol. 25, no. 1. 94–108.

15. Popescul D., Genete L.-D. (2016). Data security in smart cities: Challenges and solutions. *Informatica Economică*. Vol. 20, no. 1. 29–39.

16. Howard P.N., Gulyas O. (2014). Data breaches in europe: Reported breaches of compromised personal records in europe, 2005-2014 // Available at SSRN 2554352. 22.

17. Nicola C. Almost 700 doxxing cases reported since june, majority directed at hong kong police (2020). Retrieved from https://www.scmp.com/yp/discover/news/hong-kong/article/3066122/almost-700-doxxing-cases-reported-june-majority-directed.

18. 32-year-old male technician sentenced to 2 years in prison for doxxing - dimsum daily (2020). Retrieved from https://www.dimsumdaily.hk/32-year-old-male-technician-sentenced-to-2-years-in-prison-for-doxxing/.

19. Wheatley S., Maillart T., Sornette D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B. — Springer*, Vol. 89, no. 1. 1–12.

20. Eling M., Wirfs J. (2019). What are the actual costs of cyber risk events?. *European Journal of Operational Research*. Vol. 272, no. 3. 1109–1119.

21. Qian J., Li X.-Y., Zhang C., Chen L. (2016). De-anonymizing social networks and inferring private attributes using knowledge graphs. IEEE infocom 2016-the 35th annual ieee international conference on computer communications. — IEEE, 1–9.

22. Alasdair A., Pete W. (2020). Got an iPhone or 3G iPad? Apple is recording your moves - o'Reilly radar. Retrieved from http://radar.oreilly.com/2011/04/apple-location-tracking.html.

23. Abalenkovs D., Bondarenko P., Pathapati V. K., Nordbø A., Piatkivskyi D., Rekdal J. E., Ruthven P. B. (2012). Mobile forensics: Comparison of extraction and analyzing methods of ios and android // Gjovik University College, Gjovik, Norway. Retrieved from https://www.semanticscholar.org/paper/Mobile-Forensics-%3A-Comparison-of-extraction-and-of-Abalenkovs-Bondarenko/ed402e51fdc47b5459ec804f6bdbeb05cd75d96e.

24. Beltramelli T., Risi S. (2015). Deep-spying: Spying using smartwatch and deep learning // CoRR. Vol. abs/1512.05616. Retrieved from https://www.researchgate.net/publication/287249444_Deep-Spying_Spying_using_Smartwatch_and_Deep_Learning/link/572ceb7008aee02297598033/download

25. Souza A., Pereira J., Batista T., Cavalcante E., Cacho N., Lopes F., Almeida A. (2018). A geographic-layered data middleware for smart cities. Proceedings of the 24th brazilian symposium on multimedia and the web. 411–414.

26. Mazhelis O., Hämäläinen A., Asp T., Tyrväinen P. (2016). Towards enabling privacy preserving smart city apps. 2016 ieee international smart cities conference (isc2). 1–7.

27. Strava data heat maps expose military base locations around the world (2020). Retrieved from https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

28. Strava suggests military users 'opt out' of heatmap as row deepens | technology (2020). — https://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban.

29. Why was it so easy for hackers to take down the internet – cnet (2020). — https://www.cnet.com/how-to/ddos-iot-connected-devices-easily-hacked-internet-outage-webcam-dvr/.

30. Lagnese N., Lacey Henning E. B., Kimball T., Reagan B. Lizard squad. — 2018.

31. Peeping into 73,000 unsecured security cameras via default passwords | cso online (2020). Retrieved from https://www.csoonline.com/article/2844283/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html.

32. Marketer of internet-connected home security video cameras settles ftc charges it failed to protect consumers' privacy | federal trade commission (2020). Retrieved from https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

33. Beckers K. (2012). Comparing privacy requirements engineering approaches. 2012 seventh international conference on availability, reliability and security. 574–581.

34. Spiekermann S., Cranor L.F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering*. Vol. 35, no. 1. 67–82.

35. Yang M., Yu Y., Bandara A. K., Nuseibeh B. (2014). Adaptive sharing for online social networks: A trade-off between privacy risk and social benefit. 2014 ieee 13th international conference on trust, security and privacy in computing and communications. P. 45–52.

36. Ye X., Zhu Z. (2009). Privacy compliance engineering process. 2009 second international symposium on electronic commerce and security. Vol. 1. 255–259.

37. El Masri A.A., Sousa J.P. (2009). Limiting private data exposure in online transactions: A user-based online privacy assurance model. 2009 international conference on computational science and engineering. Vol. 3. 438–443.

38. American bank systems hit by ransomware attack, full 53 gb data dump leaked - security report (2020). Retrieved from https://securityreport.com/american-bank-systems-hit-by-ransomware-attack-full-53-gb-data-dump-leaked/.

39. McCallister E., Grance T., Scarfone K.A. (2010). Sp 800-122. Guide to protecting the confidentiality of personally identifiable information (pii). — National Institute of Standards & Technology, Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

40. Jutla D.N., Bodorik P. (2015). PAUSE: A privacy architecture for heterogeneous big data environments. 2015 ieee international conference on big data (big data). 1919–1928.

41. Solomon M.G., Sunderam V., Xiong L., Li M. (2016). Enabling mutually private location proximity services in smart cities: A comparative assessment. 2016 ieee international smart cities conference (isc2). 1–8.

Рецензент: д-р техн. наук, проф. В.М. Тупкало, Інститут інтелектуальної власності та права Національного Університету "Одеська юридична академія", Україна

Автор: БОЙКО Віктор Дмитрович
кандитат технічних наук, доцент кафедри кібербезпеки, Національний університет «Одеська юридична академія»
E-mail – boyko-work@ukr.net
ID ORCID: https://orcid.org/0000-0001-5929-657X

Автор: ВАСИЛЕНКО Микола Дмитрович
доктор фізико-математичних наук, доктор юридичних наук, професор, завідувач кафедри кібербезпеки, Національний університет «Одеська юридична академія»
E-mail – nvas08@ukr.net
ID ORCID: http://orcid.org/0000-0002-8555-5712

CYBERSECURITY OF "SMART CITIES": SOCIAL ASPECTS, RISKS OF DEANONYMIZATION AND DOXING

V. Boyko, M. Vasilenko
National University "Odessa Law Academy", Ukraine

The paper analyzes possible risks and threats posed by the transition from modern cities to smart cities. The concept and scheme of doxing implementation are analyzed. Moreover, the essence of deanonymization is revealed and threats to the privacy and security of smart city residents associated with these processes are identified. Furthermore, the reasons for the growth of doxing practice are clarified. The social aspect of the cybersecurity of a smart city is seen primarily in the increased risks of privacy disclosure, which can lead to deanonymization, which can later be used for doxing, cyberbullying, blackmail or social engineering schemes. This demands that personal data must not only be protected by reliable cryptographic and technical measures but also - where it allows by work tasks - be specifically or partially impersonalised. Also, when planning personal data protection in smart city informational ecosystems, it should be considered that such protection will be existing in the context of an overall eco-information system of the city. Therefore, the one's always set priorities balanced between data protection, identify threats, measures and mechanisms for their implementation and daily routine tasks of system administration. The article analyzes cases and schemes of deanonymization, shows the vulnerability of modern information and communication systems to obtain data that can be used by an attacker. Based on the analysis and taking into account the specifics of the functioning of information ecosystems of smart cities, the main recommendations for protecting data stored in information systems are developed and systematized, which will reduce the risks of hacking such data and minimize harm from deanonymization and doxing. Finally, the authors proved that deanonymization is a sequential hacking process, and doxing is a hacking process and publishing private information. Such information can be obtained by collecting and analyzing open ("white"), stolen ("black") and stolen by third parties, but conditionally freely available ("Gray") sources of information. With the development of the smart city infrastructure, the amount of information collected, stored and processed will grow. This will lead to an increase in the "digital footprint" of every user of information system, that is, almost everyone who lives in the city.

Keywords: *smart city, deanonymization, doxing, personal data, cybersecurity, risks.*