© Fedynyshyn T., Mykhaylova O., Opirskyy I. Method to Detect Suspicious Individuals through Mobile Device Data// Ukrainian Scientific Journal of Information Security, 2023, vol. 29, issue 3, pp. 154-161. ©

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ОБЛАДНАННЯ / SOFTWARE & HARDWARE ARCHITECTURE SECURITY

DOI: 10.18372/2225-5036.29.18075

МЕТОД ВИЗНАЧЕННЯ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ОСІБ ПО ДАНИХ BLUETOOTH

Тарас Фединишин, Ольга Михайлова, Іван Опірський

Національний університет «Львівська політехніка»

ФЕДИНИШИН Тарас Олегович, аспірант
Рік та місце народження: 1989 рік, м. Червоноград, Львівська обл., Україна.
Освіта: Київський національний університет імені Тараса Шевченка, 2013 рік.
Посада: аспірант кафедри захисту інформації, з 2023 року.
Наукові інтереси: Мобільні та веб технології і їх безпека, інформаційна безпека держави, безпровідні технології та їх захист.
E-mail: fedynyshyn.taras@gmail.com.
Orcid ID: 0009-0006-8233-8057.

МИХАЙЛОВА Ольга Олександрівна, к.ф-м.н., доц.
Рік та місце народження: 1992 рік, м. Львів, Україна.
Освіта: Львівський національний університет імені Івана Франка, 2014 рік.
Посада: доцент кафедри захисту інформації з 2021 року..
Наукові інтереси: методи і засоби технічного захисту інформації, безпека програмного забезпечення, безпека інфраструктури комп'ютерних мереж, математичні методи та моделі захисту інформації, БПЛА.
Публікації: більше 10 публікацій, серед яких наукові статті, монографія.
E-mail: olha.o.mykhailova@lpnu.ua.
Orcid ID: 0000-0002-3086-3160.

ОПІРСЬКИЙ Іван Романович, д.т.н., проф.
Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: завідувач кафедри захисту інформації з 2023 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання.
Публікації: : більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

Анотація. *Розумні мобільні пристрої сьогодні використовуються все частіше, що робить їх справжньою знахідкою для слідчих. Відповідне обладнання та методи інспекції можуть допомогти виявити та відновити велику кількість прихованої інформації на цих пристроях. Apple iPhone використовується великою кількістю людей по всьому світу завдяки своїм функціям та характеристикам. iPhone використовують багато різних типів людей, включаючи студентів, вчителів, бізнесменів та людей інших професій. В даній статті вводи-*

ться концепція потенційно небезпечної особи, описуються особливості врахування контексту при класифікації особи як потенційно небезпечної, описуються фактори, які можуть впливати на процес класифікації. Пропонується діаграма, яка описує процес класифікації особи на потенційну небезпечність. Розглядаються базові методи криміналістики мобільних пристроїв та показуються результати практичного дослідження. Аналізуються дані, виявлені в результаті криміналістичного дослідження мобільного пристрою на базі операційної системи iOS. Пропонується метод класифікації потенційно небезпечних осіб на основі Bluetooth-даних мобільного пристрою. Представляється псевдокод який описує алгоритм роботи запропонованого методу. Пропонуються додаткові джерела даних для покращення методу, а саме використання інформації про збережені Wi-Fi мережі до яких підключався пристрій та GPS координати збережені під час роботи системних застосунків операційної системи iOS. Підкреслюється необхідність практичної реалізації запропонованого методу та необхідність його апробації.

***Ключові слова**: цифрова криміналістика мобільних пристроїв, iOS, методи класифікації потенційно небезпечних осіб, Bluetooth.*

Постановка проблеми

У сучасному світі використання мобільних пристроїв є широко поширеним явищем. Середньостатистична людина використовує смартфон приблизно 4 години на день [1]. Мобільний пристрій завжди залишається в нашій кишені, де б ми не були. Навіть коли ми не використовуємо пристрій активно, цілий набір комунікаційних технологій, таких як SMS, 3G, LTE, Wi-Fi, GPS, Bluetooth та інші, все ще працює на ньому. Кожна служба, яка використовує ці технології, залишає певну кількість даних про свою роботу. Навіть якщо певна служба вимкнена, це не гарантує, що дані не будуть накопичуватися, оскільки, наприклад, в операційній системі iOS служби Bluetooth та Wi-Fi, за замовчуванням, налаштовані на автоматичне увімкнення через деякий час [2]. Накопичені дані не завжди доступні користувачеві, часто вони є прихованими і можуть бути отримані лише за допомогою спеціальних інструментів. Таким чином, більшість користувачів не замислюються про те, скільки і як детально та чутливо дані зберігаються на їхніх пристроях. Водночас ці дані можуть бути використані у спробах ідентифікації потенційно небезпечних осіб у криміналістичних розслідуваннях.

Аналіз останніх досліджень і публікацій

Концепція "потенційно небезпечної особи" у контексті безпеки, правоохоронної діяльності та криміналістики є багатогранною і може варіюватися залежно від ситуації та точки зору спостерігача. Загалом, так можна охарактеризувати особу, яка, як вважається, демонструє поведінку, характеристики або діяльність, що виходять за рамки звичайного і можуть вказувати на потенційну загрозу або участь у злочинних чи шкідливих діях. Однак, визначення того, що робить особу "потенційно небезпечною", є суб'єктивним і на нього можуть впливати різні фактори:

- особливості поведінки: певні особливості поведінки можуть вважатися підозрілими у конкретних контекстах. Наприклад, особа, яка безцільно перебуває у забороненій зоні [3], проявляє незвичайний інтерес до заходів безпеки, або намагається уникнути виявлення, може викликати підозру;
- контекст та оточення: контекст відіграє вирішальну роль у визначенні підозрілості. Поведінка, яка є нормальною в одному середовищі, може вважатися підозрілою в іншому. Наприклад, носіння рюкзака є звичайним у університетському середовищі, але може розглядатися з підозрою у зоні високої безпеки;
- історичні дані: якщо особа має історію кримінальної діяльності або відомо, що вона асоціюється зі злочинцями, вона може вважатися підозрілою у певних розслідуваннях або сценаріях [4];
- аномалії у комунікаціях або транзакціях: у цифровій криміналістиці та кібербезпеці, відхилення від норми, такі як незвичайні фінансові транзакції, шифровані комунікації у несекретному контексті, або нерегулярні маршрути подорожей, можуть вказувати на підозрілість особи [5];
- візуальні ознаки: певні фізичні особливості також можуть вважатися підозрілими, наприклад, носіння теплого одягу в теплу погоду (що може вказувати на приховування чогось), нервова поведінка, або уникнення зорового контакту на контрольно-пропускному пункті;
- аналіз даних: у цифрову епоху інструменти аналізу даних можуть виявляти шаблони, які вказують на підозрілу поведінку. Це може включати аналіз активності в соціальних мережах, фінансових транзакцій або шаблонів комунікації [6];
- моделі оцінки ризиків: у сфері безпеки та протидії тероризму використовуються моделі оцінки ризиків для оцінки рівня загрози, яку може становити особа, на основі різних факторів, включаючи деякі з вищезазначених [7].

Мета та постановка завдання

Важливо зазначити, що помітка "потенційно небезпечна" не обов'язково означає, що особа в чомусь винна або залучена до незаконної діяльності. Це попередня оцінка, яка вимагає подальшого спостереження або розслідування. Концепція сильно залежить від контексту, і потребує відповідального застосування для уникнення упередженості та забезпечення використання об'єктивних та обґрунтованих критеріїв.

Виклад основного матеріалу дослідження

Концепція потенційно небезпечної особи

Схематична ілюстрація процесу класифікації особи відповідно концепції у вигляді діаграми перед-

бачає врахування різних факторів та процесів, які призводять до класифікації когось як підозрілого. Нижче зображено один з можливих методів (рис. 1).

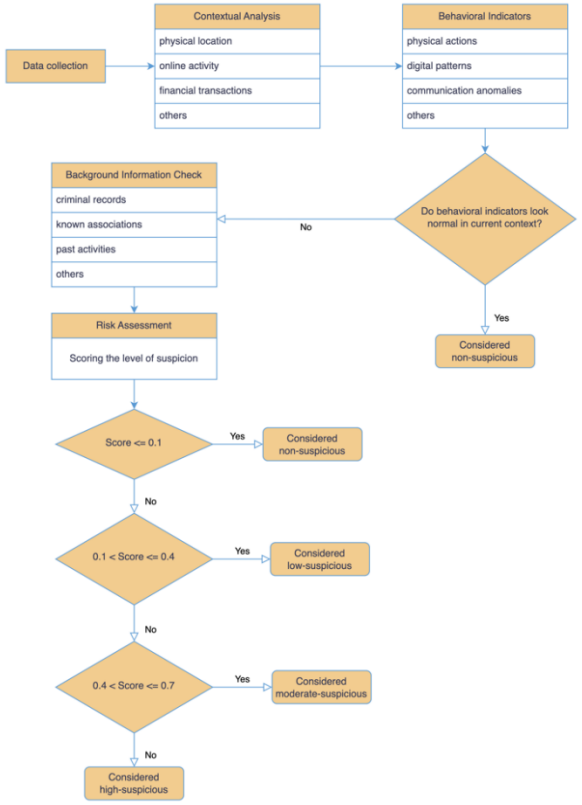

Рис. 1. Блок-схема методу класифікації потенційно небезпечної особи

Концепція "потенційно небезпечної особи" є по своїй суті складною, оскільки вона значною мірою залежить від суб'єктивних інтерпретацій поведінки, які можуть значно відрізнятися серед різних спостерігачів та культур. Вона залежить від контексту, оскільки дії, які вважаються підозрілими в одному середовищі (наприклад, безцільне перебування у захищеній зоні), можуть бути абсолютно нормальними в іншому (наприклад, безцільне перебування в парку).

Ця складність ще більше посилюється необхідністю збалансувати питання безпеки з етичними та юридичними міркуваннями, забезпечуючи щоб судження про підозрілість не призводили до порушень прав особи.

Цифрова криміналістика мобільних пристроїв

Цифрова криміналістика мобільних пристроїв – процес відновлення цифрових доказів з мобільного пристрою в умовах, що відповідають криміналістичним стандартам. Зазвичай цифрова криміналістика складається з декількох ключових етапів. Ці етапи розроблені для забезпечення цілісності та надійності зібраних доказів. Загальні етапи процесу криміналістики мобільних пристроїв включають [8]:

- вилучення пристрою: перший крок включає в себе отримання доступу мобільного пристрою в законний спосіб, так, щоб гарантувати, що він не може бути віддалено очищений або змінений. Це часто вимагає забезпечення ізоляції пристрою від будь-яких мережевих з'єднань;
- екстракція даних: цей етап включає в себе вилучення даних з пристрою. Існують різні методи отримання даних, включаючи фізичний, логічний, вилучення файлової системи та вилучення з хмарного сховища. Обраний метод часто залежить від моделі пристрою, операційної системи та типу необхідних даних;
- аналіз: на цьому етапі вилучені дані обстежуються та аналізуються. Це включає використання різних криміналістичних інструментів та технік для відновлення видалених файлів та зашифрованих даних, а також аналізу журналів дзвінків, повідомлень, електронних листів, зображень та інших відповідних даних, збережених на пристрої.

Перший етап (вилучення пристрою) виходить за рамки цього дослідження, так само як і опрацювання пристроїв які працюють на операційній системі Android.

Операційна система iOS, відома своєю надійною безпекою [9] та закритим середовищем, використовується на різних пристроях, включаючи iPhone, iPad та iPod. Вона обмежує встановлення лише тими додатками, які схвалені Apple і доступні в App Store. Це обмеження може ускладнювати підтримку цифрової ідентифікації та використання деяких програмних інструментів. Крім того, пристрої iOS повністю залежать від внутрішньої пам'яті, оскільки вони не підтримують зовнішні картки пам'яті. Це робить вилучення даних залежним виключно від внутрішньої пам'яті, ускладнюючи процес екстракції даних [17]. Внутрішня пам'ять у пристроях iOS поділена на дві частини. Системний розділ містить операційну систему та стандартні програми Apple, захищені від змін шляхом встановлення для цього розділу режиму читання. Це забезпечує цілісність операційної системи. Інший розділ, призначений для даних користувача, зберігає інформацію, таку як дані додатків, профілі користувачів, фотографії, відео, текстові повідомлення та контакти. Цей розділ є важливим для криміналістичних розслідувань. У цифровій криміналістиці вилучення даних з пристроїв iOS підрозділяється на три основні категорії: ручне, логічне та фізичне вилучення. Кожен тип має свої особливості та методології, які є важливими для ефективного аналізу в цифровій криміналістиці.

Ручне вилучення зазвичай включає безпосередню взаємодію з пристроєм, що перевіряється, включаючи навігацію по його файловій системі та внутрішній пам'яті. Цей процес відображає дані на екрані пристрою через операції в реальному часі, дозволяючи слідчим робити висновки про те, яка інформація

зберігається в пристрої. Цифрові докази, зібрані таким чином, часто представляють собою знімки екрану пристрою. Відповідно, дані, які були видалені і більше не відображаються на екрані пристрою, не можуть бути відновлені через ручне вилучення.

Логічна екстракція даних базується на логічній структурі операційної системи, включаючи вилучення даних, пов'язаних з директоріями та індексами читаючи файли у вигляді потоку біт за бітом. У цьому процесі, якщо файл або дані видалені, їх відповідний індекс у директорії також видаляється.В результаті логічне вилучення не може відновити видалені файли або дані. Для пристроїв iOS, які зазвичай не піддаються джейлбрейкінгу, використовується метод логічного резервного копіювання для дослідження записів програм миттєвого обміну повідомленнями. Чітка логічна структура операційних систем у мобільних пристроях допомагає криміналістичному програмному забезпеченню організовувати цю структуру для вилучення даних. Відповідно, криміналістичне програмне забезпечення, як правило, більш ефективне у підтримці логічного вилучення.

Фізичне вилучення даних включає створення точної копії всієї фізичної пам'яті пристрою біт за бітом. Основна перевага цього методу полягає в здатності зберегти всі цифрові докази у фізичній пам'яті, включаючи дані, які були видалені. Криміналістичні програмні інструменти можуть отримати доступ до цих даних і потенційно відновити їх до їхнього первісного стану в пристрої. Однак, реалізація фізичного вилучення є більш складною. Вона вимагає встановлення спеціалізованого криміналістичного програмного забезпечення на системний розділ. Крім того, для створення повного образу розділу даних користувача, необхідно запустити криміналістичний інструмент. Оскільки ці криміналістичні інструменти не є сертифікованими додатками Apple, їх встановлення та робота, як правило, вимагають використання програми Jailbreak для отримання повного контролю над пристроєм iOS. У рамках цього дослідження автори використовували програмне забезпечення iMazing [10] для виконання логічного вилучення сирих файлів iPhone 13 mini з iOS 17.1.1.

Під час етапу обстеження та аналізу автори знайшли базу даних SQLite [11] під назвою com.apple.MobileBluetooth.ledevices.other.db, розташовану в директорії SysSharedContainerDomain-systemgroup.com.apple.bluetooth/Library/Database. База даних містить таблиці: "CustomProperties", "OtherDevices" та "_SqliteDatabaseProperties". Таблиця "OtherDevices" містить в собі пристрої, які були в зоні дії радіосигналу по протоколу Bluetooth, але до яких не було виконано підключення [12]. Рисунок ілюструє дані, виявлені в таблиці "OtherDevices" (рис. 2).

Таблиця містить понад 6000 записів, що може означати, що вона дійсно зберігає інформацію про пристрої Bluetooth, які були в межах досяжності, але не були підключені. Найцікавішими колонками таблиці є: "Uuid", "Address" та "LastSeenTime". Це спостереження спонукало авторів розробити новий метод для ідентифікації потенційно небезпечних осіб на основі даних з цієї таблиці та інших джерел.

Uuid	Name	NameOrigin	Address	ResolvedAddress	LastSeenTime	LastConnectionTime	GATTServiceChangeConfig	Tags
126E72C0-2AC9-386F-BED6-1CF0EC4F6CB9		0	Random EA:F3:5D:1A:EC:63	NULL	398367...	136473	0	NULL
127B37F7-FBE7-18FB-DC13-2F4083724FB5		0	Random CF:14:74:72:1D:BA	NULL	39125813	133752	0	NULL
12824579-AC5A-F398-020E-C5C98EA1E534		0	Random DF:B4:90:3C:EC:FB	NULL	46211775	152415	0	NULL
12912B9F-4096-90E9-9CCE-4787A1623AB2		0	Random DD:7C:6B:4C:3B:40	NULL	491724...	165601	0	NULL
12AF97D3-82D5-1154-B9DB-F0C0EC916F5D		0	Random ED:EC:A9:BD:5B:96	NULL	500874...	0	0	NULL
12B09987-025C-5266-F3F8-AC064EBA144A		0	Random DB:17:47:1B:B9:4E	NULL	423226...	143287	0	NULL
12C2E7F8-91B2-71A7-EB1B-067573FED8D4		0	Random D0:A4:47:97:27:D5	NULL	469748...	154911	0	NULL
12C857A0-238A-FCB9-951F-381D7154A696		0	Random F2:1B:04:CD:FE:7B	NULL	396720...	135388	0	NULL
12CC8E30-0E27-88A7-BCED-9AFEC9378634		0	Random E0:C9:86:97:CC:E5	NULL	473947...	157910	0	NULL
12CF499D-823F-F0A7-E9BB-88C5E8032180		0	Random E2:67:9F:B7:0A:0A	NULL	500881...	0	0	NULL
12D74EED-E1CC-04A4-0FC6-EA9486F54704		0	Random E8:65:2B:74:28:57	NULL	480841...	161163	0	NULL
12D7ADFE-FAA4-1393-4CA7-1B7F72AA7D6F		0	Random F2:0E:62:43:39:E1	NULL	498668...	167421	0	NULL
12DA5F9D-7772-0EF8-8132-288DCD169DEA		0	Random EC:8C:D5:E4:A0:EC	NULL	462332...	152572	0	NULL
12E06164-6F4B-69E2-FA86-CB489C74FDDA		0	Random E5:A9:77:DA:24:3E	NULL	500920...	0	0	NULL
12E94DC4-D032-AC9E-4C39-712D28D53822		0	Random E3:7F:27:14:94:91	NULL	417032...	140563	0	NULL
130973DE-627A-81A7-2EBA-B2242B3652B7		0	Random F8:A0:AF:73:92:59	NULL	473957...	157924	0	NULL
132286B0-80D6-7E79-D83D-4E4884B5D2BC		0	Random DE:25:F0:63:F9:0E	NULL	462803...	152785	0	NULL
1323FDC6-48BF-A69C-59D0-5CCC84734AEC		0	Random EA:E3:89:E8:E4:99	NULL	43424...	145683	0	NULL
132F273F-FAD8-688A-609C-1CF3A6F6996A		0	Random E0:81:9C:EB:5E:7D	NULL	424129...	143697	0	NULL
1335C5FF-8812-81F3-1AB6-9D0FB5BFD080		0	Random EC:30:97:C4:18:DD	NULL	450184...	150160	0	NULL
13361048-735E-5F75-AD84-89C7D0C1302F		0	Random C2:D2:F8:FA:12:66	NULL	482723...	162578	0	NULL
13362999-EAD2-46FB-9D18-8CEED2347F9A		0	Random F2:27:74:E6:4C:19	NULL	488812...	164854	0	NULL
1338AE8E-A6A7-5213-8C71-089CEC3E2885		0	Random F7:8A:E6:35:D3:09	NULL	41291471	137951	0	NULL
134CAF77-83C9-54CB-4485-443828861BA0		0	Random F5:BE:44:6B:65:76	NULL	477951...	158777	0	NULL
1358E6AA-94BF-D9E6-87BD-2448ABBC7D31		0	Random D5:FF:CA:10:1C:D5	NULL	42442...	143905	0	NULL
1364D562-F687-890D-0C6F-29725EB7374B		0	Random F8:DD:37:F6:51:7C	NULL	483867...	163261	0	NULL
136B6CC6-CE34-7A13-C7FB-00C144D15CAC		0	Random CF:81:57:33:1F:EA	NULL	423082...	143203	0	NULL
1380E4F3-3560-0A88-2F0A-3190C181C2A6		0	Random E0:DD:7A:57:78:D6	NULL	499629...	167677	0	NULL
1384F182-F612-4D28-9E0F-FDCB9088A9EC		0	Random D5:91:86:A2:7A:FC	NULL	434183...	145662	0	NULL
13884CB7-925F-71BF-F057-E7B3DB7A98F9		0	Random E4:4B:7D:35:41:B8	NULL	484611...	163522	0	NULL
138E02DF-0535-E95C-03A4-3BAE33CB07AC		0	Random DD:4C:56:37:7C:B8	NULL	500893...	0	0	NULL
1395E78A-1F71-1CBA-B986-3FDA37CAD28A		0	Random FD:F9:F2:71:5A:39	NULL	470180...	155283	0	NULL
13A2DDDF-1313-AC15-643C-3F02A2A0D7A2		0	Random E3:5B:6A:DD:59:75	NULL	480529...	161011	0	NULL
13A9E949-FAA6-8E41-86C3-EC703039F1FE		0	Random ED:D1:92:54:D9:10	NULL	400049...	136584	0	NULL
13AA3022-648C-BF3C-6A46-B621B9479042		0	Random CB:D5:2F:E5:A2:B3	NULL	479601...	159550	0	NULL
13BBDC53-F85A-C67C-084E-E34C14397E9		0	Random D2:59:0B:A6:62:2E	NULL	500864...	0	0	NULL

Рис. 2. Блок-схема методу класифікації потенційно небезпечної особи

Використання журналу даних Bluetooth для виявлення потенційно небезпечних осіб

Технологія Bluetooth забезпечила широке миттєве бездротове підключення, охоплюючи все, від особистих переносних пристроїв до систем розумного будинку та індивідуальних покупок, залежних від місцезнаходження. З моменту її первинного інтегрування в мобільні телефони у 2000 році [14], було п'ять значних переглядів основної специфікації, а також багато поправок [15].

У початкових версіях специфікації Bluetooth пристрої регулярно передавали свої постійні MAC-адреси Bluetooth відкрито, що порушувало питання конфіденційності через потенційну можливість небажаного відстеження [13]. Bluetooth Core Specification 4.0 вирішила цю проблему, введенням стандарту Bluetooth Low Energy (BLE), також відомого як Bluetooth Smart. BLE дозволяє виробникам використовувати тимчасові випадкові адреси для комунікацій, замінюючи постійні адреси, щоб ускладнити відстеження [16]. Однак, специфікація не описує конкретного способу імплементації цих функцій анонімізації, що дозволяє виробникам мати деякий простір для маневру у їх впровадженні. Впровадження функцій підвищення конфіденційності особливо є важливим, враховуючи, що BLE був спеціально розроблений для пристроїв із низьким енергоспоживанням, таких як розумні годинники та інші переносні пристрої, які є основними цілями для зловмисного відстеження.

Пристрої BLE випромінюють, так звані, рекламні повідомлення (advertisements) через незашифровані, відкриті канали, щоб повідомити про свою доступність іншим пристроям. Ці публічні трансляції повинні передавати всю необхідну інформацію для

роботи пристрою, не розкриваючи жодної приватної інформації про пристрій або його користувача. Проте, існують випадки, коли такі трансляції можуть ненавмисно розкривати конфіденційну інформацію про пристрій або навіть інші підключені пристрої.

Дослідники у [17] розробили мобільний додаток під назвою BTLEmap. BTLEmap нагадує функціонал інструментів розвідки мережі та аудиту безпеки, таких як Nmap, які використовуються для IP-базованих мереж. Він пропонує можливості, такі як перелічення пристроїв, виявлення GATT-сервісів та ідентифікація пристроїв. Крім того, він включає аналізатор рекламних повідомлень BLE, експортер даних та інтуїтивно зрозумілий інтерфейс користувача, який візуально демонструє відстань до інших пристроїв на основі потужності сигналу. Показано знімок екрану з демонстрацією потужності сигналу виявлених пристроїв з додатку BTLEmap (рис. 3).

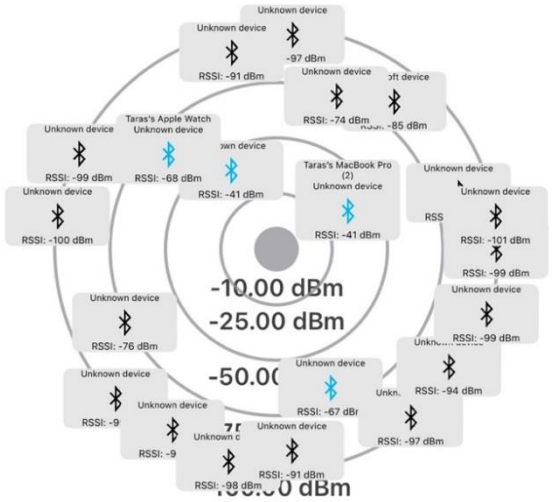

Рис. 3. Зображення виявлених Bluetooth пристроїв за допомогою додатку BTLEmap

У [13] дослідники показують, як навіть такі сучасні пристрої, як комп'ютери під управлінням операційної системи Windows 10 та iPhone, які впроваджують заходи захисту конфіденційності, такі як рандомізація адрес, можуть бути вразливими до постійного відстеження. Автори спочатку досліджують різні типи рекламних повідомлень та виявляють, так звані, ідентифікаційні токени, які є унікальними для пристрою і залишаються статичними достатньо довго, щоб використовуватися як вторинні ідентифікатори разом із Bluetooth-адресою. Автори [13] представляють онлайн-алгоритм під назвою алгоритм перенесення адреси, який використовує факт, що ідентифікаційні токени та випадкова адреса не змінюються синхронно, щоб постійно відстежувати пристрій, незважаючи на впровадження заходів анонімізації. На думку авторів, цей алгоритм працює однаково на всіх пристроях Windows 10, iOS та macOS [18]. Алгоритм не вимагає розшифровки повідомлень або порушення безпеки Bluetooth будь-яким чином, оскільки він повністю базується на публічному, незашифрованому рекламному трафіку.

На основі матеріалів описаних у [13], можна зробити висновок, що можливо використовувати історичні дані Bluetooth мобільного пристрою для розробки методу виявлення потенційно небезпечних осіб.

Пропонується метод класифікації особи як потенційно небезпечної на основі знаходження доказів її присутності в безпосередній близькості до певної, завідомо небезпечної, особи/групи осіб у конкретний момент часу. Метод класифікує особу на один із трьох класів: не підозрілий, помірно підозрілий та високо підозрілий. Припущення методу полягає в тому, що факт наявності в базі даних Bluetooth-пристрою небезпечної особи та часової мітки в межах допустимої помилки часу означає, що особа, яка перебуває під розслідуванням, є високо підозрілою. Якщо база даних містить Bluetooth-пристрій небезпечної особи, але часова мітка не входить у шуканий діапазон - особа, яка перебуває під розслідуванням, є помірно підозрілою. Інший випадок – коли записи не знайдені, означає, що особа, яка перебуває під розслідуванням, не є підозрілою.

Як показано в розділі II, визначення того, чи є особа потенційно небезпечною, залежить від контексту, в якому відбуваються події. Можна сформулювати приклади, в яких факт зустрічі з певною, завідомо небезпечною особою в конкретний час може розглядатися як ознака потенційної небезпеки. Одним із таких прикладів може бути факт зустрічі з наркодилером пізно вночі. Цей факт може вказувати на те, що особа, яка перебуває під розслідуванням, може якимось чином взаємодіяти з продавцем заборонених речовин. Тип взаємодії може бути різним. Розслідувана особа може бути покупцем, постачальником або взагалі не мати відношення до завідомо небезпечної особи. Для більш детального вивчення типу взаємодії між особами, особу, яка перебуває під розслідуванням, слід розглядати як потенційно небезпечну.

Доказом перебування в тісній близькості до певної особи/групи людей, пропонується використовувати записи Bluetooth-пристроїв, які були в межах досяжності, але не були підключені. Як показано в розділі III, пристрій iOS зберігає історію таких записів. Дані з таблиці OtherDevices у стовпцях “Uuid”, “Address” та “LastSeenTime” можуть допомогти встановити, чи була особа, яка перебуває під розслідуванням, в межах Bluetooth-досяжності адреси правопорушника в конкретний час, що може бути визначено стовпцем “LastSeenTime”.

Таким чином, метод приймає такі вхідні дані:

- список Bluetooth-адрес пристроїв, які належать відомо небезпечній особі/особам;
- час, який має значення в контексті потенційно небезпечної події;

- допустима помилка часу при визначенні факту зустрічі;
- записи з таблиці OtherDevices з бази даних com.apple.MobileBluetooth.ledevices.other.db з мобільного пристрою особи, яка перебуває під розслідуванням.

Зображено псевдокод, який ілюструє логіку роботи методу (рис. 4).

```
BEGIN MAINPROGRAM
READ intruder bluetooth addresses list
READ meeting time
READ meeting time delta
INIT OtherDevices table
FOR EACH bluetooth address IN intruder bluetooth addresses list DO:
  bluetooth address exists in database and time in range = find record in database including
time (bluetooth address, meeting time, meeting time delta)

  IF bluetooth address exists in database and time in range THEN:
    RETURN "HIGH SUSPICIOUS"

  bluetooth address exists in database = does bluetooth address exist in database
(bluetooth address)

  IF bluetooth address exists in database THEN:
    RETURN "MODERATE SUSPICIOUS"

RETURN "NON SUSPICIOUS"
END MAINPROGRAM

BEGIN SUBPROGRAM does bluetooth address exist in database (bluetooth address)
connect to database
query results = execute a query that searches for records where "Address" == bluetooth
address
IF query results length > 0:
  RETURN true
ELSE:
  RETURN false
END SUBPROGRAM does bluetooth address exist in database

BEGIN SUBPROGRAM does bluetooth address and time exist in database (bluetooth address,
time, delta)
connect to database
query results = execute a query that searches for records where "Address" == bluetooth
address and ""LastSeenTime" in range(time - delta, time + delta)
IF query results length > 0:
  RETURN true
ELSE:
  RETURN false
END SUBPROGRAM does bluetooth address and time exist in database
```

Рис 4. Псевдокод методу класифікації потенційно небезпечних осіб

Запропонований метод класифікує особу як потенційно небезпечну на основі знаходження доказів її присутності поблизу певної особи/групи осбі у конкретний момент часу. Метод повертає один з трьох класів: не підозрілий, помірно підозрілий та високо підозрілий. Припущення методу полягає в тому, що факт наявності в базі даних Bluetooth-пристрою небезпечної особи та часової мітки в межах допустимої помилки часу означає, що особа, яка перебуває під розслідуванням, є високо підозрілою. Якщо база даних містить Bluetooth-пристрій небезпечної особи, але часова мітка не входить у шуканий діапазон - особа, яка перебуває під розслідуванням, є помірно підозрілою. Інший випадок – коли записи не знайдені, означає, що особа, яка перебуває під розслідуванням, не є підозрілою.

Потенційні можливості покращення методу

Результати криміналістичного дослідження даних, які зберігаються на мобільному пристрої, показують, що існують потенційні можливості для вдосконалення запропонованого методу. Одним із напрямків вдосконалення може бути використання інших типів даних. Прикладами таких даних може бути інформація про Wi-Fi мережі, а також GPS-координати.

Факт підключення до Wi-Fi мережі може мати значний вплив у криміналістичному розслідуванні з кількох причин:

- локація та часові мітки: коли пристрій підключається до Wi-Fi мережі, він реєструє час та дату підключення. Ця інформація може допомогти встановити присутність особи або пристрою в конкретному місці в певний час, що може бути вирішальним у створенні хронології подій;
- ідентифікація пристрою: кожен пристрій має унікальний ідентифікатор, відомий як MAC-адреса. Коли пристрій підключається до Wi-Fi мережі, мережа реєструє цю MAC-адресу. Це може допомогти ідентифікувати конкретні пристрої, які були присутні на місці злочину або важливому місці;
- журнал активності мережі: Wi-Fi роутери та точки доступу часто зберігають журнали активності мережі. Це може включати відвідані веб-сайти, передані дані та сервіси, до яких було здійснено доступ під час підключення пристрою до мережі. Ця інформація може бути важливою для розуміння дій та намірів користувача.

Запропонований метод класифікує особу як потенційно небезпечну на основі знаходження доказів її присутності поблизу певної особи/групи осбі у конкретний момент часу.

Одним із результатів криміналістичного дослідження мобільного пристрою було виявлення списку відомих пристрою Wi-Fi мереж. Деякі записи включають GPS-координати Wi-Fi роутера. Показано скріншот (рис. 5).

com.apple.wifi.known-networks

com.apple.wifi.known-networks 〉 No Selection

Key	Type	Value
Root	Dictionary	(194 items)
wifi.network.ssid.You don't spell it	Dictionary	(13 items)
wifi.network.ssid.Apple Room Guest	Dictionary	(11 items)
wifi.network.ssid.chuangmi-camera-026c02_miap2C7F	Dictionary	(8 items)
wifi.network.ssid.TP-Link_EDC3	Dictionary	(11 items)
wifi.network.ssid.DIONYSOS03	Dictionary	(13 items)
wifi.network.ssid.Kuznia	Dictionary	(9 items)
wifi.network.ssid.SportLife.Guest	Dictionary	(12 items)
wifi.network.ssid.TP-Link_71B5	Dictionary	(11 items)
wifi.network.ssid.208_2.4/5G	Dictionary	(13 items)
AddReason	String	System App
SupportedSecurityTypes	String	WPA/WPA2 Personal
LastDiscoveredAt	Date	2023-11-06T09:14:34Z
UpdatedAt	Date	2023-11-06T09:46:42Z
BundleID	String	com.apple.camera
AddedAt	Date	2023-10-09T09:19:05Z
__OSSpecific__	Dictionary	(10 items)
Hidden	Boolean	NO
SSID	Data	<3230385F322E342F3547>
CaptiveProfile	Dictionary	(1 item)
Moving	Boolean	NO
BSSList	Array	(1 item)
Item 0	Dictionary	(8 items)
LocationAccuracy	Number	39.92526072623561
BSSID	String	50:d2:f5:2d:c4:47
LocationTimestamp	Date	2023-11-06T09:46:26Z
ChannelFlags	Number	10
LocationLatitude	Number	49.83882496592807
LocationLongitude	Number	24.03297284922407
Channel	Number	4
LastAssociatedAt	Date	2023-11-06T09:46:27Z
JoinedBySystemAt	Date	2023-11-06T09:46:27Z
wifi.network.ssid.TP-Link_F498_5G	Dictionary	(11 items)

Рис. 5. Інформація про Wi-Fi мережі яка зберігається на мобільному пристрої

Ще одним цікавим результатом криміналістичного дослідження є виявлена база даних SQLite під назвою PPSQLDatabase.db, яка розташована у директорії "HomeDomain / Library / PersonalizationPortrait / models". Одна з її таблиць, іменована "loc_records", містить список місць, включаючи GPS-координати та часові мітки (рис. 6). Така інформація також може бути використана покращеною версією методу.

id	cll_latitude_degrees	cll_longitude_degrees	clp_thoroughfare	clp_subThoroughfare	clp_locality	clp_subLocality	clp_administrativeArea
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
28...	38.6861656	-9.305564	Avenida Marginal	NULL	Oeiras	NULL	Lisboa
28...	38.7440382	-9.1713309	NULL	NULL	Lisboa	NULL	Lisboa
28...	51.1088459	17.1199806	Marca Polo	NULL	Wrocław	NULL	Lower Silesia
28...	47.3672378	12.6374703	Rammernweg	NULL	Saalbach-...	NULL	Salzburg
28...	49.8326297	24.0349435	Shota Rustaveli Street	NULL	Lviv	NULL	Lviv Oblast
28...	51.1116787	17.049287	most Pokoju	NULL	Wrocław	NULL	Lower Silesia
28...	49.8092641	24.0078935	Troleibusna Street	NULL	Lviv	NULL	Lviv Oblast
28...	49.4519707	22.9987218	Яблунева вулиця	NULL	Stril'bychi	NULL	Lviv Oblast
28...	51.1185	17.0414	Bolesława Prusa	NULL	Wrocław	NULL	Lower Silesia
28...	49.8281687	23.9869768	Porokhova Street	NULL	Lviv	NULL	Lviv Oblast
28...	50.5328124	30.3629067	Mykoly Yunkerova ...	NULL	Kyiv	NULL	Kyiv
28...	51.1199704	17.0394703	Jedności Narodowej	NULL	Wrocław	NULL	Lower Silesia
28...	49.9608532	24.6117449	Михайла ...	NULL	Busk	NULL	Lviv Oblast
28...	49.8342578	24.0096336	Mykhaila Starytskoh...	NULL	Lviv	NULL	Lviv Oblast
28...	49.8319849	24.001712	Volodymyra ...	NULL	Lviv	NULL	Lviv Oblast
28...	49.8359274	24.0166649	Mykoly Ustyianovyc...	NULL	Lviv	NULL	Lviv Oblast
28...	49.8235975	23.9108342	M-10-01	NULL	Lviv	NULL	Lviv Oblast
28...	38.6864229	-9.3046558	Avenida Marginal	NULL	Oeiras	NULL	Lisboa
28...	38.7116485	-9.1397264	Rua do Carmo	NULL	Lisboa	NULL	Lisboa
28...	51.0971	17.0336	Sucha	NULL	Wrocław	NULL	Lower Silesia
28...	51.1098	17.1202	Ferdynanda Magellana	NULL	Wrocław	NULL	Lower Silesia
28...	47.8078781	13.0621217	Schallmooser ...	NULL	Salzburg	NULL	Salzburg
28...	51.1172499	17.0407773	Bolesława Drobnera	NULL	Wrocław	NULL	Lower Silesia
28...	49.8265699	23.9894387	Kulparkivska Street	NULL	Lviv	NULL	Lviv Oblast

Рис. 6. Дані про місцезнаходження користувача, які зберігається на мобільному пристрої

Висновки. Стаття пропонує метод класифікації потенційно небезпечних осіб на основі записів даних Bluetooth-пристроїв, які були в межах досяжності, але не були під'єднані.

Метод пропонує класифікувати суб'єктів на основі заданого контексту, а саме: списку Bluetooth-адрес пристроїв, відомих як такі що асоціюються із небезпечними особами, часу, який має значення в контексті потенційно небезпечної події, допустимої помилки, а також записів з таблиці OtherDevices з бази даних com.apple.MobileBluetooth. ledevices.other.db мобільного пристрою особи, яка перебуває під розслідуванням. Результатом методу є віднесення розслідуваної особи до одного з трьох класів: не підозрілий, помірно підозрілий та високо підозрілий.

Запропонований метод є теоретичним і потребує практичної реалізації та перевірки у подальших дослідженнях.

Список літератури

[1]. Schuster, A.M., Cotten, S.R. & Meshi, D. Established Adults, Who Self-Identify as Smartphone and/or Social Media Overusers, Struggle to Balance Smartphone Use for Personal and Work Purposes. J Adult Dev 30, pp. 78-89 (2023).

[2]. Use Bluetooth and Wi-Fi in Control Center, https://support.apple.com/en-us/102412.

[3]. Shytierra Gaston, Rod K. Brunson, David O. Ayeni. Suspicious places make people suspicious: Officers' perceptions of place-based conditions in racialized drug enforcement, 2022. https://doi.org/10.1111/1745-9133.12606.

[4]. Kasperowski, D., & Hagen, N. (2022). Making particularity travel: Trust and citizen science data in Swedish environmental governance. Social Studies of Science, 52(3), pp. 447-462. https://doi.org/10.1177/0306312722-1085241.

[5]. P.V. Bindu, P. Santhi Thilagam, Mining social networks for anomalies: Methods and challenges, Journal of Network and Computer Applications, Volume 68, 2016, pp. 213-229.

[6]. Lokanan, Mark & Maddhesia, Vikas Kumar. (2023). Predicting Suspicious Money Laundering Transactions using Machine Learning Algorithms. 10.21203/rs.3.rs-2530874/v1.

[7]. Kenyon, J., Binder, J. F., & Baker-Beall, C. (2023). Online radicalization: Profile and risk analysis of individuals convicted of extremist offences. Legal and Criminological Psychology, 28, pp. 74-90.

[8]. Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Revision 1, 2014, http://dx.doi.org/10.6028/NIST.SP.800-101r1.

[9]. M. -H. wu, T. -C. Chang and Y. Li-Min, "Digital Forensics Security Analysis on iOS Devices," in Journal of Web Engineering, vol. 20, no. 3, pp. 775-794, May 2021, doi: 10.13052/jwe1540-9589.20310.

[10]. iMazing – iOS backups management tool, https://imazing.com/.

[11]. SQLite database, https://www.sqlite.org/.

[12]. Digital Forensics, https://bitsplease4n6.wordpress.com/.

[13]. Becker, Johannes & Li, David & Starobinski, David. (2019). Tracking Anonymized Bluetooth Devices. Proceedings on Privacy Enhancing Technologies. 2019. pp. 50-65. 10.2478/popets-2019-0036.

[14]. Bluetooth Special Interest Group (SIG). Core Specifications, 2018.

[15]. Martin Woolley. Bluetooth Technology Protecting Your Privacy, 2015.

[16]. Heinrich, Alexander & Stute, Milan & Hollick, Matthias. (2020). DEMO: BTLEmap: Nmap for Bluetooth Low Energy.

[17]. Vasylyshyn, S., Susukailo, V., Opirskyy, I., Kurii, Y., & Tyshyk, I. (2023). A model of decoy system based on dynamic attributes for cybercrime investigation. Eastern-European Journal of Enterprise Technologies, 1(9 (121), pp. 6-20. https: // doi.org / 10.15587/1729-4061. 2023. 273363.

[18]. Susukailo, V., Opirskyy, I., Vasylyshyn, S. Analysis of the attack vectors used by threat actors during the pandemic // 2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2020 - Proceedings, 2020, 2, C. 261-264.

УДК 004.056.5

Fedynyshyn T., Mykhaylova O., Opirskyy I. Method to Detect Suspicious Individuals through Mobile Device Data

Abstract. *In today's technologically advanced era, the ubiquitous use of smart mobile devices has become a significant aspect of daily life, thereby presenting a valuable opportunity for investigative purposes. These devices, when equipped*

with the right tools and subjected to thorough inspection methodologies, can yield a treasure trove of concealed information, which can be crucial in various investigative scenarios. Among these devices, the Apple iPhone stands out due to its widespread popularity and adoption across a diverse global user base. Its advanced features and user-friendly characteristics have made it a preferred choice for a wide array of individuals, ranging from students and teachers to business professionals and individuals from various other fields. This widespread usage underscores the importance of understanding the nuances of iPhone data in investigative contexts. This article delves into the intricate concept of identifying a potentially dangerous person by leveraging the data available on these smart devices. It meticulously discusses the importance of context in categorizing an individual as potentially dangerous and sheds light on the various factors that play a pivotal role in this classification process. To aid in this endeavor, the article introduces a comprehensive diagram that outlines the step-by-step procedure for assessing the potential danger posed by an individual. Furthermore, the article explores the fundamental techniques of mobile device forensics, particularly focusing on devices operating on the iOS platform. It presents the findings from practical research, offering insights into the type of data that can be extracted during a forensic investigation of these devices. A novel approach is proposed for classifying individuals as potentially dangerous based on the analysis of Bluetooth data obtained from their mobile devices. This method is elucidated through the presentation of pseudocode, which details the algorithmic steps involved in this classification process. To enhance the effectiveness of this method, the article suggests incorporating additional data sources. These include information pertaining to saved Wi-Fi networks that the device has connected to and GPS coordinates that have been logged during the operation of various system applications inherent to the iOS operating system. Finally, the article emphasizes the critical need for the practical implementation and rigorous testing of this proposed method. It underscores the importance of validating and refining the approach to ensure its effectiveness and reliability in identifying potentially dangerous individuals through the forensic analysis of mobile device data. This comprehensive approach not only broadens the scope of mobile device forensics but also contributes significantly to the field of security and investigative research.
***Keywords**: mobile forensics, iOS, suspicious individual's detection method, Bluetooth.*

Фединишин Тарас Олегович, аспірант кафедри захисту інформації Національного університету «Львівська політехніка»

Taras Fedynyshyn, Postgraduate the Department of Information Security, National University "Lviv Polytechnic".

Михайлова Ольга Олександрівна, к.т.н., доцент кафедри захисту інформації Національного університету «Львівська політехніка».

Olha Mykhaylova, Ph.D., Associate Professorat the Department of Information Security, National University "Lviv Polytechnic".

Опірський Іван Романович, , доктор технічних наук, професор, кафедра захисту інформації, Національного університету «Львівська політехніка».

Ivan Opirskyy, doctor of Technical Sciences, professor, Department of Information Security, Lviv Polytechnic National University.

Отримано *7 жовтня 2023 року*, затверджено редколегією *30 жовтня 2023 року*