

прийнятого в техніці магнітного запису трактування поняття «сигналограма», як тимчасового розподілу амплітуд сигналу запису/зчитування, техніка візуалізації даних на магнітних носіях використовує інший підхід. Під магнітною сигналограмою розуміється просторовий розподіл амплітуд залишкової намагніченості. Магнітна сигналограма дає можливість «побачити» дані на носії. Найбільш часто для дослідження магнітних полів носіїв використовуються наступні методи:

- метод Біттера;
- магнітооптичні методи;
- магнітна силова мікроскопія.

Для візуалізації магнітних доменів Біттер застосував колоїдну суспензію магнітних частинок, кожна з яких за формою нагадує мікроскопічну голку розмірами всього декілька мікронів. Перебуваючи в підвішеному стані і практично не відчуваючи тертя, такі частинки можуть швидко переорієнтовуватися в залежності від напрямку прикладеного магнітного поля. Якщо нанести на намагнічену поверхню тонкий шар суспензії, вони концентруються уздовж ділянок зразка, де намагніченість змінює свій знак, формуючи так звані картини Біттера, які можна спостерігати за допомогою оптичного мікроскопа. Для досягнення більшого контрасту зразок іноді поміщують у невелике зовнішнє магнітне поле, спрямоване уздовж його поверхні.

Таким чином, використовувач запропонований метод візуалізації магнітних доменів можна отримати інформацію про несанкціоноване вторгнення в систему пам'яті інформаційної системи, та визначити факт знищення інформації.

УДК 004.05

ОЛЕКСІЙ ВЯЧЕСЛАВОВИЧ ПЕРЕЦЬ

курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ

ОКСАНА ПЕТРІВНА МЕЛАЩЕНКО

Старший викладач кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ УСТАНОВЛЕННЯ МІСЦЕЗНАХОДЖЕННЯ РАДІОЕЛЕКТРОННОГО ЗАСОБУ В ДІЯЛЬНОСТІ ПОЛІЦІЇ

Одним з основних засобів отримання доказів у кримінальному процесі на стадії досудового розслідування є негласні слідчі (розшукові) дії, завдяки яким доводиться вина особи у вчиненні злочинів та розслідується левина частина тяжких та особливо тяжких злочинів [1]. Одним із таких засобів доказування - негласною слідчою (розшуковою) дією, є використання в діяльності поліції установа млення місцезнаходження радіоелектронного засобу.

Як відомо, у сучасному інформаційному суспільстві мобільний телефон стає продовженням нашої особистості і нашого інтелекту. Не дивно,

що аналіз даних із телефону та установлення його місцезнаходження стає все більш важливою навичкою при розкритті злочинів. Установлення місцезнаходження радіоелектронного засобу здійснюється для реалізації окремих завдань кримінального впровадження. Як зазначає О. Комарницька, дані дії не обмежують конституційні права та свободи людини, оскільки їх об'єктом є технічний засіб, а не фізична особа [2].

Щодо технічної сторони установлення місцезнаходження радіоелектронного засобу, то у відповідності з технічними вимогами, кожен мобільний телефон повинен мати спеціальний засіб ідентифікації. IMEI (англ. International Mobile Equipment Identity – міжнародний ідентифікатор мобільного обладнання) – серійний номер мобільного пристрою (п'ятнадцятизначне число, тобто 14 цифр коду плюс 15-та контрольна цифра), який встановлюється заводом-виробником та є унікальним для кожного мобільного телефону. Цей номер встановлюється заводом-виробником при виготовленні апарату та служить для точної і повної ідентифікації телефону в мережах форматів GSM та UMTS: автоматично передається апаратом у мережу оператора при підключенні [3]. Тому, слідчі або спеціалісти оперативних підрозділів їдуть на місце злочину і проводять радіорозвідку, тобто визначають, які базові станції знаходяться поряд, а отже – могли мати з'єднання із мобільним телефоном зловмисника. За результатами проведення цієї негласної слідчої (розшукової) дії може бути встановлене місцезнаходження кінцевого обладнання рухомого (мобільного) зв'язку, яке використовується особою, підозрюваною або причетною до вчинення злочину, інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, тощо [4].

Але, незважаючи на ефективність цього негласного розшукового заходу, він має і певні недоліки. Зокрема, як вказує Л. В. Бобрицький, що хоча є чіткий механізм проведення даної процедури, але здійснення такого оперативно-розшукового заходу достатньо складне, відносно довготривале і не забезпечує оперативного вирішення завдань щодо встановлення особи злочинців, або свідків та їх місцезнаходження [5].

Також, як зазначає Луцик В. В. у [6] у правозастосовній практиці виникають ситуації, коли один і той самий номер IMEI належить декільком телефонам. Така ситуація є результатом недобросовісної комерційної діяльності виробників телефонів.

Таким чином, щодо використання установлення місцезнаходження радіоелектронного засобу в діяльності поліції можна вказати, що це дійсно ефективний засіб доведення вини особи у вчиненні злочинів та розслідування тяжких та особливо тяжких злочинів. Однак при його застосуванні слідчим або спеціалістам оперативних підрозділів слід, по-перше, дотримуватися вимог механізму проведення даної процедури, передбаченої КПК України, по-друге, враховувати технічні особливості і специфіку використання радіоелектронного засобу та установлення його місцезнаходження, по-третє, знати «підводні камені», які можуть виникнути під час застосування цієї негласної слідчої (розшукової) дії.

Список використаних джерел:

1. Синявський С. М. Правові аспекти проведення негласної слідчої (розшукової) дії – установлення місцезнаходження радіоелектронного засобу. *Право і суспільство*. 2016. № 4. С. 221–224. URL: http://nbuv.gov.ua/UJRN/Pis_2016_4_39.
2. Комарницька О., Прядко В. Установлення місцезнаходження засобу радіоелектронного зв'язку: підготовка та проведення негласної слідчої (розшукової) дії. *Вісник Національної академії прокуратури України*. 2014. № 2. С. 71–78. URL: http://nbuv.gov.ua/UJRN/Vnapu_2014_2_14
3. Кримінальний процесуальний кодекс України: Науково-практичний коментар. У 2 т. Том 1. О. М. Бандурка, Є. М. Блажівський, Є. П. Бурдоль та ін. ; за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків. Право, 2012. 768 с.
4. Бобрицький Л. В. Практичні аспекти застосування кримінального процесуального законодавства України щодо установлення місцезнаходження радіоелектронного засобу. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2013. № 3(спец. вип.). С. 155–160. URL: [http://nbuv.gov.ua/UJRN/boz_2013_3\(spets\)](http://nbuv.gov.ua/UJRN/boz_2013_3(spets)).
5. Луцик В. В. Установлення місцезнаходження радіоелектронного засобу. *Юридичний науковий електронний журнал*. № 4. 2014. С. 199– 202.

УДК 004.05

ВІТАЛІЙ АНАТОЛІЙОВИЧ СВІТЛИЧНИЙ

кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ

КІБЕРБЕЗПЕКА УКРАЇНИ ТА ОСОБЛИВОСТІ КІБЕРЗЛОЧИНІВ

Відповідно до законодавства України, кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави у процесі використання кіберпростору, яка забезпечує сталий розвиток інформаційного суспільства і цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі (ст. п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»). У глобальному розумінні, кібербезпекою є реалізація заходів із захисту мереж, програмних продуктів та систем від цифрових атак.

В державі на законодавчому рівні приймаються відповідні закони та нормативні акти, які регулюють відносини в цій сфері. Станом на 2019 р. до правової основи кібербезпеки України входять такі нормативно-правові акти: Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та інші закони, Доктрина інформаційної