УДК 343.9:004

Віталій Дмитрович СКРИЛЮК,
слухач магістратури факультету № 6
Харківського національного університету внутрішніх справ

ПОРІВНЯЛЬНИЙ АНАЛІЗ АПАРАТНИХ ТА ПРОГРАМНИХ КРИМІНАЛІСТИЧНИХ РІШЕНЬ ДЛЯ РОБОТИ З ДАНИМИ З МОБІЛЬНИХ ПРИСТРОЇВ, КОМП'ЮТЕРНОЇ ТЕХНІКИ З ФУНКЦІЄЮ ТЕЛЕФОНУ

Сучасний мобільний пристрій представляє собою міні комп'ютер, в якому можливість здійснювати та приймати дзвінки є лише однією із його функції. Такий пристрій заміняє собою фото та відеокамеру, GPS-навігатор, мультимедійні пристрої для відтворення аудіо та відео контенту. Мобільні пристрої стали невід'ємною частиною життя кожної людини. В результаті такої тісної взаємодії генерується велика кількість даних, проаналізувавши які можливо отримати вичерпну інформацію про власника пристрою.

На сьогоднішній день досягнення в галузі інформаційних технологій також активно використовуються при вчиненні всіх категорій злочинів, а тому з метою отримання якісної доказової бази та оперативної інформації правоохоронні органи різних країн активно використовують програмно-апаратні криміналістичні комплекси для отримання даних з мобільних пристроїв та іншої комп'ютерної техніки з функціями телефону. Українська правоохоронна система в цьому плані не є виключенням.

Проаналізувавши інформацію про сучасні програмні та програмно-апаратних комплексів слід відмітити наступні:

1) UFED (Universal Forensic Extraction Device) – програмний комплекс від ізраїльської компанії Cellebrite [1].

Заснована в 1999 році вихідцями із підрозділів Армії оборони Ізраїлю, компанія на сьогоднішній день постачає програмно-апаратний криміналістичний комплексів під назвою «UFED TOUCH 2», а також програмний комплекс UFED 4PC. Комплекс «UFED TOUCH 2» представлений у вигляді міні-комп'ютеру з операційною системою Windows та встановленим фірмовим програмним забезпеченням, який розміщений в захисному корпусі та до якого додається органайзер з близько 80 кабелями та аксесуарами для підключення мобільних терміналів. Крім того, на бокових гранях пристрою розміщенні роз'єми USB, порти для підключення RJ 45 та кардрідер, оскільки даний пристрій дає можливість отримувати інформацію не тільки з мобільних терміналів, а і з ноутбуків, планшетів, GPS навігаторів, квадрокоптерів та різноманітних змінних носіїв. Вказаний комплекс реалізує можливість здійснювати фізичний та логічний методи зняття

інформації з мобільного терміналу, а також обхід стандартних методів захисту.

Світову славу вказаний комплекс придбав після випадку у США. Так, 2 грудня 2015 року в місті Сан-Бернардіно на південному заході США у штаті Каліфорнія відбувся теракт, який полягав у масовому розстрілі у центрі допомоги для людей із обмеженими можливостями. В результаті теракту 14 людей вбито та 21 поранено. Стрілянину влаштувала сімейна пара — Сайєд Різван Фарук і Ташфін Малік, яких поліція ліквідувала ході спецоперації. В ході розслідування цього теракту Федеральне Бюро Розслідувань звернулося до компанії Apple з метою розблокування, а також створення так званого «бекдору» для отримання повного доступу до вмісту телефону, який належав вбитому терористу. Однак, компанія Apple категорично відмовилася задовільнити запити Федерального Бюро Розслідувань. Результатом цього рішення Apple стала велика кількість судових засідань, а також слухання в Конгресі. В подальшому ФБР різко зменшило свій тиск на компанію та через деякий час заявило, що їм вдалося розблокувати телефон з допомогою сторонньої компанії. Як з'ясували в подальшому журналісти, допомогу ФБР надала ізраїльська компанія Cellebrite [2];

2) XRY – програмний комплекс від шведської компанії Micro Systemation (MSAB) [3].

Компанія заснована в 1984 році та основним видом діяльності якої є створення криміналістичних рішень для отримання та відновлення інформації з мобільних пристроїв. На даний час використовується правоохоронними органами Великої Британії. Програмний комплекс XRY постачається на базі програмно-апаратних платформ, а саме: MSAB Office, MSAB Filed, MSAB Kiosk, MSAB Tablet. Такий поділ зумовлений місцем та обставинами при яких комплекс буде використовуватися.

3) MOBILedit – програмний комплекс від американської компанії Compelson Labs [4].

Компанія з 1991 року займається питанням копіювання та відновленням даних на мобільних пристроях. Основним криміналістичним програмним рішенням компанії є MOBILedit Forensic Express. На відміну від попередніх двох комплексів, MOBILedit Forensic Express не включає в себе додаткових апаратних платформ, кабелів та аксесуарів. Крім того, його робота зосереджена виключно на отриманні інформації з мобільних терміналів.

Невід'ємною частиною досягнення результату при проведенні криміналістичного дослідження є аналіз отриманих даних та підготовка звіту. З цією метою комплекси від компаній Cellebrite та Micro Systemation містять додаткові програмні модулі, які реалізують такий функціонал.

Програмно-апаратні комплекси «UFED TOUCH 2» від компанії Cellebrite активно використовуються правоохоронними органами України. Національна поліція України також не є виключенням в

цьому питанні, де під час практичної діяльності підрозділами НПУ було доведено їх ефективність.

Список бібліографічних посилань

1. Cellebrite official site. URL: https://www.cellebrite.com/en/home/ (дата звернення: 23.10.2018).

2. The Feds Can Now (Probably) Unlock Every iPhone Model In Existence. URL: https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite (дата звернення: 23.10.2018).

3. MSAB official site. URL: https://www.msab.com/ (дата звернення: 23.10.2018).

4. Mobiledit official site. URL: https://www.mobiledit.com/ (дата звернення: 23.10.2018).

Одержано 31.10.2018

УДК 004.056.53

Михайло Анатолійович СТРЕЛЬБІЦЬКИЙ,
доктор технічних наук, доцент
начальник (завідувач) кафедри зв'язку, автоматизації та кібербезпеки
Національної академії Державної прикордонної служби імені Богдана Хмельницького;
ORCID: https://orcid.org/0000-0001-8030-3228;
Олександр Степанович АНДРОЩУК,
доктор технічних наук, професор
начальник докторантури – головний науковий співробітник
Національної академії Державної прикордонної служби імені Богдана Хмельницького;
Віталій Вікторович РАВЛЮК,
викладач кафедри зв'язку, автоматизації та кібербезпеки
Національної академії Державної прикордонної служби імені Богдана Хмельницького

ПРОБЛЕМА СПІЛЬНОГО ФУНКЦІОНУВАННЯ МОДЕЛЕЙ РОЗМЕЖУВАННЯ ДОСТУПУ НА ЗАГАЛЬНОМУ ПОЛІ ДАНИХ ГЕТЕРОГЕННИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Математичний апарат формування систем розмежування доступу (СРД) для окремих інформаційних систем (ІС) на сьогодні досить добре розроблений. Разом із тим, як показав аналіз, існуючі моделі не передбачають їх спільного функціонування на загальному полі даних гетерогенної інформаційної системи. Разом із тим, під час модернізації відомчих територіально-розподілених інформаційних систем реального часу можливе виникнення ситуації, в якій на загальному полі даних повинні функціонувати різні версії ІС з власними СРД.