4. Безконтактне (досліджується психоемоційний стан опитуваного з застосуванням безконтактних датчиків під час надання ним відповідей на завчасно підготовлені питання щодо предмету дослідження).

Ці та інші, менш відомі інструментальні методи дослідження невербальної інформації загалом надають можливість фіксувати психофізіологічний стан опитуваного в певний проміжок часу на дані, що йому повідомляються з урахуванням зовнішніх та внутрішніх чинників. Тобто, ми бачимо спільне як от єдина умова - «…під час надання ним відповідей на завчасно підготовлені питання щодо предмету дослідження…».

До того ж, використання невербальної інформації збільшує тактичний потенціал суб'єктів кримінального провадження, сприяє вирішенню важливих завдань розслідування та визначенню більш вірогідних напрямів розслідування, формуючи їх розуміння щодо події, що мала місце.

За нашою думкою, на даний момент розвитку рівня інструментальних методів не варто говорити про доказову значимість його результатів. На сьогодні ми розглядаємо отримані результати інструментальних досліджень невербальної інформації, як орієнтуючу інформацію. Однак, в перспективі в залежності від розвитку та правового закріплення застосування інструментальних методів дослідження невербальної інформації існує суттєва можливість визнання результатів дослідження, як окремих й самостійних доказів відповідно до Кримінального процесуального кодексу України.

Самойленко О.А.

Національний університет «Одеська юридична академія»,

кандидат юридичних наук, доцент, доцент кафедри криміналістики

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ ІЗ ВИКОРИСТАННЯМ КІБЕРПРОСТОРУ

Інформатизація як і будь-яке соціальне явище, має не тільки позитивну для суспільства сторону, але й негативну – використання високих інформаційних

технологій у протиправних антисоціальних злочинних цілях. Дослідження свідчать, що кіберзлочинність у світі має тенденцію до зростання. Особливу небезпеку в складі правопорушень в сфері високих інформаційних технологій мають злочини, що вчиняються організованими угрупованнями. Проникнення організованних злочинних формувань у кіберпростір (комп'ютерний інформаційний простір) породило зміну засобів і способів вивчення й традиційних злочинів. Тому сьогодні актуальним є дослідження особливостей розслідування злочинів, що вчиняються із використанням кіберпростору.

Узагальнення проблем розслідування названого виду злочинів дало можливість визначити наступні визначні положення розслідування злочинів, що вчиняються із використанням кіберпростору.

По-перше, «кіберзлочинність» – це явище міжнародного значення, рівень якого безпосередньо залежить від рівня розвитку та впровадження сучасних комп'ютерних технологій та мереж, їх загального користування та доступу до них. Тому стрімкий розвиток інформатизації в Україні несе в собі потенційну можливість використання комп'ютерних технологій с корисливих, хуліганських та інших мотивів. Не дивлячись на сучасне реформування в Україні підрозділів боротьби з кіберзлочинністю та створення кіберполіції, в політичній сфері та у засобах масової інформації наголошується про загрозу в аспекті вчинення кіберзлочинів національній безпеці української держави. В Україні за останні 10 років було проведено достатньо велику кількість криміналістичних досліджень щодо проблем протидії комп'ютерній злочинності та, зокрема, її транснаціональним формам. Суттєвим недоліком більшості з них є теоретичний характер їх рекомендації, а не практичний (тобто прикладний). Далеко не всі положення криміналістичних методик з розслідування злочинів зазначеної категорії спираються на судово-слідчу практику в України (найчастіше використовують досвід закордонних правоохоронних органів). Про це слід пам'ятати слідчому при використанні методики розслідування певного виду комп'ютерного злочину.

По-друге, у криміналістичному аспекті особливості розслідування злочинів, вчинених у сфері високих інформаційних технологій, зумовлюються наступними складовими злочинної діяльності: цілі протиправної поведінки; важливі відомості про особу злочинця; мотивація злочинної поведінки; типові способи вчинення злочину; предмет посягання; відомості про потерпілу особу; інші елементи, що мають значення для розслідування кримінальних правопорушень. Методологія дослідження названих елементів повинна базуватися на системно-структурному підході та аналізі української судово-слідчої практики.

Крім того, ми наголошуємо на необхідності організації взаємодії слідчого, якому доручено розслідувати злочин, що вчинений із використанням кіберпростору, з співробітниками Департаменту кіберполіції. Адже саме за матеріалами зібраними кіберполіцейськими сьогодні відкриваються більшість зазначених кримінальних проваджень, при цьому вони є різноманітної кримінально-правової кваліфікації, як традиційні Інтернет-шахрайства, так й незаконнє поводження зі зброєю, бойовими припасами або вибуховими речовинами, доведення до самогубства тощо. Тому найкорисніша актуально та потенційно значуща для розслідування інформація акумулюється в підрозділах кіберполіції.

По-третє, механізм вчинення названих злочинів безпосередньо залежить від типу (категорії) злочинця. Сьогодні найбільш типовими є наступні категорії комп'ютерних злочинців: а) інсайдери – особи, що мають доступ до внутрішньої інформації (працюючий або звільнений співробітник української компанії є потенційним злочинцем, адже будучи знайомим з тонкощами комп'ютерної системи компанії, він має необмежений доступ до системи з метою незаконного втручання в роботу інформаційних технологій та заволодіння інформацією, яка є власністю компанії); хакери (зламують мережі просто за ради гострих відчуттів або за ради завоювання авторитету в хакерських колах, не рідко це відбувається і з метою фінансової наживи та інших злодіянь; завдяки своїм неординарним здатностям та високим інтелектом вони ускладнюють розкриття злочинів, що були ними вчинені); в) творці вірусних програм (аналогічно хакерам); г) кібертерористи

(терористичні організації все частіше використовують нові інформаційні технології та Internet із злочинними намірами поповнення коштів, здійснення пропаганди або передачі інформації, більшу загрозу становить пошкодження важливих державних інфраструктур наприклад, енергетичної, транспортної тощо); д) шахраї в мережі (за допомогою) Internet, які одночасно можуть бути досконалим інструментом у руках організованих груп; сітьове шахрайство є сьогодні найбільш поширеним видом злочинів; є) злочинці, що порушують права інтелектуальної власності через використання інформаційного ресурсу.

Таким чином, підчас розслідування злочинів, вчинених із використанням кіберпростору , слідчому необхідно виходити з особливостей механізму певного виду злочину, рекомендацій з окремих методик розслідування комп'ютерних злочинів та наявної судово-слідчої практики в Україні, а також продуктивно взаємодіяти з нещодавно створеними підрозділами кіберполіції.

Сушко В.В.

Національний університет «Одеська юридична академія», кандидат медичних наук, доцент кафедри криміналістики

ДІАГНОСТИКА ФАКТУ ДИСИМУЛЯЦІЇ ВЖИВАННЯ НАРКОТИЧНИХ ТА ІНШИХ ПСИХОАКТИВНИХ РЕЧОВИН У ПІДЕКСПЕРТНИХ ПЕРЕД ТЕСТУВАННЯМ НА ПОЛІГРАФІ

Вживання алкоголю, наркотиків чи інших фармакологічних препаратів перед тестуванням на поліграфі спеціально практикується щоб спотворити результати тестування. Для виявлення факту дисимуляції можуть використовуватися аналізи сечі чи крові на виявлення хімічних сполук але ці методи досить коштовні і займають багато часу. Альтернативою їм є метод скринінгового тестування за допомогою електропунктурної діагностики за Р. Фоллем.

Метод електропунктурної діагностики за Р. Фоллем широко використовується у лікарській практиці. Багато кандидатських і докторських робіт