

процесу. Фонограма в опечатаному вигляді зберігається при справі (стаття 85-1. КПК України) [1].

Як висновок можна виділити, що звукозаписуючі пристрої широко використовують у попередженні злочинів та профілактичній діяльності органів дізнання, слідства й суду. Значну роль вони відіграють в адміністративно-профілактичній діяльності, попередженні проступків і правопорушень. Основною метою використання звукозапису при розслідуванні є забезпечення додаткової наочно-звукової фіксації ходу окремих слідчих дій. Особливо таких слідчих дій, як допит, очна ставка, перевірка показань на місці, пред'явлення для впізнання. У тактиці проведення зазначених слідчих дій визначені ті ситуації, коли доцільно використання звукозапису в якості допоміжного засобу їх фіксації.

Список бібліографічних посилань:

1. Кримінальний процесуальний кодекс України. Кодекс кримінальний процесуальний від 13.04.2012 № 4651-VI. Редакція: 18.10.2018.
2. Гончар В. К., Золотар О. В. Знаряддя та прилади пошукової техніки: Навч. посіб. Київ: Нац. акад. внутр. справ України, 2001.
3. Гончар В. К., Золотар О. В. Прилади спостереження в екстремальних умовах: Навч. посіб. Київ: Нац. акад. внутр. справ України, 2003.

УДК 681.3.06

АННА ОЛЕКСАНДРІВНА ОСТРОВЕРХОВА

курсант 3 курсу факультету № 4

Харківського національного університету внутрішніх справ

АНАЛІЗ ПОПУЛЯРНИХ ПРОГРАМНО-АПАРАТНИХ ДЕВАЙСІВ ТА ГАДЖЕТІВ В ДІЯЛЬНОСТІ ПОЛІЦЕЙСЬКИХ

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Усі сфери суспільного життя та виробництва модернізуються за рахунок використання електронно-обчислювальних машин. Також для забезпечення ефективної діяльності Національної поліції України треба використовувати якомога більше сучасних програмно-апаратних девайсів та гаджетів спеціального призначення.

Девайс (device) – це самостійне, багатофункціональний програмно-апаратний пристрій, яке використовується в багатьох областях, призначене для виконання приватного, спеціального завдання (наприклад комп'ютер, ноутбук, планшет, смартфон, бортовий комп'ютер до автомобілю патрульної служби).

Гаджет (gadget) – це програмно-апаратний пристрій, створений в допоміжних цілях, для роботи якого можуть знадобитися додаткові пристрої. (електронний паспорт, електронні браслети, окуляри віртуальної реальності, натільна камера, розумні відеокамери, квадрокоптер).

Рівень оснащення поліції щороку зростає. Так в Україні впроваджують такі нові інструменти забезпечення діяльності: безготівкові термінали для сплати штрафів, бортові комп'ютерами до автомобілю патрульної служби, натільні камери та квадрокоптери. За словами міністра внутрішніх справ, основні переваги цих нововведень є скорочення часу заповнення протоколів, підвищення ефективності роботи поліції і мінімізації ризиків корупції. Для цього вводиться система "електронний протокол", що також є інструментом моніторингу добропорядності роботи поліцейського.

Встановлення бортових комп'ютерів до автомобілю патрульної служби дозволить поліцейським підключатись до бази даних та отримувати інформацію про вчинення раніше правопорушення та винесені рішення, аби правоохоронці одразу могли побачити всю історію конкретного автомобіля.

Портативні мобільні принтери друкуватимуть протоколи та виписки штрафів, задля уникнення розбіжностей та конфліктів між водієм та поліцейським.

Використання квадрокоптерів допомагає у потенційно небезпечних для ситуаціях (затримання озброєних осіб, рятувальні місії, патрулювання кордонів, розшук безвісно зниклих людей тощо), не ризикуючи життям та здоров'ям правоохоронців.

Сучасні іноземні департаменти поліції мають безліч пристроїв та інструментів, які можуть революціонізувати правоохоронні органи та сприяти підтримці громадської безпеки.

Носіння натільної камери, яка фіксує всі дії патрульного та громадянина набула широкого поширення в США за останній рік, після низки конфліктів між поліцейськими та жителями.

Сучасні комп'ютерні системи тепер можуть допомагати працівникам правоохоронних органів ефективно прогнозувати, де відбуваються злочини на основі геолокації.

Наприклад, державна поліція штату Пенсільванії нещодавно розробила технологію, яка аналізує тенденції вчинення злочинів та допомагає виявляти ймовірне вчинення злочинів.

Співробітники поліції використовують електронні портативні сканери, щоб миттєво відскановувати відбитки пальців та ідентифікувати осіб, які мають причетність до вчинення зареєстрованих злочинів. Завдяки миттєвому доступу до бази даних ці пристрої дають змогу пришвидшити отримання інформації про осіб.

До перспективних гаджетів застосування в Україні належить віртуальні (розумні) окуляри. Окуляри можуть робити фотографії, знімати відео в HD-якості і відображати деякі елементи на лінзах за допомогою технології доповненої реальності. Офіцери поліції в основному користуються функцією розпізнавання осіб, щоб проводити перевірки і звіряти документи.

Говорячи про запозичення досвіду зарубіжних країн в застосуванні супутникових навігаційних систем в першу чергу необхідно звернути увагу на практику застосування на Україні таких гаджетів як електронні браслети для стеження за обвинуваченими / підозрюваними.

Таким чином, аналіз популярних програмно-апаратних девайсів та гаджетів в діяльності поліцейських показав, що їх впровадження здійснюється відповідно до національних законодавств, направлено на забезпечення правопорядку з дотриманням конституційних прав громадян та підвищення ефективності діяльності поліцейських. Аналіз дозволив виділити найбільш актуальні для впровадження в Україні програмно-апаратних засобів: натільні відеокамери, розумні відеокамери, квадрокоптери, розумні окуляри з функцією розпізнавання особистості, електронні портативні сканери відбитків пальців та ідентифікації осіб.

УДК 007[732.214]

ЯРОСЛАВ АНДРІЙОВИЧ ЧЕРКАШЕНКО

рядовий поліції курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ

КІБЕРВІЙНА ТА ІНФОРМАЦІЙНИЙ ВПЛИВ НА СУСПІЛЬСТВО

В умовах глобальної і тотальної інформатизації, коли суспільство стало залежним від інформаційних систем, політичні і військові еліти стали застосовувати віртуальний вплив на людей, приховано, а інколи й відкрито. Настав час війни не на полі бою, а в мережі Інтернет, та витрати на такий засіб бою потребується менш. При цьому ефективно проводити дезінформацію компаній, виявляти та контролювати громадську думку, направляти соціальні групи на певні дії дозволяють соціальні мережі.

Недооцінювання та нехтування тою чи іншою державою питань власної кібербезпеки й інформаційного домінування може спричинити не лише суттєві матеріальні збитки через втрату або спотворення стратегічної важливої інформації, а й можливі техногенні катастрофи, збитки цивільної, фінансової та військової інфраструктури аж до втрати суверенітету держави.

Мережева війна – це спосіб ведення конфліктів, коли її учасники застосовують мережеві форми організації, доктрини, стратегії та технології, пристосовані до сучасної інформаційної доби.

З іншого ж боку на сьогоднішній день більшість держав вже приділяють захисту від кібервійни належну увагу: виділяють необхідні кошти для організації систем захисту і підтримання спеціальні підрозділи, основним завданням яких є вдосконалення кібербезпеки країни та захисту від нападів.

[2] У кібервійні часто неможливо визначити не тільки учасників, час її початку і завершення, а й важко довести у багатьох випадках сам факт застосування руйнівної кіберзброї, не кажучи вже про шпигунське програмне забезпечення. За своїми наслідками застосування кіберзброї під час наступальних операцій в електромагнітному спектрі можна порівняти із втратами від застосування зброї масового ураження. Зокрема, використання кіберзброї може бути замасковано під техногенні катастрофи чи системні збої в системі комп'ютерних мереж і сервісів тощо. Так, прикладом, 23 грудня