УДК 681.3

СУСПІЛЬНО НЕБЕЗПЕЧНІ ДІЇ З ВИКОРИСТАННЯМ СТІЛЬНИКОВИХ ТЕРМІНАЛІВ

Вячеслав Шорошев, Микола Несторенко*
НДІ НАВС України, НДІ ІТЦ НАВС України

Анотація: **Розглянуто суспільно небезпечні дії, які мають місце при масовому застосуванні комп'ютерних технологій і стільникових терміналів та шляхи боротьби з ними з урахуванням світового досвіду.**
Summary: **Are considered общественно dangerous actions, which take place at mass application of computer technologies and cellular terminals, and also way of struggle with them in view of world(global) experience.**
Ключові слова: **Стільниковий термінал, телефон, телекомунікації, загрози, блокування.**

I Вступ

Розвиток сучасних передових телекомунікаційних та інформаційних технологій – безсумнівно прогресивний фактор, водночас створює і багато проблем правоохоронним органам України щодо попередження і розкриття злочинів з використанням цих прогресивних технологій. Це також потребує від органів виконавчої та законодавчої влади відповідних упереджених змін нормативно-правових засад в частині кримінально-процесуального визначення таких злочинів для розширення можливостей правоохоронних органів у боротьбі зі злочинами з використанням таких технологій. Набуває також все більшої актуальності гармонізація законодавчих та нормативних актів провідних країн світу під вимоги узгоджених міжнародних конвенцій, стандартів ISO/IEC тощо щодо злочинів з використанням передових інформаційних та телекомунікаційних технологій. Це, насамперед, суспільно небезпечні дії з комп'ютерними даними і системами та з використанням мобільних телефонів.

Так, з 2001 року Радою Європи запропонована Конвенція про кіберзлочинність, дотримання вимог якої країнами, які її підписують та ратифікують, відкриває нові шляхи у боротьбі проти кіберзлочинності шляхом міжнародного співробітництва. Україна з 2001 року сумлінно виконує вимоги цієї Конвенції.

У грудні 2004 року Верховною Радою України прийнято закон про внесення змін до Кримінального та Кримінально-процесуального кодексів щодо злочинів з використанням електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку за статтями КК 361, 361^1, 361^2, 362, 363, 363^1.

Аналогічні проблеми характерні для правоохоронних органів усіх провідних країн світу і мають, на наш погляд, досить актуальне значення щодо попередження та розкриття злочинів з використанням передових телекомунікаційних та інформаційних технологій, зокрема, визначення суспільно небезпечних дій з використанням мобільних телефонів мереж стільникового електрозв'язку за досвідом провідних країн світу.

II Основна частина

Охорона посольств, урядових організацій та інших об'єктів інформаційної діяльності пропонує відвідувачам виключити при вході свої мобільні (стільникові) телефони і залишити їх у спеціально виділеному приміщенні.

Мобільний телефон із вбудованим цифровим диктофоном без усякої модифікації може використовуватися для зняття інформації з об'єкта (наприклад, для запису розмови або її трансляції).

Потенційно небезпечні також апарати з вбудованими фотокамерами. Донедавна вони не дозволяли фотографувати документи, але тепер з'явилися цифрові камери з матрицею на 1,3 – 2 мегапікселя. Цього досить, щоб непомітно зробити якісний знімок текстового документа або об'єкта контролю і передати відеозображення за допомогою MMS повідомлення.

Фототелефони з мегапіксельними камерами вперше з'явилися на азіатських ринках. На виставці CTIA Wireless 2004 були анонсовані сім нових моделей трубок. Серед компаній, що представили мегапіксельні фототелефони, – Audiovox, Kyocera, LG, Nokia, Samsung, Sony Ericsson і Motorola. Серед представлених на виставці фототелефонів – моделі LG8000, Motorola V710 і A840, Sony Ericsson S700, Nokia 7610 і Samsung SGH-P735. Ці фототелефони можна розглядати як повноцінний інструмент для цифрової зйомки.

Використання мобільних телефонів з камерами в офісах і громадських місцях викликає чимало побоювань як серед борців за недоторканність приватного життя, так і у фахівців з інформаційної безпеки. Фототелефони можуть сприяти витокам важливої інформації. Багато компаній вже намагаються

заборонити використання таких телефонів у службових приміщеннях, особливо в науково-дослідних і виробничих підрозділах. На сьогодні, на заводах LG Electronics, Siemens та Samsung заборонено використовувати телефони з вбудованими цифровими камерами.

В роздягальнях спортивних клубів (в інших місцях та ситуаціях), де використання апаратів не забороняється, розширюються можливості для зловживань. Людина із сумнівними етичними принципами може одержати фотографії (у телефонах наступного покоління є можливість зйомки невеликих відеороликів) інших людей у напівроздягненому або роздягненому виді без дозволу з їх боку. Можливості сучасних апаратів дозволяють відправити зображення буквально в режимі реального часу і опублікувати фото в Інтернеті та видалити фотографію з пам'яті апарата.

У США запропонований на розгляд Конгресу закон, що забороняє одержання і поширення відеозаписів, фільмів або фотографій оголених людей або осіб у нижній білизні скрізь, де ця особа може обґрунтовано думати, що може роздягнутися, не виставляючи себе на огляд. Забороняється також прихована зйомка частин тіла, що не передбачалися виставляти на огляд, поза залежністю від того, знаходиться особа в громадському місці або в приватній обстановці. За порушення передбачається штраф або тюремне ув'язнення терміном до одного року.

Треба відзначити, що з даною проблемою в США борються вже давно. У двадцяти штатах США заборонено проведення прихованої відеозйомки. Кілька штатів поширило діючу заборону також і на знімки, одержані за допомогою камер мобільних телефонів. В штатах Айова, Каліфорнія і Меріленд відносно останніх прийняті окремі закони. В штаті Айова взагалі заборонено знаходитися з мобільними телефонами, оснащеними цифровими камерами, в місцях, де люди можуть зазвичай оголюватися.

Мобільні телефони з камерами заполонили Америку. У 2004 році їх було продано біля шести мільйонів. Найближчим часом очікується двох-триразовий ріст обсягу продажів. До 2006 року більше 80% усіх мобільних телефонів, що поставляються в США і Західну Європу, будуть оснащені камерами. За прогнозами аналітиків Meta Group, протягом наступних п'яти років у користуванні буде знаходитися близько 1 млрд. одиниць телефонів.

Ввести повну заборону на одні лише телефони з камерами, без огляду на весь спектр інших високотехнологічних пристроїв для запису і передачі інформації, було б недостатньо, та й здійснити це на практиці досить складно. В деяких країнах уже заборонено використовувати подібні пристрої в громадських місцях – таких, як басейни і роздягальні.

В Японії власники книгарень намагаються обмежити використання фототелефонів, за допомогою яких покупці знімають сторінки в журналах, що сподобалися. В Китаї влада заборонила військовослужбовцям країни будь-де користуватися мобільними телефонами і пейджерами. Ці міри направлені на забезпечення безпеки секретної військової інформації.

Міністр оборони США Дональд Рамсфелд у травні 2004 року заборонив використовувати на території військових об'єктів мобільні телефони з вбудованими фотокамерами, відеокамерами і цифрові фотоапарати. Однією з причин було те, що саме такою апаратурою була зроблена частина фотознімків, які зображують катування іракських полонених американськими військовослужбовцями.

На вимогу міністерства телекомунікацій Південної Кореї виробники стільникових телефонів зобов'язані забезпечувати телефони з вбудованою камерою сигнальним пристроєм, який супроводжує зйомку звуковим сигналом (не менше 65 децибел). Ця функція не повинна бути відключена за бажанням власника телефону.

Влада Саудівської Аравії прийняла рішення конфісковувати у населення мобільні телефони з вбудованими відеокамерами, якщо зйомка ведеться в громадських місцях.

Засоби протидії використанню мобільних телефонів у визначеній зоні вже декілька років присутні на світовому ринку – від пристрою розміром з мобільний телефон (з радіусом дії декілька метрів) до пристрою, що може блокувати сигнали стільникових телефонів у радіусі до сотні метрів. Серед них вироби США, Англії, Росії, Ізраїлю, України та ін.

Одному з перших дзвінки стільникових телефонів набридли королю Йорданії, які заважали йому молитися. На його замовлення американська фірма Image Sensing Systems за два тижні виготовила пристрій, що блокує стільникові телефони в покоях палацу [1]. Подібним способом вирішили проблему й у Великобританії, де в залах королівського палацу недоречно лунали дзвінки мобільних телефонів численної прислуги. На сьогодні є значний попит на подібні пристрої в середньоазіатських країнах, де вони використовуються для блокування стільникових телефонів у храмах і мечетях. У Франції розглядається закон, який дозволить встановлення систем блокування мобільних терміналів у бібліотеках і музеях.

Виробники електронної техніки продовжують створювати нові і нові моделі систем блокування. Приміром, компанія Image Sensing Systems розробила пристрій Mobile Blocker [2]. Цей невеликий прилад

(з пультом дистанційного керування) дозволяє блокувати стільникові телефони і пейджери в радіусі 40 м. Радіовипромінювання пристрою Mobile Blocker набагато менше, ніж звичайного стільникового телефону. Американська фірма BlueLinx розробляє електронний пристрій, здатний автоматично відключати в межах визначеного простору дзвоники трубок [3]. Компанія Zetrorі реалізує прилади, що виявляють стільникові апарати в радіусі 30 м [4]. Вони можуть оповістити охорону або зачитають звертання до власника трубки з проханням залишити її поза межами об'єкта, що охороняється.

Новітні системи зв'язку в злочинних цілях використовуються при організації терористичної діяльності, комп'ютерної й організованої злочинності, корупції, при незаконному обігу наркотичних засобів, контрабанді тощо.

З'явились злочини, направлені проти операторів та користувачів стільникових мереж [14].

Глобальний характер сучасних телекомунікаційних систем зв'язку, величезні обсяги інформації, що в них циркулює, обумовлюють необхідність зміни традиційних поглядів на проведення окремих оперативно-розшукових заходів.

Масове використання мобільних телефонів крім зручностей несе і безліч проблем та є джерелом загроз. На сьогодні людина з мобільним телефоном не викликає акцентованої до себе уваги і підозри. При проході крізь рамку металодетектора мобільний телефон прийнято проносити з зовнішньої сторони. Під його прикриттям можливо пронести будь-який предмет, включаючи зброю. Вперше був конфіскований у жовтні 2000-го року голандськими поліцейськими тризарядний пістолет у формі мобільного телефону (ствол у вигляді антени, постріл проводиться натисканням визначених кнопок на панелі набору номера) [5]. Пізніше цю зброю органи правопорядку знаходили в Німеччині і Великобританії. Останнє повідомлення про вилучення телефонів-пістолетів датується січнем 2004 року. Вироблений у Хорватії, пістолет зовні не відрізняється від телефону, але важить помітно більше. Відстрілює дрібнокаліберні патрони. У спорядженій зброї три патрони, кожний з яких розміщується у своєму стволі. Один з них замаскований під антену.

Мобільний телефон може бути використаний як програмований або дистанційно керований пристрій для здійснення терористичного акту. Замість вібратора мобільного телефону включається електродетонатор вибухового пристрою. Вибух відбувається після виклику на мобільний телефон, одержання SMS повідомлення або з використанням таймера, який є його сервісною функцією. Мобільні пристрої виявилися ідеальними детонаторами бомб, що дозволяють зробити їх активацію в будь-який момент часу з безпечної відстані.

До однієї з бомб, що вибухнули в Балі в жовтні 2002 року, був приєднаний мобільний телефон - як і при вибуху замінованого автомобіля в готелі мережі Маріотт у Джакарті в серпні 2003 року, при якому загинуло 12 чоловік.

Приміром, при вибухах у Мадриді 11 березня 2004 року вибухові пристрої були приведені в дію за допомогою вмонтованих будильників мобільних телефонів. Так, припускається, що дзвінок на мобільний телефон, захований у рюкзаку з вибухівкою, привів до вибуху в Єврейському університеті в Єрусалимі, при якому загинуло сім чоловік [6].

11 серпня 2004 року в м. Севастополі, на вулиці Кисаева 14, у дворі житлового будинку пролунав могутній вибух. Підірвали саморобний пристрій, начинений великою кількістю цвяхів. За повідомленням начальника УМВС України в місті Севастополі Віталія Маликова знайдено залишки мобільного телефону. Визначена приблизно його марка і встановлено, що це дійсно був замах. Аналогічні факти мали місце в інших регіонах, коли підривали вибуховий пристрій за допомогою мобільного телефону. Був визначений тип вибухового пристрою, в еквіваленті він складав 1250 грамів тротилу [7].

20 серпня 2004 року в Києві на ринку "Троєщина" сталися два вибухи, внаслідок яких постраждало 14 осіб. До лікарні було госпіталізовано 11 осіб, одна із постраждалих померла в лікарні. Згідно з повідомленнями мас-медіа з посиланням на Центр громадських зв'язків МВС України, саморобні вибухові пристрої були приведені в дію за допомогою стільникових телефонів [8, 9].

Узагальнимо чинники, що визначають застосування терористами мобільних телефонів: активацію бомби можна виконати з безпечного місця; простота пристосування телефону для активації вибухового пристрою; анонімність придбання у великій кількості телефонів та SIM-карт; можливість застосування різних способів активації бомби (радіоканалом, вбудованим таймером, із застосуванням часової затримки та ін.); анонімність застосування; відносна дешевизна; швидка можливість зміни номера та оператора зв'язку шляхом заміни SIM-карти, що підвищує конспіративність застосування; складність визначення і прийняття заходів протидії правоохоронними органами та ін.

Можливе розміщення вибухівки у внутрішній частині телефону (в акумуляторі) і підміни останнього. Так зробили ізраїльські спецслужби для знищення терориста Яхьи Айаша в 1996 році.

Усередині корпусу телефона можливо помістити практично будь-яку апаратуру: для перехоплення

даних з безпровідної комп'ютерної мережі, для аудіо та відеоконтролю приміщення та ін. [10].

Для блокування мобільних терміналів застосовуються генератори шуму, що створюють радіочастотні завади і не дозволяють телефону зв'язатися з базовою станцією. Дальність придушення залежить від розташування приміщення стосовно базової станції і потужності генератора завад. Такий генератор повинен створювати шумовий сигнал тільки в діапазоні роботи засобів мобільного зв'язку і не створювати завад іншим пристроям.

Існують моделі з функцією виявлення стільникових телефонів, що реалізується за допомогою приймача сигналів стільникового зв'язку, який включає генератор на короткий час, тим самим порушуючи протокол обміну між телефоном і базовою станцією. Інтелектуальний блокатор забороняє роботу мобільних телефонів, які знаходяться в заданій зоні. Телефон при цьому залишається на обслуговуванні в мережі.

Застосовуються пристрої, що використовують функцію виявлення телефону та сповіщення оператора стільникового зв'язку про те, що даний телефон знаходиться у виділеній зоні. Оператор автоматично забороняє здійснення вхідних викликів доти, поки телефон не вийде з цієї зони.

Для пасивного блокування стільникового зв'язку застосовуються спеціальні електромагнітні панелі (Faraday Cage), що екранують приміщення, розроблені японським інженером Хайдео Ока (Hideo Oka) [11]. Дерев'яні панелі з тонкими пластинами з нікель-цинкового сплаву блокують до 97% випромінювання. Такі панелі вже використовуються в США та інших країнах, де заборонено використання активних генераторів шуму.

Існують маяки, які використовують технологію Bluetooth або IR-порт для автоматичного блокування будь-якого сумісного телефону [12].

В авіації тільки деякі компанії мають Інтернет і стільникові шлюзи на своїх літаках - інші, навпаки, вимагають відключення стільникових телефонів під час польоту та проводять організаційно-технічні заходи з недопущення застосування мобільних телефонів на борту. Вони здатні створювати завади радіоелектронним пристроям лайнера. Не підкоряються вимозі не користуватися стільниковими телефонами за статистикою близько 10% пасажирів. Головну ж небезпеку становить використання мобільного терміналу як ініціюючого засобу для здійснення терористичного акту. Для блокування мобільних телефонів на борту авіалайнера може застосовуватися пристрій норвезької компанії ICE International [13].

У Великобританії і США використання подібних пристроїв рядовими громадянами заборонено законом. За цей злочин у США передбачений штраф понад $11000. Урядові органи у цих країнах вже використовують системи блокування мобільних терміналів.

У Росії, наприклад, використання будь-яких радіовипромінювальних пристроїв без дозволу на експлуатацію категорично заборонено. Одержати дозвіл на використання засобів блокування мобільних телефонів можуть тільки спецслужби, що застосовують їх переважно в боротьбі з терористами. Потужні широкосмугові генератори використовуються фахівцями при знешкодженні радіокерованих вибухових пристроїв (в тому числі і блокування стільникових телефонів, пристосованих для дистанційного підриву бомб).

За повідомленнями преси, подібний пристрій, встановлений у машині президента Пакистану Мушаррафа, дозволив запобігти підготовленому на нього замаху в грудні 2003 року.

Пентагон, наприклад, планує блокувати мобільні телефони в бойових умовах. Технологія Wolfpack дозволить запобігти використанню всіх засобів радіозв'язку противником.

За впровадження подібних пристроїв у життя виступають власники і відвідувачі театрів, концертних залів, ресторанів і інших установ, де дзвоники мобільного телефону здатні заподіяти незручність. Так, приміром, починаючи з минулого року канадська компанія Industry Canada проводить консультації щодо блокування стільникових телефонів у різних громадських місцях – від екзаменаційних кімнат до електростанцій, де використання стільникових телефонів заборонено з метою безпеки.

У більшості країн блокування стільникових телефонів є незаконним. Втім, обговорюються юридичні норми, що дозволили б громадянам заборонити використання мобільних терміналів у визначених зонах. Тому є необхідність подальшого удосконалення законодавчого та нормативно-правового регулювання щодо застосування сучасних високотехнологічних пристроїв для запису і передачі інформації.

Виробники стільникових телефонів і оператори стільникового зв'язку, навпаки, виступають проти ідеї блокування, мотивуючи це тим, що від можливості подзвонити може залежати життя і здоров'я людини. Так, відповідно до офіційної статистики, у 2001 році в канадську Службу порятунку 911 з мобільних телефонів надійшло близько 3 млн. дзвінків.

Інформація, передана за допомогою мобільних телефонів у перші години захоплення терористами глядачів мюзиклу “Норд-Ост” у Москві, допомогла спецслужбам зорієнтуватися в ситуації в той час, коли інформація була суперечлива і розрізнена.

III Висновки

1. Суспільно небезпечні дії з використанням мобільних телефонів визначаються потенційною загрозою, яка все більше має місце при масовому застосуванні стільникових терміналів. Тому напрямки боротьби з ними, безсумнівно, потребують урахування кращого світового досвіду і в нормативно-правовому забезпеченні діяльності правоохоронних органів України.

2. Новітні системи зв'язку в злочинних цілях використовуються при організації терористичної діяльності, комп'ютерної й організованої злочинності, корупції, при незаконному обігу наркотичних засобів, контрабанді тощо. Найбільшу загрозу набуває застосування терористами мобільних телефонів як ініціюючого засобу вибухового пристрою.

3. Ситуації, що виникають при масовому застосуванні сучасних мобільних терміналів і їх сервісних можливостей, потребують упередженого удосконалення законодавчого і нормативно-правового регулювання щодо застосування сучасних високотехнологічних пристроїв для запису та передачі інформації.

*Література: **1**. http://www.imagesensing.com/. **2**. http://www.mobileblocker.com/. **3**. http://www.bluelinx.com. **4**. http://www.zetron.com. **5**. http://www.megafon.com.ru. **6**. http://www.cnews.ru/. **7**. http://www.ictv.ua/content/publications/ukraine/. **8**. http://www.podrobnosti.ua/projects/vovremya/2004/11/01/159384.html/ **9**. http://www.unian.net/ukr/. **10**. Технические средства безопасности. Каталог ЗАО "SET-1" 2002. Сотовый телефон – портативный аудиовидеопередатчик в сотовом телефоне Ericsson. //http://www.set-1.ru/. **11**. http://www.mobile.news.ru. **12**. http://www.media.mit.edu/wearables/mithril/phone/. **13**. http://www.iceinternational.com. **14**. Алексей Марченков, Ярослав Бурыгин. Системы защиты от мошенничества и меры по предупреждению мошенничества в области сотовой телефонной связи // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. – Випуск 6. – К.: ПП "ЕКМО", 2003. – С. 112-120.*

УДК.621.791

КОМПЛЕКСЫ ВИБРОАКУСТИЧЕСКОЙ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТЕЧЕСТВЕННОГО ПРОИЗВОДСТВА

Владислав Галанский, Николай Ващенко, Теодор Королев, Александр Лаврентьев, Игорь Порошин, Александр Сигаев
НИЦ "ТЕЗИС" НТУУ "КПИ"

Аннотация: **Приводится анализ, сравнительные испытания и рекомендации по применению некоторых комплексов защиты речевой информации, производимых и/или сертифицированных в Украине.**
Summary: **The analysis, comparative testings and recommendations on application of some complexes of protection of the speech information, made and - or certificated in Ukraine.**
Ключевые слова: **Защита речевой информации, генераторы шума, виброизлучатели.**

Виброакустическая защита от перехвата речевой информации является одним из основных и обязательных элементов защиты выделенных помещений. А поскольку профессиональный съем речевой информации с конструктивных элементов объекта в подавляющем большинстве случаев обнаружить практически невозможно (особенно при использовании средств дистанционного съема информации), проблема совершенствования средств защиты остается и будет оставаться актуальной не только в ближайшем, но и в отдаленном будущем.

Принимая во внимание разнообразие и постоянное совершенствование электронных средств съема речевой информации с конструктивных элементов защищаемых объектов, разработчики комплексов защиты, в свою очередь, также пытаются создавать и совершенствовать устройства противодействия, представляющие собой генератор шума в комплекте с виброизлучателями. Эта тенденция прослеживается при анализе обширного рынка комплексов защиты. К примеру, сегодня потенциальный пользователь имеет возможность выбора из порядка сотни комплексов виброакустической защиты (включая устройства производства стран дальнего и ближнего зарубежья, а также устройства украинских разработчиков и производителей) стоимостью от 300 до 2000 у. е.