УДК 681.3.06

С.Л. Ємельянов,
кандидат технічних наук, доцент

СИСТЕМАТИЗАЦІЯ МЕТОДІВ ТА ЗАСОБІВ ПРОТИДІЇ СКРИТОМУ АУДІО- ТА ВІДЕОЗАПИСУ

Систематизовано методи та засоби захисту від негласного аудіо- та відеозапису, розглянуто особливості їх використання.

Ключові слова: *диктофон, відеокамера, детектор диктофонів, детектор відеокамер, подавлювач диктофонів, оперативно-розшукова діяльність.*

Систематизированы существующие методы и средства защиты от негласной аудио- и видеозаписи, рассмотрены особенности их применения.

Ключевые слова: *диктофон, видеокамера, детектор диктофонов, детектор видеокамер, подавитель диктофонов, оперативно-розыскная деятельность.*

Methods and means for the protection from non-official audio- and video recording are systemized; pecularities of its application are considered.

Keywords: *voice recorder, video camera, voice recorders detector, video camera detector, voice recorders suppressor, operatively-search activity.*

Досягнення сучасної радіоелектроніки, зокрема мініатюризація та застосування цифрової обробки сигналів, сприяли поширенню різноманітних засобів негласного (прихованого) отримання інформації, серед яких – скритий аудіозапис на диктофони (Д) як спосіб документування мовної інформації, а також перехоплення і фіксація відеозображення об'єкта спостереження за допомогою мініатюрних відеокамер (ВК) [1–3].

Вказані засоби (Д і ВК), як правило, не відносять до "*атакуючої техніки*" (спеціальних технічних засобів), придбання якої передбачає наявність у суб'єкта прав (ліцензії) на здійснення оперативно-розшукової діяльності (ОРД), адже вони перебувають у вільному продажі і можуть застосовуватися для негласного знімання інформації з виділених приміщень об'єкта технічною (агентурною) розвідкою іноземних країн, злочинними угрупованнями, окремими правопорушниками та суб'єктами ОРД.

Тому досить *актуальною проблемою* є дослідження сучасних методів та засобів протидії негласному знімання аудіо- та відеоінформації.

Загальні питання, насамперед технічного захисту мовної та відеоінформації від витоку технічними каналами, у тому числі штучно створеними за допомогою сучасних засобів скритого аудіо- та відеозапису (ЗСАВ), розглядались російськими [1–2; 4] та вітчизняними [5; 6] науковцями.

Так, у низці останніх досліджень та публікацій аналізувалися проблемні аспекти виявлення та подавлення сучасних Д [7–10] та ВК [11], а також правові аспекти використання ЗСАВ [12; 13].

Нормативно визначено [14, Ст. 1], що захист інформації – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Тому *раніше не вирішеною частиною проблеми* є систематизація та порівняльний аналіз усіх можливих методів та засобів протидії ЗСАВ.

Метою статті є систематизація сучасних методів та засобів протидії ЗСАВ та висвітлення особливостей їх використання.

На нашу думку, усі наявні методи та засоби протидії ЗСАВ доцільно розділити на чотири великі групи, що утворюють окремі (самостійні) напрями захисту (рис. 1).

Перша група спрямована на перешкоджання спробі внесення ЗСАВ у виділені приміщення, яка заснована на застосуванні організаційно-режимних заходів (заборона, контроль маршрутів пересування відвідувачів, догляд особистих речей, візуальне спостереження за відвідувачами та ін.), а також на використанні універсальних методів і засобів виявлення ЗСАВ (візуальний огляд, металодетектування, нелінійна локація, рентгеноскопія та ін.).

Ці методи та засоби добре відомі [1–2; 4–6] та є спільними для виявлення будь-яких електронних засобів негласного отримання інформації.

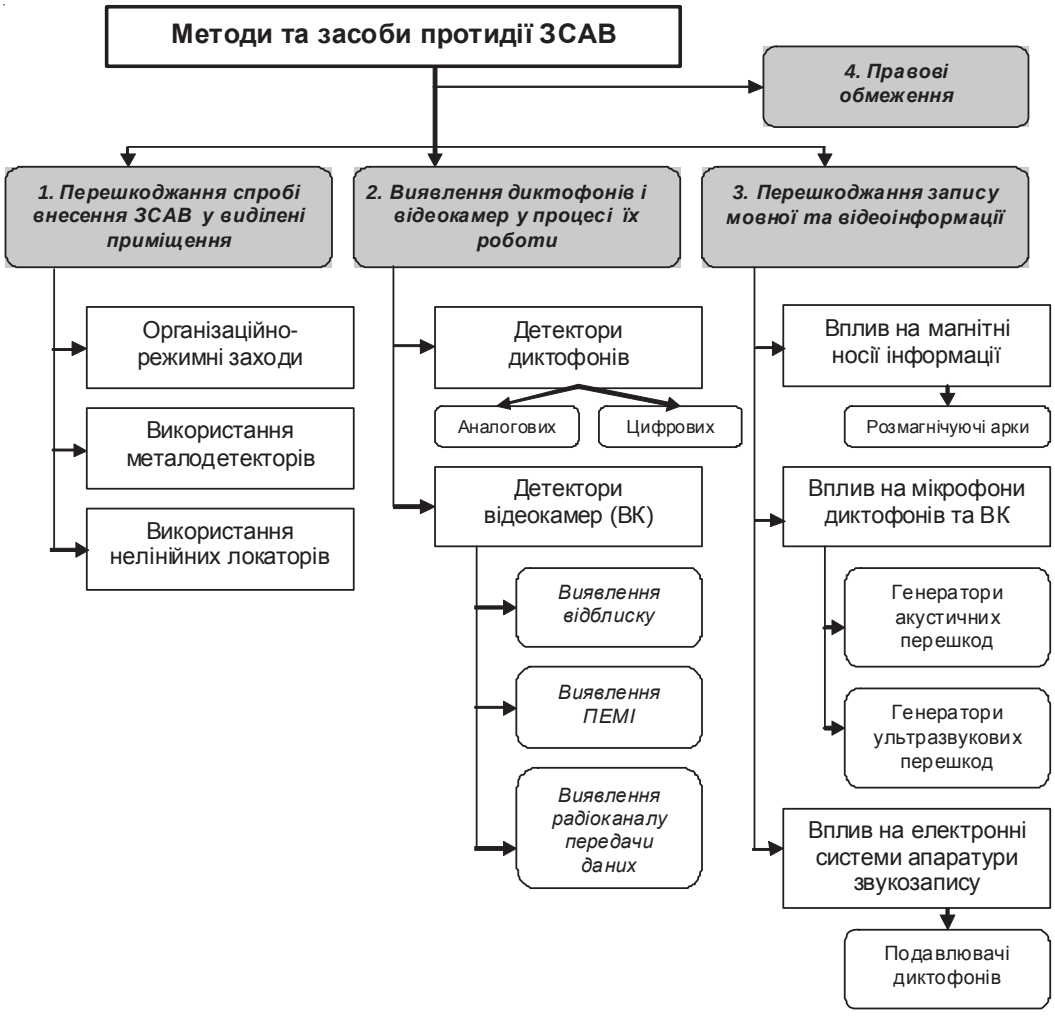

Рис. 1. Класифікація методів та засобів протидії ЗСАВ

Зазначимо, що рішення задачі захисту від несанкціонованого знімання аудіо-, відеоінформації шляхом перешкоджання спробі внесення цих засобів в приміщення, що захищаються, на основі універсальних (досить дорогих) засобів пов'язане з істотними труднощами, зумовленими як мініатюрними розмірами сучасних цифрових накопичувачів, можливістю їх камуфляжу під особисті речі, так і юридичними і морально-психологічними нюансами огляду поклажі і особистих речей відвідувачів.

Друга група методів та засобів (рис. 1) заснована на виявленні прихованих Д і ВК за їх демаскуючими ознаками, що виникають безпосередньо в процесі роботи цих ЗСАВ в приміщенні, що захищається.

Аналогові (кінематичні) Д мали суттєві демаскуючі ознаки – випромінювання електродвигуна (ЕД) та генератора стирання та підмагнічування (ГСП), яке й використовували перші портативні детектори диктофонів (ДД) типу TRD–800 (REI, США) або RM–100 (Росія). Дальність виявлення аналогових Д не перевищувала декількох метрів.

Проте сучасна малогабаритна апаратура цифрового звукозапису, у тому числі із записом оцифрованого аудіосигналу в напівпровідниковій пам'яті, не містить у складі ЕД та ГСП. Але й вона має свої демаскуючі електромагнітні випромінювання, джерелом яких в загальному випадку можуть бути (залежно від типу цифрового Д): імпульсний перетворювач напруги; дротяний шлейф знімної флеш-пам'яті; спеціалізований сигнальний процесор; рідкокристалічний дисплей; сполучні кабелі додаткових аксесуарів тощо.

Але виявлення таких слабких НЧ – випромінювань цифрових Д на фоні паразитних шумів від магнітних полів струму промислової частоти (220 В, 50 Гц) і її гармонік, а також побічних електромагнітних випромінювань і наведень (ПЕМВІН) від працюючої оргтехніки (ПК, телефони, телефакси, копіювальна техніка, різні електропобутові прилади тощо), виявилося досить складним науково-технічним завданням [6,7].

Тому зараз ДД (PTRD-018, ST-0110 тощо) являють собою складні апаратно-програмні комплекси, які використовують сукупність сучасних технологій цифрової обробки, зокрема: спектральний аналіз сигналів в N-мірному просторі; адаптацію до складної електромагнітної обстановки (ЕМО); розпізнавання подій (включення Д) за шаблонами ЕМО; багатоканальну адаптивну фільтрацію сигналів на фоні перешкод тощо.

Проте установка такої апаратури і робота з нею – досить складне завдання. Ефективність роботи таких ДД багато в чому залежить від конкретної ЕМО об'єкта, що захищається. Окрім цього, вірогідність виявлення диктофонів залишає бажати кращого, а вартість приладів сягає 4000 дол. США. Таким чином, спеціальні ДД при усіх своїх перевагах мають один істотний недолік – невелику дальність виявлення Д. Реальна відстань, на якій можна виявити типові цифрові Д, для таких пристроїв близько 30–50 см для Д у пластмасових корпусах і 2–10 см для Д у металевому корпусі [17].

Основні способи виявлення ВК у процесі їх роботи в приміщенні, що захищається (рис. 1):

– прийом відблиску спеціально сформованого лазерного променя від оптичної частини ВК;

– прийом ПЕМВІН від генераторів синхро(тактових) імпульсів камерної голівки ВК;

– виявленні ВЧ-випромінювання радіоканалу передачі даних від ВК (якщо такий використовується у системі відеоспостереження [18]).

Оптичні детектори ВК, що реалізують *перший з вказаних способів,* працюють на основі оптичної локації (ефекті світловідбиття). Оскільки усі оптичні прилади спостереження містять світлочутливий елемент (наприклад, ПЗС-матрицю), промінь, спрямований на цей елемент, відіб'ється від нього і повернеться назад до джерела, тобто до детектора ВК. Причому відбите випромінювання поширюється у вузькому куті і точно в напрямі на зондуючий випромінювач (при однопозиційній локації).

Слід зауважити, що реальна дальність виявлення ВК (захованих в одязі, сумках, різних упаковках, стелях, стінах, усередині електромагнітного екрана та ін.) залежить від типу підсвічування (імпульсний або безперервний), наявності або відсутності підстроювання по діоптріях, гостроти зору оператора, освітленості приміщення, в якому проводиться огляд, ряду інших чинників і може складати від 2 до 10 м [11].

Безперечною перевагою таких детекторів, окрім простоти застосування, відносної дешевизни є можливість виявлення будь-яких типів ВК (проводових і безпровідних, закамуфльованих, з винесеною зіницею входу, вимкнених в даний момент і так далі), що витікає з суті цього способу виявлення.

З іншого боку – вже придумані засоби протидії оптичним детекторам – спеціальні світлофільтри для відсіювання світлових хвиль, що мають певну довжину. Слід врахувати також, що оптичні детектори ВК не здатні вести прихований (непомітний для оточення) пошук.

Другий спосіб виявлення працюючих ВК заснований на прийомі й аналізі випромінювань осцилятора, що входить до складу процесора, який опитує регістри ПЗС-матриці, і, відповідно, випромінює на якійсь фіксованій частоті та її гармоніках. Дальність дії електромагнітних детекторів ВК залежить в основному від типу камери і від того, як камера випромінює, та складає у середньому 7–10 м. Час пошуку для електромагнітних Д більшою мірою залежить від кількості типів ВК (шаблонів), внесених до пам'яті Д. Сучасні електромагнітні Д здатні вести пошук ВК практично непомітно для оточення: в більшості з них існує світлова, звукова і вібраційна індикація. Є також прилади, оснащені антеною прихованого носіння, що дозволяє вести пошук максимально непомітно.

У разі наявності у ВК радіоканалу передачі даних можливий *третій спосіб* виявлення працюючих ВК на основі прийому радіовипромінювань передавача, що лежать в діапазоні 0,8–2,4 ГГц. Його реалізація пов'язана із застосуванням детекторів (індикаторів) поля, а також мобільних або стаціонарних скануючих приймачів, особливості побудови і роботи яких розглянуто у [4–6; 18].

Третя група методів протидії ЗСАВ (рис. 1) заснована на перешкоджанні запису мовної та відеоінформації на певні носії.

Так, у часи застосування у ЗСАВ магнітних стрічок, на яких записувалася аудіо- та відеоінформація, використовувалася *розмагнічувальна арка*, яка встановлювалася в прорізі дверей і створювала потужне змінне магнітне поле (зазвичай з частотою мережі або їй кратною).

Такі пристрої характеризуються високим енергоспоживанням і досить небезпечні для здоров'я. Тому організація, що застосовує такі системи, зобов'язана інформувати відвідувачів про наявність небезпеки, що є демаскуючим чинником

для захисту [16]. Крім того, сучасні цифрові ЗСАВ не містять магнітної стрічки (плівки), тому зараз цей спосіб протидії малоефективний.

Більш ефективним є створення в приміщенні активних перешкод, що безпосередньо впливають на мікрофонні пристрої ЗСАВ, в акустичному або ультразвуковому діапазоні хвиль (рис. 1) [18; 19].

Переваги акустичних генераторів полягають в тому, що вони подавлюють будь-яку підслуховуючу апаратуру, у складі якої є мікрофон. Недолік – акустичні перешкоди чутні, заважають розмові і демаскують роботу апаратури захисту. При усіх своїх недоліках цей спосіб є набагато менш витратним, безпечнішим і надійнішим способом збереження конфіденційності переговорів у порівнянні із засобами виявлення диктофонів. Доцільно його застосовувати обмежено, у випадках, коли вимагається максимальна захищеність мовної інформації.

Системи ультразвукового подавлення (наприклад, прилад "Завіса") випромінюють потужні, нечутні людським вухом ультразвукові коливання (зазвичай частота випромінювання близько 20 кГц), що впливають безпосередньо і на мікрофони диктофонів, і на акустичні закладки, що є їх безперечною перевагою. Ця ультразвукова дія призводить до значних спотворень записуваних (передавальних) аудіосигналів, часто до рівня, коли вони не піддаються подальшому дешифруванню.

Хоча спроби створити ефективні перешкоди в ультразвуковому діапазоні частот тривають, у багатьох дослідних зразках подібних систем інтенсивність ультразвукового сигналу виявляється вище за допустимі медичні норми дії на людину. При зниженні інтенсивності ультразвуку неможливо надійно подавити записувальну апаратуру. Тому відмінними рисами таких систем подавлення є: необхідність роботи в замкненомк просторі, шкідливість для здоров'я людини, ви-сока вартість.

Останніми роками також були розроблені спеціальні подавлювачі диктофонів (ПД), активні маскувальні перешкоди від яких впливають безпосередньо на звукозаписувальні ланцюги ЗСАВ ("Сапфір", "Буран", "Рамзес-Дубль", "Шумотрон" тощо).

Сучасний ПД є генератором електромагнітного випромінювання досить високої потужності, що працює в діапазоні НВЧ. Як правило, такі генератори радіоперешкод мають відносно вузьку смугу випромінювання, що мінімізує влив створюваних перешкод радіоприймальній апаратурі різного призначення і водночас максимально збільшує спектральну щільність перешкоди. Частоти, на яких працюють такі ПД, складають близько 1 ГГц, а їх середня потужність – біля 10 Вт.

Оскільки шумовий сигнал наводиться безпосередньо у вхідних ланцюгах, то однаково добре подавлюється і інша підслуховуюча апаратура, що має у своєму складі мікрофони. Як і для ДД, важливу роль відіграє рівень екранування диктофона або іншого підслуховуючого пристрою. Якщо диктофони в пластмасових корпусах подавлюються на відстані до 5 м, то в металевих – до 2-х м.

Проте розглянуті ПД мають певні недоліки.

По-перше, несприятлива дія на організм людини. Багато приладів цього класу мають медичні сертифікати. Як правило, в них вказано, на якій відстані і впродовж якого часу людина може безпечно перебувати в зоні основної пелюстки. Наприклад, для одного з виробів на відстані 1,5 м цей час складає до 40 хв. в

день, на відстані 2,0 м – до 1 години, а в зоні задньої й бічних пелюсток час перебування не обмежено.

По-друге, джерело шумового електромагнітного випромінювання наводить перешкоди в звичайній радіоелектронній апаратурі. Під найбільший вплив потрапляють радіоприймачі, активні акустичні колонки, звичайні телефонні апарати, офісні радіотелефони з аналоговими радіоканалами, аудіо- і відеодомофони, побутові телевізори, монітори комп'ютерів. Невдале розташування ПД може спричинити помилкові спрацьовування охоронної і пожежної сигналізації та ін.

Четверта група методів протидії ЗСАВ (рис. 1) має суто юридичний характер та заснована на обмеженнях у правомірності їх легального використання.

Так, основною умовою правомірності застосування ЗСАВ з метою оперативно-розшукової діяльності є використання кожного виду методів і засобів негласного добування інформації в строгій відповідності із законами України і вимогами відомчих нормативних актів уповноваженими на це суб'єктами [20; 21].

Проте застосування таких методів і засобів [20, Ст. 9], *по-перше*, не повинно принижувати честь і гідність громадян, призводити до фізичних страждань або завдавати збитку їх здоров'ю або довкіллю.

По-друге, застосування ЗСАВ повинно здійснюватися тільки за наявності достатньої інформації про підготовку або скоєння злочину; для розшуку осіб, причетних до злочинної діяльності. Рішення про застосування подібних методів і засобів приймає посадовець або оперативний працівник як винятковий спосіб тільки тоді, коли іншим шляхом отримати відповідну інформацію неможливо і за наявності достовірних, перевірених даних про факт підготовки або скоєння злочину. *По-третє*, дозвіл на застосування ЗСАВ, факт і результати їх застосування мають бути документально оформлений (рішення судової інстанції, план оперативно-розшукових заходів, акт за результатами застосування тощо).

Особливий інтерес викликає питання про відповідальність за незаконне застосування ЗСАВ [22]. Він є досить спірним, оскільки сьогодні в чинному законодавстві поняття спеціальних технічних засобів і чіткого визначення ЗСАВ не існує. Це є однією з проблем судової практики при розгляді кримінальних справ, збуджених за ст. 359 КК України [23], відповідно до якої криміналізовано "*Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації* ".

Зокрема, практика силових структур [24] свідчить про віднесення до категорії спеціальних технічних засобів негласного отримання інформації деяких моделей Д і ВК, виконаних, наприклад, в ручках; ВК, вмонтованих в датчики охоронно-пожежної сигналізації; більшості ВК, у яких чутливість вища ніж 0,01 лк; будь-яких відеосистем, що використовують аналогові ВК з передачею по "витій парі"; ВК, що використовуються в охоронному відеоспостереженні, оскільки вони поєднані із засобом передавання відеосигналу (сервер); радіоканальних відеосистем ("відеоняні"); мініатюрних ВК з об'єктивом типу "pin-hole", навіть за відсутності винесення зіниці (відстань від місця, де можна встановити діафрагму з мінімальним отвором, діаметр якого менше діаметру вхідної зіниці об'єктива, до передньої кромки об'єктива) тощо. Вочевидь, що вказані ознаки мають досить спірний та неоднозначний характер, що ускладнює правозастосовчу практику протидії ЗСАВ.

Висновки. Таким чином, проблема дослідження сучасних методів та засобів протидії ЗСАВ є досить актуальною. Визначені та проаналізовані чотири групи методів та засобів протидії ЗСАВ, які відрізняються фізичними принципами протидії та особливостями їх реалізації. Лише комплексне поєднання різноманітних методів та засобів боротьби може ефективно протидіяти сучасним високотехнологічним ЗСАВ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Энциклопедия промышленного шпионажа / [Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко] ; Под общ. ред. Е.В. Куренкова. – СПб. : ООО "Изд-во Полигон", 1999. – 512 с.

2. *Андрианов В.И.* "Шпионские штучки" и устройства для защиты объектов и информации : [справочное пособие] / В.И. Андрианов, В.А. Бородин, А.В. Соколов. – СПб. : Лань, 1996. – 272 с.

3. *Милованов А.В.* Специальные средства контроля / А.В. Милованов // Безопасность информации. – 1999. – № 1. – С. 59–62.

4. *Хореев А.А.* Способы и средства защиты информации / А.А. Хореев. –М. : МО РФ, 1998. – 316 с.

5. *Домарев В.В.* Защита информации и безопасность компьютерных систем / В.В. Домарев. – К. : Изд-во "Диа Софт",1999. – 480 с.

6. *Хорошко В.А.* Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – Юниор, 2003. – 504 с.

7. *Гудков С.А.* Проблемы и решения задачи обнаружения современных диктофонов / С.А. Гудков // Специальная техника. – 2003. – № 3.

8. *Исхаков Б.С.* Подавление диктофонов – возможности и практическое применение / Б.С. Исхаков, В.Л. Каргашин, Л.М. Юдин // Специальная техника. – 2001. – № 5.

9. Нестеренко М. Виявлення цифрових диктофонів / М. Нестеренко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – НТУУ "КПІ", ДСТС ЗІ СБУ. – 2006. – Вип. 1 (12). – С. 174–178.

10. *Захаров А.В.* Подавители диктофонов. Из опыта эксплуатации / А.В. Захаров [Електронний ресурс]. – Режим доступу : http : // www.radioscanner.ru/info/article170.

11. *Королева Е.* Обнаружители скрытых видеокамер / Е. Королева // Технологии защиты. 2008. – № 2.

12. *Арсентьев М.* Правовые аспекты использования миниатюрных видеокамер, касающиеся использования систем скрытого теле/видеонаблюдения частными лицами и организациями, не имеющими права осуществления оперативно-розыскной деятельности (ОРД) / М. Арсентьев // Системы безопасности. – 2007. – № 4.

13. *Берзин П.С.* Уголовная ответственность за незаконное использование специальных технических средств негласного получения информации (комментарий к статье 359 Уголовного кодекса Украины) / П.С. Берзин [Електронний ресурс] – Режим доступу : http : // www.crime-research.ru/library/Berzin17.htm.

14. Про внесення змін до Закону України "Про інформацію" : Закон України від 13.01.2011 // Офіційний вісник України. – 2011. – № 10. – Ст. 445.

15. Нелинейные локаторы [Електронний ресурс].– Режим доступу : http : // conard.lg.ua/security/books.html-type=more&dir=books&id=0206.htm.

16. *Адамян А.* Защита речевой информации руководителя организации от скрытой записи посетителем / А. Адамян. – [Електронний ресурс]. – Режим доступу : http : // www.bre.ru:80/security/18602.html.

17. *Бузов Г.А.* Современный взгляд на решение проблемы применения "легальных жучков" / Г.А. Бузов, А.К. Лобашев, Л.С. Лосев // Защита информации. Инсайд. – 2005. – № 2.

18. *Емельянов С.Л.* Проблема защиты информации от утечки и пути ее решения : монография / С.Л. Емельянов. – Одесса : Феникс, 2011. – 624 с.

19. *Емельянов С.Л.* Систематизация методов и средств защиты акустики помещений / С.Л. Емельянов // Системи обробки інформації. – 2012. – Вип. 4 (102). – С. 31–36.

20. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 // Відомості Верховної Ради України (ВВР). – 1992. – № 22. – Ст. 303.

21. Про міліцію : Закон України від 20.12.1990 // Відомості Верховної Ради Украї-ни (ВВР). – 1991. – № 4. – Ст. 20.

22. *Хараберюш І.Ф.* Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : монографія / І.Ф. Хараберюш, В.Я. Мацюк, В.А. Некрасов, О.І. Хараберюш. – К. : КНТ, 2007. – 196 с.

23. Кримінальний кодекс України від 5 квітня 2001 р. // Відомості Верховної Ради України (ВВР). – 2001. – № 25–26. – Ст. 131.

24. Дело компаний "Группа техники" / Вопрос-ответ [Електронний ресурс]. – Режим доступу : http : // delotex.ru/quest.

Отримано 19.04.2012