В.Г. Лісогор
старший викладач
кафедри криміналістики
Юридичної академії МВС України

ФОРМИ ВИТОКУ ІНФОРМАЦІЇ, ЩО СТАНОВИТЬ ТАЄМНИЦЮ ДОСУДОВОГО СЛІДСТВА

Слідча діяльність, як і будь-яка інша діяльність, пов'язана з пізнанням об'єктивної реальності, залежить від отримання та використання інформації. Пізнання має ретроспективний характер, оскільки в основному досліджуються події, які мали місце у минулому. Отримання інформації, достатньої для досягнення істинного знання про об'єкт, що пізнається, є одним із результатів, запланованих як мета цієї діяльності. Слідча діяльність – це процес пошуку, виявлення, закріплення, накопичення, обробки,

аналізу інформації та прийняття на цій основі певних рішень для розв'язання завдань кримінального судочинства.

Під час проведення слідчої діяльності на неї впливає ряд факторів, які сприяють їй або навпаки – діють негативно. Серед негативних є фактор, пов'язаний із тим, що заінтересовані особи намагаються отримати якомога повнішу інформацію про заходи в ході розслідування злочинів, про отримані докази, установлених свідків, осіб, які проводять розслідування тощо. І одним з основних елементів, що запобігають впливу цих негативних факторів, є захист від можливого розголошення інформації, отриманої під час розслідування злочину. У зв'язку з цим виникає доконечна потреба зберегти від розголошення певну інформацію, отриману в ході слідства, яка може становити таємницю досудового слідства. Питання щодо поняття та сутності таємниці досудового слідства розглядалися нами в попередніх працях, тому спинятися на них не будемо [4; 5].

Оскільки за режимом інформація, що становить таємницю досудового слідства, належить до інформації з обмеженим доступом, то актуальним є забезпечення її збереження від розголошення, тобто здійснення інформаційної безпеки слідчої діяльності.

У науковій літературі зазначається, що безпека не може бути знеособлена, оскільки небезпека може виходити від когось або від чогось і бути спрямована на когось або на щось [2, с.8]. Питання «від чого захищатись?» пов'язане з поняттям «загрози», під якою розуміється потенційна можливість неправомірного навмисного або випадкового впливу на об'єкт захисту, що призводить до втрати або розголошення інформації [10, с. 280].

Загрози інформації у більшості випадків спрямовані на її негласне отримання, знищення (поновлення) чи внесення певних змін (модифікацію) [2, с.9]. Ці загрози можуть бути реалізовані за допомогою певних осіб через викрадення, вивідування тощо або за допомогою спеціальних технічних засобів. Аналіз загроз інформації необхідно здійснювати виходячи з того, що інформація буває таких видів:

1) акустична (усна мова, звуки, сигнали тощо); 2) фото та відео; 3) інформація на паперових носіях; 4) інформація на електронних носіях; 5) представлена у вигляді коливань певних середовищ (дротяний і радіолокаційний зв'язок, комп'ютерні мережі, побічні випромінювання та наведення тощо) [2, с. 9–10].

Відповідно витік інформації здійснюється технічними каналами, якими є:

- радіоканали (електромагнітні випромінювання радіодіапазону);
- електричні (напруга та струм у різних струмопровідних комунікаціях);
- акустичні (розповсюдження звукових коливань у будь-якому звукопровідному матеріалі);
- оптичні (електромагнітні випромінювання у видимій, інфрачервоній та ультрафіолетовій частинах світлового спектра) [7, с.338].

Окремими вченими розглядаються три основні групи способів негласного отримання інформації:

1) незаконне вилучення носіїв інформації; 2) несанкціоноване отримання інформації; 3) неправомірне маніпулювання інформацією [9, с. 63].

До першої групи належать способи, спрямовані на вилучення як паперових, так і непаперових (магнітні диски тощо) носіїв інформації.

До другої – способи, які включають дії з несанкціонованого (незаконного, забороненого) отримання інформації. Ця група включає три підгрупи:

1) отримання інформації за допомогою технічних засобів; 2) отримання інформації за допомогою органів чуттів; 3) отримання інформації через вплив (фізичний, психічний) на людей як носіїв інформації.

За допомогою органів чуттів людини може бути отримана мовна або (та) візуальна інформація. Цей спосіб можливий на етапі підготовки та використання технічних засобів, або він може бути єдино можливим способом отримання інформації. Особою, яка намагається отримати інформацію, може бути член злочинного угруповання або співробітник, стосовно якого злочинцями використовувались підкуп, шантаж тощо. Також зазначимо, що інформація може бути отримана шляхом мимовільного її розголошення особами, яким вона відома.

Спосіб отримання інформації шляхом впливу на людину як носія інформації, яка їй відома, надзвичайно небезпечний. Цей спосіб пов'язаний з учиненням на людину фізичного, психічного та інших форм насильницького впливу. Злочинці при цьому розкривають себе, свої плани, об'єкт інтересу та часто вдаються до фізичного знищення особи, яка зазнає насильства.

Способи отримання інформації за допомогою технічних засобів полягають у перехопленні-відновленні інформації, яка реально існує у формі та середовищі, доступних для особи без впровадження у середовище, а також у несанкціонованому доступі – діях особи зі створення каналів отримання інформації шляхом упровадження в інформаційне середовище [9, с. 63–73].

Негласне отримання інформації здійснюється за допомогою технічних засобів, спеціально для цього розроблених (засоби негласного візуального спостереження, негласного акустичного контролю, негласного знімання інформації з каналів зв'язку та ін.) [7, с.20].

У науковій літературі перехоплення інформації розглядається у двох різновидах: активне (безпосереднє) та пасивне (опосередковане фізичними явищами, що сприяють процесу обробки, передачі інформації).

Активне перехоплення здійснюється шляхом безпосереднього (контактного, гальванічного) підключення до телекомунікаційного обладнання, комп'ютерної системи, каналів зв'язку. Підключення здійснюється за допомогою технічних засобів та обладнання як спеціального, так і побутового призначення: телефонних апаратів, відрізків проводів, різних щупів, зажимів, голок, набору радіомонтажних інструментів, магнітофонів, диктофонів тощо. Інформація при активному перехопленні фіксується безпосередньо в її вихідному вигляді. Після підключення до каналу зв'язку вся інформація фіксується на матеріальному носієві або переводиться у форму, що читається людиною, будь-якими доступними засобами. До способу активного перехоплення належать такі заходи, як прослуховування телефонних переговорів і зняття інформації з технічних каналів зв'язку.

Пасивне перехоплення полягає у відновленні інформації, яка розповсюджується за рахунок фізичних явищ, що виникають при функціонуванні технічних засобів обробки інформації. До цих явищ належать побічні електромагні-

тні випромінювання, наведення, сигнали, які створюються електроакустичними елементами пристроїв слаботочної техніки. Відновлення та фіксація інформації при пасивному перехопленні здійснюється технічними засобами, як правило, спеціального призначення [9, с.65–66].

Зазначимо, що серед множини технічних каналів витоку інформації два – на особливому місці, вони здатні забезпечити дуже ефективне прослуховування приміщень. Це віброакустичний і прямий акустичний канали витоку інформації.

Під прямим акустичним каналом звичайно розуміють можливість прослуховування приміщень через природні та штучно створені отвори (щілини у стінах, підлогах, стелях, вентиляційні шахти і т.д.). При такому прослуховуванні може використовуватися звукопосилювальна та звукозаписувальна апаратура.

Віброакустичний канал витоку інформації – це можливість прослуховування приміщень за допомогою електронних стетоскопів, які перетворюють вібраційні коливання будівельних конструкцій в електричний сигнал. Після посилення та найпростішого оброблення цей сигнал може бути прослуханий, записаний на магнітофон або переданий по радіоканалу. Інформація може зніматися зі стін, перекриття, дверей, віконних рам і шибок, труб опалення та водопостачання тощо [8, с.25].

Спосіб пасивного перехоплення використовується також при відновленні акустичної інформації, що розповсюджується у відкритому просторі або рідких середовищах. Засоби фіксації включають у себе спрямовані мікрофони та гідроакустичні датчики.

Далі розглянемо способи несанкціонованого доступу до інформації. Вони мають три основні різновиди: способи доступу до акустичної, способи доступу до візуальної та машинної інформації.

Способи доступу до акустичної інформації є найнебезпечнішими та достатньо розповсюдженими. Вони мають два різновиди: заходовий (заносний) та беззаходовий. Перший полягає у встановленні малогабаритного прослуховувального пристрою (закладки) в апаратуру засобів обробки інформації, у різні технічні пристрої, на наявні комунікації (радіотрансляція, телефон, телевізійний кабель, лінії сигналізації, електромережа), а також у різні конструкції, побутові предмети. Установлення закладки здійснюється під час проникнення у приміщення, будування або ремонту приміщення, або закладка заноситься у приміщення, будучи вмонтованою в апаратуру чи інші предмети. Як закладку використовують спеціальні мікрофони з передачею інформації різними каналами, а також диктофони [9, с.66–67].

До закладних пристроїв загалом належать будь-які технічні засоби, які попередньо негласно розміщаються на об'єкті або у його комунікаціях із метою негласного отримання інформації (акустичної, візуальної, текстової, комп'ютерної). Як закладні пристрої можуть використовуватися: мікрофони з дистанційною передачею інформації; стетоскопи з дистанційною передачею або накопиченням інформації; гідроакустичні датчики; мікровідеокамери з дистанційною передачею або накопиченням інформації; ендоскопи; пристрої знімання інформації з ліній зв'язку (телефонні закладки, телефони-спостерігачі та ін.).

Перелік закладних пристроїв не є вичерпним, оскільки з'являються нові їх види [3, с. 20].

Ефективність дії радіозакладок залежить не тільки від технічних параметрів, а й від наявності сприятливих умов для проникнення на об'єкт, що інтересує зловмисників. Відомо, що у приміщеннях, які займають, зокрема, оперативні підрозділи, доступ сторонніх осіб обмежений, широко використовується екранування приміщень та спеціальної техніки, у приміщеннях часто встановлюються системи просторового й лінійного зашумлення. Регулярно проводяться й апаратні заходи з перевірки техніки, що використовується, на відповідність величин побічних випромінювань допустимим рівням [6, с. 218].

Беззаходовий різновид полягає у тому, що акустичні та вібродатчики встановлюються на інженерно-технічні конструкції, які перебувають за межами приміщення, з якого необхідно приймати мовні сигнали. Датчики встановлюються або безпосередньо, або дистанційно шляхом використання пристроїв, які вистрілюються, та автоматичних захватів для утримання датчиків на конструкції. Так, можуть використовуватися мініатюрні радіопередавачі, виготовлені у вигляді загостреного або покритого липкою речовиною предмета. Крім того – безшумні пістолети: прицільний постріл із такого пістолета на відстань у декілька десятків метрів дозволяє непомітно закріпити радіопередавач на поверхні, виготовленій практично з будь-якого будівельного матеріалу [6, с. 218].

Способи доступу до візуальної інформації полягають у діях, спрямованих на отримання потрібних відомостей шляхом використання оптичних та електронно-оптичних засобів, які визначають два різновиди способів: фізичний та електронний. Способи включають візуальне спостереження, контроль, фіксацію інформації за допомогою фотоапаратури та відеотехніки [8, с. 68]. Наведемо приклад використання фотоапаратури для отримання інформації.

Через вікно будівлі, розташованої на відстані близько 50 метрів від об'єкта спостереження, з використанням довгофокусного об'єктива, були зроблені знімки документів, що викривають у корупції чиновників. У момент зйомки документи були на столі одного з керівників оперативної служби, що займалася їх розробкою. Текст на фотографіях документів читався без особливих зусиль.

Випадок отримав широке розголошення через засоби масової інформації. У результаті загинув цінний агент: злочинці інсценували його самогубство [6, с. 219].

У науковій літературі наводиться ряд способів отримання інформації за допомогою технічних засобів та органів чуттів.

1. Розмова:

а) акустичний сигнал – підслуховування, у тому числі випадкове; диктофони; закладні пристрої з передачею інформації по наявних комунікаціях (трубах, ланцюгах сигналізації, електричних мережах, телефонних лініях…), спеціальних лініях, радіо- або інфрачервоному каналу; спрямований мікрофон;

б) віброакустичний сигнал – стетоскоп; вібродатчик із передачею ін-

формації по: радіоканалу, дротах, комунікаціях, інфрачервоному каналу; оптичний лазерний мікрофон;

в) гідроакустичний сигнал – гідроакустичний датчик;

г) акустоелектричний сигнал – радіоприймач спецпризначення.

2. Розмова по телефону:

а) акустичний сигнал – аналогічно п. 1;

б) електричний сигнал у лінії – паралельний телефон; пряме підключення; підключення через електромагнітний датчик; телефонна радіозакладка;

в) побічні електромагнітні випромінювання та наведення – спеціальні радіотехнічні пристрої.

3. Розмова по радіотелефону:

а) акустичний сигнал – апаратура п. 1;

б) електромагнітні хвилі (радіохвилі) – спеціальні радіоприймальні пристрої.

4. Документ на паперовому носієві:

а) наявність – візуально, у тому числі за допомогою оптичних засобів; фотографування, у тому числі з дистанційною передачею знімка; копіювання [10, с. 18].

Наступними способами є:

5. Розмноження документа на паперовому носієві:

а) сліди на нижньому аркуші, копіювальному папері або фарбувальній стрічці – викрадення; візуально;

б) шум принтера – спеціальна апаратура акустичного контролю;

в) побічні електромагнітні випромінювання та наведення ЕОМ – спеціальні радіотехнічні пристрої.

6. Поштове відправлення:

а) наявність – викрадення; прочитування з розкриттям, без розкриття.

7. Документ на непаперовому носієві:

а) носій – копіювання; зчитування; несанкціоноване використання комп'ютера.

8. Виготовлення документа на непаперовому носієві:

а) зображення на дисплеї – візуально, у тому числі за допомогою оптичних засобів; фотографування; відео- або телевізійні закладні пристрої;

б) побічні електромагнітні випромінювання та наведення – спеціальні радіотехнічні пристрої;

в) електричні сигнали у мережах – апаратні закладки.

9. Передача документа на непаперовому носієві:

а) електричні сигнали – несанкціоноване підключення; імітація користувача [10, с. 19].

10. Виробничий процес:

а) відходи, випромінювання тощо – спеціальна апаратура різного призначення [9, с. 73].

До третьої групи способів отримання інформації (неправомірне маніпулювання) можна віднести дії, спрямовані на:

1) порушення таємниці, що охороняється законом;

2) розголошення, втрата відомостей, що охороняються законом [9, с.74].

Вивчення сучасної слідчої практики дозволяє констатувати зростання

кількості спроб отримання доступу до інформації досудового слідства у конкретних кримінальних справах із використанням технічних засобів. Так, неодноразово виявлялись факти встановлення радіомікрофонів, використання звукозаписувальних приладів, прослуховування телефонних розмов у службових приміщеннях працівників слідчих підрозділів. На це вказують опитані автором слідчі: 13,6% респондентів зазначили, що розголошення таємниці досудового слідства здійснюється шляхом прослуховування телефонних розмов у службових кабінетах, 11,2% – шляхом збирання інформації за допомогою технічних засобів.

У злочинців вилучаються засоби негласного отримання інформації. Ю.Ф. Жаріков, Ю.Ю. Орлов, Л.І. Громовенко з цього приводу наводять приклад: у квітні 1998 р. співробітники Управління МВС України у Запорізькій області під час проведення оперативних заходів вилучили в одного із запорізьких кримінальних «авторитетів» комплект новітньої прослуховувальної апаратури зарубіжного виробництва, що розміщується у кейсі, яка дозволяє проводити знімання інформації з ліній зв'язку, прослуховувати акустику приміщень, сканувати радіоефір [3, с. 20].

Окремі дослідження показують, що технічні засоби, які використовуються злочинцями, розроблюються та вдосконалюються практично одночасно з провідними світовими науковими досягненнями. Це підтверджується численними фактами виявлення в арсеналах організованих злочинних груп новітньої апаратури, у тому числі портативних лазерних систем прослуховування та пристроїв мережного перехоплення комп'ютерної інформації без безпосереднього контакту з джерелом [6, с. 219]. Зростання кількості подібних проявів має підштовхнути як самих працівників, так і керівництво правоохоронних структур до відповідного вирішення проблеми інформаційної безпеки слідчої діяльності та збереження таємниці досудового слідства.

Аналіз специфіки слідчої діяльності та випадків таємного збирання інформації за допомогою технічних засобів свідчать про те, що найбільша ймовірність витоку акустичної інформації існує крізь повітря і телефонні лінії зв'язку. Підтвердженням такого висновку є те, що службові приміщення слідчих підрозділів розташовані у відокремлених будівлях, які належать Міністерству внутрішніх справ. Доступ до цих установ сторонніх осіб суворо контролюється. Окрім цього, встановлення та використання складної апаратури розвідки вимагає значних матеріальних і часових затрат, кваліфікованого персоналу. Хоча певна можливість установлення закладних пристроїв може й виникати при здійсненні ремонтних та оснащувальних робіт представниками комерційних фірм. Тому здійснення робіт треба постійно контролювати, а після завершення проводити перевірку приміщень працівниками підрозділу технічного захисту інформації на наявність можливих каналів витоку інформації. Також необхідно контролювати стан суміжних приміщень.

Як свідчить практика, найпоширенішим є використання радіозакладок і диктофонів.

Виходячи з наведеного, слідчому необхідно весь час уважно слідкувати за діями відвідувача, не залишати його без нагляду в кабінеті, а після закінчення

візиту провести уважний огляд предметів, з якими він контактував (стілець, крісло, стіл тощо). Обстежити із залученням спеціаліста випадково залишені дрібниці – авторучку, запальничку, калькулятор тощо. Інколи радіозакладки закріплюють на трубах водопостачання, батареях опалення, побутових електроприладах – вони виконують функції допоміжних антен.

Бесіду треба проводити при щільно закритих дверях, вікнах і кватирках, використовувати штори та жалюзі на вікнах.

Необхідно звертати увагу на автомобілі з пасажирами, що підозріло тривалий час стоять поблизу будинку. Вони можуть слугувати пунктами приймання інформації, зокрема, автомобільною системою прихованого відеоспостереження: відеокамера, що забезпечує огляд по колу, закамуфльована під зовнішню антену стільникового телефону. Плоский екран установлюється на сонцезахисному козирку або у «бардачку», пульт управління – у попільничці або у кишені на дверях [1, с.10]. При виникненні підозри необхідно організувати спостереження за такими автомобілями та їх перевірку.

У разі використання диктофонів останні найчастіше маскуються під одягом або у портфелях чи сумочках, можуть мати виносні мікрофони, пристрої дистанційного керування або керування голосом. Зайва знервованість відвідувача, його неприродні рухи корпусом, часті занурювання рук до кишень мають привернути увагу слідчого, оскільки можуть бути ознакою використання прихованого звукозапису.

У зв'язку з тим, що габаритні розміри диктофонів значно більші, ніж радіозакладок, їх легше виявляє допоміжний персонал під час особистого огляду відвідувачів. Його можна проводити під приводом виявлення зброї за допомогою металошукача, який добре виявляє всі види диктофонів.

Сучасні прилади для виявлення диктофонів мають досить обмежений радіус дії (0,3-1 м), тому їх використання не дуже ефективне. Ще більші труднощі викликає виявлення цифрових звукозаписувальних пристроїв, у яких зовсім немає механічної частини, а інформація записується на мікрочип. Перспективнішим вважається використання заглушувачів диктофонів, які, поширюючи досить потужне спеціальне радіовипромінювання, унеможливлюють нормальне функціонування електронної частини звукозаписувальних приладів.

Що стосується можливого витоку інформації через телефон, то бажано щоб спеціалісти з технічного захисту інформації за допомогою спеціальних обладнань захистили його мікрофонну, дзвінкову лінії, розетку від можливого використання для знімання інформації, а також проводили періодичну перевірку апарата й стану телефонної лінії.

У разі проведення конфіденційних розмов у приміщенні бажано відключати телефон від лінії.

Необхідно звертати увагу на випадки, коли телефонний апарат дає один дзвінок і замовкає, інколи це може бути ознакою прослуховування приміщення. Бажано передзвонити після цього за будь-яким номером, щоб відключити вашу лінію від можливого з'єднання з апаратурою прослуховування.

Під час установлення нового телефонного апарата (особливо якщо вам його подарували) необхідно доручити спеціалісту провести його перевірку на можливий витік інформації.

Таким чином, існує широке коло форм витоку інформації, що становить таємницю досудового слідства. Ці форми відрізняються за характером і складністю, що визначається видом інформації. Розглянуті питання дозволять з'ясувати, яким чином відбувається розголошення. Це надасть можливість ефективніше здійснювати процес розслідування, уникати впливу негативних факторів, пов'язаних із розголошенням таємниці, бути досвідченішим у питаннях її збереження.

Бібліографічні посилання

1. *Анапский Е.* Защита информации – основа безопасности бизнеса // Служба безопасности. – 1999. – № 11–12. – С. 10–11.
2. *Брагин О.* Еще раз о безопасности // Служба безопасности. – 1998. – № 6. – С. 8–10.
3. *Жариков Ю.Ф., Орлов Ю.Ю., Громовенко Л.И.* О некоторых методах обнаружения закладочных устройств // Бизнес и безопасность. – 1998. – № 3. – С. 20-22.
4. *Лісогор В.Г.* Криміналістичне забезпечення збереження таємниці досудового слідства: Автореф. дис. … канд. юрид. наук: 12.00.09 / НАВСУ. – К., 2003.
5. *Лісогор В.Г.* Таємниця досудового слідства: поняття, сутність і значення // Держава і право: Зб. наук. праць. Юридичні і політичні науки. – К., 2001. – Вип. 14. – С. 351–358.
6. Практика уголовного сыска: Науч.-практ. сборник / Составитель А. Ваксян. – М., 1999.
7. *Ронин Р.* Своя разведка. – Минск, 1998.
8. Служба безопасности. – 1999. – № 5–6.
9. *Шумилов И.И.* Криминалистические аспекты информационной безопасности: Дис. … канд. юрид. наук: 12.00.09 / Санкт-Петербургск. юрид. ин-т. – СПб., 1997.
10. Энциклопедия промышленного шпионажа / Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко / Под общ. ред. Е.В. Куренкова. – СПБ., 1999.