**УДК 355.535**

**О. М. Горбов, О. В. Чайка**

# ЗАХИСТ ІНФОРМАЦІЇ У ВНУТРІШНІЙ МЕРЕЖІ ПРОВОДОВОГО ЗВ'ЯЗКУ ВІЙСЬКОВИХ ЧАСТИН ВНУТРІШНІХ ВІЙСЬК МВС УКРАЇНИ

*Розглянуто методи та засоби захисту інформації у внутрішніх мережах проводового зв'язку військових частин та підрозділів внутрішніх військ МВС України.*

**Постановка проблеми.** Забезпечення технічного захисту інформації у системах внутрішнього зв'язку стає з кожним роком все більш актуальним. Засоби прослуховування та закладні пристрої доступні широкому колу осіб, схеми їх виготовлення розміщені у відкритих публікаціях та Інтернеті. Неможливий постійний контроль за станом кабельних ліній внутрішньої мережі зв'язку військових частин.

У зв'язку з цим постає питання захисту кабельних ліній від несанкціонованого прослуховування телефонних переговорів та розмов у приміщеннях, де встановлений телефонний апарат, через виникнення паразитних мікрофонних наведень.

**Аналіз останніх досліджень і публікацій.** Стільниковий зв'язок стрімко увійшов у наше життя, 95 % всіх населених пунктів держави, шляхи сполучення і т. ін. знаходяться у зонах покриття систем мобільного зв'язку. Абонентами ведучих компаній є понад 20 млн осіб. Проводовий зв'язок втратив свою значимість і використовується як допоміжний засіб ведення переговорів. Системи захисту інформації, яку передають проводовим телефонним зв'язком, науковцями практично не досліджуються, проблема залишається на рівні 90-х років XX ст.

**Метою статті є** визначення методів захисту інформації у внутрішній мережі проводового зв'язку військових частин та підрозділів внутрішніх військ.

**Виклад основного матеріалу.** До засобів проводового зв'язку внутрішніх військ віднесено АТС, польові й постійні кабелі зв'язку, а також каналоутворюючу апаратуру.

У тактичній ланці управління внутрішніх військ проводовий зв'язок, як правило, організовують за напрямками з прив'язкою до стаціонарної мережі зв'язку (система вузлів зв'язку) з широким використанням державної мережі зв'язку або за радіально-вузловою схемою.

Одним із способів захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ) від несанкціонованого доступу (НСД) і від витоку технічними каналами. Під НСД розуміють доступ до інформації з порушенням встановлених в інформаційній системі правил розмежування. Під технічними каналами розуміють канали сторонніх електромагнітних випромінювань і наведень (ПЕМІН), акустичні канали, оптичні канали та ін.

У процесі організації захисту телефонних ліній необхідно враховувати кілька аспектів:

– телефонні апарати (навіть якщо трубка не знята) можуть бути використані для прослуховування розмов у приміщеннях, де вони встановлені;

– телефонні лінії, що проходять через приміщення, можуть бути використані як джерела живлення електронних пристроїв перехоплення мовної (акустичної) інформації у цих приміщеннях, а також для її передавання;

– прослуховування телефонних розмов можливе шляхом гальванічного (або через індукційний датчик) підключення до телефонної лінії електронних пристроїв перехоплення мовної інформації;

– можливе несанкціоноване використання телефонної лінії для ведення телефонних розмов.

Прослуховування розмов у приміщеннях можливе шляхом перетворення акустичних коливань в електричні елементами телефонного апарата, такими як дзвінковий ланцюг, телефонні та мікрофонні капсулі. Внаслідок акустично-електричних перетворень у цих елементах виникають інформаційні (небезпечні) сигнали. Якщо телефонна трубка не знята, телефонний та мікрофонний капсулі гальванічно відключені від телефонної лінії, і інформаційні сигнали виникають тільки в елементах дзвінкового ланцюга.

Для захисту телефонного апарата від витоку мовної інформації електроакустичним каналом використовують пасивні та активні методи і засоби.

Найбільш широко застосовуваними пасивними методами захисту є такі [2, 3]:

– обмеження небезпечних сигналів;

– фільтрація небезпечних сигналів;

– відключення джерел (перетворювачів) небезпечних сигналів.

Можливість *обмеження небезпечних сигналів* ґрунтується на нелінійних властивостях напівпровідникових елементів, головним чином діодів. У схемі обмежника малих амплітуд використовують два зустрічно увімкнені діоди, що мають вольт-амперну характеристику, наведену на рис. 1 [2]. Такі діоди мають великий опір (сотні кОм) для струмів малої амплітуди і малий опір (одиниці Ом і менше) – для струмів великої амплітуди (корисних сигналів), що виключає проходження небезпечних сигналів малої амплітуди в телефонну лінію і практично не впливає на проходження крізь діоди корисних сигналів [1].

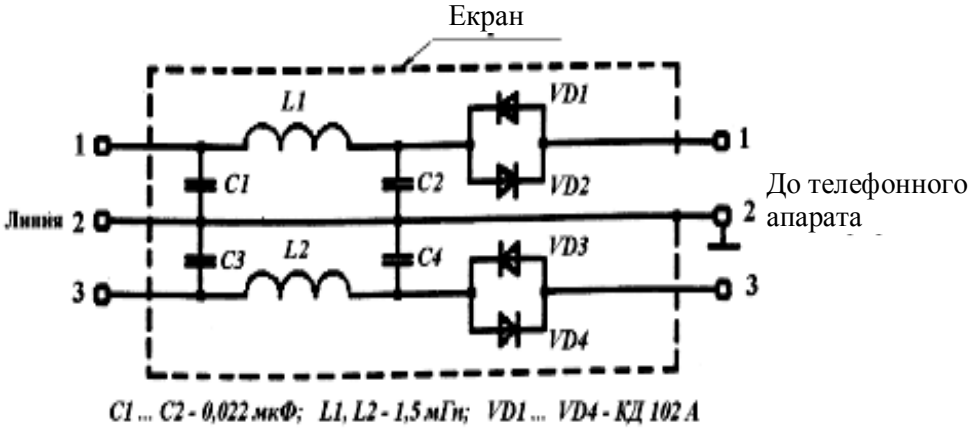


Рис. 2. Схема пристрою захисту телефонних апаратів типу “Граніт-8”

Діодні обмежники включають послідовно в лінію дзвінка або безпосередньо в кожну з телефонних ліній [2, 4, 5, 6].

*Фільтрацію небезпечних сигналів* використовують, головним чином, для захисту телефонних апаратів від “високочастотного нав’язування”.

Найпростішим фільтром є конденсатор, який установлюють у дзвінковий ланцюг телефонних апаратів з електромеханічним дзвінком та у мікрофонний ланцюг всіх апаратів [2, 3, 4, 6]. Ємність конденсаторів вибирають такої величини, щоб зашунтувати зондувальні сигнали “високочастотного нав’язування” і виключити істотний вплив на корисні сигнали. Зазвичай у дзвінковому ланцюзі використовують конденсатори ємністю 1 мкФ, а у мікрофонному ланцюзі – 0,01 мкФ [5]. Більш складним є багатоланковий фільтр низької частоти на LC-елементах.

Для захисту телефонних апаратів, як правило, використовують пристрої, що сполучають фільтр і обмежник, такі як “Екран”, “Граніт-8” (рис. 2), “Грань-300” та ін. [5]. Вони забезпечують заглушення інформаційного низькочастотного сигналу більше ніж на 80 дБ і загасання високочастотних сигналів у діапазоні частот від 30 кГц до 30 Мгц більше 70 дБ.

*Відключення телефонних апаратів від лінії* в приміщенні є найбільш ефективним методом захисту інформації. Найпростіший спосіб реалізації такого методу – установлення в корпусі телефонного апарата або у телефонній лінії ручного вимикача. Більш зручним є спеціальний пристрій захисту, що автоматично відключає від лінії телефонний апарат, коли трубка не знята. Типовим спеціальним пристроєм захисту є “Барьер-М1” [7]. Він працює у черговому режимі, режимі передачі сигналів виклику та робочому режимі.

У черговому режимі (трубка не знята) телефонний апарат відключений від лінії, пристрій

перебуває в режимі очікування підняття трубки та надходження сигналів виклику. Опір розв'язки між телефонним апаратом і лінією АТС становить не менше 20 МОм.

З надходженням сигналів виклику пристрій переходить у режим передачі сигналів виклику – телефонний апарат через електронний комутатор підключається до лінії. Підключення здійснюється тільки на час надходження сигналів виклику. У момент підняття трубки пристрій переходить у робочий режим і телефонний апарат підключається до лінії.

Виріб установлюють в розрив телефонної лінії, як правило, при виході її з приміщення або в розподільному щитку, що розташований в межах контрольованої зони.

Використання засобів захисту типу "Барьер-М1" разом із захистом інформації від витоку електроакустичним каналом є практично єдиним методом боротьби з електронними пристроями перехоплення мовної інформації, що використовують телефонну лінію як джерело живлення.

*Активні методи захисту* телефонних апаратів від витоку інформації електроакустичним каналом полягають у подачі в телефонну лінію (трубка не знята) маскуючого низькочастотного (від 100 Гц до 10 кГц) шумового сигналу (метод маскувальної низькочастотної перешкоди).

Пристрої захисту, що реалізують зазначений метод, часто називають засобами лінійного зашумлення. Їх підключають в розрив телефонної лінії, як правило, безпосередньо в корпус телефонного апарата. Шумовий сигнал подається в лінію в режимі, коли телефонний апарат не використовується. У момент зняття трубки подавання в лінію шумового сигналу припиняється.

До сертифікованих засобів лінійного зашумлення додають пристрої типу МП-1А (захист аналогових телефонних апаратів) і МП-1Ц (захист цифрових телефонних апаратів) [8].

Для прослуховування розмов у приміщеннях також застосовують електронні пристрої перехоплення мовної (акустичної) інформації, що використовують телефонну лінію як канал передачі інформації. Передавання інформації може здійснюватися як на низьких (у мовному діапазоні частот), так і на високих частотах (від 40 кГц до 10 Мгц і більше). На низьких частотах використовують мікрофонні провідні системи й пристрої типу "телефонне вухо" [1].

З метою захисту мовної інформації від перехоплення пристроями, що використовують телефонну лінію як канал передачі інформації, застосовують пасивні й активні методи та засоби захисту.

З пасивних засобів захисту в основному використовують пристрої типу "Барьер-М1", принцип роботи яких розглянутий вище.

Захист інформації, переданої телефонними лініями зв'язку, може здійснюватися на семантичному й енергетичному рівнях. На семантичному рівні захист інформації досягається застосуванням криптографічних методів і засобів захисту й спрямований на неможливість її виділення, навіть у випадку перехоплення супротивником (зловмисником) інформаційних сигналів. Методи захисту інформації на енергетичному рівні спрямовані на виключення (утруднення) прийому супротивником (зловмисником) інформаційних сигналів шляхом зменшення відношення сигнал/шум до величин, що унеможливлюють виділення інформаційного сигналу засобом несанкціонованого знімання інформації.

Розглянемо захист інформації на енергетичному рівні. Придушення електронних пристроїв перехоплення інформації здійснюється з використанням активних методів [3]:

- синфазної маскувальної низькочастотної перешкоди;
- маскувальної високочастотної перешкоди;
- маскувальної "ультразвукової" перешкоди;
- підвищення напруги;
- "обнуління";
- низькочастотної маскувальної перешкоди;
- компенсаційного;
- "випалювання".

*Метод синфазної маскувальної низькочастотної перешкоди* полягає у подаванні під час розмови в кожний провід телефонної лінії з використанням єдиної системи заземлення апаратури АТС і

нульового проводу електромережі 220 В (нульовий провід електромережі заземлений) маскувальних, погоджених за амплітудою та фазою перешкод мовного діапазону частот. Основна потужність перешкоди зосереджена у діапазоні частот стандартного телефонного каналу від 300 до 3400 Гц [9]. У телефонному апараті ці перешкоди компенсують одна одну і не впливають на корисний сигнал (телефонну розмову). Якщо інформація знімається з одного проводу телефонної лінії, то перешкода не компенсується. Завдяки тому, що її рівень значно перебільшує корисний сигнал, перехоплення інформації (виділення корисного сигналу) стає неможливим.

Як маскувальну перешкоду, як правило, використовують дискретні сигнали (псевдовипадкові послідовності імпульсів) мовного діапазону частот.

Метод синфазної низькочастотної маскувальної перешкоди використовують для придушення:

– електронних пристроїв перехоплення мовної інформації з телефонних ліній з подальшим передаванням інформації радіоканалом (телефонні ретранслятори або телефонні радіозакладки), які підключають до телефонної лінії послідовно (у розрив одного із проводів);

– телефонних радіозакладок, диктофонів і пристроїв запису на основі використання цифрових методів, які підключають до одного з проводів телефонної лінії за допомогою індукційного датчика.

*Метод маскувальної високочастотної перешкоди* полягає в подаванні під час розмови в телефонну лінію широкосмугового сигналу (ширина спектру трохи більше 1кГц), що маскує перешкоду в діапазоні високих частот звукового діапазону (вище частот стандартного телефонного каналу) [6, 10, 11].

Частоти перешкод підбирають таким чином, щоб після проходження селективних ланцюгів модулятора радіозакладки або мікрофонного підсилювача диктофона їхній рівень виявився достатнім для придушення корисного сигналу (мовного сигналу в телефонній лінії під час розмов абонентів), але водночас вони не повинні погіршувати якість телефонних розмов. Чим нижче частота перешкоди тим вище її ефективність. Зазвичай використовують частоти в діапазоні від 6 до 20 кГц. Наприклад, у пристрої Sel SP-17/D перешкода створюється в діапазоні 8…10 кГц [12].

Для виключення впливу маскувальної перешкоди на телефонну розмову в пристрої захисту встановлюють спеціальний низькочастотний фільтр із граничною частотою вище 3,4 кГц, що придушує перешкоду та істотно не впливає на проходження корисних сигналів. Аналогічну роль виконують смугові фільтри, встановлені на міських АТС. Вони пропускають сигнали, частоти яких відповідають стандартному телефонному каналу, і корисні перешкоди.

Як маскуючі сигнали використовують широкосмугові аналогові сигнали типу “білого шуму” або дискретні сигнали типу псевдовипадкової послідовності імпульсів [2, 9, 10, 11].

Даний метод застосовують для придушення практично всіх типів електронних пристроїв перехоплення мовної інформації як контактного, так і безконтактного підключень до лінії з

використанням індукційних датчиків різного типу. Однак ефективність придушення засобів знімання інформації за допомогою підключення до лінії індукційних датчиків (особливо тих, що не мають підсилювачів) значно нижча, ніж у засобів з гальванічним підключенням до лінії.

У телефонних радіозакладок з параметричною стабілізацією частоти як послідовного, так і паралельного включень спостерігається “відхід” несучої частоти, що може призвести до втрати каналу прийому [11].

Типові спектрограми випромінювання телефонних радіозакладок в умовах високочастотних маскувальних перешкод наведені на рис. 3 та 4 [2].

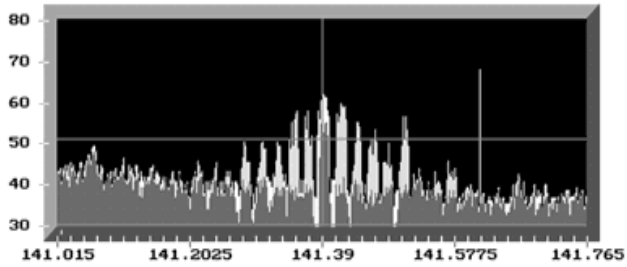


Рис. 3. Спектрограма випромінювання телефонної радіозакладки з кварцовою стабілізацією частоти й вузькосмуговою частотною модуляцією в умовах високочастотних маскувальних перешкод, створюваних пристроєм УЗТ-01

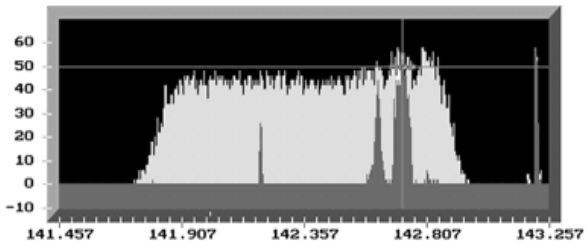


Рис. 4. Спектрограма випромінювання телефонної радіозакладки з параметричною стабілізацією частоти й вузькосмуговою частотною модуляцією з виключеним (темно-сірий тон) і включеним (світло-сірий тон) пристроєм УЗТ-01

*Метод маскувальної "ультразвукової" перешкоди* в основному аналогічний розглянутому вище. Відмінність полягає в тому, що діапазон частоти перешкоди складає 20…100 кГц.

*Метод підвищення напруги* полягає у підвищенні напруги в телефонній лінії під час розмови й використовується для погіршення якості функціонування телефонних радіозакладок внаслідок переведення їхніх передавачів у нелінійний режим роботи [11]. Підвищення напруги в лінії до 18…24 В спричинює в телефонних радіозакладках з послідовним підключенням і параметричною стабілізацією частоти "відхід" несучої частоти й погіршення розбірливості мови, що є результатом розмиття спектра сигналу. У телефонних радіозакладках з послідовним підключенням і кварцовою стабілізацією частоти спостерігається зменшення відношення сигнал/шум на 3…10 дБ. Телефонні радіозакладки з паралельним підключенням за таких напруг у деяких випадках просто відключаються.

*Метод "обнуління"* передбачає подавання під час розмови в лінію постійної напруги, що дорівнює напрузі в лінії у момент ведення розмови, але зворотної полярності.

Метод використовують для порушення функціонування та живлення електронних пристроїв перехоплення інформації з контактним підключенням до лінії. До таких пристроїв ставлять паралельні телефонні апарати й телефонні радіозакладки.

*Метод низькочастотної маскувальної перешкоди* полягає у подаванні в лінію у черговому режимі маскувальної низькочастотної перешкоди. Його застосовують для активізації (включення на запис) диктофонів, які підключають до телефонної лінії за допомогою адаптерів або індукційних датчиків, що призводить до змотування плівки в режимі запису шуму (корисний сигнал відсутній).

*Компенсаційний метод* використовують для маскування (приховування) мовних повідомлень, переданих абонентові телефонною лінією з високою ефективністю придушення всіх відомих засобів несанкціонованого знімання інформації [8].

Суть методу полягає у такому [8]: під час передавання приховуваного повідомлення на прийомній стороні в телефонну лінію за допомогою спеціального генератора подається маскувальна перешкода (цифровий або аналоговий сигнал мовного діапазону з відомим спектром). Одночасно цей сигнал ("чистий" шум) подається на один із входів двоканального адаптивного фільтра, на інший вхід якого надходить адитивна суміш прийнятого корисного сигналу і маскувальної перешкоди. Адитивний фільтр компенсує (придушує) шумовий складник і виділяє корисний сигнал, який подається на телефонний апарат або пристрій звукозапису.

*Метод "випалювання"* реалізується шляхом подавання в лінію високовольтних (більше 1500 В) імпульсів, що призводить до електричного "випалювання" вхідних каскадів електронних пристроїв перехоплення інформації та блоків їх живлення, гальванічно підключених до телефонної лінії [12, 14]. Телефонний апарат від лінії відключається. Імпульси у лінію подають два рази. Перший (для "випалювання" паралельно підключених пристроїв) – коли телефонна лінія розімкнена, другий (для

“випалювання” послідовно підключених пристроїв) – коли телефонна лінія закорочена.

Для захисту телефонних ліній використовують як прості пристрої, що реалізують один метод захисту, так і складні, що забезпечують комплексний захист ліній декількома методами, включаючи захист від витоку інформації електроакустичним каналом.

Перш ніж вибирати методи і засоби захисту, необхідно визначити, які можливості й засоби є у вірогідного зловмисника.

Існують два підходи до захисту переговорів, які засновані на передаванні мовного сигналу у аналоговому або цифровому вигляді за допомогою модему. Як правило, для захисту застосовують шифрування, що визначає в першому випадку динаміку мовних перетворень, а в другому – безпосередній захист цифрового потоку в каналі. Апаратура, що передає сигнал в аналоговому вигляді, віднесена до класу тимчасової стійкості, а та, що передає сигнал у цифровому вигляді – до класу гарантованої стійкості.

Зразками апаратури тимчасової стійкості є скремблери й маскиратори, у яких для захисту інформації здійснюють частотні тимчасові перетворення мовного сигналу. Дешифрування базується на наявних довгострокових кореляційних властивостях параметрів мовного сигналу, які дозволяють відновлювати первинний сигнал із зашифрованого автоматичними й напівавтоматичними методами. Процес безключового дешифрування нагадує складання картинки з дитячих кубиків і не гарантує успішного завершення.

Зразки апаратури гарантованої стійкості, у яких передавання мовного сигналу в каналі здійснюється у цифровому вигляді, часто називають вокодерами (від англ. voice coder). Кількість інформації, необхідної для формування високоякісного мовного цифрового сигналу, відповідає швидкості передавання 64 Kbps, тому обов’язковим є попереднє ущільнення мовлення в діапазоні 2400 – 9600 bps, що відповідає реальній швидкості передавання у телефонній мережі загального користування. Сигнал у каналі має шумовий характер і, за умови застосування стійких шифраторів, гарантовану стійкість до дешифрування.

Однією з характеристик апаратури для захисту переговорів є якість мовлення після перетворень. У скремблерах вона залежить від складності перетворень та характеристик каналу зв’язку. За наявності якісного каналу забезпечується розбірливість більш як 90 %. Оцінка якості багатьох скремблерів за п’ятибальною шкалою знаходиться між 3 й 4,5.

Якість мовлення у випадку цифрових перетворень залежить від застосовуваних алгоритмів ущільнення мовлення та швидкості передавання каналом зв’язку. Якщо використовують алгоритми на основі синтезу, наприклад CELP, на швидкостях 4800 й 9600 bps розбірливість складає 92 – 96 %, а оцінка 4 – 4,5. На швидкості 2400 bps із застосуванням алгоритмів лінійного програмування типу LPC-10 з оптимізацією сигналу порушення розбірливість дорівнює 86 %, а оцінка якості – близько 3,5 балів. Особливістю цифрового передавання мовлення є те, що якість сигналу у каналі зв’язку практично не змінюється. Більше того, для випадку великого рівня загасання абонентської лінії якість мовлення з використанням вокодерних систем у захищеному режимі визнана більш високою, ніж у звичайного телефонного зв’язку.

Незважаючи на множину різних характеристик апаратури для захисту переговорів, конкретний її тип вибирають за ступенем захищеності, що вона забезпечує, і цінності інформації, яку необхідно захистити. Слід пам’ятати правило: витрати на захист інформації не повинні перевищувати збитків від можливої її втрати.

Найпростіший пристрій контролю телефонних ліній являє собою вимірювач напруги. У процесі настроювання оператор фіксує значення напруги, що відповідає нормальному стану лінії (сторонні пристрої не підключені), і поріг тривоги. Якщо напруга в лінії менше встановленого порога, пристрій видає світловий або звуковий сигнал тривоги.

На принципі вимірювання напруги в лінії побудовані й пристрої, що сигналізують про розмикання телефонної лінії, яке виникає у разі послідовного підключення закладного пристрою. Як правило, подібні пристрої містять фільтри для захисту від прослуховування, у яких використано “мікрофонний ефект” в елементах телефонного апарата та високочастотне “нав’язування”.

Пристрої контролю телефонних ліній, побудовані на зазначеному принципі, реагують на зміни напруги, спричинені не тільки підключенням до лінії засобів знімання інформації, а й коливаннями напруги на АТС (для вітчизняних ліній достатньо часте явище), наслідком чого є помилкові спрацьовування сигнальних пристроїв. Крім того, вони не дозволяють виявити паралельне підключення до лінії високоомних (одиниці МОм) підслуховуючих пристроїв. Тому їх широко не застосовують на практиці.

Принцип роботи більш складних пристроїв заснований на періодичному вимірюванні й аналізуванні декількох параметрів лінії: напруги, сили струму та комплексного (активного й реактивного) опору.

Найбільш ефективним методом визначення факту несанкціонованого підключення до лінії, який реалізований у більшості контролерів телефонних ліній, є вимірювання струму витоку після зміни напруги в лінії. Метод базується на стрибкоподібному збільшенні струму витоку в телефонній лінії після включення передавача передавального пристрою. У черговому режимі в лінію подається постійна напруга зворотної полярності, амплітуда якої стрибкоподібно (наприклад, із кроком 1 В) збільшується в певному інтервалі. Внаслідок цього напруга в лінії буде стрибкоподібно зменшуватися. Після кожної зміни амплітуди напруги вимірюється амплітуда струму витоку в лінії, значення якої порівнюється з попереднім значенням. Якщо різниця перевищить деяке граничне значення, це свідчить про наявність несанкціонованого підключення до лінії.

Сучасні контролери дозволяють визначити не тільки факт підключення до лінії засобів знімання інформації, але й спосіб підключення (послідовне або паралельне). Наприклад, контролери телефонних ліній КТЛ-2, КТЛ-3 й КТЛ-400 за 4 хв дозволяють виявити закладки з живленням від телефонної лінії незалежно від способу, місця й часу їхнього підключення, а також параметрів лінії й напруги АТС [8]. Прилади також видають світловий сигнал тривоги у разі короткочасного (не менше 2 с) розмикання лінії.

Контролери телефонних ліній, як правило, крім засобів виявлення підключення до лінії пристроїв несанкціонованого знімання інформації, обладнані й засобами їхнього придушення за методом маскувальної високочастотної перешкоди. Режим придушення включається автоматично або оператором у разі виявлення несанкціонованого підключення до лінії.

Разом із захистом телефонних ліній від підслуховування також необхідно виключити *несанкціоноване використання телефонної лінії* для ведення телефонних розмов. Для цих цілей використовують: метод блокування набору номера і метод маскувальної низькочастотної перешкоди.

**Висновки**

Проведений аналіз показав, що комплексне застосування різних технічних засобів повністю виключає можливість використання телефонних ліній для прослуховування розмов у приміщеннях, через які вони проходять, прослуховування розмов у телефонних лініях і несанкціоноване використання телефонних ліній для ведення телефонних розмов.

**Список використаних джерел**

1. Андрианов В. И. “Шпионские штучки” и устройства для защиты объектов и информации: справочное пособие / В. И. Андрианов, В. А. Бородин, А. В. Соколов. – С Пб. : Лань, 1996.

2. Гюнтер Миль. Электронное дистанционное управление моделями / Миль Гюнтер. – М. : Изд-во ДОСААФ, 1980.

3. Андрианов В. И. Охранные устройства для автомобилей / В. И. Андрианов, А. В. Соколов. – С Пб. : Лань, 1997.

4. Охранные системы. Информационное издание. – М. : Солон, 1996. – Вып. 4.

5. Гавриш В. Практическое пособие по защите коммерческой тайны / В. Гавриш. – Симф. : Таврида, 1994.

6. Алексеенко В. Н. Системы защиты коммерческих объектов. Технические средства защиты / В. Н. Алексеенко, Б. Е. Сокольский. – М., 1992.

7. Системы безопасности. – М. : Гротек, 1997. – № 4.

8. Технические средства охраны, безопасности и сигнализации: справ. – М. : ВИМИ, 1994.

9. Информационно-технический журнал “Техника охраны”. – М. : НИЦ “Охрана” ВНИИПО МВД России, 1996.

10. Предпринимательство и безопасность. – М. : Универсум, 1991. – № 1.

11. Коммерческая безопасность / А. Е. Кисилев и др. – М. : Иноро Арт, 1993.

12. Рейке Ч. Д. 55 электронных схем сигнализации / Ч. Д. Рейке. – М. : Энергоатомиздат, 1991.

13. Про Внутрішні війська МВС України: закон України від 26.03.1992 р. // Відомості Верхов. Ради України. – 1992. – № 29.

14. Никулин О. Ю. Системы телевизионного наблюдения / О. Ю. Никулин, А. Н. Петрушин. – М. : Оберег-РБ, 1997.

*Стаття надійшла до редакції 05.02.2010 р.*