УДК 004.415.056:658.115

А. О. Азарова
Ю. П. Михайлюк

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ МОВНОЇ ІНФОРМАЦІЇ У ПРИМІЩЕННЯХ ШЛЯХОМ СТВОРЕННЯ КОМБІНОВАНОЇ ШУМОВОЇ ТА РЕВЕРБЕРАЦІЙНОЇ ЗАВАДИ

Вінницький національний технічний університет

Анотація

Проаналізовано основні загрози інформації та існуючі методи захисту інформації від витоку прямим акустичним технічним каналом. Доведено доцільність використання генераторів акустичного шуму для маскування інформації, що озвучується на об'єкті. Обґрунтовано необхідність розроблення пристрою, який створює акустичний шум із більшим маскувальним ефектом та при цьому меншим рівнем гучності сигналу.

Ключові слова: захист інформації, технічний захист інформації, витік інформації акустичним каналом, генератор акустичного шуму.

Abstract

The main threats of information and existing methods of protection of information from leakage by direct acoustic technical channel are analyzed. The expediency of using acoustic noise generators to mask the information sounded on the object has been proved. The necessity of developing a device that creates acoustic noise with a greater masking effect and at the same time a lower signal volume level is substantiated.

Keywords: information protection, technical information protection, information leakage by acoustic channel, acoustic noise generator.

Загрози інформаційній безпеці – це чинник або сукупність чинників, що створюють небезпеку функціонуванню й розвитку інформаційного простору, інтересам особистості, суспільства, держави [1]. Основним питанням початкового етапу впровадження системи безпеки є призначення відповідальних осіб за безпеку і розмежовування сфер їх впливу. Системні програмісти та адміністратори відносять це завдання до компетенції загальної служби безпеки, тоді як остання вважає, що цим питанням мають займатися спеціалісти по комп'ютерах.

Технічний захист інформації – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації [2].

У свою чергу, питання технічного захисту інформації поділяють на два великих класи завдань:

1) захист інформації від несанкціонованого доступу (НСД);
2) захист інформації від витоку технічними каналами, а саме каналами побічних електромагнітних випромінювань і наведень, акустичними, оптичними каналами тощо.

Технічний захист інформації є важливим чинником реалізації організаційно-правових та інженерно-технічних заходів з метою запобігання витоку інформації за рахунок несанкціонованого доступу до неї, несанкціонованим діям та впливам на інформацію, які призводять до її знищення, порушення цілісності або блокування, а також протидії технічним розвідкам [3].

У прямих акустичних технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря, вода й інші гідромеханічні середовища. Як засоби розвідки використовуються високочутливі мікрофони, які перетворюють акустичний сигнал на електричний. В апаратурі акустичної розвідки використовуються мікрофони різних типів, що забезпечують реєстрацію мови середньої гучності на відстані до 7 до 10 метрів від її джерела. При цьому частотний діапазон становить в основному від 50 герц до 20 кілогерц.

Використання тих чи інших засобів акустичної розвідки визначається можливістю доступу в контрольоване приміщення сторонніх осіб. У тому випадку, якщо є постійний неконтрольований доступ відвідування під різними приводами (наприклад, для перевірки системи освітлення, кондиціонування або прибирання приміщення), то для перехоплення мовної інформації можуть використовуватися портативні пристрої звукозапису (в основному цифрові диктофони), які приховано встановлюються в інтер'єрах приміщень, як правило, безпосередньо перед проведенням закритого заходу, на якому ймовірно буде озвучено інформацію, що цікавить зловмисника. Після закінчення заходу диктофон з приміщення вилучається. Такі пристрої також можуть маскувати під предмети повсякденного вжитку,

наприклад, книги, письмові прилади, пачки сигарет тощо. В даний час закордонними і вітчизняними фірмами випускається величезна кількість портативних цифрових диктофонів, які дуже легко заховати практично в будь-якому приміщенні.

Звукові хвилі в закритих приміщеннях, багаторазово відбиваючись від кордонів, утворюють складне поле коливального руху повітря, залежне не тільки від джерела звуку, але також від геометричних розмірів, форми приміщення і здатності підлоги, стелі, вікон і дверей поглинати або відбивати акустичну енергію. При поширенні звуку в закритих приміщеннях можливі явища відбиття звуку, заломлення, поглинання звуку, рефракції звуку, а також дифракції та інтерференції.

Рефракція звуку – викривлення напрямку поширення хвиль в неоднорідному середовищі. Рефракція звуку в атмосфері зумовлена просторовими змінами температури повітря, швидкості і напряму вітру [2].

Дифракція звуку – це відхилення звуку від законів геометричної акустики, пов'язане з неоднорідністю середовища, в якій поширюється звукова хвиля. Внаслідок дифракції звук може огинати зустрічні перешкоди, потрапляти в область геометричної тіні, концентруватися на отворах і т.п. Картина дифракції істотно залежить від співвідношення між розміром перешкоди або отвори і довжиною хвилі.

Інтерференція – це складання в просторі декількох хвиль, при якому в різних його точках виникає стійке в часі посилення або ослаблення амплітуди результуючої хвилі.

Для захисту приміщень застосовують генератори шуму і системи вібраційного зашумлення, які формують шумові «мовоподібні» і комбіновані перешкоди. Найбільш часто з шумових використовуються такі види перешкод:

- «Білий» шум – шум з постійною спектральною щільністю в мовному діапазоні частот;
- «Рожевий» шум – шум з тенденцією спаду спектральної щільності 3 дБ на октаву в бік високих частот;
- шум з тенденцією спаду спектральної щільності 6 дБ на октаву в бік високих частот;
- шумова «мовоподібна» перешкода – шум з обвідної амплітудного спектра, подібної мовному сигналу.

Якість захисту від витоків мовної інформації сильно залежить від алгоритму генерації шуму, тому що зловмисник може використовувати інструментарій, що «очищує» корисний сигнал від перешкод, що генеруються. Більш надійними методом ніж білий або рожевий шум вважається генерація шумів із «зворотним зв'язком» – адаптивний шум. Суть генерації полягає в аналізі корисного звукового сигналу в приміщенні за допомогою вбудованого мікрофона. Після чого генератор автоматично встановлює рівень шуму на тих чи інших частотах, що дозволяє знизити негативні моменти роботи людей у виділеному приміщенні.

Основним недоліком розглянутих вище методів акустичного зашумлення є досить великий рівень шуму в приміщенні, де здійснюється оброблення та озвучування інформації, що спричиняє не комфортні умови для роботи з інформацією в такому приміщенні, а також знижує рівень захисту через необхідність озвучувати інформацію голосніше.

Частково вирішують цю проблему генератори шуму, що створюють адаптивний шум на основі самої розмови, і на відміну від білого чи рожевого шуму мають більший маскувальний ефект при меншому рівні сигналу. Адаптивний або мовоподібний шум краще маскує розмову за рахунок ефективного аналізу звукових частот, та відтворенні лише тих, що потрібні в даний момент часу, проте рівень гучності такого шуму для ефективного захисту інформації також повинен бути вищим, ніж рівень гучності розмови. Підвищити рівень захищеності інформації що озвучується у приміщенні можна шляхом створення комбінованої шумової завади на основі мовоподібного шуму, створеного з використанням реверберації звукової хвилі, а також інтерференції звукової хвилі, що дозволить знизити рівень гучності шумового сигналу, та підвищити його маскувальні властивості [4-19].

Явище реверберації полягає у суперпозиції різних ехосигналів від одного джерела звуку. Ефект реверберації можна спостерігати в закритих приміщеннях після вимкнення джерела звуку. Штучно створювана реверберація в певних межах сприяє поліпшенню якості звучання, створюючи відчуття приємного «резонансу» приміщення, проте надлишкова тривалість реверберації призводить до неприємного гулу, при цьому сигнал залишається в межах частот людської мови, а тому зливається з розмовою, і унеможливлює її підслуховування.

Узгоджений перебіг у часі і просторі декількох звукових коливальних або хвильових процесів пов'язують з поняттям когерентності [1]. Звукові хвилі однакової частоти називаються когерентними, якщо різниця їх фаз залишається постійною в часі. При накладенні в просторі двох або кількох когерентних звукових хвиль у різних точках виходить посилення або ослаблення результуючої хвилі в залежності від співвідношення між фазами цих хвиль. Це явище називається інтерференцією звукових хвиль. Використовуючи цю властивість звукових хвиль, можна, створюючи сигнал, протилежний у фазі

до сигналу розмови, зменшити рівень її гучності в місці потенційного прослуховування. Таким чином стає можливим зменшити рівень гучності мовоподібної шумової завади, створеної з використанням ефекту реверберації завдяки зменшенню рівня гучності розмови в місці прослуховування.

Головною частиною схеми генератора радіошуму автори пропонують мікроконтроллер Arduino Nano та Інвертр для відтворення сигналу в протифазі реалізований на мікросхемах NE5532, для роботи яких було використано радіоелементи, такі як резистори та конденсатори необхідні, згідно схеми. Усі компоненти є доступними, простими у використанні та мають невисоку вартість.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Богуш В. М., Юдин О. К. Інформаційна безпека держави. К. : «МК-Прес», 2005. 432 с.
2. Іванченко С. О., Гавриленко О. В., Липський О. А., Шевцов А. С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. К. : ІСЗЗІ НТУУ «КПІ», 2016. 104 с.
3. Зайцев А. П., Шелупанов А. А, Мещеряков Р. В., Скрыль С. В., Голубятников И. В. Технические средства и методы защиты информации. М. : «Машиностроение». 2009. 508 с.
4. Азарова А. О., Ляхович Л. М. Розроблення захищеного консолідованого інформаційного ресурсу засобів електронного врядування. *Вісник ХНУ. Технічні науки.* 2020. № 3. С. 81–87.
5. Azarova A.A., Shyian A.A., Nikiforova L.O., Tkachuk L.M., Azarova V. V. The modeling of communication between the public and authorities during the innovative projects implementing in the context of e-democracy and public administration. *Science and innovation*. 2020. № 6. P. 18–27.
6. Азарова А. О., Шиян А. А., Мурза С. П., Кудлик А. В., Костюк Т. С. Розроблення захищеного консолідованого інформаційного ресурсу аналізу ринку надання послуг медичними лабораторіями в Україні. *Вісник ХНУ. Технічні науки.* 2019. № 6 (279). С. 105–109.
7. Azarova A., Shiyan A., Mironova Y., Shturma L. The development of secured consolidated information resource of activity analysis of the poultry industry in Ukraine. *Technology audit and production reserves.* №6/2 (50), 2019. P. 14–18.
8. Азарова А. О., Ткачук Л. М., Нікіфорова Л. О., Шиян А. А., Хошаба О. М. Публічне управління та адміністрування в контексті захисту його інформаційного простору. *Вісник Житомирського державного технічного університету.* 2019. № 2 (88). С. 149–155.
9. Azarova A., Azarova L., Rosol N., Bystritskiy O. Models and methods of electronic digital signature. Theoretical and scientific foun dations of engineering: collective monograph / International Science Group. Boston : Primedia eLaunch, 2020. 180 p. P. 24 – 33.
10. Азарова А. О., Погребняк О. В., Азарова Л. Є., Міронова Ю. В., Ляхович Л. М. Комп'ютерна програма «Автентифікація користувача на основі клавіатурного почерку в режимі реального часу». Свідоцтво про реєстрацію авторського права на твір № 98144. Дата реєстрації 16.06.2020 р. Заявка № 99489 від 15.06.2020 р.
11. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Отримання та надсилання повідомлень користувачами у створеному месенджері для реалізації комунікаційного процесу на підприємстві». Свідоцтво про реєстрацію авторського права на твір № 97858. Дата реєстрації 05.06.2020 р. Заявка № 99246 від 02.06.2020 р.
12. Азарова А. О., Азарова Л. Є., Міронова Ю. В., Бойчук Ю. В., Пазюк О. С. Комп'ютерна програма «Захист потокового відео засобів масової інформації з використанням підпису векторів руху». Свідоцтво про реєстрацію авторського права на твір № 98401. Дата реєстрації 06.07.2020 р. Заявка №99598 від 18.06.2020 р.
13. Азарова А. О., Азарова Л. Є., Міронова Ю. В., Пазюк О. С., Бойчук Ю. В. Комп'ютерна програма «Автентифікація аудіо-сигналів у судовій системі на основі крихких водяних знаків». Свідоцтво про реєстрацію авторського права на твір № 99597. Дата реєстрації 18.06.2020 р. Заявка №99597 від 18.06.2020 р.
14. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Захищений засобами двофакторної авторизації месенджер для організації комінікаційних процесів на підприємстві». Свідоцтво про реєстрацію авторського права на твір №97856. Дата реєстрації 05.06.2020 р. Заявка № 99244 від 02.06.2020 р.
15. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Процедура реєстрації у захищеному месенджері для організації комунікаційних процесів на підприємстві». Свідоцтво про реєстрацію авторського права на твір № 97857. Дата реєстрації 05.06.2020 р. Заявка №99245 від 02.06.2020 р.
16. Свідоцтво № 90163 про реєстрацію авторського права на твір "Комп'ютерна програма «Модуль захисту програмного забезпечення від несанкціонованого копіювання у процесах публічного управління»" / Азарова А. О., Азарова Л. Є., Ткачук Л. М., Шиян А. А., Нікіфорова Л. О., Кудлик А. В. Дата реєстрації 25.06.2019 р.
17. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Захист інформації від несанкціонованого копіювання шляхом прив'язки до унікальних параметрів вінчестера і використання ключа активації" / Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Заявка від 05.06.2018 р. №80958. Дата реєстрації 11.06.2018 р.
18. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Програмний модуль ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією" / Азарова А. О., Азарова Л. Є., Мисько Ю. О., Колган В. А. Заявка від 05.06.2018 р. №80951. Дата реєстрації 11.06.2018 р.
19. Свідоцтво про реєстрацію авторського права на твір №80464. Комп'ютерна програма „Мобільний додаток для захищеного передавання конфіденційних даних у смартфонах" / Азарова А. О., Азарова Л. Є., Бадя Ю. В. Заявка від 12.06.2018 р. №81238. Дата реєстрації 24.07.2018 р.

Азарова Анжеліка Олексіївна, кандидат технічних наук, професор, заступник декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва.

Михайлюк Юрій Петрович, Вінницький національний технічний університет, м. Вінниця, факультет менеджменту та інформаційної безпеки, УБ-19м, yura.myhayliuk@gmail.com.

Anzhelika Azarova, PhD in technique, Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia.

Yurii Mykhailiuk, Vinnytsia National Technical University, Vinnytsia, Department of Management and Security of Information Systems, yura.myhayliuk@gmail.com.