Ministry of Education and Science of Ukraine
Ministry of Education and Research of Romania
Yuriy Fedkovych Chernivtsi National University
Stefan cel Mare University of Suceava

PHYSICAL AND TECHNOLOGICAL PROBLEMS OF TRANSMISSION, PROCESSING AND STORAGE OF INFORMATION IN INFOCOMMUNICATION SYSTEMS

Proceedings of IXth International Scientific-Practical Conference

21-23 October 2021,
Chernivtsi-Suceava (Ukraine-Romania)

UDC 621.37/39(06)
ВВС 32я431
Ф 503

CONFERENCE ORGANIZING:

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
MINISTRY OF EDUCATION AND RESEARCH OF ROMANIA
YURIY FEDKOVYCH CHERNIVTSI NATIONAL UNIVERSITY
STEFAN CEL MARE UNIVERSITY OF SUCEAVA

Ф 503 **Physical and technological problems of transmission, processing and storage of information in infocommunication systems:** Proceedings of IXth International Scientific-Practical Conference. – Chernivtsi: «Ruta», 2021. – pp.

The proceeding contains materials of the conference on theoretical and practical problems of modern radio engineering, telecommunications and electronics.

The materials are submitted in the author's edition

ISBN 978-617-652-091-7

PROGRAM COMMITTEE:

Samila A.	Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine – chair
Milici L.D.	Stefan Cel Mare University, Suceava, Romania – co-chair
Potorac A.	Stefan Cel Mare University, Suceava, Romania
Graur A.	Stefan Cel Mare University, Suceava, Romania
Dimian M.	Stefan Cel Mare University, Suceava, Romania
Fedorovich O.	National Aerospace University «Kharkiv Aviation Institute»
Kharchenko V.	National Aerospace University «Kharkiv Aviation Institute»
Leshchenko O.	National Aerospace University «Kharkiv Aviation Institute»
Paranchuk Ya.	Lviv Polytechnic National University, Lviv, Ukraine
Osadchuk O.	Vinnytsia National Technical University, Vinnytsia, Ukraine
Rotshtein O.	Jerusalem Politechnic University, Jerusalem, Israel
Rozorinov H.	National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky", Kyiv, Ukraine
Semenov A.	Vinnytsia National Technical University, Vinnytsia, Ukraine
Stakhira P.	National University Lviv Polytechnic, Lviv, Ukraine
Shpatar P.	Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine
Yaremchuk Yu.	Vinnytsia National Technical University, Vinnytsia, Ukraine
Vovchuk D.	Conference secretary

CONFERENCE ORGANIZING COMMITTEE:

Kushnir M.	Yuriy Fedkovych Chernivtsi National University, Chernivtsi – chair
Gherman O.	Stefan Cel Mare University, Suceava, Romania – co-chair
Balan D.	Stefan Cel Mare University, Suceava, Romania
Rotaru A.	Stefan Cel Mare University, Suceava, Romania
Khobzei M.	Yuriy Fedkovych Chernivtsi National University, Chernivtsi
Lesinskii V.	Yuriy Fedkovych Chernivtsi National University, Chernivtsi
Hres O.	Yuriy Fedkovych Chernivtsi National University, Chernivtsi
Veryga A.	Yuriy Fedkovych Chernivtsi National University, Chernivtsi
Derevesnikova Ye.	Yuriy Fedkovych Chernivtsi National University, Chernivtsi
Andriychuk K.	Yuriy Fedkovych Chernivtsi National University, Chernivtsi

CONTENTS

Method of protection of information against laser microphones

Yurii Yaremchuk, Vitalii Kataiev, Vadim Siniuhin
Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, Ukraine, E-mail: kataev@vntu.net

Abstract – The current level of development of spy devices make it possible to listen a conversations inside of a room that has a window without ever getting near the room. Devices that allow listening are called laser microphones or Laser Based Listening System (LBLS). There are several common methods of protection against this type of threat, but they all have drawbacks. We proposed a method of laser counteraction as an alternative to existing ones, and presented the concept of its implementation. This method is based on the process of "mixing" the probing laser beam of the attacker with opposing radiation, which will considerably complicate the process of receiving and extracting an informative signal on the receiving side of the laser microphone.

Keywords – information security, leakage of speech information, laser microphones.

I. Introduction

The analysis of modern methods of protection against laser microphones, made it possible to identify their shortcomings and formalize the tasks of scientific research. Among the shortcomings identified are the inabilities to ensure sufficient security of information, significant financial costs of building a protection system, deteriorating comfort in the room. Moreover, these shortcomings are often related. The reason is that most methods are not able to provide the necessary security by themselves. Therefore, they are used in combination, and this leads to a situation where removal of one shortcoming leads to further deterioration of another.

II. Problems of current methods

The simplest method of passive protection against laser microphones is to provide sound and vibration isolation of windows, from the surface of which can be removed acoustic information [1]. This will eliminate or significantly reduce dangerous informative vibrations on the outer surfaces of windows. But the implementation of this method will require significant financial costs associated not only with the manufacture and purchase of special windows, but also with a significant amount of construction work. Alternatively, you can use protective and tinting films [2], which are glued to the window glass. They, in theory, can also reduce the level of vibration of the glass and, accordingly, complicate the emission of the sound signal in the received laser radiation. The disadvantage of such protection is that the capture of information is complicated only by reducing the modulation factor of the reflected beam, which is not a significant problem for modern laser microphones.

Active protection against laser microphones is implemented by using noise generators that generate electrical noise signals in the speech frequency range, and these signals are transmitted to the surface by using piezoelectric and electromagnetic vibrators [3]. These vibrators are installed on all problem surfaces from which it is possible to intercept information vibrations. But such protection also has disadvantages. The problem is that sometimes there can be a lot of such vibrators, because at least one sensor must be installed on each windowpane. As a result, the overall level of acoustic interference will be so high that will create uncomfortable conditions for conversation in the room.

There is another important disadvantage of these methods of protection - the inability to ensure completed security of information. It consists in the fact that the laser beam when hitting the window is partially reflected, but also partially passes through it, because glass is an optically transparent material. This means that the information vibration can be read not only from the surface of the window, but also from any other surface outside the window inside the room (such as a mirror on the wall).

III. Proposed Method

For a solution the above shortcomings, we propose a fundamentally different approach and method to build protection [5]. It is proposed to solve the problem of the laser getting into the middle of the room not by physically blocking the beam, but by preventing or significantly complicating the interception of the already reflected beam by the attacker. This can be achieved by creating counter laser radiation, which will be directed from the middle of the room through the window to the outside. In this case, this radiation will consist of a set of rays, the direction of which can change in space randomly and which will have parameters (in particular, spectral, energy and space-energy parameters) similar to the parameters of the intruder beam. Also, the opposing radiation must have a wide radiation pattern, sufficient to cover all possible angles of reflection of the attacker's laser. In addition, the opposing rays must be modulated by noise or false signals, while realizing the noise interference. As a result, there will be a situation in which the reflected beam of the attacker at the output will be "mix" with the opposing interfering beams, which will considerably complicate to interception and separation on the receiving side of the laser microphone. Also, since the rays will pass through the glass and propagate to the outside, the issue of protection is solved not only from the removal of vibration inside the room, but also from the surface of the window too.

That is, theoretically, this method will ensure the security of information without the use of vibration noise and the use of various optically opaque structures, such as blinds. The device that will implement this method must be located taking into account the capabilities of laser microphones.

IV. Conclusion

In this paper new method of protection of information against laser microphones was proposed. A method based on creating an indoor noise in the form of masking laser radiation. This radiation consists of many rays with parameters similar to those of a possible probe beam of the attacker. It is directed from the inside of the room through the window to the outside, so that the reflected beam of the attacker is masked by mixing with interfering opposing rays, which makes it difficult for the attacker to isolate its beam from many masking interference rays.

V. References

[1] Eavesdropping Protection System URL: http://cambridgesound.com/wp-content/uploads/2017/06/EavesdroppingProtection_8x11.pdf

[2] Glass-shield. Glass to protect against laser microphones URL: http://www.zoohall.com.ua/2541-glass-shield-steklo-proslushivanie.html.

[3] How practical is a laser microphone and how to protect against it? URL: https://security.stackexchange.com/questions/151972/how-practical-is-a-laser-microphone-and-how-to-protect-against-it

[4] Y. Yaremchuk, V. Kataiev. Method of creating active interference to counteract unauthorized removal of information through laser acoustic intelligence systems. Patent of Ukraine for utility model, № 137710; Published 11/11/2019, Bul. №21.