Современные инновации, системы и технологии // Modern Innovations, Systems and Technologies

2024; 4(1)
eISSN: 2782-2818
https://www.oajmist.com

УДК: 004.056.5 EDN: **EZZOCD**
DOI: https://doi.org/10.47813/2782-2818-2024-4-1-0176-0184

Обеспечение защиты информации от утечки по акустическому каналу

И. Н. Карцан[1, 2]

[1]ФГБУН ФИЦ «Морской гидрофизический институт РАН», г. Севастополь, Россия
[2]ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», г. Красноярск, Россия

Аннотация. Защита акустической речевой информации от ее утечки по техническим каналам является одной из важнейших задач обеспечения конфиденциальности переговоров, проводимых в различных помещениях, на различных предприятиях или организациях, не исключение являются и научно-исследовательские организации. Одной из важнейших задач при формировании комплекса средств защиты является оценка эффективности защиты речевой информации. Органы слуха человека сначала слышат акустический сигнал, а затем распознают звуки речи, среда распространения акустической информации является окружающий нас воздух, в связи с этим нужно тщательно подойти к защите передаваемой информации по акустическому каналу. В статье рассмотрены проблемы утечки конфиденциальной информации через акустический канал связи и методах ее предотвращения. Описываются различные подходы к защите от утечки через акустический канал, такие как использование шумоподавляющих материалов, защитных экранов и программного обеспечения, а также приведены примеры успешной реализации мер защиты. Важно отметить, что защита информации от утечки через акустический канал является частью комплексной системы безопасности, представляющей собой алгоритмически упорядоченные и взаимосвязанные совокупности централизованно управляемых функционально самостоятельных технических подсистем конкретного целевого назначения.

Ключевые слова: утечка информации, акустический канал, защита информации, шумоподавление, защитные экраны, программное обеспечение, звуковой замок.

Благодарности: Работа выполнена в рамках государственного задания по теме № FNNN-2024-0016.

Для цитирования: Карцан, И. Н. (2024). Обеспечение защиты информации от утечки по акустическому каналу. Современные инновации, системы и технологии - Modern Innovations, Systems and Technologies, 4(1), 0176–0184. https://doi.org/10.47813/2782-2818-2024-4-1-0176-0184

Ensuring protection of information from acoustic channel leakage

Igor Kartsan[1, 2]

[1]*FSBUN FIC "Marine Hydrophysical Institute of the Russian Academy of Sciences", Sevastopol, Russia*
[2]*Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia*

Abstract. Protection of acoustic speech information from its leakage through technical channels is one of the most important tasks to ensure the confidentiality of conversations held in various premises, at various enterprises or organizations, and research organizations are no exception. One of the most important tasks in the formation of a set of protection means is to assess the effectiveness of protection of speech information. The human hearing organs first hear the acoustic signal, and then recognize the sounds of speech, the medium of distribution of acoustic information is the air around us, in this regard, it is necessary to carefully approach the protection of transmitted information on the acoustic channel. The article considers the problems of leakage of confidential information through the acoustic channel of communication and methods of its prevention. Various approaches to protection against leakage through the acoustic channel are described, such as the use of noise-reducing materials, protective screens and software, and examples of successful implementation of protection measures are given. It is important to note that the protection of information against leakage through the acoustic channel is part of a complex security system, which is an algorithmically ordered and interconnected set of centrally controlled functionally independent technical subsystems of a specific purpose.

Keywords: information leakage, acoustic channel, information protection, noise reduction, security screens, software, sound locks.

Acknowledgements: This section provides information on research funding under various grants This study was supported by the Russian Federation State Task № FNNN-2024-0016.

For citation: Kartsan, I. N. (2024). Ensuring protection of information from acoustic channel leakage. Modern Innovations, Systems and Technologies, 4(1), 0176–0184. https://doi.org/10.47813/2782-2818-2024-4-1-0176-0184

ВВЕДЕНИЕ

В настоящее время, информационные технологии играют ключевую роль во всех сферах жизни, включая бизнес и общество. С появлением новых технологий и возможностей, становится все более важно обеспечить надежную защиту конфиденциальной информации от утечек [1, 2]. Необходимо помнить, что цифровые технологии, хоть и предоставляют множество преимуществ, но также несут в себе риски. Одной из таких угроз является утечка конфиденциальной информации через акустический канал (рисунок 1). Сегодня многие компании и организации становятся жертвами утечки информации, которая может стать причиной серьезных проблем и

потерь. Утечка через акустический канал является одной из наиболее опасных угроз, поскольку позволяет злоумышленникам получить доступ к конфиденциальной информации, используя звуковые волны [3-6]. Для предотвращения утечек конфиденциальной информации через акустический канал, необходимы соответствующие меры защиты, такие как использование защищенных коммуникационных каналов, шифрования и маскировки звуковых сигналов. Также важно проводить регулярные проверки и аудиты для выявления уязвимостей в системах защиты информации. Утечка информации через акустический канал является серьезной угрозой для безопасности данных и может происходить в различных сценариях.

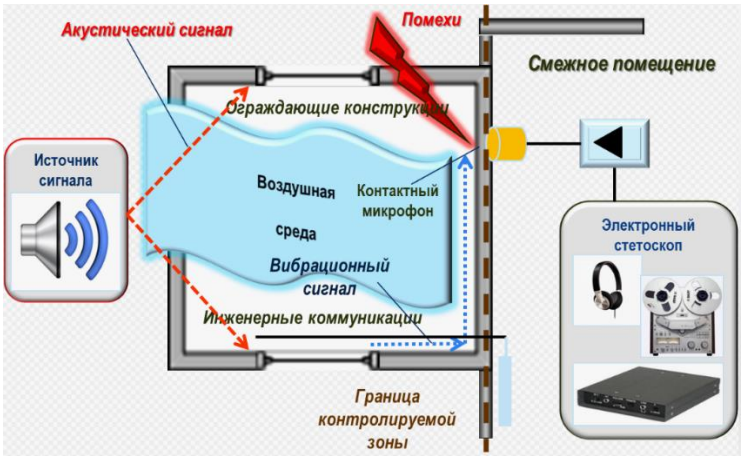

Рисунок 1. Технический канал утечки акустической речевой информации.

Figure 1. Technical channel of leakage of acoustic speech information.

Например, звук, издаваемый клавиатурой при наборе текста или звук, издаваемый при работе с микрофоном на компьютере или мобильном устройстве, может распространяться за пределы помещения, где находится устройство, генерирующее звук. Это может привести к утечке конфиденциальной информации, такой как пароли, логины или банковские данные, что может иметь серьезные последствия. Чтобы предотвратить такие утечки, необходимо принимать меры по защите акустических каналов, такие как использование клавиатур с защитой от звука и микрофонов с шумоподавлением [2, 7]. Кроме того, следует обучать пользователей правильному использованию устройств и информировать их о возможных угрозах безопасности данных.

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ КАНАЛУ

Способы защиты речевой информации от утечки по акустическому каналу основаны на уменьшении отношения «сигнал/шум». Существует несколько способов защиты информации от утечки по акустическому каналу. При выборе способа защиты, необходимо учитывать особенности помещения, в котором находится обрабатываемая информация, а также уровень конфиденциальности этих данных [8-11].

Шумоподавляющие материалы

Один из эффективных подходов - использование шумоподавляющих материалов. Эти материалы поглощают звук и предотвращают его распространение за пределы помещения. Шумоподавляющие материалы могут быть использованы для защиты помещений, в которых обрабатывается конфиденциальная информация, таких как офисы, серверные и аудитории. В качестве таких материалов могут использоваться специальные панели из пены или губки, которые прекрасно поглощают звук и не пропускают его наружу, характеристики звукопоглощающих свойств различных конструкций окон приведены в таблице 1. Эти материалы, такие как минеральная вата, каменная вата или пористый бетон, могут заметно снизить уровень звука в помещении. Это особенно полезно для офисов, где много людей работают вместе, и шум может отвлекать сотрудников от работы. Кроме того, звукопоглощающие материалы могут улучшить качество звука внутри помещения, делая его более приятным для слуха.

Таблица 1. Звукоизоляция конструкций.

Table 1. An example of a table.

Тип	Звукоизоляция (Дб) на частотах, Гц					
	125	250	500	1000	2000	4000
Одинарное остекление						
толщина 3 мм	17	17	22	28	31	32
толщина 4 мм	18	23	26	31	32	32
толщина 6 мм	22	22	26	30	27	25
Двойное остекление с воздухом						
57мм (толщина 3 мм)	15	20	32	41	49	46
90 мм (толщина 3 мм)	21	29	38	44	50	48
57мм (толщина 4 мм)	21	31	38	46	49	35
90 мм (толщина 4 мм)	25	33	41	47	48	36

Также можно установить шумопоглощающие шторы или жалюзи на окна, которые будут предотвращать проникновение звука в помещение. Использование шумоподавляющих материалов — это важная мера для защиты конфиденциальной информации, которая обрабатывается в помещении от утечки по акустическому каналу.

Защитные экраны

Кроме использования звукопоглощающих материалов, другой подход - использование защитных экранов. Защитные экраны могут быть изготовлены из специальных материалов, таких как металлические сетки или стеклянные панели, которые поглощают звук и предотвращают его распространение вне помещения. Экраны можно установить на окна, двери, стены или другие поверхности, которые могут быть источником утечки информации. Это может быть особенно полезно для конференц-залов или комнат для переговоров, где конфиденциальность информации крайне важна (рисунок 2).

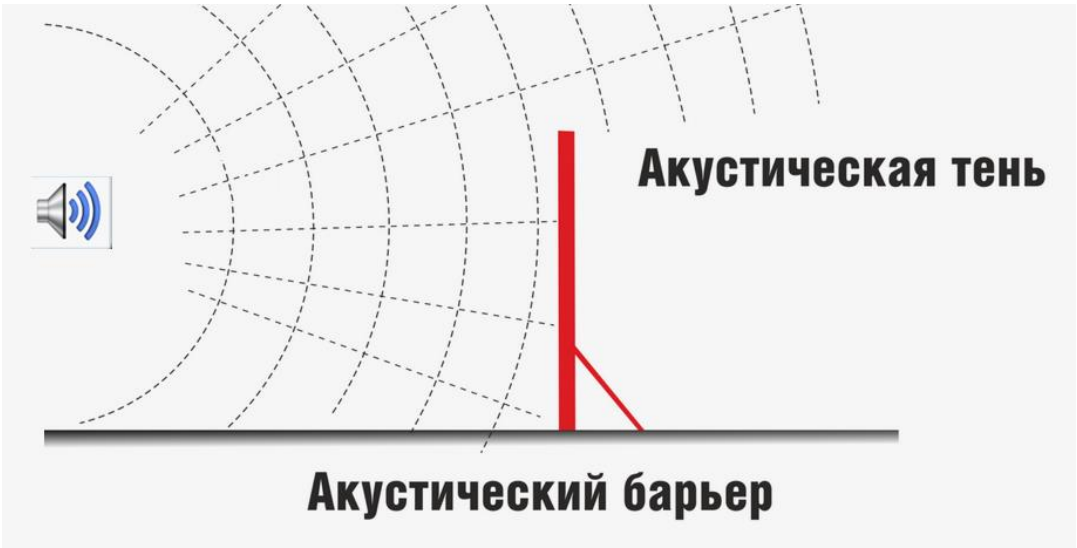

Рисунок 2. Работа защитного экрана.

Figure 2. Operation of the protective screen.

Как вариант, можно использовать экранирование помещения, где происходят конфиденциальные переговоры, с помощью специальных материалов, которые блокируют звуковые волны.

Программное обеспечение

Другим способом является использование шифрования звуковой информации с помощью специальных программных алгоритмов, которые защищают информацию от перехвата и расшифровки. Это позволяет сделать информацию недоступной для несанкционированного доступа, так как для расшифровки аудиосигнала необходимо иметь специальный ключ.

Кроме того, помимо использования программного обеспечения, которое блокирует звуковые сигналы, передаваемые через устройства, можно применять другие способы защиты от перехвата звуковой информации. К такому способу можно отнести использование автоматических генераторов белого шума, которые маскируют звуки, производимые во время разговора, и делают их неуловимыми для устройств, которые могут их перехватывать.

Одним из примеров успешной реализации мер защиты информации от утечки по акустическому каналу является применение такой технологии, как "звуковой замок". Эта технология может быть расширена, чтобы обеспечить еще большую безопасность передачи конфиденциальных данных. Например, в звуковой замок могут быть добавлены звуки, которые производятся при работе приложений или оборудования, что позволит обеспечить безопасность при передаче конфиденциальных данных. Звуковой замок может использовать алгоритмы для создания уникальных звуковых сигнатур, которые позволяют устройствам распознавать собственные звуковые сигналы и блокировать все остальные звуки, кроме тех, которые заданы как безопасные. Эта технология может быть расширена, чтобы обеспечить еще большую безопасность передачи конфиденциальных данных. Кроме того, звуковой замок может быть дополнен другими мерами защиты, такими как шифрование данных или использование биометрических данных для авторизации пользователей. В целом, использование звукового замка с другими мерами защиты может создать более надежную защиту от утечки конфиденциальных данных.

ЗАКЛЮЧЕНИЕ

Важно отметить, что защита информации от утечки через акустический канал — это только один из важных элементов системы безопасности. Эта мера направлена на предотвращение возможности получения доступа к конфиденциальной информации через звуковые сигналы. Кроме того, немаловажным аспектом безопасности является

защита от взлома. Для этого необходимо применять представленные способы, в совокупности.

Каждый из представленных способов является важной частью комплексной системы безопасности, которая должна быть реализована на предприятиях (организациях). Без сомнения, все эти меры помогают защитить конфиденциальную информацию предприятия (организации) от утечки и несанкционированного доступа.

СПИСОК ЛИТЕРАТУРЫ

[1] Бударный Г.С., Ахметов Р.Р., Камалова А.О., Соколов И.В. Виды утечки информации при помощи радиоволн и способы защиты. Научный аспект. 2024; 1(41): 5377-5390.

[2] Мифтахова Л.И. Каналы утечки и искажения информации. Информационные технологии обеспечения комплексной безопасности в цифровом обществе: материалы VI Всероссийской молодежной научно-практической конференции с международным участием. Уфа; 2023: 149-152.

[3] Хорев А.А., Дворянкин С.В., Козлачков С.Б., Василевская Н.В. Анализ предельных возможностей методов шумопонижения и реконструкции речевых сигналов, маскируемых различными типами помех. Вопросы кибербезопасности. 2024; 1(59): 89-100.

[4] Аверьянов В.С., Карцан И.Н. Методы оценки защищенности автоматизированных систем на базе квантовых технологий согласно CVSSV2.0/V3.1. Защита информации. Инсайд. 2023; 1(109): 18-23.

[5] Карцан И.Н., Жуков А.О. Механизм защиты промышленной сети. Информационные и телекоммуникационные технологии. 2021; 52: 19-26.

[6] Мосолов А.С., Прус Ю.В., Мальцев Н.В., Урбан Н.А. К вопросу построения надёжной системы обеспечения информационной безопасности предприятия. Информационная безопасность: вчера, сегодня, завтра. Сборник статей по материалам VI Всероссийской научно-практической конференции. Москва; 2023: 117-123.

[7] Мясников К.П., Микаева С.А., Журавлева Ю.А. Программированный микроконтроллер для устройств защиты информации. Автоматизация. Современные технологии. 2024; 3(78): 138-143.

[8] Гаиашвили Е.В., Абрамов Д.Е., Прощенков К.Ю. Разработка алгоритмов

криптографии для защиты данных. Развитие науки и практики в глобально меняющемся мире в условиях рисков. Сборник материалов XXII Международной научно-практической конференции. Москва; 2023: 120-125.

[9] Астапов Е.А., Ляхов С.Ю., Прохоров М.В. Безопасность программного обеспечения: основные уязвимости и методы защиты. Программная инженерия: современные тенденции развития и применения (ПИ-2023). Сборник материалов VII-й Всероссийской научно-практической конференции. Курск; 2023: 125-127.

[10] Алексеенко И.А., Волобуев В.А., Головской В.А. Одна алгоритмическая проблема технической защиты информации. Прикладная математика: современные проблемы математики, информатики и моделирования. Материалы V Всероссийской научно-практической конференции, молодых ученых. Краснодар; 2023: 133-137.

[11] Кузнецов Е.С., Ананьева Е.С. Современные методы защиты информации. Современные и информационные технологии в социальной сфере: сборник научных трудов III Всероссийской научно-практической конференции. Чебоксары; 2023: 144-149.

REFERENCES

[1] Budarnyj G.S., Ahmetov R.R., Kamalova A.O., Sokolov I.V. Vidy utechki informacii pri pomoshchi radiovoln i sposoby zashchity. Nauchnyj aspekt. 2024; 1(41): 5377-5390. (in Russian)

[2] Miftahova L.I. Kanaly utechki i iskazheniya informacii. Informacionnye tekhnologii obespecheniya kompleksnoj bezopasnosti v cifrovom obshchestve: materialy VI Vserossijskoj molodezhnoj nauchno-prakticheskoj konferencii s mezhdunarodnym uchastiem. Ufa; 2023: 149-152. (in Russian)

[3] Horev A.A., Dvoryankin S.V., Kozlachkov S.B., Vasilevskaya N.V. Analiz predel'nyh vozmozhnostej metodov shumoponizheniya i rekonstrukcii rechevyh signalov, maskiruemyh razlichnymi tipami pomekh. Voprosy kiberbezopasnosti. 2024; 1(59): 89-100. (in Russian)

[4] Aver'yanov V.S., Karcan I.N. Metody ocenki zashchishchennosti avtomatizirovannyh sistem na baze kvantovyh tekhnologij soglasno CVSSV2.0/V3.1. Zashchita informacii. Insajd. 2023; 1(109): 18-23. (in Russian)

[5] Karcan I.N., Zhukov A.O. Mekhanizm zashchity promyshlennoj seti. Informacionnye i telekommunikacionnye tekhnologii. 2021; 52: 19-26. (in Russian)

[6] Mosolov A.S., Prus YU.V., Mal'cev N.V., Urban N.A. K voprosu postroeniya nadyozhnoj sistemy obespecheniya informacionnoj bezopasnosti predpriyatiya. Informacionnaya bezopasnost': vchera, segodnya, zavtra. Sbornik statej po materialam VI Vserossijskoj nauchno-prakticheskoj konferencii. Moskva; 2023: 117-123. (in Russian)

[7] Myasnikov K.P., Mikaeva S.A., Zhuravleva YU.A. Programmirovannyj mikrokontroller dlya ustrojstv zashchity informacii. Avtomatizaciya. Sovremennye tekhnologii. 2024; 3(78): 138-143. (in Russian)

[8] Gaiashvili E.V., Abramov D.E., Proshchenkov K.YU. Razrabotka algoritmov kriptografii dlya zashchity dannyh. Razvitie nauki i praktiki v global'no menyayushchemsya mire v usloviyah riskov. Sbornik materialov XXII Mezhdunarodnoj nauchno-prakticheskoj konferencii. Moskva; 2023: 120-125. (in Russian)

[9] Astapov E.A., Lyahov S.Yu., Prohorov M.V. Bezopasnost' programmnogo obespecheniya: osnovnye uyazvimosti i metody zashchity. Programmnaya inzheneriya: sovremennye tendencii razvitiya i primeneniya (PI-2023). Sbornik materialov VII-j Vserossijskoj nauchno-prakticheskoj konferencii. Kursk; 2023: 125-127. (in Russian)

[10] Alekseenko I.A., Volobuev V.A., Golovskoj V.A. Odna algoritmicheskaya problema tekhnicheskoj zashchity informacii. Prikladnaya matematika: sovremennye problemy matematiki, informatiki i modelirovaniya. Materialy V Vserossijskoj nauchno-prakticheskoj konferencii, molodyh uchenyh. Krasnodar; 2023: 133-137. (in Russian)

[11] Kuznecov E.S., Anan'eva E.S. Sovremennye metody zashchity informacii. Sovremennye i informacionnye tekhnologii v social'noj sfere: sbornik nauchnyh trudov III Vserossijskoj nauchno-prakticheskoj konferencii. Cheboksary; 2023: 144-149. (in Russian)

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Карцан Игорь Николаевич, доктор технических наук, доцент, ведущий научный сотрудник Морского гидрофизического института РАН, Севастополь, Россия

Igor Kartsan, Dr. Sc., Docent, Leading Researcher, Marine Hydrophysical Institute, Russian Academy of Sciences, Sevastopol, Russia

Статья поступила в редакцию 20.03.2024; одобрена после рецензирования 29.03.2024; принята к публикации 30.03.2024.

The article was submitted 20.03.2024; approved after reviewing 29.03.2024; accepted for publication 30.03.2024.