ТЕОРИЯ УПРАВЛЕНИЯ

Дата поступления рукописи в редакцию: 19.05.2026 г.
Дата принятия рукописи в печать: 30.06.2026 г.
DOI: 10.24412/3034-4271-2026-3-90-95

ДАХНОВ Андрей Игоревич,
магистрант,
НИУ «МИЭТ»,
e-mail: frogigrog1221@gmail.com

АКУСТИЧЕСКИЕ ЗАКЛАДНЫЕ УСТРОЙСТВА, ВНЕДРЯЕМЫЕ В СЕТИ ПИТАНИЯ

Аннотация. *Актуальность исследования обусловлена возрастающей угрозой утечки конфиденциальной речевой информации через акустические закладные устройства, использующие сети электропитания 220 В в качестве среды распространения сигнала. В отличие от радиозакладок, такие устройства не создают демаскирующего излучения, что делает их особо опасными. Научная новизна работы заключается в разработке метода обнаружения сетевых закладок на основе корреляционного анализа высокочастотных шумов. Предложено математическое описание модели сигнала закладки с амплитудной модуляцией речью и псевдослучайной перестройкой рабочей частоты (ППРЧ). Алгоритм использует преобразование Гильберта для выделения огибающей, вычисление автокорреляционной функции и пороговое решение. Проведено имитационное моделирование в среде MATLAB: при отношении сигнал/шум –6 дБ вероятность правильного обнаружения составила 0,92 при вероятности ложной тревоги 0,05. Углублённо проанализированы принципы работы корреляционных приёмников, нелинейной локации и рефлектометрии применительно к сетевым закладкам. Рассмотрены сценарии маскировки с использованием протоколов PLC Prime и G3-PLC, включая внедрение закладного сигнала в шифрованный трафик IoT-устройств. Показано, что традиционные анализаторы спектра неэффективны против закладок с ППРЧ и адаптивной модуляцией, тогда как корреляционный метод сохраняет работоспособность. Полученные результаты могут быть использованы при создании систем непрерывного мониторинга проводных линий и разработке методик противодействия техническим каналам утечки речевой информации.*

Ключевые слова: *акустические закладные устройства, сетевые закладки, корреляционный анализ, преобразование Гильберта, метод обнаружения, PLC, Prime, G3-PLC, защита информации.*

DAKHNOV Andrew Igorevich,
Master's student,
NIU «MIET»

ACOUSTIC COVERT SURVEILLANCE DEVICES INSERTED INTO POWER SUPPLY NETWORKS

Annotation. *The relevance of the study is determined by the increasing threat of confidential speech information leakage through acoustic covert surveillance devices that use 220 V power supply networks as a signal propagation medium. Unlike radio bugs, such devices do not produce revealing emissions, which makes them particularly dangerous. The scientific novelty of the work lies in the development of a detection method for mains bugs based on correlation analysis of high-frequency noise. A mathematical description of the bug signal model with speech amplitude modulation and pseudo-random frequency hopping is proposed. The algorithm uses the Hilbert transform to extract the envelope, computes the autocorrelation function, and applies a threshold decision. Simulation in MATLAB environment was carried out: at a signal-to-noise ratio of –6 dB, the probability of correct detection was 0.92 with a false alarm probability of 0.05. The principles of operation of correlation receivers, nonlinear location and reflectometry in relation to mains bugs are analyzed in depth. Masking scenarios using Prime and G3-PLC protocols are considered, including the injection of a covert signal into encrypted IoT device traffic. It is shown that traditional spectrum analyzers are ineffective against bugs with frequency hopping and adaptive modulation, while the correlation method remains operational. The obtained results can be used in the creation of continuous monitoring systems for wired lines and the development of methods for counteracting technical channels of speech information leakage.*

Key words: *acoustic covert surveillance devices, mains bugs, correlation analysis, Hilbert transform, detection method, PLC, Prime, G3-PLC, information security.*

Введение

Проблема противодействия техническим каналам утечки информации сохраняет свою остроту в условиях цифровой трансформации общества. Среди наиболее распространённых и опасных методов негласного получения конфиденциальной речевой информации особое место занимают закладные устройства. Под такими устройствам понимаются скрытно размещаемые малогабаритные электронные средства, предназначенные для съёма информации в зонах её возможного появления или обработки. Если классические радиозакладки могут быть обнаружены по факту излучения в эфир, то устройства, использующие для передачи данных существующие проводные коммуникации (телефонные линии или сеть 220 В), обладают существенно более высокой степенью скрытности: их сигналы могут маскироваться под естественные помехи либо передаваться в паузах между сеансами связи.

Актуальность темы обусловлена несколькими факторами. Во-первых, широкое распространение интеллектуальных систем управления энергопотреблением («умных сетей») и устройств интернета вещей (IoT) создаёт новую среду распространения сигналов, которая может быть использована для маскировки закладных устройств.

Во-вторых, традиционные методы обнаружения, ориентированные на поиск радиоизлучения, оказываются неэффективными против устройств, передающих информацию по проводам.

В-третьих, наблюдается тенденция к миниатюризации и камуфлированию таких устройств под штатные элементы электрооборудования, что требует пересмотра существующих подходов к их выявлению

Целью данной работы является разработка метода обнаружения сетевых акустических закладок на основе корреляционного анализа высокочастотных шумов в сети 220 В с математическим обоснованием и экспериментальной проверкой. Для достижения цели решаются следующие задачи: построение модели сигнала закладки; разработка алгоритма обнаружения; углублённый анализ современных методов (корреляционные приёмники, нелинейная локация, рефлектометрия); исследование сценариев маскировки с использованием протоколов Prime и G3-PLC.

Классификация закладных устройств, внедряемых в проводные линии

По типу среды распространения информативного сигнала закладные устройства, внедряемые в проводные линии, подразделяются на две основные категории: телефонные закладки, подключаемые к абонентским или соединительным линиям, и сетевые закладки, использующие сеть переменного тока напряжением 220 В. Каждая из групп, характеризуется специфическими способами подключения, типами источников питания и конструктивными решениями.

Телефонные закладки

Телефонные закладки предназначены для перехвата переговоров, ведущихся как непосредственно по линии, так и в помещении, где находится телефонный аппарат. Их классификация может быть проведена по следующим признакам:

Рисунок 1. Классификация телефонных закладных устройств

Наиболее совершенной и скрытной разновидностью является конструкция, известная как «телефонное ухо» [2]. Устройство врезается в разрыв линии между абонентским аппаратом и АТС, питается непосредственно от линии (напряжение 48–60 В), что обеспечивает практически неограниченное время работы. Активация осуществляется дистанционно: оператор набирает номер контролируемого абонента, устройство после распознавания вызова глушит первые звонки и, приняв кодированный сигнал, имитирует снятие трубки, подключая к линии встроенный микрофон. Радиус действия такого устройства ограничен лишь доступностью телефонной сети, включая между-

городные и международные соединения.

Существуют модификации, в которых телефонная линия служит только источником питания, а перехваченная информация передается по радиоканалу. Это решение сохраняет энергетическую автономность, но вносит демаскирующий фактор радиоизлучения. Наибольшую сложность для обнаружения представляют устройства, встроенные непосредственно в корпус телефонного аппарата или микрофонную трубку и питающиеся от линии.

Сетевые закладки

Сетевые закладки используют силовую проводку 220В в качестве среды передачи перехваченной акустической информации.

Рисунок 2. Классификация сетевых закладных устройств

Информационный сигнал после усиления и, при необходимости, аналого-цифрового преобразования модулирует высокочастотную несущую (от десятков килогерц до единиц мегагерц), которая через развязывающие устройства вводится в фазу и/или нулевой провод. В пределах одного здания или группы зданий, питающихся от общей трансформаторной подстанции, дальность передачи достигает 300–500 м применение ретрансляторов позволяет расширить этот радиус [2].

Для повышения скрытности такие устройства часто выполняются в виде стандартных электротехнических изделий: удлинителей, тройников, сетевых адаптеров (блоков питания), розеток. Питание осуществляется непосредственно от сети 220 В через встроенный импульсный или трансформаторный блок, что обеспечивает неограниченное время непрерывной работы — ключевое преимущество перед автономными закладками.

Модель сигнала сетевой акустической закладки

Сетевая закладка осуществляет амплитудную или частотную модуляцию высокочастотной несущей f_c (от 50 кГц до 30 МГц) речевым сигналом s(t). Сигнал на выходе закладки можно представить в виде:

$$x(t) = A \cdot (1 + m \cdot s(t)) \cdot cos(2\pi f_c t + \varphi_0) + n(t), \quad (1)$$

где A – амплитуда несущей, m – коэффициент модуляции, φ_0 – начальная фаза, n(t) – собственные шумы устройства. При использовании псевдослучайной перестройки рабочей частоты (ППРЧ) частота изменяется по закону: $f_c(t)=f_0+k(t)\cdot\Delta f$, где k(t) – псевдослучайная последовательность.

При передаче по сети 220 В сигнал затухает и накладывается на импульсные помехи от бытовых приборов (выпрямители, инверторы) и PLC-сигналы. Модель наблюдаемого сигнала в точке подключения анализатора:

$$y(t) = \sum_i h_i \cdot x(t - \tau_i) + \sum_j p_j(t) + \sum_k q_k(t) + \omega(t), \quad (2)$$

где h_i, τ_i – коэффициенты и задержки многолучевого распространения, p_j (t) – импульсные помехи, q_k (t) – PLC-сигналы (например, Prime или G3-PLC), ω(t) – белый гауссов шум.

Метод обнаружения на основе корреляционного анализа

Предлагаемый метод использует тот факт, что речевой сигнал s(t) обладает высокой автокорреляцией на интервалах 20–40 мс (период основного тона). Корреляционный приёмник вычисляет функцию взаимной корреляции между принятым сигналом y(t) и опорным сигналом, сформированным как модель типовой речевой огибающей.

Алгоритм обнаружения:

1. Оцифровка сигнала y[n] с частотой дискретизации не менее 100 кГц.

2. Полосовая фильтрация в диапазоне предполагаемой несущей (например, 1–10 МГц).

3. Демодуляция огибающей: |e[n]=Hilbert(y[n])|

4. Вычисление автокорреляционной функции для задержек τ от 0 до 40 мс.

$$R_e[\tau] = \frac{1}{N}\sum_{n=0}^{N-1} e[n] \cdot e[n+\tau] \quad (3)$$

5. Пороговое решение: если максимум R_e [τ], при τ > 0 превышает $0{,}6\cdot R_e$ [0], фиксируется нали-

чие речевой модуляции.

Для случая ППРЧ используется параллельный банк корреляторов с адаптивным слежением за частотой. Вероятность правильного обнаружения P_d и ложной тревоги P_{fa} связаны соотношением:

$$P_d = Q\left(\frac{Q^{-1}P_{fa} - \sqrt{N}\cdot SNR}{\sqrt{2}}\right) \quad (4)$$

Имитационное моделирование. В среде MATLAB проведены эксперименты с моделью сигнала закладки (несущая 5 МГц, модуляция речью, ППРЧ с 10 частотами, скорость перестройки 100 скачков/с). При SNR = –6 дБ и длительности анализа 1 с получено P_d=0,92, при P_{fa}=0. Метод устойчив к импульсным помехам благодаря предварительной медианной фильтрации.

Углублённый анализ методов обнаружения сетевых закладок

Корреляционные приёмники используются для выделения слабых периодических сигналов из шума. В контексте сетевых закладок они позволяют обнаружить скрытую модуляцию речью, даже если несущая нестабильна. Принцип основан на накоплении энергии сигнала за счёт суммирования произведений принятой и опорной функций. Для ППРЧ применяются многоканальные корреляторы или согласованные фильтры с адаптивной подстройкой.

Нелинейная локация – метод обнаружения полупроводниковых элементов (диодов, транзисторов) в отключенном от питания оборудовании. Генератор излучает основную частоту f_0 (например, 100 МГц) и вторую гармонику $2f_0$. Полупроводниковый переход переизлучает вторую и третью гармоники. Применительно к сетевым закладкам, камуфлированным под удлинители, нелинейный локатор позволяет выявить наличие электронной схемы даже при отключенном питании

Недостаток – невозможность различения закладки и легитимного электронного устройства (например, блока питания).

Рефлектометрия – метод определения аномалий в линии по отражённым импульсам. Импульсный рефлектометр посылает короткий импульс и измеряет время задержки отражённых сигналов от неоднородностей волнового сопротивления. Сетевая закладка, подключённая параллельно, создаёт отражение, по которому можно оценить расстояние до неё. Однако для закладок с высоким входным сопротивлением (индуктивное или ёмкостное подключение) отражённый сигнал может быть слишком слабым. Современные частотные рефлектометры (FDR) используют сканирование по частоте и преобразование Фурье для повышения чувствительности.

Сценарии маскировки закладок с использованием IoT-протоколов Prime и G3-PLC

Протоколы PLC для «умных сетей» – Prime и G3-PLC – работают в диапазоне от десятков до сотен килогерц и используют модуляцию OFDM. Злоумышленник может выполнить маскировку двумя способами:

1. Интеграция закладного сигнала в штатный PLC-трафик. Перехваченная речь кодируется в виде псевдослучайных пакетов, имитирующих данные счётчика. Поскольку протоколы поддерживают шифрование (например, AES-128), легитимный трафик выглядит как шум, и закладной сигнал становится неотличим.

2. Использование уязвимостей IoT-устройств. Внедрение вредоносного кода в «умную» розетку или адаптер питания, который штатными средствами передаёт данные по PLC, но дополнительно собирает акустическую информацию через встроенный микрофон.

Для противодействия необходимы: (а) мониторинг целостности прошивок IoT-устройств; (б) анализ аномалий в трафике (например, нехарактерная для счётчика полоса пропускания); (в) использование внешних корреляционных обнаружителей, не зависящих от протокольной маскировки.

Заключение

В результате проведённого исследования получен новый метод обнаружения сетевых акустических закладок на основе корреляционного анализа высокочастотных шумов. Представлены математическая модель сигнала, алгоритм обработки и результаты имитационного моделирования (P_d=0,92, при SNR = –6 дБ). Углублённо проанализированы корреляционные приёмники, нелинейная локация и рефлектометрия, а также сценарии маскировки с использованием протоколов Prime и G3-PLC. Разработанный метод может быть интегрирован в системы непрерывного мониторинга проводных линий и использован для противодействия техническим каналам утечки речевой информации.

Список литературы:

[1] Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

[2] Хорев А. А. Технические каналы утечки акустической (речевой) информации // Специальная техника. – М.: 2009. – № 5. – С. 12–26.

[3] Хорев А. А. Классификация электронных устройств перехвата информации // Спецтехника и связь. 2009. №1. С. 46-49.

[4] Авсентьев А. О. Обоснование структуры подсистемы защиты речевой информации от утечки по акустическим каналам в составе многоагентной системы защиты / А. О. Авсентьев // Вестник Воронежского института МВД России. – 2023. – № 4. – С. 96-106.

[5] Дубровина А. Д. Анализ методов и средств обнаружения закладных устройств негласного получения информации / А. Д. Дубровина, А. С.

Кравченко // Актуальные проблемы деятельности подразделений УИС : Сборник материалов Всероссийской научно-практической конференции, Воронеж, 20 октября 2022 года. – Воронеж: Издательско-полиграфический центр «Научная книга», 2022. – С. 84-86.

[6] Рахматуллин Т. Ф. Основы технической защиты информации. Этапы развития технической защиты информации в области защиты государственной тайны / Т. Ф. Рахматуллин, Р. Р. Фаттахов // Студенческий. – 2025. – № 14-2(310). – С. 40-45.

[7] Пантелеймонова Д. Ю. Разработка методики выявления электронных устройств перехвата акустической речевой информации, построенных на базе средств сотовой связи с использованием анализатора спектра / Д. Ю. Пантелеймонова, Д. А. Бабчук // Аллея науки. – 2017. – Т. 2, № 11. – С. 475-478.

[8] Баженов С. В. Оперативно-розыскное мероприятие «Получение компьютерной информации» / С. В. Баженов // Научный вестник Омской академии МВД России. – 2017. – № 2(65). – С. 31-33.

[9] Кульбякина Н. Д. Обнаружение сетевых закладных устройств в периметре организации / Н. Д. Кульбякина, Г. В. Попков // Интерэкспо Гео-Сибирь. – 2022. – Т. 6. – С. 127-133.

[10] Порхун А. С. Классификация полуактивных закладных устройств аудиотранспондеров / А. С. Порхун // Радиоэлектронные устройства и системы для инфокоммуникационных технологий» («РЭУС-ИТ 2024») : Доклады Всероссийской конференции, посвященной Дню радио, Москва, 31 мая 2024 года. – Москва: Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова, 2024. – С. 399-403.

[11] Сурвило И. С. Выявление закладных устройств с использованием импульсно-рефлекторного метода / И. С. Сурвило, С. Н. Петров // Управление информационными ресурсами : Материалы XXI Международной научно-практической конференции, Минск, 28 марта 2025 года. – Минск: Академия управления при Президенте Республики Беларусь, 2025. – С. 304-305.

[12] Степанов М. О. Анализ современных закладных устройств / М. О. Степанов // Прикладная электродинамика, фотоника и живые системы - 2025 : Сборник тезисов докладов XII Международной молодежной научно-технической конференции молодых ученых, аспирантов и студентов, посвященной 70-летию со дня образования кафедры электронных и квантовых средств передачи информации КНИТУ-КАИ, 20-летию со дня образования кафедры радиофотоники и микроволновых технологий КНИТУ-КАИ, 60-летию выхода в открытый космос А.А. Леонова, Казань, 10–12 апреля 2025 года. – Казань: ИП Сагиев А.Р., 2025. – С. 763-765.

[13] Жуйков Е. А. Разработка математической модели обнаружения программных закладных устройств / Е. А. Жуйков // НБИ технологии. – 2023. – Т. 17, № 1. – С. 17-23.

[14] Степанов М. О. Обнаружение скрытых передающих устройств на основе анализа частотных характеристик / М. О. Степанов, Р. Р. Шарипов // Цифровые системы и модели: теория и практика проектирования, разработки и использования : Материалы международной научно-практической конференции, Казань, 10–11 апреля 2025 года. – Казань: Казанский государственный энергетический университет, 2025. – С. 2318-2320.

[15] Асанов Э. И. Методы утечки информации через проводную среду с помощью электронных закладных устройств / Э. И. Асанов, Р. Р. Шарипов // Цифровые системы и модели: теория и практика проектирования, разработки и использования : Материалы международной научно-практической конференции, Казань, 10–11 апреля 2025 года. – Казань: Казанский государственный энергетический университет, 2025. – С. 2047-2049.

[16] Асанов Э. И. Исследование гальванических характеристик проводной среды при подключении электронных закладных устройств / Э. И. Асанов, Р. Р. Шарипов // Цифровые системы и модели: теория и практика проектирования, разработки и использования : Материалы международной научно-практической конференции, Казань, 10–11 апреля 2025 года. – Казань: Казанский государственный энергетический университет, 2025. – С. 2040-2043.

[17] Попова Е. А. Учебно-тренажерный комплекс для проведения поиска закладных устройств / Е. А. Попова, А. В. Фурсова, А. В. Яковлев // Виртуальное моделирование, прототипирование и промышленный дизайн : Материалы IX Международной научно-практической конференции, Тамбов, 24–25 октября 2023 года. Том Выпуск 9. – Тамбов: Тамбовский государственный технический университет, 2023. – С. 190-195.

[18] Исютин А. С. Различные методы и технологии по поиску радиоакустических приборов / А. С. Исютин // Научно-исследовательский центр «Technical Innovations». – 2023. – № 11. – С. 166-170.

References:

[1] Khorev, A. A. Technical Information Security: A Textbook for University Students. In 3 Volumes. Vol. 1. Technical Channels of Information Leakage. Moscow: Research and Production Center «Analytics», 2008. 436 p.

[2] Khorev, A. A. Technical Channels of Acoustic (Speech) Information Leakage // Special Equipment. Moscow: 2009. No. 5. pp. 12–26.

[3] Khorev, A. A. Classification of Electronic Devices for Information Interception // Special Equipment and Communications. 2009. No. 1. pp. 46–49.

[4] Avsentyev, A. O. Justification of the Structure of the Subsystem for Protecting Speech Information from Leakage via Acoustic Channels as Part of a Multi-Agent Security System / A. O. Avsentyev //

Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. – 2023. – No. 4. – P. 96-106.

[5] Dubrovina A. D. Analysis of methods and means of detecting bugs for covert information retrieval / A. D. Dubrovina, A. S. Kravchenko // Actual problems of the activities of the UIS units: Collection of materials of the All-Russian scientific and practical conference, Voronezh, October 20, 2022. – Voronezh: Publishing and printing center «Scientific book», 2022. – P. 84-86.

[6] Rakhmatullin T. F. Fundamentals of technical information protection. Stages of development of technical information protection in the field of protecting state secrets / T. F. Rakhmatullin, R. R. Fattakhov // Student. – 2025. – No. 14-2 (310). – P. 40-45.

[7] Panteleimonova D. Yu. Development of a methodology for identifying electronic devices for intercepting acoustic speech information built on the basis of cellular communication facilities using a spectrum analyzer / D. Yu. Panteleimonova, D. A. Babchuk // Alley of Science. - 2017. - Vol. 2, No. 11. - Pp. 475-478.

[8] Bazhenov S. V. Operational-search measure «Obtaining computer information» / S. V. Bazhenov // Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia. - 2017. - No. 2 (65). - Pp. 31-33.

[9] Kulbyakina N. D. Detection of network eavesdropping devices within the perimeter of an organization / N. D. Kulbyakina, G. V. Popkov // Inter Expo Geo-Siberia. – 2022. – T. 6. – P. 127-133.

[10] Porkhun A. S. Classification of semi-active eavesdropping devices of audio transponders / A. S. Porkhun // Radioelectronic devices and systems for infocommunication technologies» («REUS-IT 2024»): Reports of the All-Russian conference dedicated to Radio Day, Moscow, May 31, 2024. - Moscow: Russian Scientific and Technical Society of Radio Engineering, Electronics and Communications named after A.S. Popov, 2024. - P. 399-403.

[11] Survilo I. S. Detection of eavesdropping devices using the pulse-reflex method / I. S. Survilo, S. N. Petrov // Information Resources Management: Proceedings of the XXI International Scientific and Practical Conference, Minsk, March 28, 2025. - Minsk: Academy of Public Administration under the President of the Republic of Belarus, 2025. - P. 304-305.

[12] Stepanov M. O. Analysis of modern buggy devices / M. O. Stepanov // Applied Electrodynamics, Photonics and Living Systems - 2025: Collection of abstracts of reports of the XII International Youth Scientific and Technical Conference of Young Scientists, Postgraduates and Students, dedicated to the 70th anniversary of the foundation of the Department of Electronic and Quantum Information Transmission Means of KNITU-KAI, the 20th anniversary of the foundation of the Department of Radio Photonics and Microwave Technologies of KNITU-KAI, the 60th anniversary of A. A. Leonov's spacewalk, Kazan, April 10-12, 2025. - Kazan: IP Sagiyev A.R., 2025. - P. 763-765.

[13] Zhuykov E. A. Development of a mathematical model for detecting software buggy devices / E. A. Zhuykov // NBI technology. - 2023. - Vol. 17, No. 1. - Pp. 17-23.

[14] Stepanov M. O. Detection of hidden transmitting devices based on frequency response analysis / M. O. Stepanov, R. R. Sharipov // Digital systems and models: theory and practice of design, development and use: Proceedings of the international scientific and practical conference, Kazan, April 10-11, 2025. - Kazan: Kazan State Power Engineering University, 2025. - Pp. 2318-2320.

[15] Asanov E. I. Methods of information leakage through a wired environment using electronic eavesdropping devices / E. I. Asanov, R. R. Sharipov // Digital systems and models: theory and practice of design, development and use: Proceedings of the international scientific and practical conference, Kazan, April 10-11, 2025. - Kazan: Kazan State Power Engineering University, 2025. – P. 2047-2049.

[16] Asanov E. I. Study of galvanic characteristics of a wired environment when connecting electronic eavesdropping devices / E. I. Asanov, R. R. Sharipov // Digital systems and models: theory and practice of design, development and use: Proceedings of the international scientific and practical conference, Kazan, April 10-11, 2025. – Kazan: Kazan State Power Engineering University, 2025. – P. 2040-2043.

[17] Popova E. A. Educational and training complex for searching for eavesdropping devices / E. A. Popova, A. V. Fursova, A. V. Yakovlev // Virtual modeling, prototyping and industrial design: Proceedings of the IX International Scientific and Practical Conference, Tambov, October 24-25, 2023. Volume Issue 9. – Tambov: Tambov State Technical University, 2023. – P. 190-195.

[18] Isyutin A. S. Various methods and technologies for searching for radio acoustic devices / A. S. Isyutin // Research Center «Technical Innovations». – 2023. – No. 11. – P. 166-170.