

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ,
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004

DOI: 10.17212/2782-2230-2026-2-68-90

**ВЛИЯНИЕ ГЕОМЕТРИЧЕСКИХ ПАРАМЕТРОВ
АНТЕННЫХ СИСТЕМ НА ФОРМИРОВАНИЕ
ГАРАНТИРОВАННЫХ ЗОН ПОДАВЛЕНИЯ
КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ***

И.В. ТРУБИН¹, И.В. ВОЖОВ², П.Р. ЧЕРНЫШЕВ³

¹ РФ, 630087, г. Новосибирск, ул. Немировича-Данченко 138 офис 2/2, Общество с ограниченной ответственностью «КБ Автоматика», заместитель директора. E-mail: i.trubin@corp.nstu.ru

² РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: ivozhov@mail.ru

³ РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: p.chernyshev.2021@stud.nstu.ru

Статья посвящена исследованию пространственно-энергетических характеристик систем активного радиоподавления и их влиянию на информационную безопасность объектов. В работе проводится детальный анализ формирования зон гарантированного подавления сигналов в диапазоне 2,4 ГГц в зависимости от геометрических параметров и типа применяемых антенных систем. На базе программно-аппаратного комплекса (nRF24L01+PA+LNA и ESP32) и векторного анализатора спектра LIG Nex1 NS-30A проведено экспериментальное сравнение эффективности полуволновых диполей и четвертьволновых монополей с целью выявления зависимости между геометрией излучателя и равномерностью пространственного распределения помехи. Особое внимание уделено выявлению «коридоров радиопрозрачности» – зон критического падения мощности помехи (до 12...20 дБ), обусловленных формой диаграммы направленности и поляризационным рассогласованием. Результаты исследования позволяют количественно оценить риски утечки информации и сформулировать рекомендации по оптимизации пространственной конфигурации средств РЭБ для обеспечения непрерывного защитного поля.

Ключевые слова: информационная безопасность, диаграмма направленности, зона подавления, поляризация, полуволновой диполь, четвертьволновой монополь, техническая защита информации, nRF24L01, ESP32

* Статья получена 05 мая 2026 г.

ВВЕДЕНИЕ

Обеспечение информационной безопасности в современном мире неразрывно связано с контролем радиочастотного пространства. Широкое распространение протоколов Wi-Fi, Bluetooth и устройств интернета вещей (IoT), функционирующих в нелицензируемом ISM-диапазоне (2,4 ГГц), создает серьезные вызовы для технической защиты информации (ТЗИ), связанные с прозрачностью физических границ зданий для радиоизлучения, с доступностью аппаратных средств для перехвата данных и с высокой чувствительностью беспроводных интерфейсов к преднамеренному блокированию каналов связи. Одной из наиболее эффективных мер противодействия несанкционированному съему данных и деструктивным радиовоздействиям – преднамеренному блокированию каналов связи (DoS-атаки), подмене сигналов управления (спуфинг) или нарушению целостности передаваемой телеметрии – является применение систем активного радиоподавления.

Однако на практике эффективность защиты часто оценивается лишь по интегральной выходной мощности передатчика, без учета пространственной конфигурации электромагнитного поля. Подобный подход не охватывает всей специфики, так как любая реальная антенная система обладает неизотропной диаграммой направленности (ДН). Это приводит к возникновению «мертвых зон» и секторов с недостаточным энергетическим потенциалом помехи, через которые возможна скрытная передача данных злоумышленником.

Актуальность настоящей работы заключается в необходимости научного обоснования формирования «гарантированных зон подавления» с учетом геометрических параметров излучателей. Понимание физических процессов формирования ДН и специфики многолучевого распространения позволяет дополнить типовые методики размещения оборудования высокоточными данными о пространственных аномалиях поля, обеспечивая переход к адаптивному проектированию зон защиты в условиях сложных интерьеров.

Объектом исследования является структура электромагнитного помехового поля, формируемого в условиях реального интерьерного окружения (офисные/лабораторные помещения). В отличие от идеализированных измерений в дальней зоне, данный подход позволяет учесть влияние переотражений и интерференции на формирование зон подавления. В качестве генератора помех используется двухканальный модуль на базе микроконтроллера ESP32 и трансиверов nRF24L01+PA+LNA, функционирующий в режиме быстрого сканирования несущей VCO Sweeper в полосе 2,4 ГГц.

Научная новизна исследования состоит в экспериментальной верификации зон радиопрозрачности, возникающих при различных комбинациях типов антенн (полуволновой диполь Е-3000 и четвертьволновой монополюс штатная

штыревая антенна с коэффициентом усиления 2 дБи (децибел относительно изотропного излучателя) модели SMA-2.4G-2) и их пространственной ориентации. Методика измерений предполагает использование векторного анализатора спектра LIG Nex1 NS-30A на дистанциях 4...5 метров, что гарантирует работу в области полностью сформированного поля излучения.

Особое внимание уделено анализу наихудшего сценария – ситуации поляризационного и геометрического рассогласования антенн передатчика и приемника. Экспериментально доказывается, что некорректная пространственная ориентация антенн блокиратора может снижать эффективность защиты до 20...30 дБ, превращая систему активной защиты в «номинальную».

Реализация поставленной цели предполагает последовательное выполнение нескольких этапов эксперимента. На первом этапе проводится анализ характеристик сигнала при прямом кабельном соединении блокиратора с измерительным прибором. Это необходимо, чтобы зафиксировать точную мощность системы и оценить стабильность работы генератора без влияния внешних помех.

Дальнейшие исследования направлены на изучение сигнала уже в открытом пространстве. Это позволяет оценить реальную силу помехи в условиях помещения, где радиоволны отражаются от стен и препятствий. В рамках этого этапа сравниваются свойства полуволновых и четвертьволновых антенн, что помогает понять, как форма антенны влияет на надежность защиты.

1. ДИАПАЗОН 2,4 ГГц

Диапазон 2,4 ГГц занимает важное место в современных системах беспроводной связи, поскольку именно в нем реализуется работа большого числа распространенных технологий передачи данных. Его широкое применение связано не только с универсальностью, но и с доступностью элементной базы, используемой при построении радиосистем. В пределах этого диапазона одновременно функционируют такие стандарты, как Wi-Fi и Bluetooth, а также ряд других решений. Совместное использование одного и того же частотного ресурса различными технологиями неизбежно приводит к возникновению взаимных помех, что отрицательно сказывается на качестве и эффективности передачи данных [1]. Кроме того, специфика беспроводного радиоканала делает системы уязвимыми к воздействию внешних помех. При целенаправленном создании помехового сигнала возможно существенное нарушение или полное подавление работы технологии передачи данных [2].

1.1. ИНТЕРФЕЙСЫ ПЕРЕДАЧИ ДАННЫХ, ФУНКЦИОНИРУЮЩИЕ В ДИАПАЗОНЕ 2,4 ГГц

Одной из наиболее распространенных технологий беспроводной передачи данных является Wi-Fi, основанный на стандартах семейства IEEE 802.11 [3]. Согласно отчету WBA, в мире на 2023 год использовалось более 18 млрд Wi-Fi-устройств [4]. В диапазоне 2,4 ГГц сети Wi-Fi используют каналы шириной 20 или 40 МГц, при этом большинство каналов частично перекрываются по спектру. Технология Bluetooth, используемая для организации персональных беспроводных сетей, использует иной принцип организации передачи данных. Например, чтобы повысить устойчивость связи, используется механизм адаптивной перестройки частоты. Передача осуществляется посредством быстрого переключения между множеством узких каналов, что позволяет уменьшить влияние узкополосных помех и повысить надежность соединения [5].

Wi-Fi и Bluetooth функционируют в одном частотном диапазоне, что неизбежно приводит к взаимному влиянию этих технологий. Активность устройств Bluetooth может снижать пропускную способность устройств Wi-Fi и увеличивать задержки передачи данных, особенно в условиях высокой плотности спектра [6].

1.2. УЯЗВИМОСТИ БЕСПРОВОДНЫХ СЕТЕЙ К ПОМЕХОВОМУ ВОЗДЕЙСТВИЮ

Ключевой проблемой беспроводных систем связи является их высокая чувствительность к внешним электромагнитным воздействиям. В отличие от проводных каналов передачи данных, радиосигнал распространяется в открытой среде и может подвергаться воздействию различных источников помех. Помехи могут возникать как вследствие наложения сигналов устройств, работающих в одном диапазоне частот, так и в результате преднамеренных воздействий на радиоканал. Генерация радиочастотных помех может приводить к значительному снижению качества передачи данных. В исследовании «Against Jamming Attack in Wireless Communication Networks: A Reinforcement Learning Approach. Electronics» показано, что в условиях помехового воздействия успешность передачи пакетов снижалась до 0,5...0,7, тогда как применение специализированных алгоритмов позволяло повысить этот показатель до 0,84 при smart jamming и до 0,99 при sweep jamming [7].

Особую угрозу представляют атаки типа радиочастотного подавления, при которых злоумышленник намеренно формирует сигнал помехи для нарушения функционирования беспроводной сети. Такие воздействия способны

занимать радиочастотный спектр и препятствовать корректной передаче данных между легитимными устройствами [2].

Экспериментальные результаты показывают высокую эффективность подобных атак: в работе «Practical Realization of Reactive Jamming Attack on Long-Range Wide-Area Network» для пакетов с полезной нагрузкой 5 байт и более была зафиксирована полная потеря пакетов практически для всех исследованных режимов передачи, для некоторых конфигураций потери достигали 50...100 %. В каждом экспериментальном режиме оценка проводилась по серии из ста переданных пакетов [8].

В условиях развития беспроводных технологий и увеличения количества подключенных устройств задача обеспечения устойчивости радиосетей к подобным воздействиям приобретает особую актуальность. Поэтому исследование методов формирования помех, анализа их влияния на работу беспроводных интерфейсов и создание алгоритмов передачи данных, учитывающих наличие помех, является важным направлением современных исследований в области развития радиоэлектроники.

2. АРХИТЕКТУРА ЛАБОРАТОРНОГО СТЕНДА

Экспериментальный стенд представляет собой программно-аппаратный комплекс, предназначенный для формирования управляемых радиопомех и регистрации их пространственно-энергетических характеристик. Архитектура стенда разделена на три функциональных узла: 1) блок генерации помех, 2) сменный антенный комплекс и 3) измерительная система на базе анализатора спектра (рис. 1).

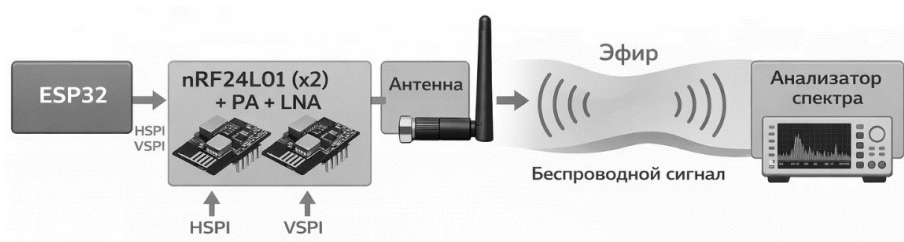


Рис. 1. Общая схема взаимодействия компонентов

Fig. 1. General diagram of component interactions

Блок генерации помех реализован на базе 38-пинового микроконтроллера ESP32 WROOM, который выступает в роли центрального узла управления.

Для создания помехового воздействия в диапазоне 2,4 ГГц используют два независимых радиомодуля nRF24L01+PA+LNA. Модули оснащены встроенными усилителями мощности (PA) и малошумящими усилителями (LNA), что критически важно для имитации высокомошных заградительных помех.

Для обеспечения максимальной скорости перестройки частоты модули подключены по отдельным аппаратным шинам: первый модуль подключен по интерфейсу HSPI (Hardware SPI), второй – по интерфейсу VSPI (Virtual SPI). В архитектуре микроконтроллера ESP32 эти интерфейсы представляют собой два независимых аппаратных блока (контроллера) стандартного протокола SPI. В отличие от традиционного последовательного подключения нескольких ведомых устройств к одной шине SPI (через выбор кристалла CS), использование двух отдельных шин позволяет осуществлять параллельную передачу данных. Это критически важно для реализации алгоритма VCO Sweep, так как минимизирует задержки на переключение между регистрами радиомодулей и позволяет в два раза увеличить скорость перестройки несущей частоты, обеспечивая формирование более плотного и непрерывного помехового спектра. Для стабилизации питания и компенсации пиковых токов потребления, возникающих в моменты активации выходных каскадов усилителей мощности (PA), в схему интегрированы электролитические конденсаторы емкостью 10 мкФ. Это позволяет минимизировать просадки напряжения на шине питания при высокой частоте переключения передатчиков в режиме сканирования диапазона (рис. 2).

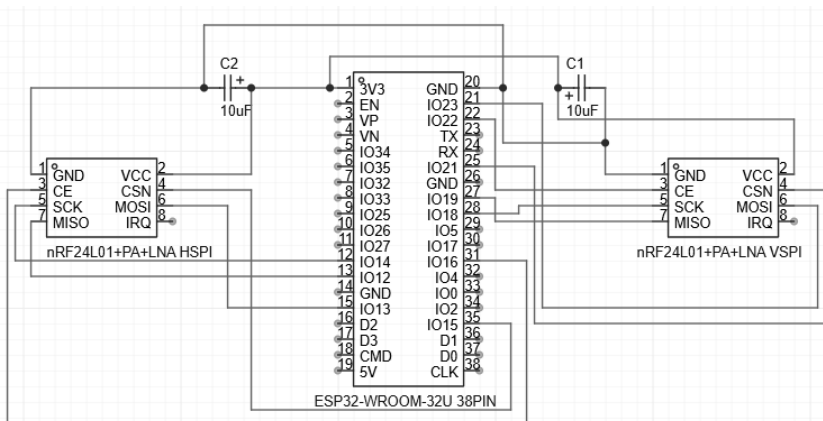


Рис. 2. Электрическая принципиальная схема

Fig. 2. Electrical schematic diagram

Важной особенностью эксплуатации стенда является обеспечение безопасности выходных каскадов радиомодулей. Поскольку архитектура предполагает одновременную работу двух передатчиков, а исследование проводится для одиночных антенных систем, ВЧ-выход неиспользуемого в конкретном замеры модуля нагружался на согласованную величину номиналом 50 Ом. Это позволило избежать критического роста коэффициента стоячей волны (КСВ) и предотвратить выход из строя усилителя мощности из-за отраженной энергии.

Сменный антенный комплекс включает два типа излучателей с различными волновыми характеристиками. Основным объектом исследования является промышленная полуволновая дипольная антенна Е-3000 (длина волны $\lambda/2$), обладающая выраженной тороидальной диаграммой направленности. В качестве альтернативной конфигурации используется четвертьволновой монополюс ($\lambda/4$), работающий совместно с корпусом стенда как единой излучающей системой. Сравнение типов антенн (рис. 3) позволяет оценить влияние геометрических параметров на формирование зон безопасности.

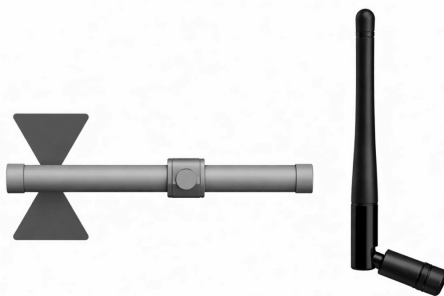


Рис. 3. Используемые антенны

Fig. 3. Antennas used

Измерительная система построена на базе векторного анализатора спектра LIG Nex1 NS-30A (рис. 4). Прибор обеспечивает фиксацию уровней мощности в режиме реального времени с высокой разрешающей способностью. Для калибровки источника использовалось прямое соединение через коаксиальный кабель с волновым сопротивлением 50 Ом, а для пространственных измерений применялась вертикально ориентированная широкополосная приемная антенна, установленная на штативе.



Рис. 4. Анализатор спектра LIG Nex1 NS-30A

Fig. 4. LIG Nex1 NS-30A Spectrum Analyzer

Такая архитектура стенда позволяет проводить комплексные испытания: от анализа «чистого» спектрального состава помехи внутри тракта до исследования сложных эффектов деполяризации и пространственного затухания в условиях реального интерьера.



Рис. 5. Общий вид стенда

Fig. 5. General view of the stand

Измерения проводились в условиях реального лабораторного помещения (рис. 5), что позволило оценить не только теоретическую форму лепестков диа-

граммы направленности, но и влияние переотражений от стен и мебели на общую устойчивость помехового поля.

3. МЕТОДИКА И РЕЗУЛЬТАТЫ ИСПЫТАНИЙ

Перед проведением испытаний были учтены действующие ограничения, связанные с использованием радиоэлектронных средств в полосе радиочастот 2400...2483,5 МГц. В соответствии с ФЗ 126 «О связи» использование радиочастотного спектра без соответствующего разрешения не допускается, если иное не предусмотрено законодательством [9]. Для ряда устройств малого радиуса действия в полосе 2400...2483,5 МГц допускается применение без оформления отдельных решений ГКРЧ и разрешений на использование радиочастот при соблюдении установленных условий, в том числе по параметрам излучения и режиму эксплуатации внутри закрытых помещений [10, 11].

В настоящей работе эксперимент проводился в пределах закрытого помещения на территории университета, а параметры стенда и схема размещения оборудования были выбраны таким образом, чтобы излучение не оказывало воздействия на сторонние радиоэлектронные средства за пределами лабораторной зоны. Следовательно, исследование является лабораторным моделированием помехового воздействия в контролируемых условиях.

В основу экспериментального исследования заложен принцип оценки эффективности активной радиоэлектронной защиты в условиях, максимально приближенных к реальной эксплуатации. Для получения достоверных данных о распределении электромагнитной энергии в пространстве измерения проводились в частотном диапазоне 2,4 ГГц, который является критически важным с точки зрения информационной безопасности (каналы Wi-Fi, Bluetooth).

Для изменения геометрических параметров антенных систем были выбраны два типа антенн (четвертьволновой монополь и полуволновой диполь).

Четвертьволновой монополь – это несимметричная антенна, представляющая собой один проводник длиной $1/4$ длины волны, установленный над проводящей поверхностью. Такая антенна имеет конструкцию в виде одного штыва. В роли второго «плеча» выступает земля, металлический корпус прибора. Пространственная диаграмма направленности четвертьволнового монополя представляет собой тороидальную структуру, усеченную бесконечной проводящей плоскостью. Излучение сосредоточено исключительно в верхнем полупространстве и образует радиально-симметричную фигуру вращения относительно оси излучателя (рис. 6). Из-за отражения от земли энергия не уходит вниз, а концентрируется в верхнем полушарии.

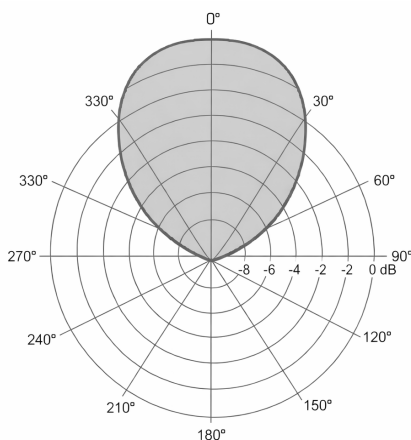


Рис. 6. Диаграмма направленности
четвертьволнового монополя

Fig. 6. Radiation pattern of
a quarter-wave monopole

Полуволновой диполь – это классическая симметричная антенна, состоящая из двух проводников длиной по $1/4$ длины волны каждый. Общая длина антенны составляет примерно половину длины волны. Конструкция представляет собой два «плеча», запитанных посередине, и требует обязательного заземления для работы. Пространственная диаграмма направленности симметричного полуволнового вибратора представляет собой тороидальную структуру (тор), обладающую осевой симметрией относительно проводника. Максимум интенсивности излучения сосредоточен в плоскости, перпендикулярной геометрической оси антенны, при наличии глубоких минимумов (нулей излучения) вдоль самой оси (рис. 7).

Дистанция измерения от антенны до анализатора спектра была выбрана (4...5 метров), это обусловлено требованиями электродинамической корректности. При длине волны $\lambda \approx 12,3$ см для используемых типов антенн ($\lambda/2$ и $\lambda/4$) граница дальней зоны (зоны Фраунгофера) начинается на удалении 0,3...0,5 м. Таким образом, проведение замеров на дистанции 5 метров гарантирует работу измерительного комплекса в области полностью сформированной диаграммы направленности (ДН), исключая влияние реактивных компонентов ближнего поля и фазовых искажений.

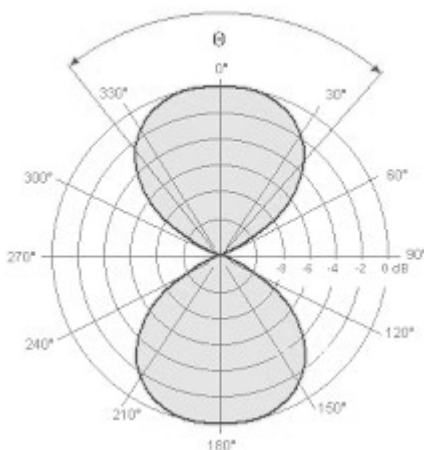


Рис. 7. Диаграмма направленности полуволнового диполя

Fig. 7. Radiation pattern of a half-wave dipole

С позиций информационной безопасности такой подход позволяет с высокой точностью верифицировать «зоны гарантированного подавления» и, что более важно, выявить «коридоры радиопрозрачности» – пространственные секторы, в которых энергетический потенциал помехи минимален. Исследование этих зон позволяет сформировать модель угроз, основанную на физических параметрах антенных систем, и разработать рекомендации по минимизации вероятности успешного перехвата данных в условиях активного радиопротиводействия.

3.1. КАЛИБРОВКА ИСТОЧНИКА И ОПРЕДЕЛЕНИЕ ЭНЕРГЕТИЧЕСКОГО ПОТЕНЦИАЛА

На первом этапе была произведена оценка спектральной плотности мощности генератора путем прямого подключения к анализатору спектра через коаксиальный кабель (рис. 8).

Анализ спектрограммы выявил «гребенчатую» структуру помехи, характерную для генераторов, управляемых напряжением (VCO). Было зафиксировано наличие амплитудной изрезанности (пик-фактор до 30...40 дБ), что свидетельствует о потенциальных временных лакунах в процессе сканирования диапазона, которыми могут воспользоваться адаптивные системы передачи данных.

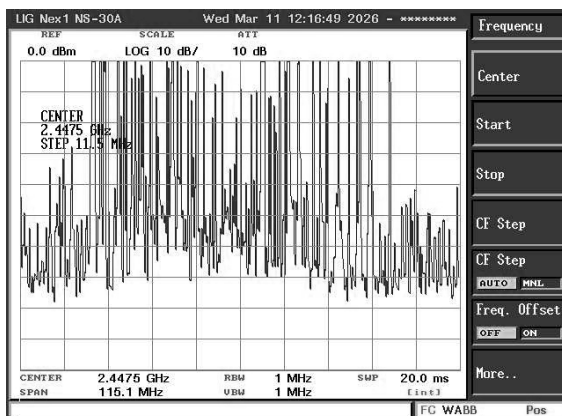


Рис. 8. Аппаратная спектрограмма выходного сигнала блокиратора при прямом соединении

Fig. 8. Hardware spectrogram of the blocker output signal with direct connection

3.2. ОЦЕНКА ЗАТУХАНИЯ В КАНАЛЕ И ВЛИЯНИЕ ДИСТАНЦИИ

Второй этап включал замеры уровня сигнала в эфире на дистанциях 1,5 и 5 м. Испытуемое устройство располагалось на фиксированной высоте (рис. 9).

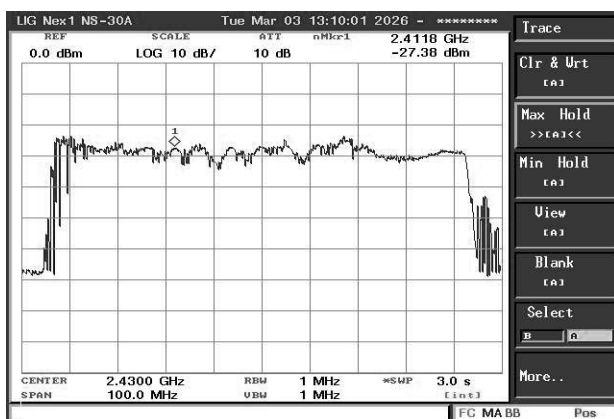


Рис. 9. Спектрограмма помехового поля на удалении 1,5 м

Fig. 9. Spectrogram of the interference field at a distance of 1,5 m

Сравнение результатов показало снижение уровня сигнала до $-27,38$ дБм на дистанции 1,5 м. Отмечено сглаживание спектральной «гребенки» за счет эффекта многолучевого распространения в закрытом помещении, что способствует более равномерному заполнению спектра шумом в точке приема.

3.3. ИССЛЕДОВАНИЕ ПРОСТРАНСТВЕННЫХ ХАРАКТЕРИСТИК (ДИАГРАММЫ НАПРАВЛЕННОСТИ)

Ключевой частью испытаний стало снятие сечений ДН. Испытуемая антенна вращалась относительно оси анализатора спектра с шагом 90° (рис. 10).

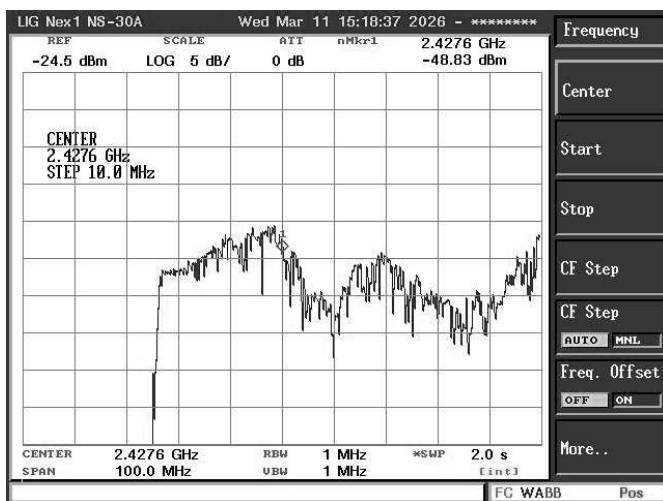


Рис. 10. Изменение мощности сигнала при различных угловых положениях полуволнового диполя (1-е положение)

Fig. 10. Change in signal power at different angular positions of the half-wave dipole (1th position)

При повороте на 90° (промежуточное положение) наблюдается начало спада амплитуды сигнала (рис. 11). Это демонстрирует постепенный выход приемника из основного лепестка диаграммы направленности.

Наиболее критическое падение мощности зафиксировано, когда антенна была направлена торцом к анализатору (рис. 12). Уровень сигнала снизился до $-58,11 \dots -60,97$ дБм.

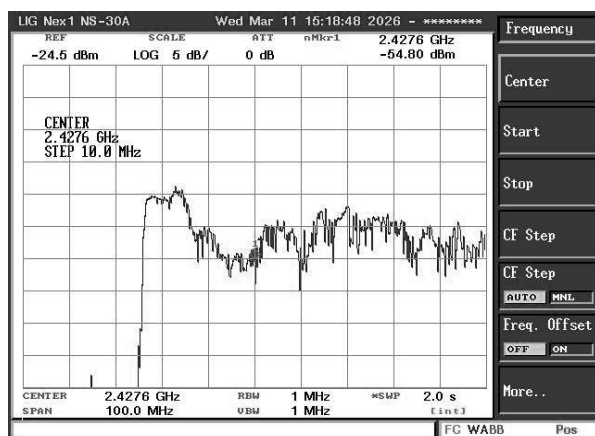


Рис. 11. Изменение мощности сигнала при различных угловых положениях полуволнового диполя (2-е положение)

Fig. 11. Change in signal power at different angular positions of the half-wave dipole (2th position)

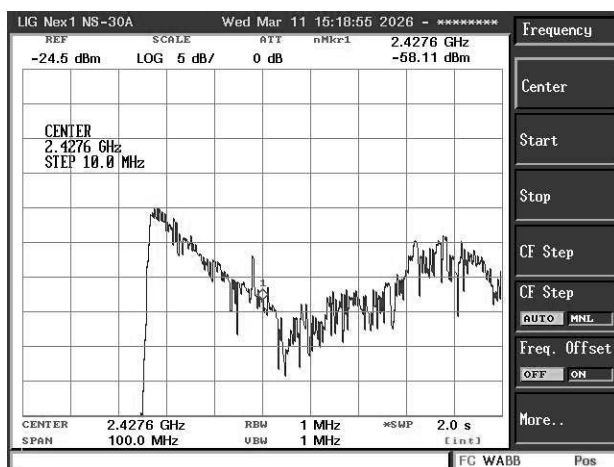


Рис. 12. Изменение мощности сигнала при различных угловых положениях полуволнового диполя (3-е положение)

Fig. 12. Change in signal power at different angular positions of the half-wave dipole (3th position)

Завершающий замер (рис. 13) подтвердил симметричность ДН диполя при возвращении в зону основного излучения.



Рис. 13. Изменение мощности сигнала при различных угловых положениях полуволнового диполя (4-е положение)

Fig. 13. Change in signal power at different angular positions of the half-wave dipole (4th position)

Исходя из полученных данных можно сделать вывод, что при подключенном полуволновом диполе, при ориентации «широкой стороной» (broadside) зафиксирован максимум излучения (−48,83 дБм). При развороте антенны торцом (end-fire) к анализатору уровень сигнала снизился до −58,11...−60,97 дБм.

Зафиксированный провал мощности в 12,14 дБ (более чем в 16 раз) подтверждает наличие выраженных «мертвых зон» вдоль оси антенны. С точки зрения ИБ эти зоны являются критическими уязвимостями, позволяющими обходить систему защиты. В частности, наличие выявленных «коридоров радиопрозрачности» означает, что в определенных секторах пространства (вдоль геометрической оси антенны) отношение сигнал/помеха (SNR) остается достаточным для декодирования информации приемным устройством.

Поскольку мощность помехового поля в этих зонах падает более чем в 16 раз относительно максимума, эффективный радиус подавления сокращается пропорционально квадрату расстояния. Это создает условия, при которых в пределах одного помещения могут существовать локальные зоны,

где блокирование каналов связи фактически не осуществляется. Злоумышленник, обладающий информацией о пространственной ориентации антенн системы защиты, может физически разместить средства съема данных (например, Wi-Fi-микрофоны или скрытые камеры) именно в осевых «нулях» диаграммы направленности. В таком сценарии полезный сигнал будет успешно передаваться в обход основного лепестка помехового воздействия, что делает систему активной защиты номинальной и неэффективной против квалифицированной атаки

Далее были проведены испытания с четвертьволновой антенной. Уровень сигнала в основном сечении показан на рис. 14.

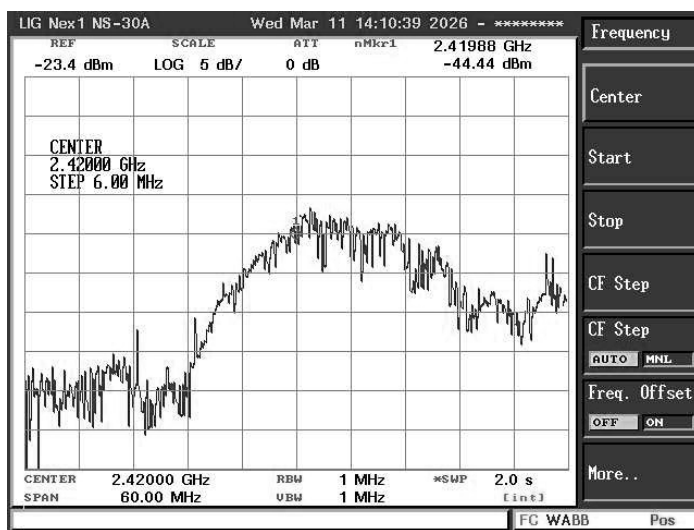


Рис. 14. Спектральные характеристики помехового поля при использовании четвертьволновой антенны (1-е положение)

Fig. 14. Spectral characteristics of the interference field when using a quarter-wave antenna (1th position)

При вращении монополя (рис. 15) уровень сигнала оставался стабильным (средний уровень – 44,44 дБм), что значительно выше, чем в «нулях» диполя.

Различное количество контрольных точек при снятии характеристик для полуволнового диполя и четвертьволнового монополя обусловлено фундаментальными различиями в их диаграммах направленности и результатами предварительного сканирования поля.

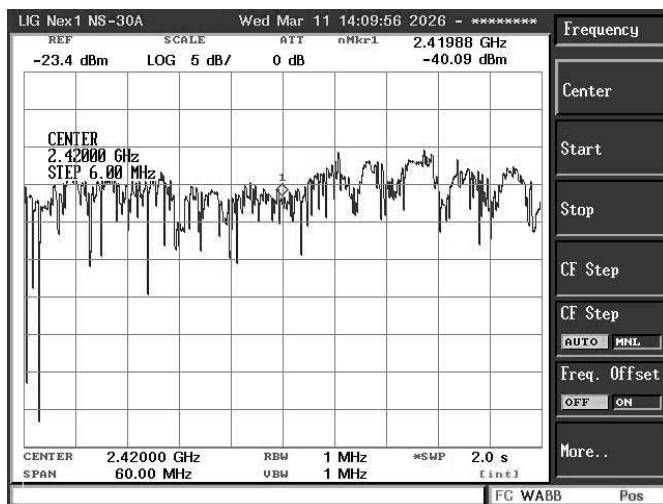


Рис. 15. Спектральные характеристики помехового поля при использовании четвертьволновой антенны (2-е положение)

Fig. 15. Spectral characteristics of the interference field when using a quarter-wave antenna (2th position)

Для полуволнового диполя было выбрано четырехточечное измерение (шаг 90°), так как теоретическая модель его излучения («тор») предполагает наличие выраженных экстремумов: двух максимумов в экваториальной плоскости и двух глубоких минимумов вдоль геометрической оси. Проведение четырех замеров позволило достоверно зафиксировать эти критические перепады мощности (до 12...20 дБ), которые являются ключевыми факторами риска в задачах ТЗИ.

Для четвертьволнового монополя количество контрольных точек было ограничено двумя диаметрально противоположными векторами (0° и 180°). Такое решение базируется на предварительной верификации стабильности помехового поля: в ходе первичного вращения было установлено, что отклонение уровня мощности не превышает 4,35 дБ. Высокая степень взаимодействия монополя с корпусом блокиратора, выполняющим роль противовеса, привела к «размытию» диаграммы направленности и формированию равномерного покрытия. В этих условиях увеличение числа измерительных позиций до четырех было признано избыточным, так как две контрольные точки уже подтвердили отсутствие глубоких осевых провалов, характерных для дипольной системы.

Зафиксированный максимум излучения для полуволнового диполя ($-48,83$ дБм) при номинальном кросс-поляризационном расположении антенн требует детального физического обоснования. В условиях идеального свободного пространства (отсутствие отражений) теоретические потери из-за несоответствия плоскостей поляризации могут составлять более $20...30$ дБ, что привело бы к практически полному исчезновению помехового сигнала на входе приемника.

Однако в реальных условиях эксперимента (размещение на диэлектрической опоре в замкнутом пространстве) наблюдается эффект деполяризации и вращения вектора E . Полученный уровень $-48,83$ дБм объясняется суммированием прямой волны и волн, отраженных от подстилающей поверхности (пола) и стен помещения. Отражение от диэлектрических и проводящих поверхностей приводит к «докручиванию» вектора поляризации до вертикальной составляющей, что и фиксируется анализатором спектра.

Этот факт имеет критическое значение для информационной безопасности: он доказывает, что в закрытых помещениях эффект многолучевого распространения частично компенсирует ошибки в ориентации антенн, «размазывая» энергию помехи по плоскостям поляризации.

3.4. РЕЗУЛЬТАТЫ ИСПЫТАНИЙ

Итоговым этапом стало моделирование условий эксплуатации, характеризующихся максимальным рассогласованием параметров (горизонтальное положение блокиратора при вертикальной поляризации приемника).

В ходе этого эксперимента было установлено катастрофическое снижение эффективности подавления: суммарные потери из-за кросс-поляризации и попадания в осевой «ноль» ДН превысили 20 дБ. В терминах практического применения это означает сокращение радиуса эффективного подавления в 10 раз (например, с 10 до 1 м).

Выводы по результатам испытаний

1. Экспериментально доказано, что при тестировании устройств на способность работать в условиях помех ключевым фактором является не только мощность генератора, но и пространственная ориентация антенн.

2. Обнаруженный эффект деполяризации в закрытом помещении частично компенсирует ошибки позиционирования за счет отражений, однако он не является достаточным для обеспечения гарантированной блокировки во всех ракурсах.

3. Для проведения корректных испытаний на помехоустойчивость рекомендуется использовать четвертьволновые антенны или антенные системы с круговой поляризацией, что минимизирует вероятность возникновения «ко-

ридеров радиопрозрачности», через которые испытываемое устройство может поддерживать связь в обход помехового воздействия.

4. Полученные количественные данные позволяют более точно рассчитывать необходимый энергетический запас (Safety Margin) при проектировании систем активной защиты информации.

ЗАКЛЮЧЕНИЕ

Проведенный сравнительный анализ экспериментальных данных показал, что переход от полуволнового диполя к четвертьволновому монополю привел к росту уровня сигнала в точке приема на 4,4 дБ. Этот эффект объясняется концентрацией излучаемой энергии в верхнюю полусферу относительно корпуса устройства, который в данном случае выполняет роль противовеса. Экспериментально подтверждено, что монополярная антенна в составе малогабаритного корпуса демонстрирует более высокую изотропность излучения, тогда как дипольная антенна показала глубокий провал мощности до 12 дБ вдоль собственной оси. Это свидетельствует о наличии выраженных пространственных зон радиопрозрачности, которыми могут воспользоваться сторонние устройства для поддержания связи в обход системы активной защиты.

При выборе типа антенной системы для конкретных прикладных задач необходимо учитывать их функциональные особенности и физические ограничения. Полуволновой диполь обладает преимуществом высокого усиления в плоскости, перпендикулярной оси антенны, что делает его эффективным инструментом для создания направленных радиочастотных барьеров (например, для защиты оконных проемов или периметра помещений). Однако наличие глубоких осевых минимумов требует строгого контроля пространственной ориентации излучателя. В свою очередь, четвертьволновой монополь отличается компактностью и обеспечивает более равномерное купольное покрытие пространства без критических осевых провалов. Это предпочтительное решение для портативных блокираторов и проведения лабораторных испытаний мобильных устройств на помехоустойчивость, так как в этом случае значительно снижается вероятность случайного попадания испытываемого прибора в мертвую зону диаграммы направленности.

В итоге для обеспечения гарантированного уровня технической защиты информации следует учитывать не только номинальную мощность передатчика, но и сложную геометрию формируемого поля с учетом поляризационных характеристик. Наиболее надежным подходом при тестировании систем на устойчивость к помехам является применение комбинированных антенных

решений, исключающих возникновение выявленных коридоров радиопрозрачности. Результаты выполненной работы могут служить методической базой для проектирования защищенных пространств внутри зданий и подготовки специалистов в области радиоэлектронной борьбы и информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Experimental Evaluation of Interference in 2.4 GHz Wireless Network / V. Agarwal, S. Mahmud, S. Kasera, M. Ji. – Office of Scientific and Technical Information, 2023. – DOI: 10.2172/2242485.
2. Pirayesh H., Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey // IEEE Communications Surveys & Tutorials. – 2022. – Vol. 24 (2). – P. 767–809. – DOI: 10.1109/COMST.2022.3159185.
3. A survey of IEEE 802.11ax WLAN temporal duty cycle for the assessment of RF electromagnetic exposure / Y. Yang, G. Vermeeren, L. Verloock, M. Guxens, W. Joseph // Applied Sciences. – 2025. – Vol. 15 (5). – P. 2858. – DOI: 10.3390/app15052858.
4. Wireless Broadband Alliance. WBA Annual Industry Report 2023.
5. Subhagato Dutta. The evolution of Bluetooth: A deep dive // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. – 2025. – Vol. 11 (1). – DOI: 10.32628/cseit251112261.
6. Lim S. IACR: An interference-aware channel reservation for wireless sensor networks // International Journal of Electrical and Computer Engineering. – 2019. – Vol. 9 (2). – DOI: 10.11591/ijece.v9i2.pp1220-1225.
7. Ma D., Wang Y., Wu S. Against jamming attack in wireless communication networks: A reinforcement learning approach // Electronics. – 2024. – Vol. 13 (7). – P. 1209. – DOI: 10.3390/electronics13071209.
8. Practical realization of reactive jamming attack on long-range wide-area network / J. Šabić, T. Perković, D. Begušić, P. Šolić // Sensors. – 2025. – Vol. 25 (8). – P. 2383. – DOI: 10.3390/s25082383.
9. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».
10. Каков порядок использования радиочастотного спектра радиоэлектронными средствами беспроводного доступа в диапазоне радиочастот 2,4 ГГц? // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: сайт. – URL: <https://digital.gov.ru/faq/kakov-poryadok-ispolzovaniya-radiochastotnogo-spektra-radioelektronnymi-sredstvami-besprovodnogo-dostupa-v-diapazone-radiochastot-24-ggcz> (дата обращения: 26.05.2026).

11. Условия использования радиоэлектронных средств малого радиуса действия в полосе радиочастот 2400–2483,5 МГц // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: сайт. – URL: <https://23.rkn.gov.ru/news/news114683.htm> (дата обращения: 26.05.2026).

Трубин Игорь Витальевич, заместитель директора ООО «КБ “Автоматика”». Основное направление научных исследований – защита технических каналов утечки информации. E-mail: i.trubin@corp.nstu.ru

Возов Илья Вадимович, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – разработка систем предотвращения утечки информации по техническим каналам. E-mail: ilvozhov@mail.ru

Чернышев Павел Романович, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – разработка систем обнаружения утечки информации по техническим каналам. E-mail: p.chernyshev.2021@stud.nstu.ru

DOI: 10.17212/2782-2230-2026-2-68-90

The influence of geometric parameters of antenna systems on the formation of guaranteed suppression zones for information leakage channels*

I.V. Trubin¹, I.V. Vozhov², P.R. Chernyshev³

¹ «DB “AUTOMATION”» LTD, 138 Nemirovich-Danchenko Street, Novosibirsk, 630087, Russian Federation, associate director. E-mail: i.trubin@corp.nstu.ru

² Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of Information Security Department. E-mail: ilvozhov@mail.ru

³ Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of Information Security Department. E-mail: p.chernyshev.2021@stud.nstu.ru

The article is devoted to the study of the spatial and energy characteristics of active radio suppression systems and their impact on the information security of facilities. The paper provides a detailed analysis of the formation of guaranteed signal suppression zones in the 2.4 GHz

* Received 05 May 2026.

band depending on geometric parameters and the type of antenna systems used. Based on a software and hardware complex consisting of nRF24L01+PA+LNA and ESP32 modules, as well as a LIG Nex1 NS-30A vector spectrum analyzer, an experimental comparison of the efficiency of half-wave dipoles and quarter-wave monopoles was conducted in order to identify the relationship between radiator geometry and the uniformity of the spatial distribution of interference.

Special attention is paid to identifying “radio-transparent corridors” – zones of critical interference power reduction of up to 12–20 dB, caused by the shape of the radiation pattern and polarization mismatch. The research results make it possible to quantitatively assess the risks of information leakage and to formulate recommendations for optimizing the spatial configuration of electronic warfare systems to ensure a continuous protective field.

Keywords: information security, radiation pattern, suppression zone, polarization, half-wave dipole, quarter-wave monopole, technical protection of information, nRF24L01, ESP32

REFERENCES

1. Agarwal V., Mahmud S., Kasera S., Ji M. *Experimental Evaluation of Interference in 2.4 GHz Wireless Network*. Office of Scientific and Technical Information, 2023. DOI: 10.2172/2242485.
2. Pirayesh H., Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2022, vol. 24 (2), pp. 767–809. DOI: 10.1109/COMST.2022.3159185.
3. Yang Y., Vermeeren G., Verloock L., Guxens M., Joseph W. A survey of IEEE 802.11ax WLAN temporal duty cycle for the assessment of RF electromagnetic exposure. *Applied Sciences*, 2025, vol. 15 (5), p. 2858. DOI: 10.3390/app15052858.
4. Wireless Broadband Alliance. *WBA Annual Industry Report 2023*.
5. Subhagato Dutta. The evolution of Bluetooth: A deep dive. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2025, vol. 11 (1). DOI: 10.32628/cseit251112261.
6. Lim S. IACR: An interference-aware channel reservation for wireless sensor networks. *International Journal of Electrical and Computer Engineering*, 2019, vol. 9 (2). DOI: 10.11591/ijece.v9i2.pp1220-1225.
7. Ma D., Wang Y., Wu S. Against jamming attack in wireless communication networks: A reinforcement learning approach. *Electronics*, 2024, vol. 13 (7), p. 1209. DOI: 10.3390/electronics13071209.
8. Šabić J., Perković T., Begušić D., Šolić P. Practical realization of reactive jamming attack on long-range wide-area network. *Sensors*, 2025, vol. 25 (8), p. 2383. DOI: 10.3390/s25082383.
9. Federal Law of July 7, 2003 N 126-FZ. "On Communications". (In Russian).
10. Kakov poryadok ispol'zovaniya radiochastotnogo spektra radioelektronny-mi sredstvami besprovodnogo dostupa v diapazone radiochastot 2,4 GGts? [What is

the procedure for using the radio-frequency spectrum by radio-electronic equipment for wireless access in the 2.4 GHz radio-frequency band?]. *Ministerstvo tsifrovogo razvitiya, svyazi i massovykh kommunikatsii Rossiiskoi Federatsii* [Ministry of Digital Development, Communications and Mass Media of the Russian Federation]. Website. Available at: <https://digital.gov.ru/faq/kakov-poryadok-ispolzovaniya-radiochastotnogo-spektra-radioelektronnymi-sredstvami-besprovodnogo-dostupa-v-diapazone-radiochastot-24-ggcz> (accessed 26.05.2026).

11. *Usloviya ispol'zovaniya radioelektronykh sredstv malogo radiusa deistviya v polose radiochastot 2400–2483,5 MGts* [Conditions for the Use of Short-Range Radio-Electronic Equipment in the 2400–2483.5 MHz Radio-Frequency Band]. *Federal'naya sluzhba po nadzoru v sfere svyazi, informatsionnykh tekhnologii i massovykh kommunikatsii* [Federal Service for Supervision of Communications, Information Technology and Mass Media]. Website. Available at: <https://23.rkn.gov.ru/news/news114683.htm> (accessed 26.05.2026).

Для цитирования:

Трубин И.В., Вожов И.В., Чернышев П.П. Влияние геометрических параметров антенных систем на формирование гарантированных зон подавления каналов утечки информации // Безопасность цифровых технологий. – 2026. – № 2 (121). – С. 68–90. – DOI: 10.17212/2782-2230-2026-2-68-90.

For citation:

Trubin I.V., Vozhov I.V., Chernyshev P.R. Vliyanie geometricheskikh parametrov antennykh sistem na formirovanie garantirovannykh zon podavleniya kanalov utechki informatsii [The influence of geometric parameters of antenna systems on the formation of guaranteed suppression zones for information leakage channels]. *Bezopasnost' tsifrovyykh tekhnologii = Digital Technology Security*, 2026, no. 2 (121), pp. 68–90. DOI: 10.17212/2782-2230-2026-2-68-90.