

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ**

**«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ**

**Студенттер мен жас ғалымдардың  
«GYLYM JÁNE BILIM - 2024»  
XIX Халықаралық ғылыми конференциясының  
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ  
XIX Международной научной конференции  
студентов и молодых ученых  
«GYLYM JÁNE BILIM - 2024»**

**PROCEEDINGS  
of the XIX International Scientific Conference  
for students and young scholars  
«GYLYM JÁNE BILIM - 2024»**

**2024  
Астана**

**УДК 001**

**ББК 72**

**G99**

**«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.**

**ISBN 978-601-7697-07-5**

Жинаққа студенттердің, магистранттардың, докторанттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

**УДК 001**

**ББК 72**

**G99**

**ISBN 978-601-7697-07-5**

**©Л.Н. Гумилев атындағы Еуразия  
ұлттық университеті, 2024**

## ПРОЕКТИРОВАНИЕ АНТЕННЫ С КРУГОВОЙ ПОЛЯРИЗАЦИЕЙ ДЛЯ RFID – СИСТЕМЫ В ЧАСТОТНОМ ДИАПАЗОНЕ 868-903 МГц

Акбаров Байсултанбекмырзахан Бақытжанұлы<sup>1</sup>, Толстой Айланыш<sup>2</sup>  
[baisultan.akbarov@mail.ru](mailto:baisultan.akbarov@mail.ru)

<sup>1</sup>Магистрант кафедры «Радиотехника, электроника и телекоммуникации»  
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан

<sup>2</sup>Старший преподаватель кафедры «Радиотехника, электроника и телекоммуникации»  
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан  
Научный руководитель: Канымгазиева Ильмира Айдосовна

**Аннотация.** В данной статье приводятся результат исследования и разработки антенн с круговой поляризацией для применения в системах радиочастотной идентификации (RFID) в частотном диапазоне 868-903 МГц.

Были рассмотрены и исследованы две антенны: оригинальная с симметричным согласующим трансформатором и изготовленная без согласующего трансформатора. В ходе исследования частота, на которой излучала антенна составляла 868 МГц.

**Ключевые слова:** RFID – технология, антенна, круговая поляризация, считыватель.

Актуальность Название RFID расшифровывается как Radio Frequency Identification, а переводится как радиочастотная (бесконтактная) идентификация, это современная технология идентификации, предоставляющая существенно больше возможностей по сравнению с традиционными системами маркировки [1]. RFID система представляет собой метод автоматической идентификации через радиосигнал.

Система состоит из считывателей, меток и программного обеспечения. Метка – это микросхема, в которой хранятся данные, а также антенна для беспроводной передачи информации. Внешний считыватель сканирует память метки радиочастотной идентификации и обрабатывает полученные данные. Программное обеспечение отвечает за целостную работу системы.

Спектр применения RFID технологий широк и возрастает с каждым годом. К примеру, можно отметить следующие: автоматизация пропускных пунктов; отслеживание перемещения товаров с помощью встроенного высокопроизводительного RFID-считывателя; регистрация товаров, проходящих через линии торговых точек в магазинах розничной торговли или в точках самовывоза на складе; определение и регистрация движения запасов, маркированных RFID-метками, с момента поступления в подсобное помещение/складское хозяйство до момента их отгрузки; интеллектуальное управление дорожным движением; отслеживание транспортных средств; управления производственной линией, интеллектуального измерения веса [2-3] и т.д.

Наиболее интересными с точки зрения практического применения являются антенны с круговой поляризацией и дальностью действия не менее 10 метров. Это связано с тем, что улавливает сигнал от RFID-меток/карточек при любой её ориентации, и качество сигнала не зависит от расположения устройства.

Из отмеченного выше следует, что RFID систем с антеннами круговой поляризации являются наиболее востребованными, так как обеспечивают универсальность ее применения.

RFID-устройства подразделяются на три диапазона действия: ближнего, среднего и дальнего расстояния, причем устройства среднего диапазона наиболее востребованы.

Технология RFID может функционировать на различных частотах [4]:

- низкочастотные (LF) от 125 до 134 кГц;
- высокочастотные (HF) на 13,56 МГц;

- ультравысокочастотные (UHF) в диапазоне от 860 до 960 МГц.

Целью данной работы является проектирование и создание антенны с круговой поляризацией для системы RFID на частоте 868-903 МГц.

### Полученные результаты и их обсуждение.

Проектирование печатных плат (PCB) осуществлялось с использованием программного обеспечения Altium Designer 2023, обеспечивающего интегрированный процесс проектирования. Предварительно в среде CorelDRAW был разработан чертеж разрабатываемой антенны. Рисунок Чертеж PCB платы изображен на рисунке 1.

Размеры PCB антенны составляют 332x34x1.6 миллиметра.



Рисунок 1 Чертеж изготавливаемой PCB — антенны

### Создание PCB антенны в Altium Designer 2023:

Шаг 1 — Создание контура платы: открыть Altium Designer и создать новый проект. Перейти в редактор схемы и создать новую плату. Определить размеры и форму платы, а также расположение отверстий для разъемов и компонентов.

Шаг 2 — Размещение полигонов на верхнем и нижнем слое платы: выбрать верхний (Top Layer) или нижний (Bottom Layer) слой. Использовать инструмент полигона (Polygon Pour) для создания областей меди, которые будут служить для формирования антенных элементов. Разместить полигоны так, чтобы они соответствовали требованиям дизайна антенны.

Шаг 3 — Объединение полигонов: после того как полигоны созданы на обоих слоях, нужно убедиться, что они не пересекаются и не создают коротких замыканий. Если требуется, объединить полигоны на разных слоях для формирования антенных структур.

Шаг 4 — Создание антенных элементов: использовать инструменты Altium Designer для создания антенных элементов, таких как микролинии, печатные антенны, или другие типы антенн. Разместить и соединить антенные элементы с полигонами, учитывая требования к согласованию импеданса и другие характеристики антенны.

Гербер файл изготавливаемой PCB — антенны показана на рисунке 2. После гербер файл был отправлен на завод изготовителю.

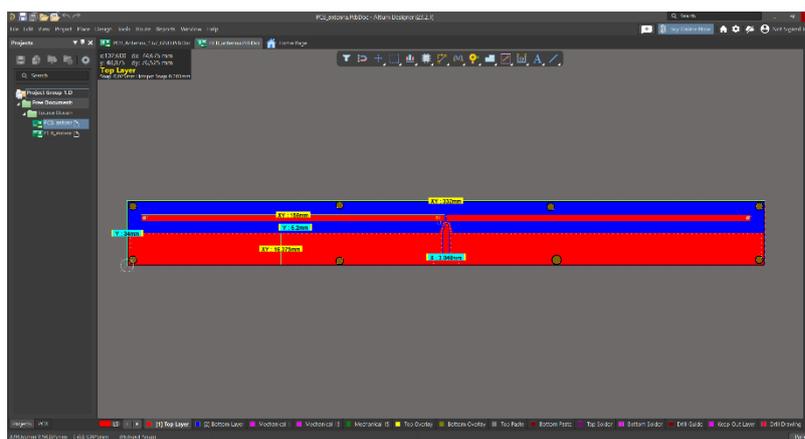


Рисунок 2 PCB – плата в среде проектирования Altium Designer 2023

После получения платы РСВ возникла потребность в создании подложки для крепления этой платы. Кроме того, были изготовлены два излучателя из латуни. Вид антенны с установленными излучателями с передней стороны показан на рисунке 3. Вид антенны сзади, со стороны РСВ, изображен на рисунке 4.



Рис.3 Вид изготовленной антенны спереди

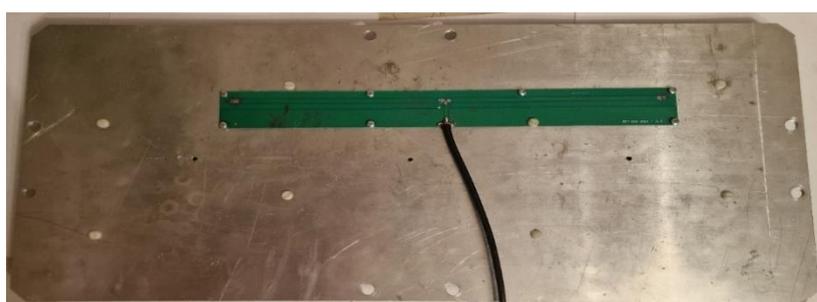
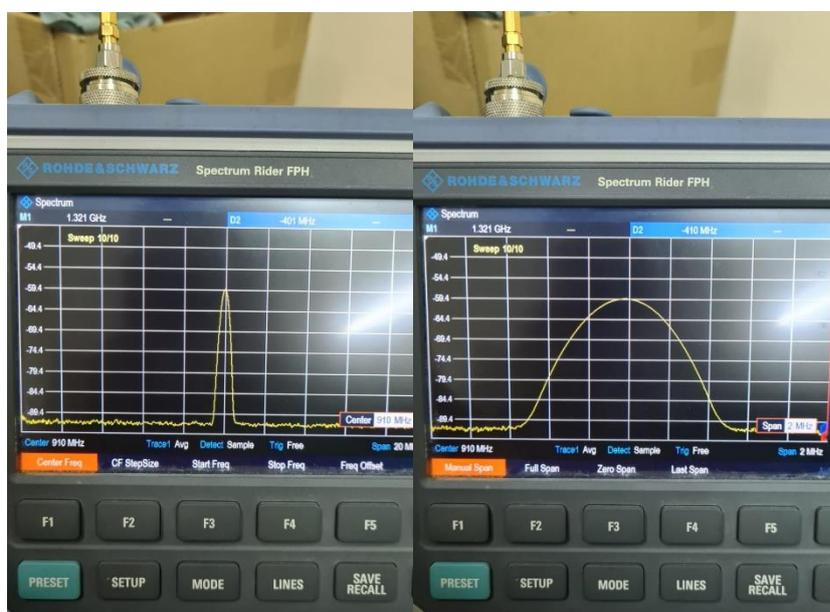


Рисунок4 Вид изготовленной антенны сзади

Провели измерение распределения энергии электромагнитных колебаний в полосе частот антенны с помощью спектрального анализатора Spectrum Rider FPH. На рисунке 5 представлен спектр электромагнитных колебаний двух антенн: одной с симметричным согласующим трансформатором (а), и другой - без согласующего трансформатора (б).



(а)

(б)

Рисунок5 Спектр оригинальной антенны с согласующим трансформатором (а), спектр антенны изготовленной без согласующего трансформатора (б).

В качестве источника был использован модем с настраиваемой частотой и уровнем сигнала. Частота, на которой излучала антенна модема составляла 868 МГц. Ослабление выставлено 20 dB.

В результате проведенных исследований по разработке антенн с круговой поляризацией для RFID в диапазоне 868-903 МГц было выявлено несколько ключевых аспектов. RFID технология широко применяется в различных сферах, таких как логистика, медицина, производство, транспорт, розничная торговля и другие, благодаря своим преимуществам в бесконтактной идентификации и работе на различных частотах. С использованием спектрального анализатора Spectrum Rider FPH было произведено измерение распределения энергии электромагнитных колебаний в полосе частот антенны, что позволило получить детальное представление о её спектральных характеристиках. Эти результаты имеют значение для дальнейшего использования антенны в RFID системах.

#### **Список использованных источников**

1. Таратун В. Е., Лось Е. А. Исследование технологии радиочастотной идентификации и ее роль для космической отрасли // Системный анализ и логистика: журнал.: выпуск №1(23), ISSN 2007-5687. – СПб.: ГУАП., 2020 – с. 47- 54. РИНЦ.
2. Путилина М.В. RFID-технологии в продвижении. — Новосибирск // Проблемы современной экономики, 2014 г. — № 18.
3. Зиборов, И. А. Применения RFID технологий в деятельности различных субъектах хозяйствования / И. А. Зиборов. — Текст: непосредственный // Молодой ученый. — 2009. — № 12 (12). — С. 17-22.
4. Хамзаев Д.И., Хамзаев И.Х. Сравнительный анализ между RFID и NFC технологиями // Universum: технические науки: электрон. научн. журн. 2024. 1(118).

УДК 004.56

### **ВЛИЯНИЕ СОВРЕМЕННЫХ АТАК SQL-ИНЪЕКЦИЙ НА РАДИОЧАСТОТНЫЙ СПЕКТР: ПРИМЕРЫ И ПОСЛЕДНИЕ ТЕНДЕНЦИИ**

**Байжанова Диана Намиговна**

[diana.baizhanova00@mail.ru](mailto:diana.baizhanova00@mail.ru)

Магистрант кафедры «Радиотехника, электроника и телекоммуникации» ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Научный руководитель- к.т.н профессор Бурамбаева Н.А.

В настоящее время рост числа компьютерных атак на информационные ресурсы, как государственного, так и частного сектора очевиден, что и подтверждают статистические данные от ведущих компаний, специализирующихся в области информационной безопасности. При этом, возникает закономерный вопрос о возможности снизить риски от ущерба компьютерных атак на информационные ресурсы и/или исключить возможности их реализации. С этой целью в рамках поиска решений в работе представлена модель сетевых атак типа XSS- и SQL-инъекций, позволяющая учесть различные уровни сложности их реализации, и выявить новые функциональные зависимости, которые могут быть учтены исследователями и разработчиками средств активного и пассивного тестирования веб-ресурсов [1, с.115].

В настоящее время в сфере информационной безопасности наблюдается устойчивый рост количества компьютерных атак, которые в свою очередь способствуют снижению уровня защищенности веб-ресурсов, данный факт изображен на рисунке 1.