

# Евразийский Союз Ученых. Серия: технические и физико-математические науки

Ежемесячный научный журнал  
№ 4 (97)/2022 Том 1

## ГЛАВНЫЙ РЕДАКТОР

**Макаровский Денис Анатольевич**

AuthorID: 559173

Заведующий кафедрой организационного управления Института прикладного анализа поведения и психолого-социальных технологий, практикующий психолог, специалист в сфере управления образованием.

## РЕДАКЦИОННАЯ КОЛЛЕГИЯ

• **Штерензон Вера Анатольевна**

AuthorID: 660374

Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, Институт новых материалов и технологий (Екатеринбург), кандидат технических наук

• **Синьковский Антон Владимирович**

AuthorID: 806157

Московский государственный технологический университет "Станкин", кафедра информационной безопасности (Москва), кандидат технических наук

• **Штерензон Владимир Александрович**

AuthorID: 762704

Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, Институт фундаментального образования, Кафедра теоретической механики (Екатеринбург), кандидат технических наук

• **Зыков Сергей Арленович**

AuthorID: 9574

Институт физики металлов им. М.Н. Михеева УрО РАН, Отдел теоретической и математической физики, Лаборатория теории нелинейных явлений (Екатеринбург), кандидат физ-мат. наук

• **Дронсейко Виталий Витальевич**

AuthorID: 1051220

Московский автомобильно-дорожный государственный технический университет (МАДИ), Кафедра "Организация и безопасность движения" (Москва), кандидат технических наук

Статьи, поступающие в редакцию, рецензируются. За достоверность сведений, изложенных в статьях, ответственность несут авторы. Мнение редакции может не совпадать с мнением авторов материалов. При перепечатке ссылка на журнал обязательна. Материалы публикуются в авторской редакции.

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Художник: Валегин Арсений Петрович  
Верстка: Курпатова Ирина Александровна

Адрес редакции:  
198320, Санкт-Петербург, Город Красное Село, ул. Геологическая, д. 44, к. 1, литера А  
E-mail: [info@euroasia-science.ru](mailto:info@euroasia-science.ru) ;  
[www.euroasia-science.ru](http://www.euroasia-science.ru)

Учредитель и издатель ООО «Логика+»  
Тираж 1000 экз.

# СОДЕРЖАНИЕ

## ТЕХНИЧЕСКИЕ НАУКИ

<i>Алексеев А.Г., Пикалов В.А., Алексеев П.А.</i> ИЗМЕРЕНИЕ ЭФФЕКТИВНОСТИ БИОЛОГИЧЕСКОЙ ЗАЩИТЫ ЭЛЕМЕНТОВ СИСТЕМЫ ГЕРМЕТИЧНОГО ОГРАЖДЕНИЯ.....3	НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТЕЙ .....12
<i>Ларин В.П.</i> СИСТЕМНЫЙ АНАЛИЗ В ЗАДАЧАХ ТЕХНОЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ КОНСТРУКЦИЙ ОПТИКО-ЭЛЕКТРОННЫХ МОДУЛЕЙ АНТЕННОЙ РЕШЁТКИ.....9	<i>Афонин П.Н., Титов А.В.</i> ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ПРОГРАММНЫХ ПРОДУКТОВ ООО «НАНОСОФТ РАЗРАБОТКА» В УЧЕБНОЙ И НАУЧНО-ПРОИЗВОДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ЭЛЕКТРОТЕХНИЧЕСКОГО УНИВЕРСИТЕТА.....18
<i>Самадов А.Р.</i> МОДЕЛИРОВАНИЕ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ МИКРОКЛИМАТА ТЕПЛИЦЫ	<i>Фам Хак Хоан, Нгуен Тьен Тхай, Ву Шон Ха</i> МЕТОД НАХОЖДЕНИЯ КОРНЕЙ МНОГОЧЛЕНА НАД РАСШИРЕННЫМ ПОЛЕМ ГАЛУА НА ОСНОВЕ КОРНЕЙ АФФИННОГО МНОГОЧЛЕНА.....21

# ТЕХНИЧЕСКИЕ НАУКИ

## ИЗМЕРЕНИЕ ЭФФЕКТИВНОСТИ БИОЛОГИЧЕСКОЙ ЗАЩИТЫ ЭЛЕМЕНТОВ СИСТЕМЫ ГЕРМЕТИЧНОГО ОГРАЖДЕНИЯ

*Алексеев Александр Григорьевич*  
старший научный сотрудник,  
«НИЦ Курчатовский институт»-ИФВЭ, г.Протвино  
*Пикалов Владимир Александрович*  
Ведущий инженер  
«НИЦ Курчатовский институт»-ИФВЭ, г.Протвино  
*Алексеев Павел Александрович*  
старший научный сотрудник, к.т.н  
АО «ГНЦ РФ-ФЭИ», г.Обнинск

## INVESTIGATION OF THE EFFECTIVENESS OF RADIATION SHIELDING OF ELEMENTS OF THE SAFETY CONTAINMENT SYSTEMS

*Alexeev A.G.*  
*Pikalov V.A.*  
NRC «Kurchatov Institute» – IHER  
*Alexeev P.A.*  
JSC "SSC RF – IPPE"

DOI: 10.31618/ESU.2413-9335.2022.1.97.1651

### АННОТАЦИЯ

Приведена методика измерения кратности ослабления гамма-квантов элементами системы герметичного ограждения АЭС типа ВВЭР, доработанная по результатам измерений, выполненных на Ростовской АЭС. Приведены результаты измерений, полученные при пуске Белорусской АЭС. Показано, что Ленинградская АЭС-2 является референтной в части биологической защиты для Белорусской АЭС.

### ABSTRACT

A Method for measuring the attenuation ratio of gamma radiation by the elements of the safety containment system of VVER-type NPPs, which was developed based on the results of studies carried out at the Rostov NPP, is presented. The results of measurements obtained during the start-up of the Belarusian NPP are presented. It is shown that the Leningrad NPP-2 is a reference in terms of radiation shielding for the Belarusian NPP.

**Ключевые слова:** фотоны, биологическая защита, локализующие системы безопасности, АЭС  
**Keywords:** gamma radiation, dosimeter, radiation shielding, safety containment systems of NPP

### ВВЕДЕНИЕ

Системы безопасности современных АЭС можно разделить на четыре группы: защитные, локализующие, управляющие и обеспечивающие. Локализирующие системы безопасности (ЛСБ) (или система герметичного ограждения) это системы (элементы), предназначенные для предотвращения или ограничения распространения выделяющихся при авариях радиоактивных веществ и излучений за установленные проектом границы и выхода их в окружающую среду. Локализирующая система безопасности АЭС включает в себя защитную оболочку для ядерного (энергетического) реактора, оснащенную пассивными и активными конденсаторами, спринклерными и аварийными вентиляционными устройствами, транспортными трубопроводами с необходимой трубопроводной арматурой.

ЛСБ и их элементы должны проходить проверку на соответствие проектным показателям при вводе в эксплуатацию, после ремонта и периодически в течение всего срока службы блока АЭС. Нормативный документ [1] предусматривает, что испытания биологической защиты ЛСБ (элементов ЛСБ) необходимо проводить при вводе

блока АЭС в эксплуатацию. Испытанию биологической защиты подлежат следующие участки герметичного ограждения (ГО): места расположения дверей, люков, шлюзов и проходок; места возможного нахождения персонала (при нормальной эксплуатации, во время аварий и после них) с наружной стороны ГО.

Для реализации требования проведения испытаний биологической защиты ЛСБ авторами была разработана методика, которая прошла апробацию при пуске ряда новых энергоблоков ВВЭР-1000 и ВВЭР-1200.

В данной работе рассмотрены методические особенности испытаний биологической защиты ЛСБ, способ реализации, результаты испытаний при пуске 1-го и 2-го энергоблоков Белорусской АЭС.

### МЕТОД ИЗМЕРЕНИЯ

В качестве меры эффективности биологической защиты таких элементов ЛСБ, как защитная бетонная оболочка (ЗО), двери шлюзов для персонала и транспортного шлюза, трубопроводные и кабельные проходки, в проектах АЭС (например [2]) выбрана кратность ослабления гамма квантов радионуклидного источника 60-

кобальт. Средняя энергия гамма квантов этого источника составляет 1,25 МэВ.

В зависимости от элемента ЛСБ кратность ослабления им гамма квантов  $^{60}\text{Co}$  может варьироваться от 5 до  $2 \cdot 10^5$ , т.е. необходимо применять радионуклидный источник высокой активности.

При использовании такого высокоактивного источника  $^{60}\text{Co}$  в условиях пуско-наладочных работ (в период, когда выполняется данный вид испытаний биологической защиты ЛСБ), требуются значительные организационные мероприятия, связанные с радиационной безопасностью проведения работы. Как показал опыт работ при пуске 3го энергоблока Ростовской АЭС, это сказывается на качестве и сроках

выполнения данного испытания. Учитывая это, при пуске 4-го энергоблока Ростовской АЭС, был разработан метод определения кратности ослабления с использованием радионуклидного источника  $^{192}\text{Ir}$ . С одной стороны, спектр  $^{192}\text{Ir}$  является сложным и состоит из 17 линий различной интенсивности с энергиями в пределах 0,063–0,8845 МэВ. Средняя энергия спектра равна 0,359 МэВ. На рисунке 1, приведен спектр гамма квантов радионуклида  $^{192}\text{Ir}$ . С другой стороны, данный радионуклид используется для неразрушающего контроля сварных швов при монтажных работах на АЭС, а переносные устройства типа ГАМАРИД 120/92 позволяют использовать источники с большой активностью - до 120 Ки.

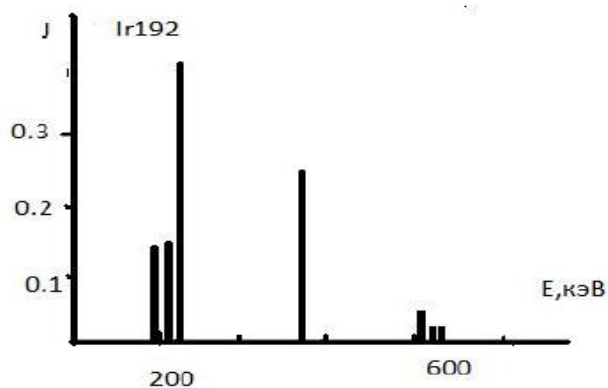


Рисунок 1 – Спектр гамма квантов радионуклида  $^{192}\text{Ir}$

### Спектр иридиевого источника жесткого излучения

Методика определения кратности ослабления основана на измерении мощности AMBIENTного эквивалента дозы (МАЭД)  $H_0^*(10)$  от источника в отсутствие защиты между источником и дозиметром и измерении  $H_1^*(10)$  на том же расстоянии R (источник-детектор), когда между источником и детектором находится элемент ЛСБ. Кратность ослабления определяется отношением:

$$k_{Ir} = \frac{H_0^*(10)}{H_1^*(10)}$$

При расчете кратности ослабления гамма-квантов  $^{60}\text{Co}$  используется параметр d

$$k_{Co} = d \times k_{Ir}$$

Параметр d зависит от конструкции ЛСБ (материал защиты, толщины защиты и др.). Были выполнены расчеты данного параметра для конкретных типов элементов ЛСБ с использованием метода Монте-Карло по программе MCNP[3].

### ОБЪЕКТ ИССЛЕДОВАНИЯ

Система герметичного ограждения (СГО) состоит из ряда элементов, для которых

предусматривается проверка эффективности биологической защиты:

А) Герметичное ограждение (ГО) – железобетонное ограждение для энергоблоков ВВЭР-1200 состоит из внутренней защитной оболочки и внешней защитной оболочки. Толщина внутренней оболочки составляет 120 см, дополнительно внутренняя часть облицована сталью. Толщина внешней оболочки составляет 80 см бетона. На рисунке 2 приведены расчеты кратности ослабления в бетоне для  $^{192}\text{Ir}$  и  $^{60}\text{Co}$  (средняя энергия гамма-квантов составляет 1,25 МэВ), так же приведены данные из работы [4]. Можно отметить хорошее согласие результатов расчетов данной работы и [4].

Б) Шлюз для персонала и транспортный шлюз имеют сложную геометрию для определения эффективности биологической защиты шлюза как цельного элемента, поэтому в проектной документации регламентируется кратность ослабления только защитных дверей шлюза. На рисунке 4 представлена конструкция шлюза для персонала. На рисунке 5 приведены расчеты кратности ослабления гамма-квантов с энергией 1,25 МэВ ( $^{60}\text{Co}$ ) и  $^{192}\text{Ir}$ , для сравнения приведены данные из [4]. Наблюдается хорошее согласие данных для энергии 1,25 МэВ.

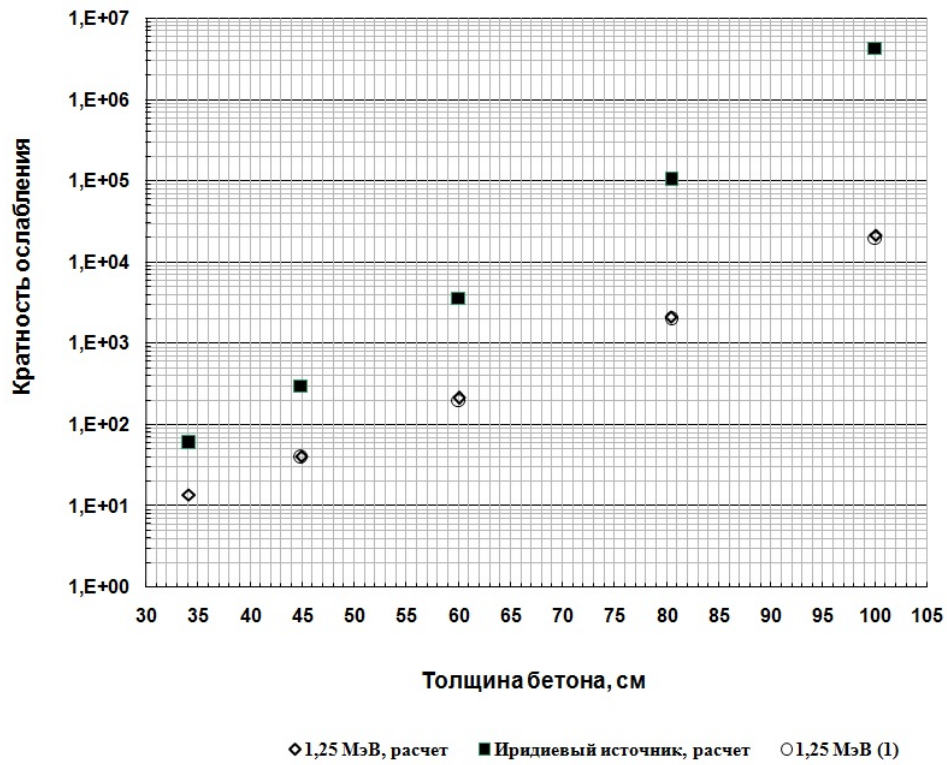


Рисунок 2 – Расчет кратности ослабления для бетона: 1,25 МэВ расчет, 1,25 МэВ (1) – данные [4], 192Ir расчёт

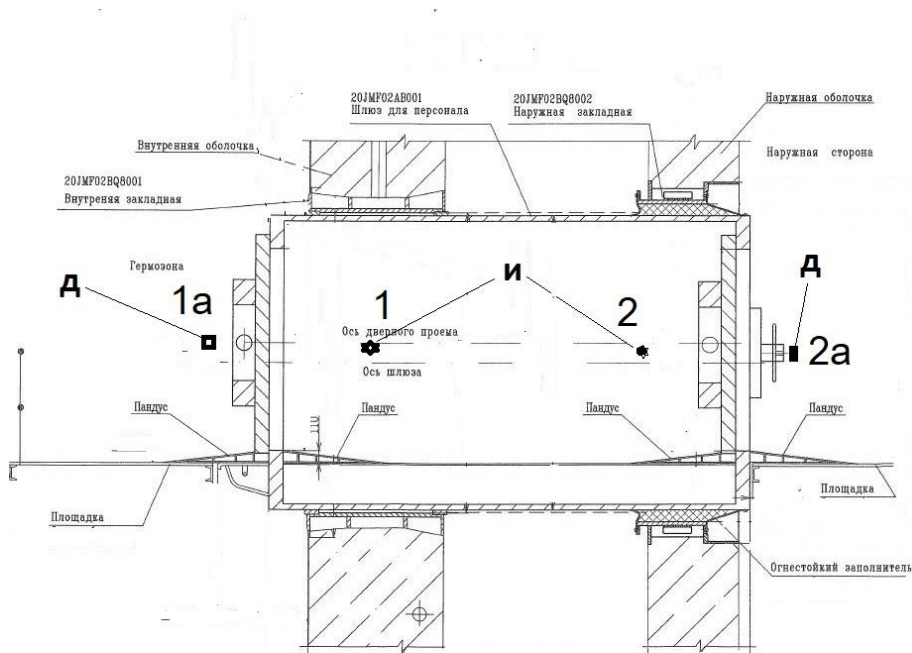


Рисунок 4 – Шлюз для персонала; д – точки измерения; и – места положения источника 192 Ir, при проведении измерений.

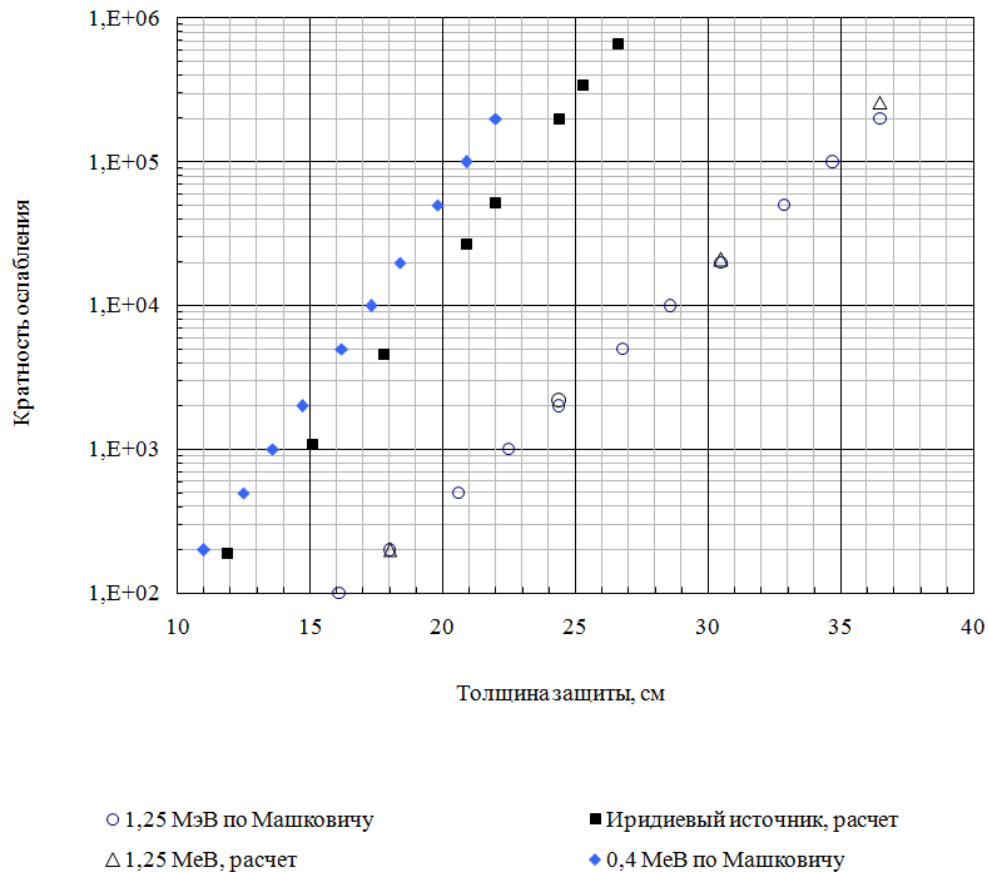


Рисунок 5 – Кратность ослабления гамма-квантов с энергией 1,25 МэВ, 0,4 МэВ и  $^{192}\text{Ir}$  в железе; расчет и данные работы [4].

В) Трубопроводные проходки различаются по типам (в том числе по диаметру). На рисунке 6

приведены два типа проходок (в том числе контрольно-измерительные КИП).

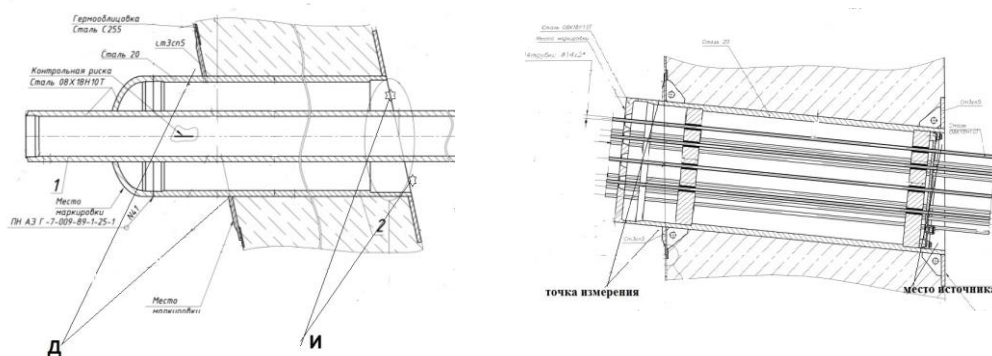


Рисунок 6 – Трубопроводные проходки. Д-точка измерения, И- положение источника.

Для каждого типа выполнен расчет кратности ослабления и коэффициенты  $d$ .

Г) Кабельные сигнальные и силовые проходки так же имеют несколько типов. Следует отметить,

что кабельные проходки установленные на ВВЭР-1000 отличаются от установленных на ВВЭР-1200. Для них так же были выполнены расчеты кратности ослабления.

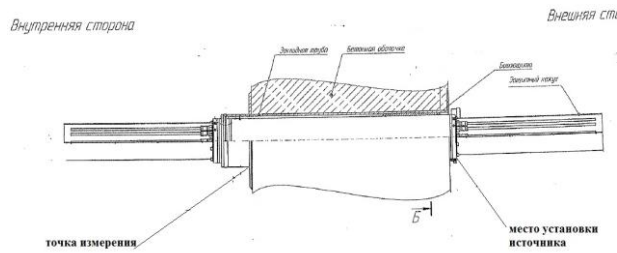


Рисунок 7 – Кабельная проходка.

Надо отметить, что производители кабельных проходок гарантируют кратность ослабления такую же, как бетонная защита, в которую они вставлены. Однако проведенные авторами измерения (на Ростовской АЭС, Нововоронежской АЭС-2) показывают, что реально кратность ослабления кабельных проходок существенно ниже, проектанты это было учтено, и в более поздних проектах АЭС заложены существенно менее жесткие требования в кратности ослабления кабельных проходок.

Следует отметить, что для разных проектов АЭС конструкция и типы элементов ЛСБ отличаются и соответственно меняется параметр  $d$  (в зависимости от конструкции применяемых элементов).

#### РЕЗУЛЬТАТЫ

Для измерения МАЭД (кроме измерений кратности ослабления внутренней оболочки ГО)

использовался дозиметр ДКС-АТ1121. В измерениях внутренней оболочки применялся сцинтилляционный гамма-спектрометр УДС-ГЦА-63х63-RS/ВТ1. Метод использования сцинтилляционного гамма-спектрометра для измерения кратности ослабления описан ранее в работе [5].

На рисунках 8а и 8б приведена геометрия измерения для внутренней и внешней оболочек. Для измерений внешней оболочки источник помещался снаружи оболочки (между стеной здания и внешней оболочкой), измерения выполнялись в межоболочечном пространстве. Для измерений внутренней оболочки источник помещался в межоболочечном пространстве, измерения выполнялись в гермообъеме. На рисунках 9а и 9б приведены результаты измерения с помощью гамма-спектрометра.

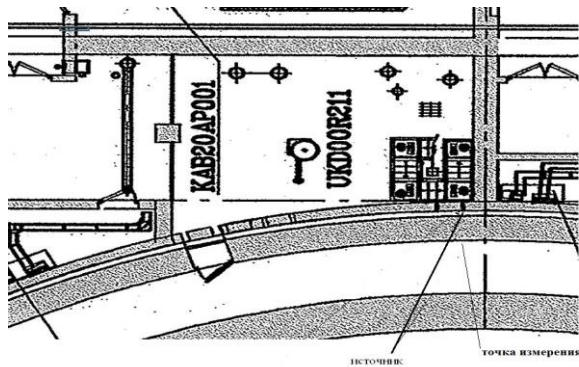


Рисунок 8а – Схема расположения источника и точек измерения для внешней оболочки. Источник помещался в проем между стеной здания 10UKD и внешней ЗО. Измерения выполнялись в межоболочечном пространстве.

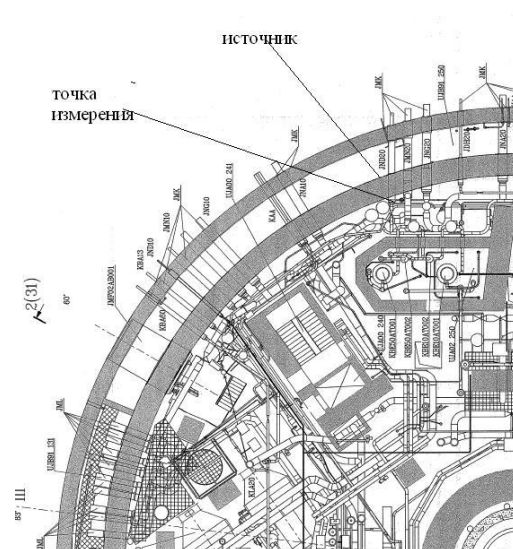


Рисунок 8б – Схема расположения источника и точек измерения. Источник помещался в межоболочечном пространстве. Измерения выполнялись в гермообъеме.

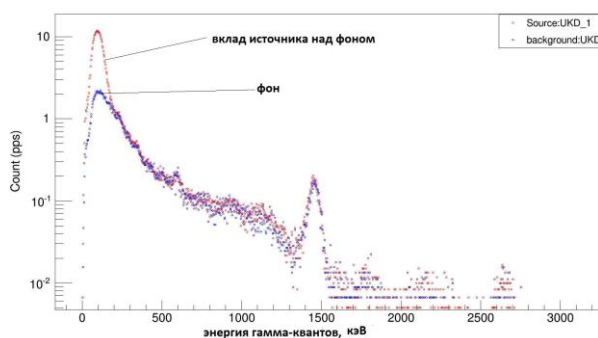


Рисунок 9а – Спектр гамма квантов (имп/с).  
Измерение внешней защитной оболочки.

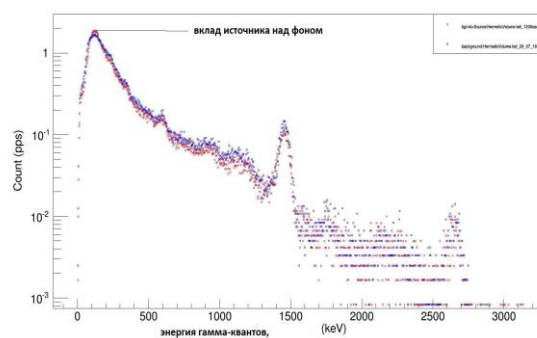


Рисунок 9б – Спектр гамма квантов (имп/с).  
Измерение внутренней защитной оболочки

В таблице 1 приведены результаты измерения кратности ослабления гамма квантов точечного источника излучения  $^{60}\text{Co}$  (энергией гамма-излучения 1,17 и 1,33 МэВ) для элементов СГО и значения кратности ослабления, заложенные в проектах. Измерения проводились с использованием высокоактивного источника  $^{192}\text{Ir}$  с последующим пересчётом на энергию гамма квантов источника  $^{60}\text{Co}$ . Представлены результаты для 2го энергоблока Ленинградской АЭС-2 (результаты измерений на 1м энергоблоке

ЛАЭС-2 близки по своим значениям к результатам 2го энергоблока), 1 и 2го энергоблоков Белорусской АЭС. Ленинградская АЭС-2 считается референтной для Белорусской АЭС. «Не менее» – означает, что из всей совокупности элементов (количество герметичных кабельных проходок несколько сотен) выбрана минимальная измеренная величина. По результатам испытаний для всех элементов кратность ослабления больше величины, заложенной в проекте.

Таблица 1

**Результаты испытаний эффективности биологической защиты элементов СГО на 2м энергоблоке Ленинградской АЭС-2, на 1 и 2м энергоблоках Белорусской АЭС**

Кратность ослабления мощности дозы ионизирующего излучения (точечный источник излучения $^{60}\text{Co}$ с энергией гамма-излучения 1,17 и 1,33 МэВ)	2й энергоблок ЛАЭС-2	1й энергоблок БелАЭС	2й энергоблок БелАЭС	Проектные данные
внутренняя оболочка	-*	$2,55 \cdot 10^5$	$2,9 \cdot 10^5$	$2,0 \cdot 10^5$
дверей шлюза транспортного	5,79	4,06	3,75	3
двери шлюза для персонала	$4,88 \cdot 10^{-3}$	$1,75 \cdot 10^{-3}$	$1,05 \cdot 10^{-3}$	$1,0 \cdot 10^{-3}$
герметичные кабельные проходки	Не менее $1,02 \cdot 10^3$	не менее $1,344 \cdot 10^3$	Не менее $8,4 \cdot 10^2$	$1,0 \cdot 10^2$
Трубопроводные проходки	Не менее 43	не менее 25	не менее 18	не менее 5

-\* измерения не проводились.

### ЗАКЛЮЧЕНИЕ

Опыт проведения проверки эффективности биологической защиты элементов системы герметичного ограждения, полученный при пуске 3 и 4 го энергоблока Ростовской АЭС и 1 и 2го энергоблоков Новоронежской АЭС-2 был перенесен и использован при пуске ЛАЭС-2 и Белорусской АЭС.

Результаты подтвердили, что в части биологической защиты системы герметичного ограждения ЛАЭС-2 является референтной для Белорусской АЭС. Разработанная методика измерений [6] может применяться для других проектов АЭС.

Работы выполнялась в рамках договоров между АО «АтомТехЭнерго» и ООО «АтомПромИнжиниринг» при личном участии Генерального директора А.Ю.Соколова, в измерениях так же участвовали Н.Н.Бараненков, А.А. Степанов.

### ССЫЛКИ

- 1.Правила устройства и эксплуатации локализирующих систем безопасности атомных станций (НП-010-16) М.2016г.
- 2.«Окончательный отчет по обоснованию безопасности» Белорусская АЭС Блок 1. Глава 12 Системы безопасности. BLR1.P.110.1.120204.0.2&&.021.HD.0001.
- 3.MCNP – General Monte Carlo N-Particle Transport code. LA-12625-M, Vers. 4B, 1997.
- 4.Машкович В.П., Кудрявцева А.В. Защита от ионизирующих излучений: Справочник – 4-е изд. – М.: Энергоатомиздат, 1995. – 496 с..
- 5.А.Г.Алексеев, П.А.Алексеев, А.А.Янович/ Использование гамма-спектрометра при проверке эффективности биологической защиты.// Журнал: Евразийский Союз Ученых. 2019. №63 т.1 стр. 8-13. <https://euroasia-science.ru/pdf-arxiv/8-13-alekseev-a-g-alekseev-p-a-yanovich-a-a-gamma-spectrometer-for-the-testing-of-radiation-shielding>.



6. Методика измерения кратности ослабления мощности дозы гамма излучения биологической защитой элементов локализирующих систем СТО № 81632696-0001-2015. ООО «АПИ».

УДК 623.7.396.383

---

## СИСТЕМНЫЙ АНАЛИЗ В ЗАДАЧАХ ТЕХНОЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ КОНСТРУКЦИЙ ОПТИКО-ЭЛЕКТРОННЫХ МОДУЛЕЙ АНТЕННОЙ РЕШЁТКИ

---

*Ларин В.П.*

*доктор технических наук, профессор*

*Санкт-Петербургский государственный университет аэрокосмического приборостроения,  
Россия, 190000, Санкт-Петербург, ул. Большая Морская, 67*

## SYSTEM ANALYSIS IN THE PROBLEMS OF TECHNOLOGICAL DESIGN OF STRUCTURES OF OPTOELECTRONIC MODULES OF THE ANTENNA ARRAY

*V.P. Larin*

*Doctor of Technical Sciences, Professor*

*Saint-Petersburg State University of Aerospace Instrumentation*

### АННОТАЦИЯ

Изложены материалы с решением задач, связанных с технологическим проектированием элементов интегральной оптики ждя использования в оптико-электрических приёмо-передающих модулях активных антенных решёток бортовых РЛС.. Их применение позволяет значительно улучшить функциональные и массогабаритные характеристики РЛС. Рассмотрены технологические операции, необходимые для получения полимерных световодов, заглубленных в поверхность диэлектрической подложки. Выполнен анализ обеспечения минимальных светопотерь и помех при передаче световой волны по полимерному световоду. Изложена последовательность выполнения технологических операций по предлагаемому варианту наноимпринтинга, как способа получения встроенных полимерных световодов.

### ABSTRACT

The materials with the solution of problems related to the technological design of integral optics elements are presented, waiting for the use of active antenna arrays of on-board radars in the optiko-electric transceiver modules. Their use can significantly improve the functional and weight and size characteristics of the radar. The technological operations necessary for the production of polymer light guides buried in the surface of the dielectric substrate are considered. The analysis of ensuring minimal light losses and interference during the transmission of a light wave along a polymer light guide is carried out. The sequence of technological operations on the proposed version of nanoimprinting, as a method for obtaining embedded polymer light guides, is described.

**Ключевые слова:** оптико-электронный модуль, полимерный заглубленный световод, технология изготовления, наноимпринтинг, уменьшение светопотерь

**Keywords:** optiko-electric modules, polymer light guides, manufacturing technology, nanoimprinting, reduction of light loss.

**Введение.** В современных системах радиолокации, радионавигации и радиоэлектронного противодействия широко используются активные фазированные антенные решётки. Основу конструкции антенны составляет множество приемо-передающих модулей (ППМ), размещенных в полотне антенной решётки [2]. Конструкторско-технологическое развитие антенных решёток и ППМ идет в направлениях создания планарных конструкций с оптико-электронным и электронно-оптическим построением схем передающих и приемных каналов ППМ. Использование принципов фотоники и интегральной оптики для реализации схем и конструкций таких модулей имеет огромное значение для всех конструктивных уровней радиолокационной системы (РЛС).

В интегральной оптике конструктивной основой многих устройств является планарный (двумерный) оптический световод. При проектировании устройств интегральной оптики

приходится решать две основные группы взаимосвязанных задач: конструирования оптических элементов и технологической реализации этих элементов. Задачи нуждаются в проведении системного анализа, необходимого для формирования точной постановки и содержания задач и эффективного их решения.

Процесс системного анализа рассмотрим на примере поиска возможных решений для проектирования планарных канальных световодов в конструктивном варианте заглубленного исполнения. Планарный световод представляет собой плоский диэлектрический элемент, расположенный на диэлектрической подложке. Планарные полимерные световоды в настоящее время находят всё большее применение в устройствах передачи оптических сигналов, в том числе в канальной заглубленной конструктивной форме [1,3]. Основу пленочного световода (рис. 1) составляет диэлектрическая пленка с параметрами  $\epsilon_{\text{пл}}$ ,  $\mu_0$ , выращенная на диэлектрической подложке

или сформированная методами интегральной технологии. Конструкция такого световода ограничена подложкой и верхним покрытием. Для распространения волн по световоду необходимо, чтобы показатели преломления пленки, подложки и покрытия находились в следующих отношениях  $n_1 > n_2 > n_0$ . Если увеличить угол  $\varphi$  так, чтобы выполнялось условие полного внутреннего

отражения от подложки, то наблюдается полное внутреннее отражение, как от границы раздела «канал—подложка», так и от границы раздела «канал—покрытие». Световая волна, попавшая в канал, будет распространяться в нем по зигзагообразному пути (рис. 1, а). Подобные световоды используются для передачи света в пределах оптической или оптико-электронной подложки и в локальных линиях связи.

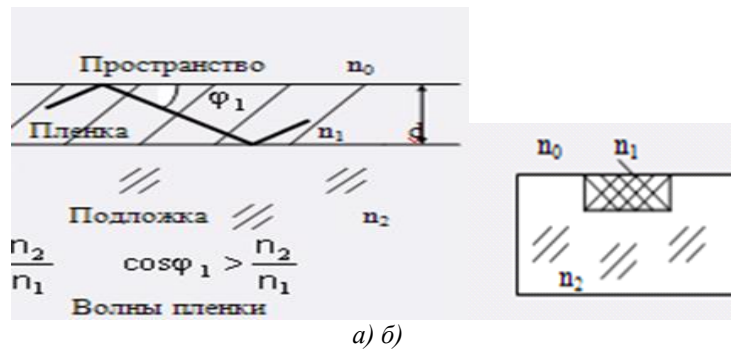


Рис. 1. Вид волны при полном внутреннем отражении в планарном световоде (а) и структура световода заглублен-ного канального типа (б)

С позиции наиболее эффективной защиты канала от внешних факторов данный вариант рассматривается и развивается как перспективное направление проектирования световодов, внедряемых в поверхность подложки. Но, в таких световодах, при последовательном отражении волн света от поверхностей  $n_0$  и  $n_2$ , возникают проблемы светопотери, имеют место помехи, различного рода деградации и др. Необходимы технологические решения по обеспечению необходимых условий прохождения волны по каналу.

**Цель.** Цель исследования заключалась в поиске технологических решений по обеспечению неискаженного прохождения световой волны по световоду заглубленного канального типа. При этом главной задачей является рассмотрение таких влияющих факторов, как свойства и параметры поверхности подложки и наносимого покрытия и возможные загрязнения, образующиеся при выполнении технологических операций. Для реализации цели выполнены исследования по технологическому проектированию процессов формирования световодов с минимизацией потерь и искажений, что является важнейшим условием применения оптико-электронных элементов в приёмно-передающих модулях РЛС.

**Материал и методы исследования.** К методам, позволяющим сформировать световодные пленки непосредственно в подложке, относятся методы, основанные на диффузии, имплантации ионов, электрооптическом эффекте и др. Эти методы широко используются при создании планарных и канальных световодов интегрально-оптических (фотонных) устройств [3]. В данной статье ограничимся рассмотрением только полимерных световодов, формируемых на подложках из керамики (включая ЛТСС-керамику), ниобата лития, плавленного кварца, полиимида, на тонких слоях карбида кремния (SiC),

поликристаллического CVD-алмаза или графитовых пленках PGS. В отличие от широко распространенных оптических сред, таких как оптическое стекло или монокристаллы, полимерные материалы являются привлекательными для создания систем с широкой полосой пропускания частот, с малым светорассеянием, устойчивых к динамическим нагрузкам. Полимерные световоды относительно дешевы и просты в изготовлении. Эти преимущества делают их незаменимыми для использования в локальных линиях связи, в качестве датчиков и индикаторов в рекламных и декоративных целях. Но реализация этих достоинств ограничена из-за высокого уровня светопотерь, потребовавших проведения исследований комплекса оптических и физико-механических характеристик полимерных световодов и технологий их изготовления. Проведен анализ по всей технологической цепочке изготовления полимерных световодных систем: материал полимерного световода [1]; материал подложки; технологии подготовки поверхности к нанесению полимерного слоя [4]; способы формирования канальной топологии световодной системы на подложке [3]; технологии заполнения канальных образований полимерным материалом; финишные операции полирования и нанесения покрытия на сформированные элементы.

К методам непосредственного формирования заглубленных волноводов можно отнести метод электростимулированной диффузии, ионной имплантации, твердотельной диффузии и ионного обмена. Наибольшее внимание в опубликованных результатах исследований относится к формированию световодов на подложке из ниобата лития ( $\text{LiNbO}_3$ ) методами твердотельной диффузии и ионного обмена.

Метод на основе диффузии Ti в LiNbO<sub>3</sub> для заглубленных световодов технологически сложен в реализации из-за высоких требований к изготовлению пленочной титановой полоски, проблем с высокой температурой и поляризацией.

Метод ионного обмена наиболее часто используется в акустоэлектронике, интегральной оптике и для изготовления оптических световодов может быть рассмотрен в варианте протонно-ионного обмена. Суть этого метода состоит в том, что в образце LiNbO<sub>3</sub> ионы лития замещаются на протоны (ионы водорода), которые имеют лучшие показатели преломления в той области, где произошло данное замещение. Преимуществом метода ионного обмена являются малые потери в световодах (от 0,2 до 0,5 дБ/см). по сравнению с другими методами. К недостаткам можно отнести проблемы с выбором диффузантов под определенный тип кристалла.

Заслуживают внимания специализированные комплексные технологии, примером которых может служить наноимпритная технология. Обычно эти методы используются для изготовления субмикронных элементов или элементов, имеющих микронные размеры с высокими требованиями к точности, например, планарные световоды имеют характерные размеры на уровне 5 – 10 мкм, но точность должна быть порядка 50 нм. Наноимпритная технология рассматривалась как вариант формирования полимерных световодных структур на кремниевых подложках в каналах, полученных с помощью CO<sub>2</sub> лазера. Типовая технология наноимпринтинга состоит из двух самостоятельных процессов: изготовления «инструмента» и непосредственного формирования полимерного рисунка на подложке. Изготовление «инструмента» - штампа с необходимой топологией применяется для получения гребенчатых («ребристых») и поверхностных наложенных световодов. Для рассматриваемого варианта канальных заглубленных световодов, показанных на рис. 1, форма наноимпритного штампа должна быть совершенно плоской, покрытой антиадгезионным

составом для работы с полимером. Процесс образования полимерных каналов световодов начинается с нанесения на подложку тонкого слоя полимера. Полимер нагревается обычно до 90-100 °С, т.е. до температуры, при которой полимер приобретает пластичность. Плоским штампом на полимерный слой оказывается давление с выдержкой в несколько минут, чтобы полимер мог заполнить каналы подложки. Для полиметилметакрилата рассмотрен режим стеклования около 105 °С, температура печати порядка 155 °С и давление – до 10 МПа.

Так как после прессования на поверхности имеются остатки полимера, то для его удаления используется ионное травление поверхности, которое обеспечивает равномерное удаление полимера. В результате остатки тонкого слоя полимера будут удалены, а верхние границы заполненных полимером каналов, сравняются с поверхностью подложки. Для придания требуемых свойств поверхностям световодов и подложки выполняются операции полировки и плазмохимической очистки. Вся полученная система световодов (или локально отдельные световоды) покрывается полиимидной пленкой. Тем самым выполняется формирование топологии световода по рис. 1.

Технологические операции, применяемые в описанном модернизированном технологическом процессе от получения углублений (каналов) необходимой формы и размеров до финишной обработки полученных полимерных световодов (включая операции изготовления формы наноимпритного штампа), показаны на рис. 2.

Использование электрохимической полировки и плазмохимической очистки позволяет устранить практически любые макроскопические дефекты и микродфекты, пыль или другие инородные включения, сравнимые или меньше длины волны.

На выбор технологических операций влияют свойства рассматриваемых полимерных материалов [1]. Так большинство полиимидов и поликарбонатов не фоточувствительны, что вызывает необходимость применения



Рис. 2. Схема технологических операций, составляющих процесс формирования световодов

определенных технологий с использованием шаблона из фоторезиста и ионное травление. А

фоточувствительные полимеры не требуют дорогостоящего оборудования и вспомогательных

материалов и могут быть использованы в качестве фоторезиста, что позволяет значительно сократить время получения полимерных планарных структур по всем технологическим операциям.

**Результаты исследования и выводы.** В результате использования рассмотренных технологий возможно создание световодных соединений в устройствах интегральной оптики с минимальными потерями и искажениями при обработке и преобразовании сигналов. Актуальность и перспективность применения устройств интегральной оптики в бортовых аэрокосмических системах подтверждено практикой. Использование помехозащищенных оптических элементов с минимальными потерями в конструкциях ППМ активных антенных решёток бортовых РЛС позволяет значительно улучшить их функциональные характеристики, уменьшить массогабаритные параметры и упростить решение задач обеспечения теплового режима. Уменьшение габаритов ППМ и улучшение функциональных характеристик создают необходимые условия для получения РЛС с существенным ростом технических характеристик (помехозащищенности, снижения потерь в линиях передачи сигналов, повышение стабильности и повторяемости характеристик, пропускной способности каналов передачи информации и её уплотнения и др.). Следует отметить, что улучшение каждой из перечисленных системных характеристик вызывает улучшение связанных с ними характеристик вторичного плана. Таким образом, технологии создания полимерных

заглубленных световодов, рассмотренные в статье, с реализацией задачи минимизации потерь и искажений проходящих сигналов, имеют в конечном итоге высокую значимость для бортовых и мобильных РЛС.

#### Список литературы

1. Зубков А.И. Структура и свойства полимерных световодов : автореферат дис. доктора физико-математических наук : 02.00.04 / Инженер. центр полимер. оптических волокон.- Тверь, 2000.- 40 с.
2. Ларин В.П. Системный анализ в процессе проектирования приемо-передающих модулей активной фазированной антенной решетки // The Way of Science. International scientific journal. 2022. № 6 (100).- С. 20 - 23.
3. Ларин В.П., Шелест Д.К. Технологическое проектирование гибридных оптоэлектронных устройств // Датчики и системы. 2019. № 11. - С. 25-32.
4. Ларин В.П. Технологии подготовки поверхности подложек оптико-электронных узлов / Волновая электроника и инфокоммуникационные системы: Двадцать третья международная научная конференция (СПб., 1-5 июня 2020 г.): сб. статей в 2 ч. Ч. 2. СПб.: ГУАП, 2020. С. 92 – 102.



© В.П. Ларин, 2022

2.

---

## МОДЕЛИРОВАНИЕ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ МИКРОКЛИМАТА ТЕПЛИЦЫ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТЕЙ

---

Самадов А.Р.

### АННОТАЦИЯ

Нечеткая логика позволяет разработчикам управлять сложными системами более эффективно, чем традиционные подходы. Поскольку это обеспечивает простой способ прийти к определенному выводу на основе неоднозначной, неточной или шумной информации. В этой статье мы предложили нечеткую логику для управления микроклиматом теплицы. Предлагаемая управления моделируется с использованием инструментария нечеткой логики MATLAB. Результат используется для вычисления температуры и влажности воздуха для различных типов теплиц в условиях неопределенностей. Процесс полностью основан на принципе получения неточных входных данных от датчиков, подвергая их нечеткой арифметике и получая четкое значение микроклиматических периодов.

**Ключевые слово.** Моделирование, смарт теплицы, нечеткая логика, Матлаб.

Теплица - это решение для защиты растительности от болезней и непогоды, представляющее собой сложную систему [1, 2]. Основной функцией управления теплицей является поддержание микроклимата, на который влияющие факторы такие как, солнечная излучения, скорость ветра, внешняя и внутренняя температура и влажность [3]. Микроклимат теплицы поддерживается с помощью нечеткой логики, который, позволяет управлять температурой и влажностью воздуха теплицы [4, 5].

Поскольку теплица гарантирует подходящие микроклиматические условия для постоянного

выращивания [6]. Для управления теплицей создано физическая модель, который, должна быть способна предвидеть изменения во внутренней среде параметры, которые основаны на нескольких граничных условиях. В этой работе представлена модель теплицы разработанный на основе нечеткой логики, который, на четырех основных слоях: техническая конструкция теплицы, воздух внутри теплицы, растения и почва. Значимость любого покрова состоит в последующем: теплица сохраняет тепло (покрытие обычно изготавливается из пластиковой пленки или стекла); воздух в помещении - это микроклимат в

помещении, который регулируется температурой и влажностью; растения играют стратегическую роль в воде и тепловой баланс за счет процесса испарения; почва характеризуется поглощением и диффузией теплового излучения[7,8]. Предлагаемая система была протестирована в среде Матлаб с использованием реальных измерений.

Значения коррелированы и подчиняются нормальному закону, распределяются как по часам, так и по году. Моделирование температуры и влажности в теплице проводилось с использованием дифференциальных уравнений, экспериментальные внешние значения измерялись с помощью датчиков. (Рис.1).

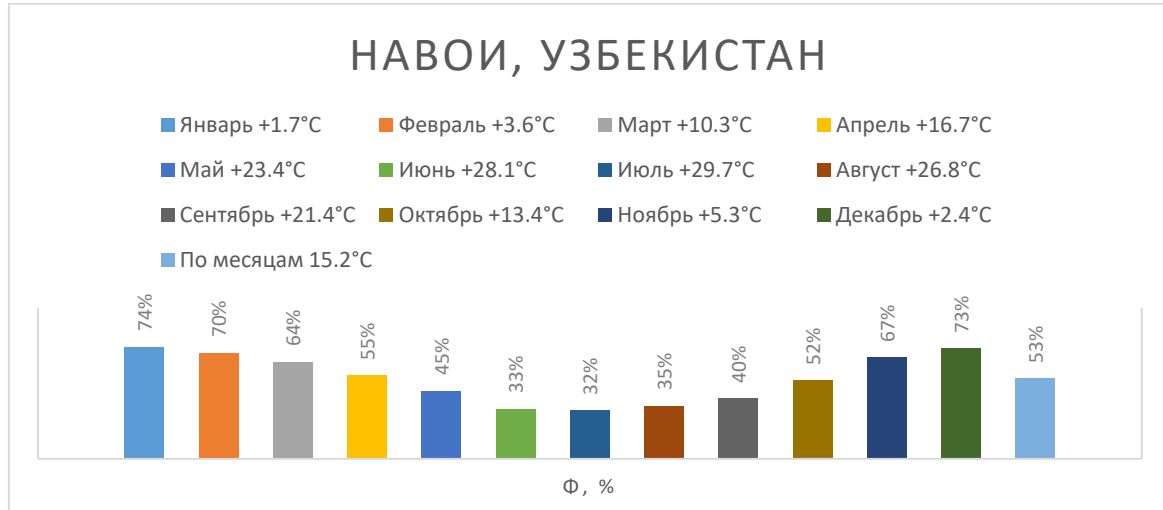


Рис.1. Данные о солнечной радиации представлены на основе данных средней статистики по городу Навоий, Узбекистан. Среднегодовое значение близко к  $4 \text{ кВт} \cdot \text{ч} / \text{м}^2$ .

Для проектирование нечеткого регулятора, как и любой другой процесс проектирования, состоит из следующих основных шагов:

- первоначальный выбор контроллера структура и параметры (синтез регулятора);
- оценка влияние параметров на работу регулятора (анализ контроллера);
- корректировка и изменение параметров и структура по результатам анализа.

После всех этапов разработан физическая модель, который, сравнивает температуру и

влажности воздуха внутри теплицы с исходными параметрами, и исходя из погрешностей, регулируется, исполнительные механизмы влияющие на температуру и влажности воздуха.

Построим нечеткую систему в MATLAB, рис.2. На основе механизма нечеткого вывода работает нечеткий контроллер, который основан из 11 подсистем для обработки сигналов. Первый интерфейс преобразует, все входные переменные сигналы в числовые значения показано как на рис.3.

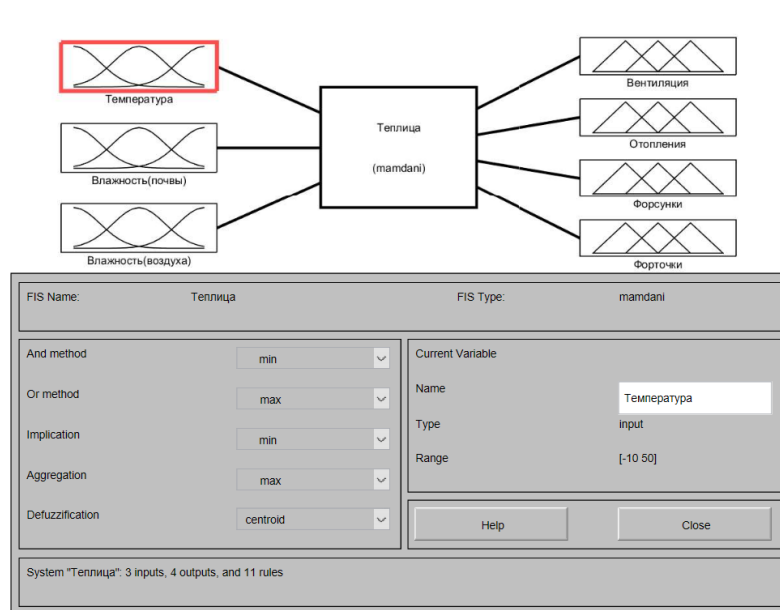


Рис.2. Моделирование с помощью нечеткого контроллера в Matlab.

Входные переменные нечеткого регулятора влажности почвы, температуры и влажность воздуха. А выходные переменные система вентиляции, система отопление, форсунки и форточки для проветривания (рис.3).

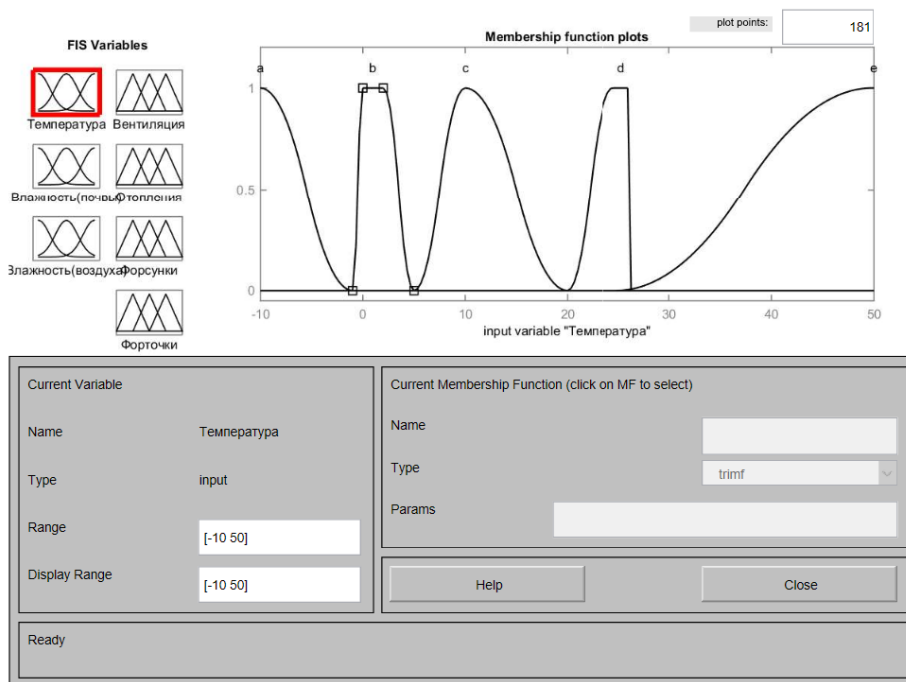


Рис.3. Моделирование температурной среды в теплице.

Функции принадлежности ошибки входной температуры показаны, где имеет, отрицательное значение, отрицательное среднее значение, ноль, положительное среднее значение и положительное большое значение.

Все выходные переменные нечёткого регулятора зависит друг от друга, скорость проветривание и скорость отопление. Выходные переменные вентиляции и отопление показаны функции принадлежности на рисунке 4:

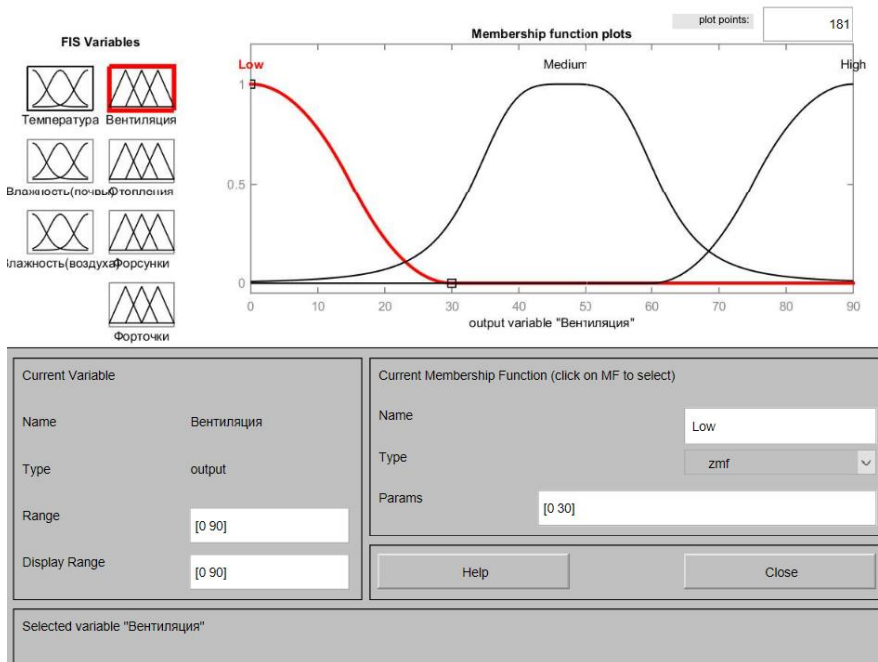


Рис.4. Регулирование скорости вентиляции теплицы.

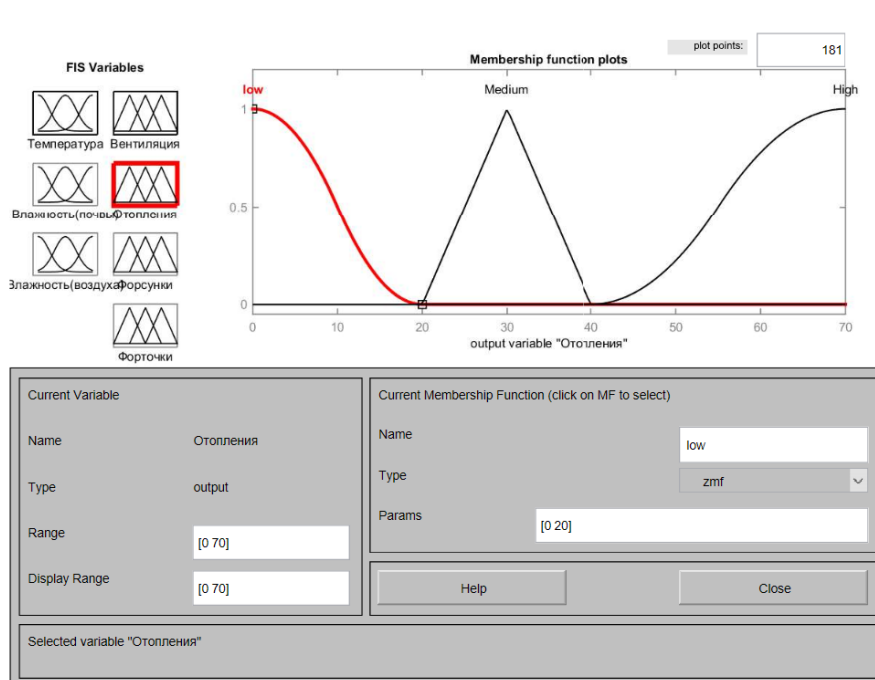


Рис.5. Регулирование скорости обогрева теплицы.

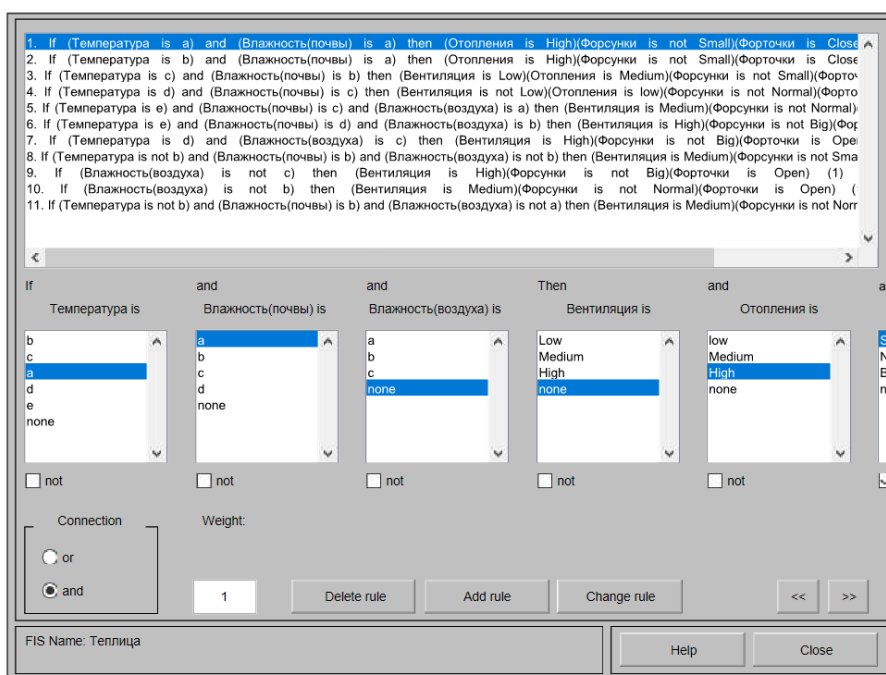


Рис.6. Нечеткие правила вывода

Результат моделирования можно продемонстрировать следующим образом на рис. 7-10.

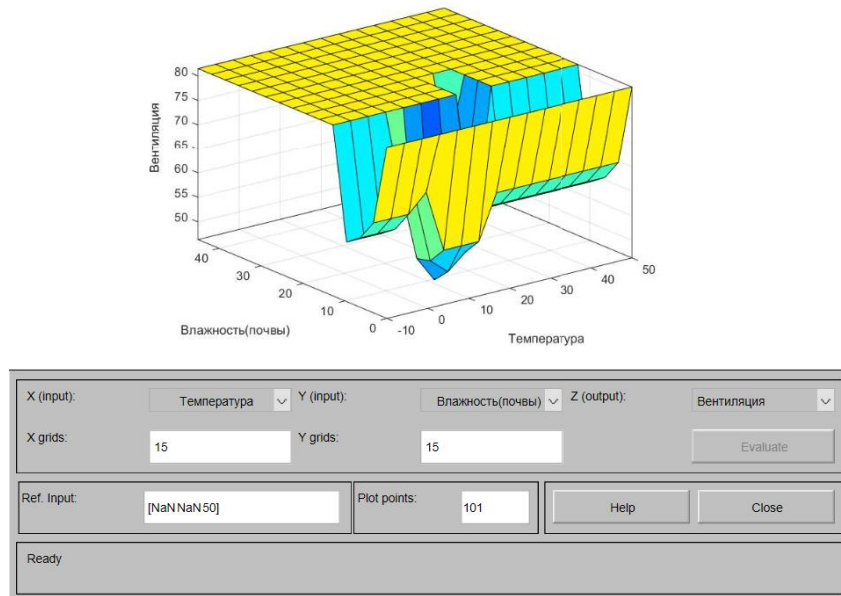


Рис.7. Моделирование скорости вентиляции в теплице

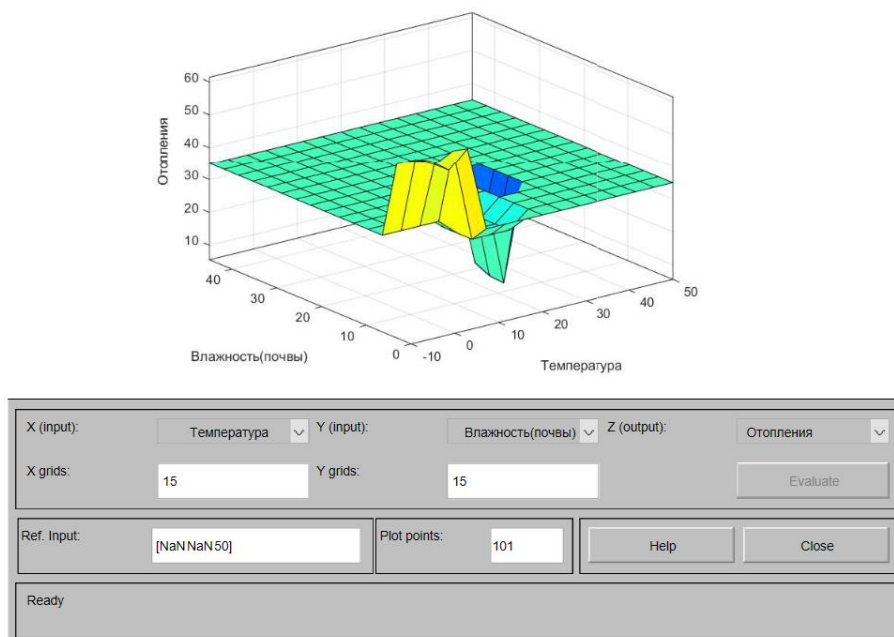


Рис.8. Моделирование скорости нагрева в теплице



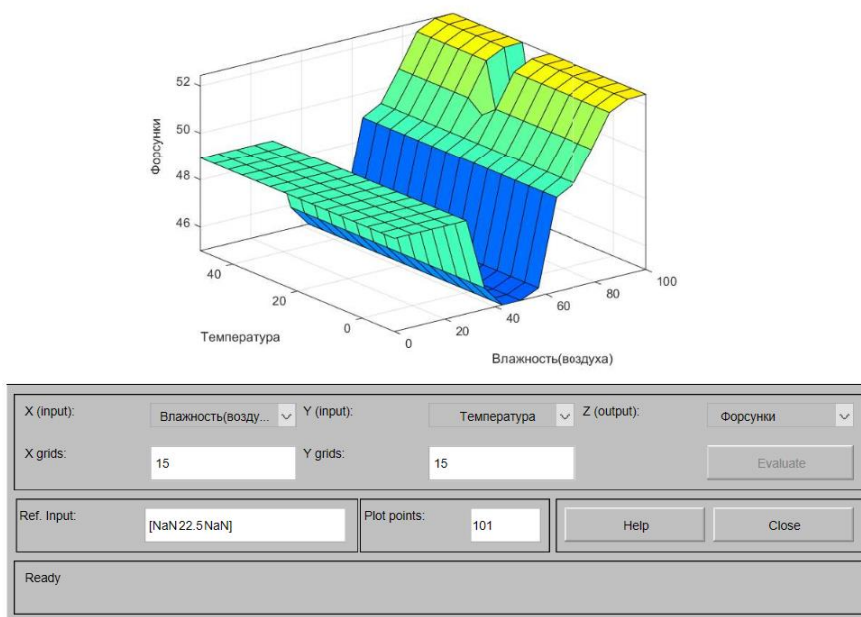


Рис.9. Моделирование скорости увлажнения воздуха в теплице

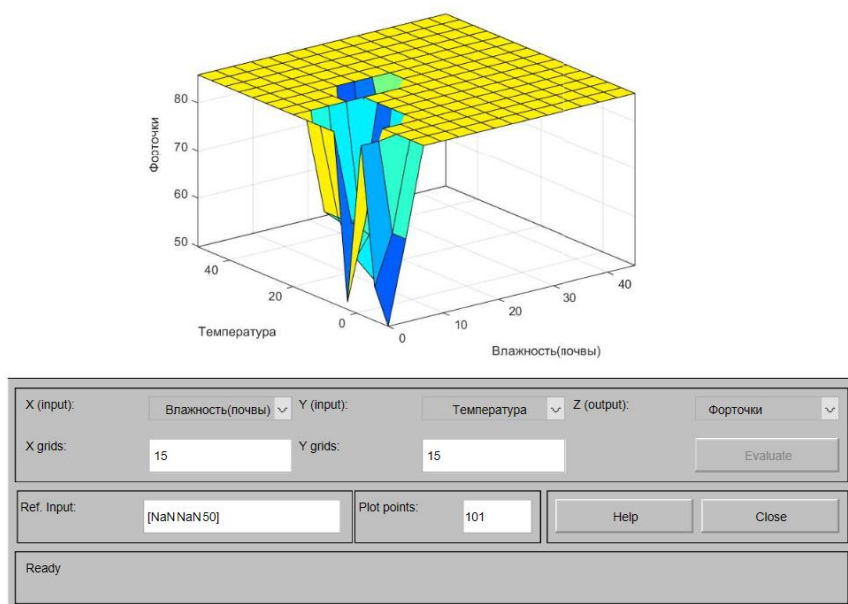


Рис.10. Моделирование скорости осушения воздуха в теплице

После моделирования всех настроек можно сделать следующие выводы, то что концепция способен постоянно трудиться вплоть до таких времен, до тех пор пока никак не возникнет решающее роль, вследствие чего же монтаж подстраивается около перемены концепции а также выравнивает значимости локального климата уже после механических перемен в концепции.

С помощью нечеткого логического управления мы смогли регулировать микроклимат теплицы зимнего и летнего периода. Традиционный метод требовал вмешательства человека, чтобы решить, каким должно быть время регулирование для времени года [9,10]. Другими словами, это была

встроена возможность анализа ситуации, что делает управление намного более автоматической и представляет способность принимать решения в новом ситуации. Здесь датчики воспринимают входные значения, и с использованием приведенной выше модели входные данные преобразуются в нечеткие, а затем с помощью простых правил «если-иначе» и других простых операций с нечеткими множествами получается выходная нечеткая функция и используя критерии. На рис. 7-10 показана поверхность отклика отношений ввода-вывода, определяемая блоком нечеткого интерфейса.

**Список использованной литературы**

1. Avazov, Yu Sh; Kadirov, Yo B; Mukhitdinov, DP; Defining the Parameters of the Models Depending on the Temperature of the Vapor Pressure in the Mathematical Modeling and Calculation of Vapor-Liquid Equilibrium Algorithmization Multicomponent Mixtures, parameters, 1, 4.5763, 0.3821, 2008,
2. Yusupbekov, Nodirbek; Mukhitdinov, Djalolitdin; Kadirov, Yorkin; Sattarov, Olim; Samadov, Abdukhalil; Control of non-standard dynamic objects with the method of adaptation according to the misalignment based on neural networks, International Journal, 8, 9, 2020.
3. Kadirov, Y; Samadov, A; Rahimova, M; MONITORING OF DYNAMIC CHARACTERISTICS OF THE CONTROL SYSTEM IN GREENHOUSES, Eurasian Union Scientists, 7-9, 2021.
4. Jumaev, OA; Sayfulin, RR; Samadov, AR; Arziyev, EI; Jumaboyev, EO; Methods for the Synthesis of Digital Controllers for an Asynchronous Brushless Motor, New Visions in Science and Technology Vol. 9, 45-53, 2021.
5. Adams G.J. and Goodwin G.C. 'A Multivariable Control Design Toolbox.' In: Proceedings of the International Conference 'Control-95', Melbourne, 20-24 October 1995, Institution of Engineers, Australia, 1995, 1, pp. 193-197.
6. Филипчук А.С., Бондарчук А.А., Меркер Э.Э., Кожухов А.А. Интенсификация плавления металлизированных окатышей ДСП. // Материалы международной научно-технической конференции «Азовсталь 2005». Мариуполь, 2005, стр. 26-27.
7. Сысоев В.В., Матвеев М.Г., Бугаев Ю.В., Рязских В.И. Математическое моделирование детерминированных технологических и технических систем // Воронеж: ВГТА, 1994.-80 с.
8. Рутковская Д., Пилинский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы: пер. с польск. — М.: Горячая линия Телеком. 2006. - 452 с.
9. Кадиров, Ёркин; Самадов, Абдухалил; Разработка дистанционного управления токарно-винторезного станка, ТЕСНика, 2, 12-14, 2020, ООО «re-health»
10. Красовский, А.А. Современная прикладная теория управления: Оптимизационный подход в теории управления / А.А. Колесникова. - Таганрог: Изд-во ТРТУ, 2000. - Ч. 1. - 400 с.

---

**ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ПРОГРАММНЫХ ПРОДУКТОВ ООО «НАНОСОФТ РАЗРАБОТКА» В УЧЕБНОЙ И НАУЧНО-ПРОИЗВОДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ЭЛЕКТРОТЕХНИЧЕСКОГО УНИВЕРСИТЕТА**

---

**Афонин П.Н.**

*д.т.н, доцент, проректор по стратегическому развитию заведующий кафедрой прикладной механики и инженерной графики, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» г. Санкт-Петербург, Российская Федерация*

**Титов А.В.**

*к.т.н, доцент, старший научный сотрудник кафедры Прикладной механики и инженерной графики, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» г. Санкт-Петербург, Российская Федерация*

**PROSPECTS OF APPLICATION OF SOFTWARE PRODUCTS OF NANOSOFT DEVELOPMENT COMPANY IN THE EDUCATIONAL AND SCIENTIFIC-PRODUCTION ACTIVITIES OF THE ELECTROTECHNICAL UNIVERSITY**

**АННОТАЦИЯ**

В статье проведен анализ программных продуктов ООО «Нанософт разработка» и перспектив их применения в учебном процессе ГЭТУ «ЛЭТИ» с учетом важности решения задачи по импорт замещению продукции с целью технологического совершенствования отечественного производства, увеличения инновационной активности предприятий и роста производительности труда.

**ANNOTATION**

The article analyzes the software products of Nanosoft Development LLC and the prospects of their application in the educational process of GETU LETI, taking into account the importance of solving the problem of import substitution of products for the purpose of technological improvement of domestic production, increasing the innovative activity of enterprises and labor productivity growth.

**Ключевые слова:** Нанософт разработка, САД-системы, импортозамещение, автоматизированное проектирование, электротехническое оборудование, учебный процесс, инженерная графика, интеллектуальный пункт пропуска, конструирование

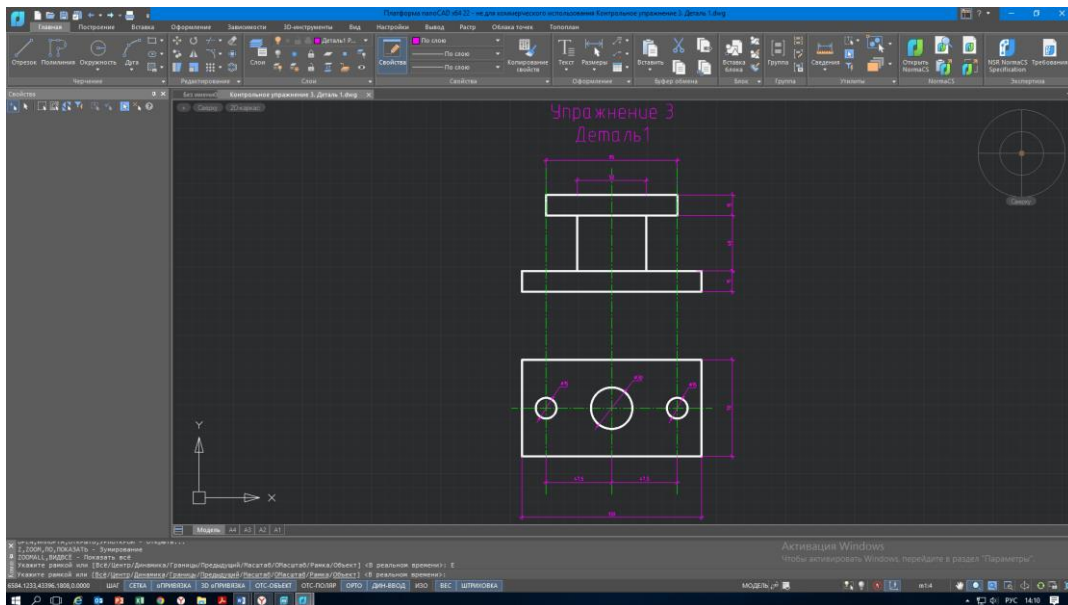
**Keywords:** Nanosoft development, CAD systems, import substitution, computer-aided design, electrical equipment, educational process, engineering graphics, intelligent checkpoint, design

В Санкт-Петербургском государственном электротехническом университете «ЛЭТИ» (далее – СПбГЭТУ «ЛЭТИ») неизменно повышенное внимание уделяется использованию в учебном

процессе передовых знаний и технологий. Широко развиваются направления, связанные с прямым и обратным инжинирингом, предусматривающим применение современных САПР – систем, 3D принтеров и 3D сканеров. В процессе конструирования электротехнического оборудования и устройств ключевое значение имеет наличие у инженерного состава компетенций по применению современных CAD (computer-aided-design) – систем, предназначенных для создания чертежей и 3D моделей, формирование которых является непосредственной задачей кафедры Прикладной механики и инженерной графики (далее – кафедра ПМИГ) СПбГЭТУ «ЛЭТИ». В настоящее время на предприятиях широко применяются CAD-системы, преимущественно иностранного производства: AutoCAD («Autodesk», США), SolidWorks («Dassault Systemes», Франция), SolidEdge («Siemens PLM Software», США), Power Shape («DelCAM», Англия), NX («Siemens PLM Software», США), PTC Creo («PTC», США), CATIA («Dassault Systemes», Франция) и другие, однако, актуальной задачей современности является импортозамещение иностранной продукции отечественными разработками. С каждым годом повышается качество российских систем в области САПР и, как следствие, их доля на рынке, составляющая в настоящее время около 25%. Лидерами российских CAD- систем являются Компас-3D (АО «Аскон», Россия), T-FLEX (ЗАО «Топ Системы», Россия), NanoCAD (ООО «Нанософт разработка», Россия).

Достоинствами российских программ является удобный для пользователя интерфейс (на русском языке); полная адаптация к отечественным стандартам (ГОСТ, ЕСКД, ЕСПД, ЕСТД); меньшая цена, чем у аналогичных зарубежных аналогов. В интересах обеспечения опережающего развития учебного процесса и готовности выполнения НИР и НИОКР по тематике работ, выполняемых СПбГЭТУ «ЛЭТИ» и предприятиями – стратегическими партнерами, профессорско-преподавательский состав кафедры ПМИГ в июле-августе 2022 года прошел обучение в «Летней инженерной онлайн-школе Академии Наносов» использованию инженерной САПР-платформы «NanoCAD», программа которой предусматривала формирование как знаниевой компоненты в рамках тематических вебинаров, так и практических навыков, путем выполнения практико-ориентированных заданий-упражнений (рис.1).

Приобретенные компетенции по работе с программой NanoCAD, позволяют использовать этот программный продукт для обучения студентов в рамках дисциплин: «Автоматизированное проектирование и дизайн приборов и систем», «Прикладная механика», «Теория машин и механизмов», «Конструирование и технология средств приборостроения», «Основы конструирования», «Инженерная и компьютерная графика», «Учебная практика», а также для совместной работы с предприятиями в хозяйственных и научно-исследовательских работах [1].



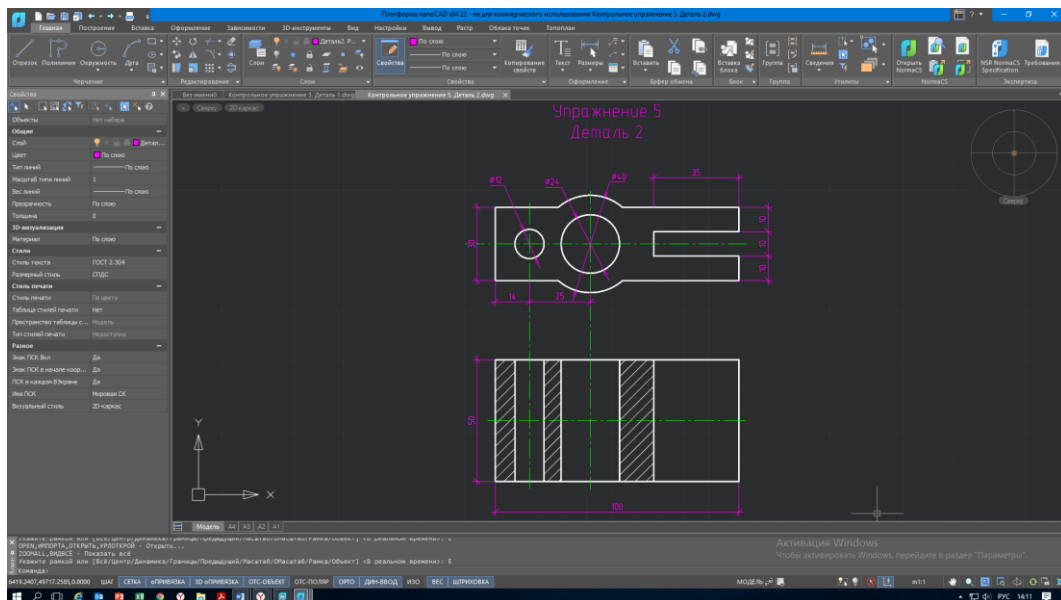


Рис. 1. Контрольные упражнения в системе NanoCAD

Платформа NanoCAD предлагает пользователю выбор между привычным (классическим) и современным (ленточным) интерфейсом. Удобное расположение инструментов, простая логика работы, совместимость с популярными САПР-форматами (\*.dwg, \*.dxf, \*.dwt и др.). Особенностью NanoCAD является высокопроизводительная графическая подсистема, в которой задействованы новейшие достижения в области алгоритмов визуализации и вычислительной геометрии.

На основе платформы NanoCAD, разработаны модули СПДС, Механика, Топоплан, 3D, Растр, Организация.

Модуль «Механика» предоставляет большой выбор параметрических стандартных элементов. В сочетании с возможностью создания пользовательских типовых элементов это обеспечивает сокращение сроков разработки проекта. Разработан обширный функционал для автоматического создания спецификаций по ГОСТу: простой, встраиваемой, электромонтажной, плазовой, групповых типов А и Б. Широкий спектр настроек дает возможность учитывать особенности подготовки спецификаций на различных предприятиях, а также создавать пользовательские спецификации. Специализированный модуль обеспечивает создание высокоточных чертежей зацеплений с учетом множества параметров нагружения, специфики используемого материала деталей и других особенностей. В основу расчетного модуля положены ГОСТ 21354-87 и ГОСТ 16532-70, что позволяет контролировать разработку на соответствие стандарту прочности и стандарту геометрии. Встроенный редактор технических требований предназначен для максимально быстрого и в соответствии со стандартом оформления текста на чертеже, создания ссылок на элементы оформления, а также вставки в текст обозначений.

В модуле «3D» реализована конвертация в наиболее распространенные 3D-форматы (C3D, IGS, SAT, STEP, STL, JT, WRL, X\_B, X\_T) позволяющая обмениваться информацией с большинством САПР. Любую модель, выполненную в nanoCAD с применением модуля «3D», можно передать на 3D-принтеры и станки с ЧПУ, используя функцию экспорта. Широкие возможности формирования параметрических моделей позволяют создавать умные 3D-объекты, управляемые числовыми параметрами, а также накладывать геометрические ограничения, задавая условия изменения формы объектов. Грамотное и продуманное использование параметризации значительно сокращает время моделирования и повышает эффективность. Ассоциативная связь моделей и их проекций позволяет пользователям сконцентрироваться на проектировании в 3D-среде, уделяя внимание 2D-графике в основном лишь для оформления чертежей. Все изменения 3D-модели в любой момент будут отображаться и на чертежах, причем элементы оформления, внесенные в 2D-графику, также будут соответствовать этим изменениям. Инструментарий 3D-зависимостей предназначен не только на создание сложных сборок из отдельных компонентов, но и, на управление параметрами разнесения, создание демонстрационных моделей, а также наглядных схем сборок изделий. Пользователям доступны пять 3D-зависимостей: «Вставка», «Касание», «Симметрия», «Совмещение», «Угловая». В режиме прямого моделирования доступны восемь типов 3D-примитивов – элементов, не требующих для создания дополнительных 2D-построений.

Используя модуль «3D», пользователи могут не только визуализировать объекты в трехмерном пространстве, но и создавать структуру проектируемого изделия. Данная возможность особенно полезна при выполнении работ по проектированию сложных многокомпонентных

изделий, когда на каждой стадии проектирования важно видеть их реальный конструкторский состав [2], что имеет принципиальное значение как для подразделений СПбГЭТУ «ЛЭТИ», осуществляющих выполнение НИР и НИОКР, так и для выполнения работ по заказу предприятий – стратегических партнеров.

С учетом отмеченных выше достоинств, использование программных продуктов ООО «Нанософт разработка» является основой повышения эффективности учебного процесса в рамках дисциплин, реализуемых кафедрой Прикладной механики и инженерной графики – «Инженерная графика», «Прикладная механика», «Биомеханика», программы которых имеют вариативную адаптацию для подготовки студентов по большинству направлений подготовки, реализуемых в СПбГЭТУ «ЛЭТИ», в частности: 11.03.03 «Конструирование и технология электронных средств», 11.03.04 «Электроника и наноэлектроника», 11.05.01 «Радиоэлектронные системы и комплексы», 13.03.02

«Электроэнергетика и электротехника» и другие [3], а также для выполнения НИР и НИОКР в широком диапазоне задач проектирования изделий электронной техники, медицинского приборостроения, систем обеспечения функционирования интеллектуальных пунктов пропуска.

#### Список литературы

1. Афонин П.Н., Титов А.В. Разработка технических средств потокового контроля веса транспортных средств в пунктах пропуска через государственную границу Российской Федерации // Бюллетень инновационных технологий. 2022. Т. 6. № 3 (23). С. 75-77.

2. ООО «Нанософт разработка»: официальный сайт. – Москва, 2022 – URL: <http://www.nanocad.ru> (дата обращения 12.08.2022)

3. СПбГЭТУ «ЛЭТИ» Первый электротехнический: официальный сайт. – СПб, 2022 – URL: <http://www.etu.ru> (дата обращения 12.08.2022).

---

### МЕТОД НАХОЖДЕНИЯ КОРНЕЙ МНОГОЧЛЕНА НАД РАСШИРЕННЫМ ПОЛЕМ ГАЛУА НА ОСНОВЕ КОРНЕЙ АФФИННОГО МНОГОЧЛЕНА

---

**Фам Хак Хоан**

докцент, к.т.н, Технический университет им. Ле Куи Дона,  
Социалистическая Республика Вьетнам

**Нгуен Тьен Тхай**

к.т.н, Технический университет им. Ле Куи Дона,  
Социалистическая Республика Вьетнам

**Бу Шон Ха**

к.т.н, Институт науки и технологии,  
Социалистическая Республика Вьетнам

**Pham Khac Hoan**

Assoc. Prof., PhD, Le Quy Don Technical University, Ha Noi, Vietnam

**Nguyen Tien Thai**

PhD, Le Quy Don Technical University, Ha Noi, Vietnam

**Vu Son Ha**

PhD, Institute of Science and Technology, Ha Noi, Vietnam

#### АННОТАЦИЯ

В статье предложен метод нахождения корней многочлена над расширенным полем Галуа на основе корней аффинного многочлена. Предложенный метод позволяет уменьшить задержку вычисления по сравнению с традиционными методами, что дает возможность использования в высокоскоростной системе передачи информации.

#### ABSTRACT

The article proposes a method for finding the roots of a polynomial over an extended Galois field based on the roots of an affine polynomial. The proposed method makes it possible to reduce the calculation delay in comparison with traditional methods, which makes it possible to use in a high-speed communication system.

**Ключевые слова:** Поле Галуа; кодирование, контролирующее ошибки; полиномиальный базис; нормальный базис.

**Key words:** Galois field, error control coding, polynomial basis, normal basis.

#### 1. ВВЕДЕНИЕ

Конечное поле широко используется в радиотехнике и компьютерной технике, например в помехоустойчивом кодировании, шифровании на основе кодов и шифровании на эллиптических кривых. Не только неполное понимание теоретических основ конечного поля, но и

реализация устройства для решения задач над конечным полем вызывают множество трудностей для исследовательского процесса.

Некоторые задачи, связанные с решением уравнения над конечным полем, например необходимо решить ключевое уравнение при декодировании БЧХ-кода, кодов Рида-Соломона,

Гоппы в помехоустойчивом кодировании и в шифровании на основе кодов. Берлекэмп один из авторов имеет большой вклад в решении проблем анализа сомножителей над конечным полем [1].

Некоторые методы решения уравнения над конечным полем: циклические алгоритмы на основе процедуры Ченя, преобразования Фурье над полем Галуа...[2, 3, 4]. Но перечисленные методы имеют большое время задержки, связанное с высокой сложностью вычисления.

Линеаризованный многочлен и аффинный многочлен имеют особенные свойства, позволяющие облегчить процесс их нахождения решений. Но незначительные многочлены являются линеаризованными или аффинными многочленами. На основе алгебраических преобразований и нахождения наименьшего

аффинного кратного заданного многочлена возможно найти корни исходного многочлена в множестве корней аффинного многочлена [5, 6].

В данной статье исследован метод нахождения корней многочлена над полем  $GF(p^n)$  на основе корней аффинного многочлена, также дано основание создания устройства для эффективного решения задачи. Полученные результаты могут использоваться в других случаях, включая поля с разными размерностями.

Статья включает в себе следующие части: введение; часть 2 – основы конечного поля; часть 3 – исследование классы особенных многочленов: линеаризованные многочлены над конечным полем и проблема нахождения их корней; заключение.

## 2. Основы конечного поля

### 2.1. Представление элементов конечного поля

Пусть простое число  $p$ , обозначим конечное поле с порядком  $p$  как  $F_p$  или  $GF(p)$ , это множество целых чисел  $Z_p$  с операцией  $\text{mod } p$ . Расширенное поле  $F_q$  содержит  $q = p^n$  элементов является векторным пространством над  $F_p$  некоторой размерности  $n \geq 1$ .

Функция “след” для элемента  $c \in F_q$  определяется следующим образом:

$$\text{Tr}(c) = c + c^p + c^{p^2} + \dots + c^{p^{n-1}}. \quad (1)$$

Имеется:  $\text{Tr}(nc) = n \cdot \text{Tr}(c)$ .

В частности, при  $p = 2$ ,  $\text{Tr}(1) = 1$  при  $n$  нечетном и  $\text{Tr}(1) = 0$  при  $n$  четном. Отметим, что уравнение  $x^2 + x + D = 0$ ,  $D \in GF(2^n)$  имеет корни тогда и только тогда, когда  $\text{Tr}(D) = 0$ .

Конечное поле  $GF(p^n)$  порождается неприводимым многочленом  $\pi(x)$  степени  $n$ . Особенно когда используется примитивный многочлен  $\pi(x)$ , то расширенное поле  $GF(p^n)$  построится на основе присоединения к  $GF(p)$  корней  $\alpha$  многочлена  $\pi(x)$  над  $GF(p)$ . На практике существуют два вида представления с использованием полиномиального и нормального базисов.

#### \* Полиномиальный базис

Пусть поле  $GF(p^n)$  и  $\alpha \in GF(p^n)$  – корень примитивного неприводимого многочлена степени  $n$  над полем  $GF(p)$ . Полиномиальным базисом поля  $GF(p^n)$  над  $GF(p)$  является базис  $\{1, \alpha, \alpha^2 \dots \alpha^{n-1}\}$ , где  $\alpha$  – примитивный элемент поля  $GF(p^n)$ .

#### \* Нормальный базис

Известно, что всегда существует нормальный базис конечного поля  $GF(p^n)$  над  $GF(p)$ . Если  $\gamma \in GF(p^n)$  порождающий элемент над полем  $GF(p)$ , то нормальным базисом поля  $GF(p^n)$  называется базис вида

$$\{\gamma, \gamma^{p^1}, \gamma^{p^2} \dots \gamma^{p^{n-1}}\}.$$

Например, для поля  $GF(2^4)$  с порождающим многочленом  $\pi(x) = x^4 + x + 1$ , имеющим 2 нормального базиса, порождающие примитивным элементом  $\gamma = \alpha^7$  и непримитивным элементом  $\gamma = \alpha^3$ .

### 2.2. Операции над конечным полем

Обычные алгебраические операции над полем  $GF(2^n)$  осуществляются по модулю неприводимого многочлена  $\pi(x)$  над  $GF(2)$ . Операции сложения и вычитания по модулю 2. Операция сложения двух многочлена осуществляется с помощью операции XOR, операция умножения над полем  $GF(2^n)$  имеет высокую сложность и большой затрат времени для ее вычисления. Сложность еще зависит от выбора неприводимого многочлена и базиса, используемая для представления конечных элементов.

При реализации устройства, квадрат элемента с нормальным базисом может осуществляться циклическим сдвигом, а операция умножения более сложно реализуется. Умножение двух элементов поля с полиномиальным базисом может выполняться как умножение двух обычных многочленов, а результат

получается по модулю порождающего многочлена  $\pi(x)$ . На практике часто используются устройства умножения использованием логарифмически-антилогарифмической таблицы и функции Зеха. В процессе вычисления, если сложение и умножение чередуются, то необходимо преобразовать векторное представление в степенное с помощью логарифмической и антилогарифмической [7, 8].

### 3. Линеаризованный многочлен и его корни

Процедура Ченя и аналитический способ предназначены для нахождения корней многочлена над конечным полем имеет высокую сложность, особенно для поля с большой размерности и с большой степеней многочлена. Существует класс особенных многочленов – линеаризованные многочлены, нахождение корней которых является облегченной задачей. В данном разделе рассматриваются линеаризованный многочлен, нахождение линеаризованного многочлена, как наименьшее кратное заданного многочлена, корни которого могут определены на основе анализа корней линеаризованного многочлена.

#### 3.1. Линеаризованный многочлен

Многочлен  $L(z)$  над полем  $\text{GF}(p^n)$  называется линеаризованным, если он имеет вид

$$L(z) = \sum_i L_i z^{p^i} \quad (2)$$

Например, многочлен  $L(z) = z + z^2 + z^4$  - это линеаризованный многочлен для всех  $n$ . Кроме этого, выше приведенная функция “след” тоже является линеаризованным многочленом.

Отметим, что автор в [2] доказал, что пусть корни многочлена  $L(z)$  принадлежат расширенному полю  $\text{GF}(p^m)$ ,  $m > n$ , они образуют векторное подпространство в  $\text{GF}(p^m)$ . Наоборот, для векторного подпространства  $n$  размерности над  $\text{GF}(p^m)$ , многочленом  $L(z) = \prod_{\beta \in U} (z - \beta)$  является

линеаризованным над  $\text{GF}(p^m)$ , т. е.

$$L(z) = \sum_i L_i z^{p^i} = L_0 z + L_1 z^p + \dots + L_{n-1} z^{p^{n-1}} + z^{p^n}. \quad (3)$$

Корни линеаризованного многочлена  $L(z)$  образуют подпространство  $M$  над  $\text{GF}(p^n)$ . Если  $\gamma \in M$  то  $\gamma^p \in M$  так  $L^p(\gamma) = L(\gamma^p)$ . Если векторное подпространство обладает этим свойством, то оно называется модулем. Если  $L_0 \neq 0$ , то  $L(z)$  не имеет кратные корни, и в дальнейшем мы будем рассматривать только этот случай.

#### 3.2. Корни линеаризованного многочлена

Учитывая, что линеаризованный многочлен  $L(z)$  над  $\text{GF}(p^n)$ , описываемый выражением (2), предполагая  $\gamma$  его примитивный корень,  $L(z)$  является многочленом степени  $p^n$ , корни этого многочлена имеют вид:

$$\delta_0 \gamma + \delta_1 \gamma^p + \dots + \delta_{n-1} \gamma^{p^{n-1}}, \quad (4)$$

где  $\delta_i \in \text{GF}(p)$  и эти корни образуют модуль с нормальным базисом  $\left\{ \gamma, \gamma^p, \dots, \gamma^{p^{n-1}} \right\}$ .

Рассмотрим задачу нахождения корней линеаризованного многочлена.

Пусть  $\alpha^0, \alpha^1, \dots, \alpha^{n-1}$  - полимиальный базис поля  $\text{GF}(p^n)$ .

Теорема 1 [2]

$L(z)$  - линеаризованный многочлен над  $\text{GF}(p^n)$ , элемент  $z$  представляется следующим образом

$$z = \sum_k Z_k \alpha^k, \quad Z_k \in \text{GF}(p) \text{ тогда}$$

$$L(z) = \sum_k Z_k L(\alpha^k) \quad (5)$$

Используя представление элементов  $L(\alpha^i) = \sum_{j=0}^{m-1} C_{i,j} \alpha^j$ , тогда коэффициент разложения многочлена по базисом многочлена рассчитывается следующим образом:

$$[L_0, L_1, \dots, L_{n-1}] = [Z_0, Z_1, \dots, Z_{n-1}] \cdot C, \quad (6)$$

где

$$C = \begin{bmatrix} C_{0,0} & C_{0,1} & C_{0,1} & \cdot & \cdot & \cdot & C_{0,n-1} \\ C_{1,0} & C_{1,1} & C_{1,2} & \cdot & \cdot & \cdot & C_{1,n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ C_{n-1,0} & C_{n-1,1} & C_{n-1,2} & \cdot & \cdot & \cdot & C_{n-1,n-1} \end{bmatrix} \quad (7)$$

Многочлен  $A(z)$  над  $\text{GF}(p^n)$  называется аффинным, если  $A(z) = L(z) - u$ , где  $L(z)$  линейризованный многочлен и  $u \in \text{GF}(p^n)$ . Корни аффинного многочлена можно найти, решая систему линейных уравнений, как показано в примере 1.

Основные свойства линейризованных и аффинных многочленов [2].

1. Многочлен  $L(z)$  является линейризованным тогда и только тогда, когда его корни образуют линейное пространство над  $\text{GF}(p)$ , их корни имеют одинаковые кратные и являются степенями  $p$ .

2. Многочлен  $A(z)$  является аффинным тогда и только тогда, когда его корни образуют аффинное пространство над  $\text{GF}(p)$ , их корни имеют одинаковые кратные и являются степенями  $p$ .

3. Наибольший общий делитель двух линейризованных многочленов является линейризованным многочленом.

4. Наибольший общий делитель двух аффинных многочленов является аффинным многочленом.

Частный случай аффинного полинома 2-ой степени над  $\text{GF}(2^n)$  позволяет вычислить его корни без решения системы линейных уравнений. Квадратное уравнение можно привести к каноническому виду

$$y^2 + y = u \quad (8)$$

Уравнение (8) имеет корни над  $\text{GF}(2^n)$  тогда и только тогда, когда  $\text{Tr}(u) = 0$ . Обозначая  $\alpha \in \text{GF}(2^n)$  - произвольный элемент со степенью  $n$ ,  $g = \alpha^k$  - элемент, при котором  $\text{Tr}(g) = 1$ . Тогда с  $i = 0, 1, \dots, n-1$ , можно найти  $y_i$  такое, что:

$$y_i^2 + y_i = \begin{cases} \alpha^i & \text{при } \text{Tr}(\alpha^i) = 0; \\ \alpha^i + \alpha^k & \text{при } \text{Tr}(\alpha^i) = 1. \end{cases} \quad (9)$$

Для решения уравнения  $y^2 + y = u = \sum_{i=0}^{n-1} U_i \alpha^i$ ,  $U_i \in \text{GF}(2)$ , предположим

$$y = \sum_{i=0}^{n-1} U_i y_i \quad (10)$$

Тогда имеем:



$$\begin{aligned}
 y^2 + y &= \sum_{i=0}^{n-1} U_i (y_i^2 + y_i) = u + \alpha^k \sum_{i=0}^{n-1} U_i \text{Tr}(\alpha^i) = \\
 &= u + \alpha^k \text{Tr} \left( \sum_{i=0}^{n-1} U_i \alpha^i \right) = u + \alpha^k \text{Tr}(u).
 \end{aligned}
 \tag{11}$$

Поэтому корни уравнения (8) являются  $y' = \sum_{i=0}^{n-1} U_i y_i$  и  $y'' = 1 + \sum_{i=0}^{n-1} U_i y_i$ .

Половина элементов поля  $\text{GF}(2^n)$  имеет след равен 0, а другая половина имеет след равен 1. Разделив поле на циклотомические смежные классы, можно хранить корни более эффективно, за чем используя формулы (9) - (11) для нахождения корней. При использовании орбитального представления по циклотомическим смежным классам сохраняются только ведущие элементы, образующие циклотомические классы. Следовательно, количество рассматриваемых элементов уменьшается от  $2^n$  примерно до  $n$ , что значительно снижает объем памяти, необходимый для хранения приблизительно  $2^n / n$  раз. В табл. 1 представлены орбиты с параметром  $u$ , соответствующим смежным классом, и соответствующие корни  $y', y''$  над  $\text{GF}(2^n)$  с порождающими многочленами  $x^3 + x + 1; x^4 + x + 1; x^5 + x^2 + 1; x^6 + x + 1; x^7 + x + 1$ . Параметры  $u$  соответствуют элементам (их следы равны нулями), ведущим циклотомическими классами. Аналогичным образом можно строить орбиты для поля большего размера и хранить их в памяти, используемой для вычисления корней квадратных уравнений. Обратите внимание, что в этой таблице элементы поля представлены десятичными числами  $N$ , называются модифицированными логарифмами:

$$N = \log_{\alpha}(\alpha^i) + 1 = i + 1 = \text{Log}(\alpha^i). \tag{12}$$

Таблица 1.

**Орбитальное представление по параметру  $u$  над  $\text{GF}(2^n)$  и корни**

n	u	y'	y''	n	u	y'	y''	n	u	y'	y''
3	2	3	7	6	1	22	43	7	2	17	113
4	1	6	11		2	18	48		4	26	106
	2	8	10		4	15	53		6	7	127
	6	2	5		8	2	7		10	27	111
	2	4	30		10	23	57		12	45	95
5	8	3	6		14	31	47		16	37	107
	16	22	26	28	37	55	24		72	80	
							30		43	115	
									56	81	103

### 3.3. Кратный аффинный многочлен

Большинство многочленов над  $\text{GF}(p^n)$  не являются аффинными. Например, при  $p=2$  многочлен 3-ой степени не является аффинным, однако можно найти аффинный многочлен 4-ой степени, кратный многочлену 3-ой степени. Корни многочлена 3-ей степени можно найти через корни многочлена 4-ой степени. В общем случае для многочлена  $f(z)$   $d$ -ой степени мы можем использовать следующий алгоритм для нахождения кратного аффинного  $L(z) - u$  этого многочлена.

Алгоритм 1 [2]

1. Вычисление  $z^k \text{ mod } f(z)$  с  $k = d, d + 1, \dots, (d - 1)p$ ;
2. На основе результатов вычисления на первом шаге вычислить остатки  $r^{(0)}(z), r^{(1)}(z), \dots, r^{(i)}(z)$ , с  $r^{(i)}(z) = z^{p^i} \text{ mod } f(z)$ ;
3. Решение системы линейных уравнений

$$[u, L_0, L_1, \dots, L_{d-1}] \begin{bmatrix} 0 & 0 & \dots & 0 & -1 \\ r_{(d-1)}^{(0)} & \dots & \dots & r_1^{(0)} & r_0^{(0)} \\ r_{(d-1)}^{(1)} & \dots & \dots & r_1^{(1)} & r_0^{(1)} \\ \dots & \dots & \dots & \dots & \dots \\ r_{(d-1)}^{(d-1)} & \dots & \dots & r_1^{(d-1)} & r_0^{(d-1)} \end{bmatrix}. \quad (13)$$

Рассмотрим решение уравнения 3-ей степени с помощью кратного аффинного многочлена 4-ой степени.

Пусть многочлен  $f(z) = z^3 + \alpha^{13}z^2 + z + \alpha^3$ , с  $\alpha^4 + \alpha + 1 = 0$ . Найти аффинный многочлен, который является кратным  $f(z)$ . Вычисляем:

$$z^3 \bmod f(z) = \alpha^{13}z^2 + z + \alpha^3;$$

$$\begin{aligned} z^4 \bmod f(z) &= \alpha^{13}z^3 + z^2 + \alpha^3z = \\ &= \alpha^{26}z^2 + \alpha^{13}z + \alpha^{16} + z^2 + \alpha^3z = \\ &= (\alpha^{11} + 1)z^2 + (\alpha^{13} + \alpha^3)z + \alpha = \\ &= \alpha^{12}z^2 + \alpha^8z + \alpha. \end{aligned}$$

Вычисляем  $r^{(i)}(z) = z^{2^i} \bmod f(z)$ ;

$$r^{(0)}(z) = z^1 \bmod f(z) = z;$$

$$r^{(1)}(z) = z^2 \bmod f(z) = z^2;$$

$$r^{(2)}(z) = z^4 \bmod f(z) = \alpha^{12}z^2 + \alpha^8z + \alpha.$$

Имеем систему уравнений

$$[u, L_0, L_1, L_2] \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ \alpha^{12} & \alpha^8 & \alpha \end{bmatrix} = 0.$$

Предположим, что выбраны корни  $u = \alpha^2, L_0 = \alpha^8, L_1 = \alpha^{12}, L_2 = 1$  и  $L(z) = \alpha^8z + \alpha^{12}z^2 + z^4$ .

Для нахождения корней этого линеаризованного многочлена, мы вычисляем значения:

$$L(1) = \alpha^8 + \alpha^{12} + 1 = 1 + \alpha + \alpha^3;$$

$$L(\alpha) = \alpha^9 + \alpha^{14} + \alpha^4 = 0;$$

$$L(\alpha^2) = \alpha^{10} + \alpha^{16} + \alpha^8 = 0;$$

$$L(\alpha^3) = \alpha^{11} + \alpha^{18} + \alpha^{12} = 1 + \alpha^3.$$

Отсюда можно найти корни уравнения  $L(z) = \alpha$ , решив систему уравнений

$$[Z_0, Z_1, Z_2, Z_3] \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = [0100].$$

Выше упомянутая система уравнений имеет корни  $Z = [1011] = \alpha^{13}$ ;  $Z = [1111] = \alpha^{12}$ . Корень  $\alpha^{13}$  - ненужный посторонний корень,  $\alpha^{12}$  корень многочлена  $f(z)$ , который можно разложить на множители:

$$f(z) = z^3 + \alpha^{13}z^2 + z + \alpha^3 = (z + \alpha^{12})(z^2 + \alpha z + \alpha^6).$$

Осуществляя нахождение корней многочлена  $z^2 + \alpha z + \alpha^6$  по изложенной выше методике, находим две корни  $\alpha^7, \alpha^{14}$ .

Кроме того, для многочлена третьей степени вида  $f(z) = z^3 + az^2 + bz + c$  проще найти кратный аффинный многочлен вида:

$$A(z) = (z^3 + az^2 + bz + c)(z + a) = z^4 + (a^2 + b)z^2 + (ab + c)z + ac.$$

#### 4. Решение уравнения четвертой степени

Поле  $\text{GF}(2^n)$  комбинированный метод алгебраического преобразования и аффинного многочлена реализован для более эффективного поиска решения следующим образом.

Рассмотрим уравнение 4-ой степени над  $\text{GF}(2^n)$

$$x^4 + Ax^3 + Bx^2 + Cx + D = 0. \quad (14)$$

Подстановка  $x = y^{-1} + \sqrt{C/A}$ ,  $A \neq 0$ , можно получить уравнение

$$a_3y^4 + a_2y^2 + a_1y + a_0 = 0, \quad (15)$$

где

$$a_3 = D + BC/A + (C/A)^2; \quad a_2 = B + \sqrt{AC}, a_1 = A, a_0 = 1. \quad (16)$$

При  $a_3, a_2 \neq 0$  заменяя  $y = z\sqrt{a_2/a_3}$  получим уравнение

$$z^4 + z^2 + E_1z + E_2 = 0, \quad (17)$$

где  $E_1 = a_1\sqrt{a_3/a_2^3}$ ;  $E_2 = a_3/a_2^2$ .

В этом случае левая часть (17) является аффинным многочленом и его решение можно найти на основе решения системы линейных уравнений, описанного в разделе 3.2. Как только решение найдено, используя обратные замены для нахождения корней исходного уравнения.

#### 5. Заключение

В статье представлено улучшение формулы расчета корней уравнения 2-ой степени для уменьшения объема памяти таблиц в примерно  $2^n/n$  раз за счет орбитального представления в циклотомическом смежном классе. В статье также предлагается метод решения уравнений 3-ой и 4-ой степеней над конечным полем за счет нахождения корней аффинных многочленов 4-ой

степени. Метод решения уравнений над конечным полем с помощью процедуры Ченя (путем перебора всех элементов поля) использует  $O(2^n t^2)$  умножений. С помощью нахождения корня аффинного многочлена сложность вычисления составляет примерно  $O(nt)$ . Таким образом, предлагаемый метод позволяет значительно снизить сложность при решении уравнения не слишком большой степени, тем самым повысит

быстродействие в схемах декодирования кодов БЧХ и Рида-Соломона.

#### Литература

1. Bijan Ansari, *Finite field arithmetic and its application in cryptography* / Dissertation for the degree Doctor of Philosophy in Electrical Engineering, University of California, Los Angeles, 2012.
2. Elwyn R Berlekamp, *Algebraic Coding Theory (Revised Edition)*, World Scientific Publishing Co. Pte. Ltd., 2015.
3. Муггер, В.М. Основы помехоустойчивой телепередачи информации, Л.: Энергоатомиздат, Ленинградское отделение, 1990.
4. Конопелько, В.К. и др. Теория прикладного кодирования. Мн.: БГУИР, 2004.
5. F. J. MacWilliams, N. J. A. Sloane, *The theory of error correction codes*, Elsevier, 1977.
6. Fedorenko S. V., Trifonov P. V. Finding roots of polynomials over finite fields, *IEEE Transactions on Communications*, 2002, Vol. 50, Issue 11, pp. 1709–1711
7. Johann Großschadl, A low-power bit serial multiplier for finite fields  $GF(2^m)$ . 34<sup>th</sup> IEEE International symposium on circuits and system, vol. IV, 2001.
8. Chin-Chin Chen, Chiou Yng Lee, Erl-Huei Lu, Scalable and systolic montgomery multipliers over  $GF(2^m)$ , *IEICE Transaction Fundamentals*, Vol. E91, No.7 July 2008.

# Евразийский Союз Ученых.

## Серия: технические и физико-математические науки

Ежемесячный научный журнал  
№ 3 (96)/2022 Том 1

### ГЛАВНЫЙ РЕДАКТОР

**Макаровский Денис Анатольевич**

AuthorID: 559173

Заведующий кафедрой организационного управления Института прикладного анализа поведения и психолого-социальных технологий, практикующий психолог, специалист в сфере управления образованием.

### РЕДАКЦИОННАЯ КОЛЛЕГИЯ

**Штерензон Вера Анатольевна**

AuthorID: 660374

Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, Институт новых материалов и технологий (Екатеринбург), кандидат технических наук

**Синьковский Антон Владимирович**

AuthorID: 806157

Московский государственный технологический университет "Станкин", кафедра информационной безопасности (Москва), кандидат технических наук

**Штерензон Владимир Александрович**

AuthorID: 762704

Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, Институт фундаментального образования, Кафедра теоретической механики (Екатеринбург), кандидат технических наук

**Зыков Сергей Арленович**

AuthorID: 9574

Институт физики металлов им. М.Н. Михеева УрО РАН, Отдел теоретической и математической физики, Лаборатория теории нелинейных явлений (Екатеринбург), кандидат физ-мат. наук

**Дронсейко Виталий Витальевич**

AuthorID: 1051220

Московский автомобильно-дорожный государственный технический университет (МАДИ), Кафедра "Организация и безопасность движения" (Москва), кандидат технических наук

Статьи, поступающие в редакцию, рецензируются. За достоверность сведений, изложенных в статьях, ответственность несут авторы. Мнение редакции может не совпадать с мнением авторов материалов. При перепечатке ссылка на журнал обязательна. Материалы публикуются в авторской редакции.

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Художник: Валегин Арсений Петрович  
Верстка: Курпатова Ирина Александровна

Адрес редакции:  
198320, Санкт-Петербург, Город Красное Село, ул. Геологическая, д. 44, к. 1, литера А  
E-mail: [info@euroasia-science.ru](mailto:info@euroasia-science.ru) ;  
[www.euroasia-science.ru](http://www.euroasia-science.ru)

Учредитель и издатель ООО «Логика+»  
Тираж 1000 экз.